NSv 270/470/870

Los firewalls virtuales SonicWall Network Security NS*v* 270/470/870 proporcionan seguridad de clase empresarial, gestión optimizada, visibilidad completa y una implementación flexible, al tiempo que facilitan un rendimiento superior para las cargas virtuales.

En los entornos virtuales se descubren continuamente vulnerabilidades nuevas que conllevan implicaciones y retos de seguridad importantes. Pero para proteger todos esos vectores de seguridad se han de poder aplicar uniformemente las políticas de seguridad adecuadas a los puntos de control de red correctos, ya que algunos fallos de seguridad se pueden atribuir a políticas inefectivas o a errores de configuración.

PRESTACIONES DESTACADAS

Seguridad en las nubes públicas, privadas y de agencias gubernamentales

- Firewall de nueva generación con prestaciones automáticas de detección y prevención de brechas
- Tecnología patentada de Inspección de memoria profunda en tiempo real (RTDMI)
- Tecnología patentada de Inspección profunda de paquetes sin reensamblado (RFDPI)
- Visibilidad completa de extremo a extremo y gestión agilizada con políticas unificadas
- Inteligencia y control de aplicaciones
- 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
- Soporta las nubes AWS y Azure del Gobierno de EE UU
- Se integra con Microsoft Azure Sentinel para acelerar la respuesta ante incidentes
- Soporte para plataformas de nube privada (ESXi, Hyper-V, KVM, Nutanix) y pública (AWS, Azure)

Protección de equipos virtuales

- Confidencialidad de los datos
- Comunicación segura con prevención de filtración de datos
- Validación, inspección y monitorización del tráfico
- Resiliencia y disponibilidad de la red virtual

FICHA TÉCNICA

La serie de firewalls NS*v* ayuda a los equipos de seguridad a reducir este tipo de riesgos y vulnerabilidades, que pueden causar graves interrupciones en las operaciones y los servicios críticos de negocio. Permite a las empresas controlar el pase del tráfico dinámico a través de un firewall y proporciona visibilidad y perspectiva respecto a las políticas dispares. Ayuda a simplificar las tareas de gestión, a reducir errores de configuración y a acelerar el tiempo de implementación, todo lo cual contribuye a una mejor estrategia general de seguridad.

SonicOSX y Servicios de Seguridad

Los firewalls NS*v* 270/470/870 se basan en la arquitectura SonicOSX. Está basada en SonicOSX 7, un sistema operativo con gran cantidad de prestaciones, una interfaz de usuario (IU) intuitiva y funciones avanzadas de seguridad, redes y gestión.

Creado desde cero, SonicOSX 7.0 incorpora una configuración de políticas unificadas que permite la gestión integrada de varias políticas de seguridad. Proporciona fácilmente controles de capa 3 a capa 7 basadas en una sola norma para cada firewall, lo que ofrece una ubicación centralizada para configurar políticas. La nueva interfaz web proporciona visualizaciones gráficas de la información crítica sobre las amenazas y muestra alertas accionables que instan a configurar políticas de seguridad contextuales utilizando funciones sencillas de señalar y hacer clic.

Además, NS*v* integra SD-WAN, soporte para TLS 1.3, visualización en tiempo real, red privada virtual (VPN) de alta velocidad y otras sólidas prestaciones de seguridad. Las amenazas desconocidas se envían para su análisis al sandbox multimotor de SonicWall basado en la nube Capture Advanced Threat Protection (ATP). Capture ATP utiliza Inspección profunda de memoria en tiempo real (RTDMI), una tecnología patentada de SonicWall, para descubrir y bloquear el malware y las amenazas de día cero que residen en la memoria.

Gracias a la combinación de Capture ATP, la tecnología RTDMI y los servicios de seguridad avanzados, los firewalls de la serie NS*v* detienen el malware en la pasarela antes de que llegue a sus sistemas críticos.

