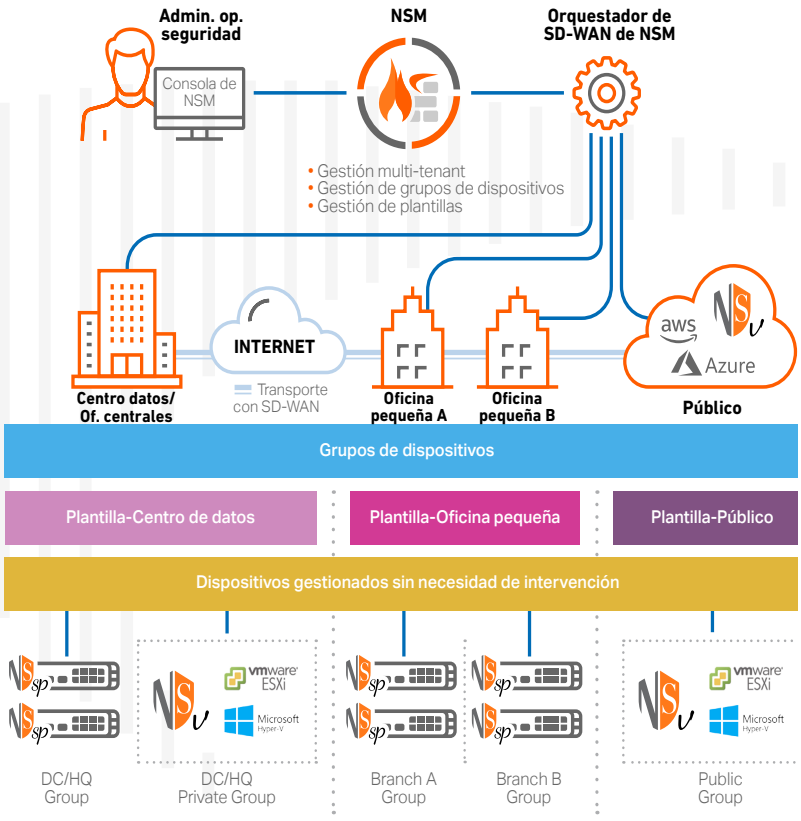
SONICWALL

Network Security Manager

Sistema de gestión unificada de firewalls escalable para adaptarse a cualquier entorno

Tanto si tiene que proteger un negocio pequeño, como una empresa distribuida, múltiples empresas o una red cerrada, su seguridad de red puede verse desbordada por el caos operacional, los riesgos imprevistos y las exigencias normativas. Antes, las prácticas de gestión de firewalls eficientes se basaban principalmente en la fiabilidad de los sistemas y en las medidas de control del servicio. Sin embargo, los errores frecuentes, las configuraciones erróneas, y tal vez incluso las violaciones de estos controles, siguen planteando retos constantes incluso a los centros de operaciones de seguridad (SOCs) bien gestionados.



PRESTACIONES DESTACADAS

Empresa

- Gastos de gestión de la seguridad reducidos
- Conocimiento del panorama de las amenazas y del estado de seguridad
- Eficiencia de la organización de TI y reducción del desgaste de los administradores
- Eliminación de los elevados costes derivados de la interrupción del negocio y los incidentes de seguridad

Operaciones

- Elimine los silos de gestión de firewalls
- Incorpore fácilmente cualquier cantidad de firewalls de forma remota
- Responda rápidamente a los problemas críticos del sistema y garantice un rendimiento óptimo de la red
- Establezca una configuración y políticas coherentes en todos los dispositivos gestionados
- Facilite la rápida implementación de redes SD-WAN

Seguridad

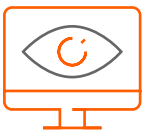
- Audite, asigne y refuerce políticas de seguridad coherentes en todos los entornos
- Establezca configuraciones de SD-WAN coherentes en todos los emplazamientos
- Descubra amenazas y responda a los problemas y los riesgos rápidamente
- Monitorice y siga con mayor precisión los resultados de las acciones basadas en políticas
- Evite la autenticación de usuarios no autorizados, incluidas las amenazas internas

Gestión centralizada. Seguridad elevada.

www.sonicwall.com/nsm

FICHA TÉCNICA

La herramienta de gestión multi-tenant centralizada SonicWall Network Security Manager (NSM) le permite gestionar de forma centralizada todas las operaciones de firewall sin cometer errores adhiriéndose a flujos de trabajo auditables. Los informes y análisis[1,2] ofrecen visibilidad en una sola consola y le permiten monitorizar y descubrir amenazas mediante la unificación y correlación de registros en todos los firewalls. NSM también le ayuda a cumplir las normas, ya que permite reforzar las políticas de forma coherente en todos los firewalls y hacer un seguimiento completo de cada cambio de configuración y de los informes granulares. La solución es escalable para adaptase a organizaciones que gestionan cientos de dispositivos de firewall implementados en múltiples tenants o numerosas ubicaciones. NSM lo hace todo con mayor rapidez y menor esfuerzo.