Implementaciones

1. Cloud Edge: Nubes públicas, privadas y de agencias gubernamentales

- Cargas virtuales seguras en Amazon Web Services (AWS) y Microsoft Azure
- Proteja de las ciberamenazas las aplicaciones y las infraestructuras en la nube, gracias a las prestaciones avanzadas de la nueva generación de firewalls que incorporan VPN, IPS, CFS, AV y mucho más
- Descifre fácilmente el tráfico encriptado y utilice el soporte de TLS 1.3 para una seguridad mejorada
- Implemente funcionalidades de prevención de amenazas y segmentación y asegúrese de que cumple los estándares de seguridad normativos
- Con las políticas unificadas, consiga una total visibilidad y control del tráfico en distintas regiones y zonas de disponibilidad
- Pase de CAPEX a OPEX y obtenga rentabilidad y eficiencia en los costes
- Proteja las nubes de AWS y Azure designadas para agencias del Gobierno de EE. UU. y sus clientes implementando firewalls NS*v*
- Asegure los recursos informáticos virtualizados y los hipervisores para proteger las cargas de trabajo de la nube privada en VMware ESXi, Microsoft Hyper-V, Nutanix y KVM
- Prevenga las amenazas con una visibilidad completa de la comunicación intrahost entre los equipos virtuales
- Asegure una aplicación adecuada de las políticas de seguridad para las aplicaciones en todo el entorno virtual
- Normas de habilitación de aplicaciones seguras por aplicación, usuario y dispositivo, independientemente de la ubicación de los equipos virtuales
- Implemente zonas y aislamientos de seguridad apropiados
- Integración con Microsoft Azure Sentinel, una solución escalable y nativa de nube de gestión de eventos e información de seguridad (SIEM) y orquestación, automatización y respuesta de la seguridad (SOAR) para acelerar la respuesta a los incidentes

2. Internet Edge

- Proteja los recursos corporativos de los ataques en la pasarela de Internet
- Utilice las características avanzadas de seguridad para proteger el borde de Internet frente a los ataques más avanzados y bloquee automáticamente las amenazas
- Implemente funcionalidades de prevención de amenazas y segmentación y asegúrese de que cumple los estándares de seguridad normativos
- Aproveche las mejoras de SonicOSX para aumentar la eficiencia y el rendimiento empresariales y reducir los costes
- Segmente los sistemas críticos de puntos de venta (PoS) para garantizar la continuidad de negocio
- Con las políticas unificadas, consiga una total visibilidad y control del tráfico en distintas regiones y zonas de disponibilidad

Especificaciones del sistema de la serie NS*v*

Generales del firewall	NS*a* 270	NS*a* 470	NS*a* 870
Sistema operativo	SonicOSX[11]		
Hipervisores soportados	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7 / v7.0 / v8.0, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[10]		
Nubes del Gobierno soportadas[12]	AWS y Azure (en las regiones Este y Oeste de EE UU)		
Tipos de instancias AWS soportados	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
Tipos de instancias Azure soportados	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
Licencias	BYOL, PAYG[1]		
vCPUs máx. soportadas	2	4	8
Número de interfaces (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
Cantidad máx. núcleos gestión/DataPlane	1/1	1/3	1/7
Memoria mín.[2]	4 GB	8 GB	10 GB
Memoria máx.[3]	6 GB	10 GB	14 GB
IP/nodos soportados	Ilimitado		
Almacenamiento mínimo	60 GB		
Usuarios con SSO	500	10000	15000
Protocolización	Analyzer, Local Log, Syslog		
Alta disponibilidad	Activa/Pasiva[4]		

Rendimiento de firewall/VPN [5, 7]	NSa 270	NSa 470	NSa 870
Rendimiento de inspección del firewall	6 Gbps	9 Gbps	14 Gbps
Rendimiento de prevención de amenazas	1,6 Gbps	2,9 Gbps	8 Gbps
Rendimiento de IPS	4 Gbps	6 Gbps	8 Gbps
Rendimiento de TLS/SSL DPI	800 Mbps	2 Gbps	4 Gbps
Rendimiento de VPN[8]	1,4 Gbps	3,5 Gbps	8 Gbps
Conexiones por segundo	13760	37270	75640
Número máximo de conexiones (SPI)	225000	1,5 millones	3 millones
Número máximo de conexiones (DPI)	125000	1,5 millones	2 millones
Conexiones TLS/SSL DPI	8000	20000	30000
VPN	**NSa 270**	**NSa 470**	**NSa 870**
Túneles VPN entre emplazamientos	75	6000	10000
Clientes VPN IPSec[13] (máximo)	50(1000)	2000(4000)	2000(6000)
Clientes SSL VPN incluidos[6]	2	2	2
Clientes SSL VPN máximo[6]	100	200	300
Cifrado/autenticación	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Suite B, Common Access Card (CAC)		
Intercambio de claves	Grupos Diffie Hellman 1, 2, 5, 14v		
VPN basada en enrutamiento	RIP, OSPF, BGP		
Redes	**NSa 270**	**NSa 470**	**NSa 870**
Asignación de direcciones IP	Estática, DHCP, servidor DHCP interno[9], relé DHCP[9]		
Modos NAT	1:1, muchos:1, 1:muchos, NAT flexible (IPs solapadas), PAT		
Interfaces lógicas VLAN y túnel (máximo) [7]	128	128	128
Protocolos de enrutamiento	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, 802.1p		
Autenticación	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos de usuarios interna, Terminal Sevices, Citrix		
Base de datos de usuarios local	250	2500	3200

[1]Actualmente, PAYG solo está disponible en AWS.
[2]Memoria con Jumbo frames desactivados.
[3]Memoria con Jumbo frames activados. Con los Jumbo frames activados se requiere memoria adicional. Azure y AWS no admiten Jumbo frames.
[4]Hay HA en la plataforma VMware ESXi y en KVM, Azure, Microsoft Hyper-V y Nutanix. NSv 270 admite HA si se utiliza el tamaño D3v2 VM. HA no soportada en AWS. HA en Azure requiere un tamaño de servidor que admita tres o más interfaces.
[5]Los números de rendimiento publicados dependen de la especificación; el rendimiento real puede variar, según el hardware base, las condiciones de la red, la configuración del firewall y los servicios activados. El rendimiento y las funcionalidades también pueden variar según la estructura de virtualización subyacente. Recomendamos pruebas adicionales dentro del entorno para garantizar que se cumplen los requisitos de rendimiento y capacidad. El rendimiento se midió mediante un procesador Intel Xeon W (Platinum 8268 @2,9GHz, 3,9GHz Turbo, 37,5M caché) con SonicOS 7.0.1 y VMware vSphere 7.0.
[6]El número de clientes SSL VPN disponibles es de 50 en NSv 270 y 75 en NSv 470. Solo habrá un número mayor de SSL VPNs disponibles para firmwares a partir de SonicOS 6.5.4.4-44v-21-723.
[7]Azure y AWS no admiten interfaces VLAN.
Métodos de prueba: Rendimiento máximo basado en RFC 2544 (para firewall). 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 y Application Control activado con los ajustes de firewall predeterminados. 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.
[8]Todos los parámetros de rendimiento probados en Dell R740 con SR-IOV y Turbo boost.
[9]Se soporta en nube privada, pero no en plataformas de nube pública.
[10]Nutanix AHV se admite en SonicWall NSv 270/470/870 con firmwares SonicOSX 7.0.0 y posteriores.
[11]Los usuarios a partir de SonicOSX 7.0.1 podrán seleccionar y cambiar entre el modo clásico/global y el modo de política.
[12]La nube del Gobierno solo está disponible mediante BYOL.
[13]Los clientes GVC disponibles para el programa para MSSPs son solo 25 en NSv 270 y 50 en NSv 470.

Resumen de las prestaciones de SonicOSX 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
- APIs REST
- Integración con SonicWall Switch[1]
- Integración de puntos de acceso SonicWall Wi-Fi 6
- Servicio de filtrado de contenido basado en la reputación (CFS 5.0)
- Filtrado de DNS
- Transporte
  - Escalabilidad de SD-WAN
  - Asistente de usabilidad de SD-WAN
- API
  - Soporte completo de APIs
- Multiempresa[3]
  - Gestión multiempresa
  - Vista de tenant con el firmware por cada tenant
- Cambio entre el modo clásico/global y el modo de política[4]

Políticas unificadas

- Las políticas unificadas combinan normas de capa 3 a capa 7:
  - Fuente/IP de destino/Puerto/Servicio
  - Control de aplicaciones
  - CFS/Web Botnet/Geo-IP
  - Diagrama de reglas
  - Refuerzo de servicios de seguridad de paso único - IPS/GAV/AS/Capture ATP
  - Objetos basados en perfiles para seguridad de endpoints/BWM/QoS/ CFS/Prevención de intrusiones
- Perfiles de acción para reglas de seguridad/DoS
- Gestión de normas:
  - Clonado
  - Análisis *shadow rule*
  - Edición en celdas
  - Exportación de reglas
  - Edición de grupos
- Gestión de vistas
  - Normas utilizadas/no utilizadas
  - Normas activas/inactivas
  - Secciones/agrupación personalizada
  - Rejilla/diseño personalizable