Tome el control: orqueste las operaciones de los firewalls desde un único lugar

NSM le ofrece todo lo que necesita para disfrutar de un sistema de gestión unificada de firewalls. Le proporciona visibilidad a nivel de tenant, control de dispositivos basado en grupos y escalabilidad ilimitada para gestionar y aprovisionar de forma centralizada sus operaciones de seguridad de red de SonicWall. Ello incluye la implementación y gestión de todos los dispositivos de firewall, grupos de dispositivos y tenants, la sincronización y el refuerzo de políticas de seguridad coherentes, incluidas de DNS y filtrado de contenido, en todos sus entornos con controles locales flexibles, y la monitorización de todo el sistema desde un dashboard dinámico con informes y análisis detallados. Asimismo, NSM permite el Control de acceso a la red mediante la integración con Aruba ClearPass. Además, NSM le permite gestionar todo a través de una única consola fácil de usar y accesible desde cualquier ubicación mediante cualquier dispositivo habilitado para navegador.

Gestión multi-tenant

A medida que crece su entorno de firewall, necesitará un sistema de gestión de firewalls escalable capaz de adaptarse a él. NSM proporciona funciones completas de gestión multi-tenant y un control de políticas independiente y separado para todos los tenants gestionados. Esta separación abarca todas las prestaciones de gestión de NSM, así como las funciones que dictan la operación de los firewalls para cada tenant. Puede crear cada tenant para que tenga su propio conjunto de usuarios, grupos y roles para llevar a cabo la gestión de grupos de dispositivos, la orquestación de políticas y todas las demás tareas administrativas dentro del ámbito de la cuenta de tenant asignada.

Gestión de grupos de dispositivos

Esta función le ofrece un efectivo método para crear y gestionar dispositivos de firewall como grupos o grupos jerárquicos y asignar e implementar plantillas de configuración en grupos de firewalls. Esto le permite sincronizar y reforzar los requisitos de políticas, objetos y configuración en cualquier grupo de firewalls seleccionado de forma consistente y fiable. Todos los cambios de políticas aprobados en la plantilla se aplican automáticamente a todos los grupos de dispositivos vinculados a esa plantilla. El agrupamiento de dispositivos puede definirse granularmente en base a cualquier característica, como el tipo de red, la ubicación, la unidad de negocio, la estructura organizacional o una combinación de estos atributos, para disfrutar de facilidad de gestión, identificación y asociación.

Gestión, asignación e implementación de plantillas

Los flujos de trabajo simplificados de NSM le permiten diseñar, validar, auditar, aprobar y asignar plantillas de configuración de forma rápida y sencilla para gestionar uno o cientos de dispositivos de firewall en numerosas ubicaciones geográficas. Se definen plantillas con varias políticas de firewall, configuraciones y objetos relacionados independientemente del dispositivo. NSM las transfiere de forma centralizada y automática a los dispositivos o grupos de dispositivos que requieren configuraciones similares.

Gracias a la combinación de plantillas con variables de plantillas, puede implementar y aprovisionar de forma centralizada cientos de firewalls remotos y establecer una configuración consistente manteniendo al mismo tiempo valores únicos específicos de los dispositivos, como IP de interfaz, configuración DNS, nombre de host del firewall, etc. Las empresas distribuidas pueden incorporar y proteger nuevos emplazamientos remotos y de oficinas pequeñas sin esfuerzo utilizando una única plantilla, eliminando así la instalación manual separada para cada dispositivo y ubicación.

Orquestación y monitorización de SD-WAN

NSM simplifica la implementación de redes SD-WAN a nivel de toda la empresa mediante un flujo de trabajo intuitivo autoguiado. Implementa y refuerza de forma centralizada las configuraciones de tráfico basadas en aplicaciones y otras configuraciones de dirección del tráfico en, y entre, cientos de emplazamientos, como oficinas pequeñas y tiendas

minoristas. Además, NSM le permite monitorizar el estado y el rendimiento de todo su entorno SD-WAN para garantizar configuraciones consistentes, fomentar el rendimiento óptimo de las aplicaciones y permitir a los equipos de infraestructura de red resolver problemas rápidamente.

Orquestación y monitorización de VPN

NSM simplifica las configuraciones y políticas de VPN con un sencillo proceso de instalación paso a paso basado en asistente. Esto permite a los administradores del sistema establecer rápidamente y sin errores una conectividad y una comunicación entre emplazamientos efectiva utilizando un flujo de trabajo autoguiado repetible. Además, la monitorización de VPN ayuda a controlar activamente el estado de sus VPNs, proporcionándole visibilidad completa de las actividades, el estado y el rendimiento de todo su entorno VPN. Los administradores de red pueden utilizar esta información para monitorizar el estado de la conexión, los datos transferidos y el ancho de banda consumido a través de esos túneles VPN. Gracias a las alertas, los administradores pueden mantener la integridad de las conexiones VPN de forma proactiva, asegurando una conectividad continua entre emplazamientos.

Sea más efectivo: trabaje de forma más inteligente y tome medidas de seguridad con mayor rapidez y menor esfuerzo

NSM es una herramienta de gestión de la productividad que le permite trabajar de forma más inteligente y tomar medidas de seguridad con mayor rapidez y menor esfuerzo. Su diseño está guiado por los procesos de negocio y basado en el principio de simplificación y, en algunos casos, automatización de los flujos de trabajo con el fin de lograr una mejor coordinación de la seguridad. Asimismo, ayuda a reducir la complejidad, el tiempo y los gastos de las operaciones de seguridad y las tareas de administración cotidianas.

Implementación sin esfuerzo ni necesidad de intervención

Integrado en NSM, el servicio de Implementación sin necesidad de intervención le permite implementar y poner fácilmente en servicio los firewalls, switches y puntos de acceso SonicWall en ubicaciones remotas y oficinas pequeñas. Todo el proceso requiere una intervención mínima por parte del usuario y está totalmente automatizado. Los dispositivos con Implementación sin necesidad de intervención se envían directamente a los emplazamientos destinados a la instalación. Una vez registrados y conectados por cable a la red, todos los dispositivos pasan instantáneamente al modo activo, ocupándose de garantizar la seguridad y la conectividad de forma fluida. Las plantillas de dispositivos preaprovisionadas se transfieren automáticamente a todos los dispositivos conectados una vez que se establecen los enlaces de comunicación con NSM. De esta forma, se elimina el tiempo, el coste y la complejidad de los tradicionales procesos de incorporación in situ.

Gestión de cambios libre de errores

NSM proporciona acceso inmediato a potentes flujos de trabajo automatizados que se ajustan a los requisitos de gestión de cambios de las políticas de firewall y de auditoría de los SOCs. Permite realizar cambios de políticas sin errores mediante la aplicación de una serie de procedimientos rigurosos. Éstos incluyen la comparación, validación y autorización de configuraciones antes de la implementación. Los grupos de aprobación son flexibles para cumplir los procedimientos de auditoría internos de varios equipos funcionales. Gracias al proceso obligatorio de aprobación, NSM le permite mejorar la eficiencia operacional, mitigar riesgos y eliminar configuraciones erróneas.

Automatización de la gestión con APIs RESTful

Las APIs RESTful de NSM proporcionan a sus operadores de seguridad cualificados un enfoque estándar para gestionar prestaciones específicas de NSM de forma programática sin una interfaz de gestión Web. Ello facilita la interoperabilidad entre NSM y consolas de gestión de terceros para aumentar la eficiencia de su equipo de seguridad interno. Los servicios API pueden automatizar operaciones de firewall para cualquier dispositivo gestionado. Éstas incluyen tareas cotidianas típicas, como la gestión de grupos de dispositivos y tenants, configuraciones de auditoría, comprobaciones del estado del sistema, etc.

Sea más consciente: investigue los riesgos ocultos con monitorización activa, informes y análisis[1,2]

El dashboard interactivo de NSM proporciona monitorización en tiempo real y datos de informes y análisis. Esta información le ayuda a resolver problemas, investigar riesgos y tomar medidas inteligentes basadas en políticas de seguridad para una seguridad más adaptativa.

Los administradores pueden actuar de forma rápida y precisa con alertas en tiempo real para mantener el óptimo funcionamiento de su organización, ayudando así a las organizaciones a evitar los elevados costes derivados de las interrupciones del negocio y los incidentes de seguridad.