Descifrado e inspección TLS/SSL/SSH

- TLS1.3
- Admite TLS 1.3 con seguridad mejorada
- 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

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 automatizado 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
- Integración del control de acceso a la red con Aruba ClearPass
- Actualizaciones automáticas de las definiciones
- Motor de 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
- 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 enrutamiento (RIP/OSPF/BGP)

Dashboard mejorado

- Vista de dispositivos mejorada
- Resumen de tráfico y usuarios principales
- Información valiosa sobre las amenazas
- Centro de notificaciones
- Monitorización de paquetes mejorada
- Terminal SSH en IU
- Nuevo diseño/plantilla
- Comparación de media en el sector/global

Redes

- PortShield[1]
- 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 SonicWall[1]
- Enrutamiento basado en políticas (ToS/métrico y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces[1] (estática y dinámica)
- Redundancia de puertos[1]
- Alta disponibilidad A/P con sincronización de estado
- Agrupación (clústeres) A/A[1]
- Equilibrio de carga entrante/saliente
- Modo puente de capa 2[1], modo wire/virtual wire,modo tap, modo NAT
- Reconexión 3G/4G WAN[1]
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)
- Contenedorización de SonicCoreX y SonicOS

Política de descifrado

- Política unificada para tráfico SSL/TLS

Política DoS

- Política unificada para prevención de ataques Dos/DDoS

VoIP

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

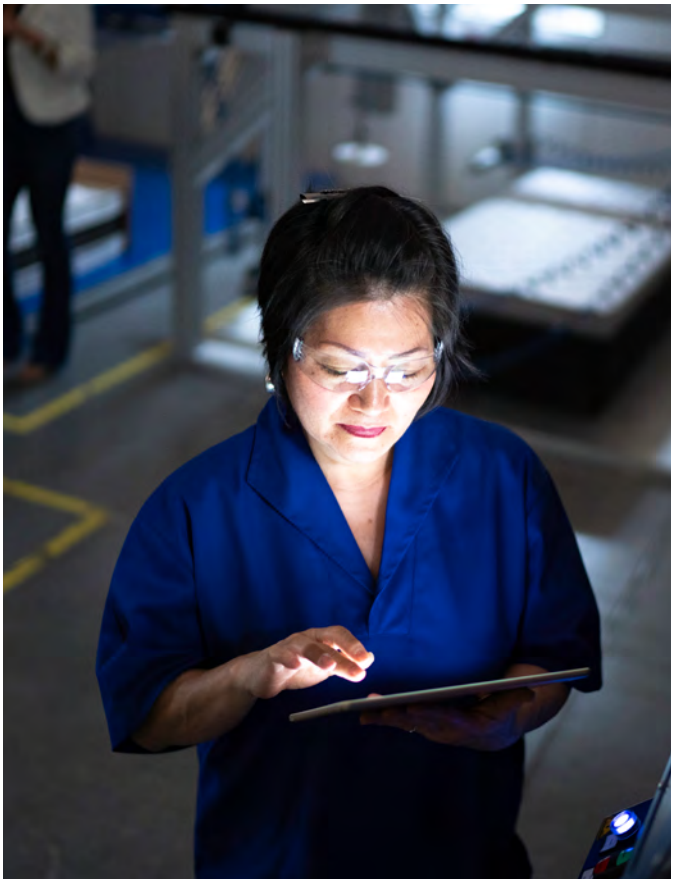
Gestión y supervisión

- GUI Web
- Interfaz de línea de comandos (CLI)
- Registro y aprovisionamiento sin necesidad de intervención
- Soporte de aplicaciones móviles SonicExpress
- SNMPv2/v3
- Gestión e informes centralizados con Network Security Manager (NSM)[2]
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6
- Informes externos (Scrutinizer)
- Pantalla de gestión LCD[1]
- Gestión de switches de la serie N y la serie X de Dell, incluidos switches en cascada[1]
- Informes de Network Security Manager

Conectividad inalámbrica[1]

- 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
- Acceso limitado para usuarios invitados
- Portal para invitados LHM

[1] Prestación no soportada en los firewalls de la serie NS*v*.
[2] Requiere suscripción adicional.
[3] Disponible solo en firewalls NSsp.
[4] Disponible a partir de SonicOSX 7.0.1.



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

Obtenga más información sobre las series NSv 270/470/870 de SonicWall

www.sonicwall.com/NSv

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