Vea todo en todos lados

En combinación con Analytics[1,2], NSM le proporciona hasta 7 días de visibilidad continua de todo su ecosistema de seguridad de SonicWall a nivel de tenant, grupo o dispositivo. Ofrece análisis estáticos y casi en tiempo real de todo el tráfico de red y de todos los datos que pasan por el ecosistema de firewall. Todos los datos de protocolización se registran, agregan, contextualizan y presentan automáticamente de forma significativa, accionable y fácilmente consumible. Puede descubrir, interpretar y priorizar los datos y tomar medidas defensivas y correctivas en base a la información relevante y al conocimiento situacional obtenidos de dichos datos. Los informes programados le permiten personalizar sus informes con cualquier combinación de datos de tráfico. Presenta hasta 365 días de registros a nivel de dispositivo, grupo de dispositivos o tenant para análisis históricos, la detección de anomalías, el descubrimiento de brechas de seguridad, etc.

Esto le ayudará a ejecutar, seguir y medir la operación de su red y de la seguridad.

Entienda su riesgo

Gracias a las prestaciones adicionales de desglose y rotación, puede investigar los datos más detalladamente y correlacionarlos para examinar y descubrir amenazas y problemas ocultos con mayor precisión y confianza. Utilizando una mezcla de informes históricos, análisis basados en usuarios y aplicaciones y visibilidad de los endpoints, puede analizar detalladamente varios patrones y tendencias asociados a la entrada/salida de tráfico, el uso de las aplicaciones, el acceso de usuarios y dispositivos, acciones de amenazas, etc. Obtendrá conocimiento situacional e información valiosa, no solo para descubrir riesgos de seguridad, sino también para orquestar la resolución, al tiempo que monitoriza y sigue los resultados con el fin de fomentar e impulsar el refuerzo de la seguridad en todo su entorno.

Optimice la productividad del personal

Los Análisis de usuarios[1,2] proporcionan una vista amplia y transparente de las actividades de uso de aplicaciones Web e Internet por parte de sus empleados. Las prestaciones de desglose permiten a los analistas rotar e investigar de forma rápida y sencilla los puntos de datos de interés a nivel de usuario y establecer medidas controladas por políticas y respaldadas por pruebas para los usuarios y las aplicaciones de riesgo a medida que se detectan en el proceso de descubrimiento. Además, la función de Informes de productividad[1,2] proporciona información valiosa sobre el uso de Internet por parte de los empleados, así como sobre su comportamiento, durante un determinado periodo. Genera potentes instantáneas e informes con funciones de desglose que clasifican las actividades Web de los usuarios en grupos de productividad, como productivas, improductivas, aceptables, inaceptables y grupos personalizados, ayudando a las organizaciones a entender y a controlar mejor el uso de Internet.

Implementación flexible

Los clientes pueden implementar NSM de varias formas, según sus requisitos operacionales, normativos y presupuestarios.

Para una experiencia libre de mantenimiento, NSM está disponible como opción SaaS hospedada por SonicWall y accesible por Internet. Con NSM SaaS, puede escalar su solución bajo demanda, reduciendo al mismo tiempo los costes operativos. No es necesario implementar ningún hardware ni software, elaborar un plan de mantenimiento, personalizar el software ni realizar configuraciones ni actualizaciones, y no hay periodos de inactividad, depreciación ni costes de retirada. Todos estos gastos se eliminan y son sustituidos por un coste de suscripción anual reducido y predecible.

Para controlar totalmente el sistema y cumplir la normativa vigente, puede implementar NSM en la nube pública de Microsoft Azure o como dispositivo virtual en una nube privada en VMWare, Microsoft Hyper-V o KVM. De este modo, disfrutará de todas las ventajas operativas y económicas de la virtualización, como la escalabilidad y la agilidad de los sistemas, la velocidad de aprovisionamiento de los sistemas, la facilidad de gestión y la reducción de costes.

Prestaciones de seguridad

Las organizaciones federales, públicas, sanitarias, farmacéuticas y otras organizaciones de gran tamaño a menudo implementan redes cerradas para mantener la privacidad y el aislamiento de sus aplicaciones de misión crítica y sus sistemas de información más sensibles, como los sistemas de documentos clasificados, SCADA y las instalaciones de investigación. NSM soporta entornos de red cerrados proporcionando a los administradores una forma fuera de línea de incorporar, licenciar, aplicar parches y actualizar el sistema NSM y los firewalls bajo su gestión sin contactar con SonicWall License Manager ni MySonicWall.

Para un nivel de seguridad adicional, NSM refuerza varias medidas de control del acceso a la cuenta a fin de prevenir el acceso no autorizado a la interfaz de gestión de NSM. Proporciona controles administrativos específicos de acuerdo con los roles del usuario y activa el bloqueo de la cuenta tras un número especificado de intentos de inicio de sesión fallidos. Además, solo se permite el acceso de los usuarios cuando inician sesión desde una lista especificada de direcciones IP de origen y con autenticación de doble factor (2FA)[3].

Resumen de las prestaciones

Gestión

- Control de acceso a la red (NAC) con Aruba Clearpass
- Gestión a nivel de tenant y de grupo de dispositivos
- Plantillas de configuración
- Agrupación de dispositivos
- Conversión de la configuración de los dispositivos en una plantilla
- Asistente de asignación e implementación
- Auditorías de la configuración
- Config – Diff
- Gestión y planificación offline
- Gestión de las políticas de seguridad de firewall
- Gestión de las políticas de seguridad de VPN
- Administración de SD-WAN
- Sincronización de servicios de seguridad
- Alta disponibilidad
- Backups de configuración
- APIs RESTful
- Actualización de firmware multidispositivo
- Administración basada en roles
- Gestión de puntos de acceso y switches
- Monitorización inteligente de plataformas (IPM)[3]
- Gestión de certificados multidispositivo

Monitorización[1,2]

- Estado y salud de los dispositivos
- Estado de las licencias y el soporte
- Resumen de la red/las amenazas
- Centro de alertas y notificaciones
- Registros de eventos
- Vista de topología

Análisis[1,2]

- Actividades basadas en usuarios
- Uso de las aplicaciones
- Visibilidad de múltiples productos con Capture Client
- Visualización dinámica en tiempo real
- Prestaciones de desglose y rotación

Informes[1,2]

- Informes programados en PDF - Nivel de tenant/grupo/dispositivo
- Informes personalizables
- Protocolización centralizada
- Informes sobre amenazas múltiples
- Informes centrados en el usuario
- Informes del uso de las aplicaciones
- Informes del ancho de banda y los servicios
- Informes del ancho de banda por usuario
- Informes de productividad

Seguridad

- Soporte de redes cerradas
- Bloqueo de cuentas
- Control de acceso a las cuentas
- Soporte de 2FA[3]
- App de autenticación con soporte de 2FA

Licencias y paquetes

Gestión			
Prestación	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Tenant	Sí	Sí	Sí
Inventario de dispositivos	Sí	Sí	Sí
Refuerzo de políticas a nivel de grupo	Sí	Sí	Sí
Grupo de dispositivos	Sí	Sí	Sí
Plantillas	Sí	Sí	Sí
Asignación e implementación (Automatización de flujos de trabajo)	Sí	Sí	Sí
Auditoría de la configuración	Sí	Sí	Sí
Config Diff	Sí	Sí	Sí
Automatización de flujos de trabajo	Sí	Sí	Sí
API	Sí	Sí	Sí
Implementación sin necesidad de intervención	Sí	Sí	Sí
Orquestación y monitorización de SD-WAN	Sí	Sí	Sí
Orquestación y monitorización de VPN	Sí	Sí	Sí
Planificación de tareas	Sí	Sí	Sí
Backup/Restauración	Sí	Sí	Sí
Actualizaciones de firmware	Sí	Sí	Sí
Gestión de puntos de acceso y switches	Sí	Sí	Sí
Filtrado DNS avanzado	Sí	Sí	Sí
Control de acceso a la red con Aruba Clearpass	Sí	Sí	Sí
Filtrado de contenido basado en reputación	Sí	Sí	Sí

Licencias y paquetes (cont.)

Informes			
Prestación	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Dashboard de nivel de grupo/tenant	Sí	Sí	No
Capture ATP (Nivel de dispositivo)	Sí	Sí	Sí
Capture Threat Assessment (Nivel de dispositivo)	Sí	Sí	Sí
Informes de productividad[5]	No	Sí	No
Informes de VPN	No	Sí	No
Informes personalizados	Sí	Sí	No
Planificación de informes (Flujos, CTA y gestión)	Sí (Excepto informe de flujos)	Sí	Sí
Días de datos de informes	7 días	365 días	365 días

Análisis			
Prestación	**NSM SaaS Essential**	**NSM SaaS Advanced**	**NSM On-Prem[2]**
Análisis basado en usuarios	No	Sí	Sí
Análisis de aplicaciones	No	Sí	Sí
Análisis forenses de la red y caza de amenazas utilizando funciones de desglose de datos y de rotación	No	Sí	Sí
Cloud App Security – Descubrimiento de TI en la sombra	Sí	Sí	No

Requisitos del sistema

Navegadores de Internet

- Microsoft® Internet Explorer 11.0 o superior y la última versión de Microsoft Edge, Mozilla Firefox, Google Chrome y Safari

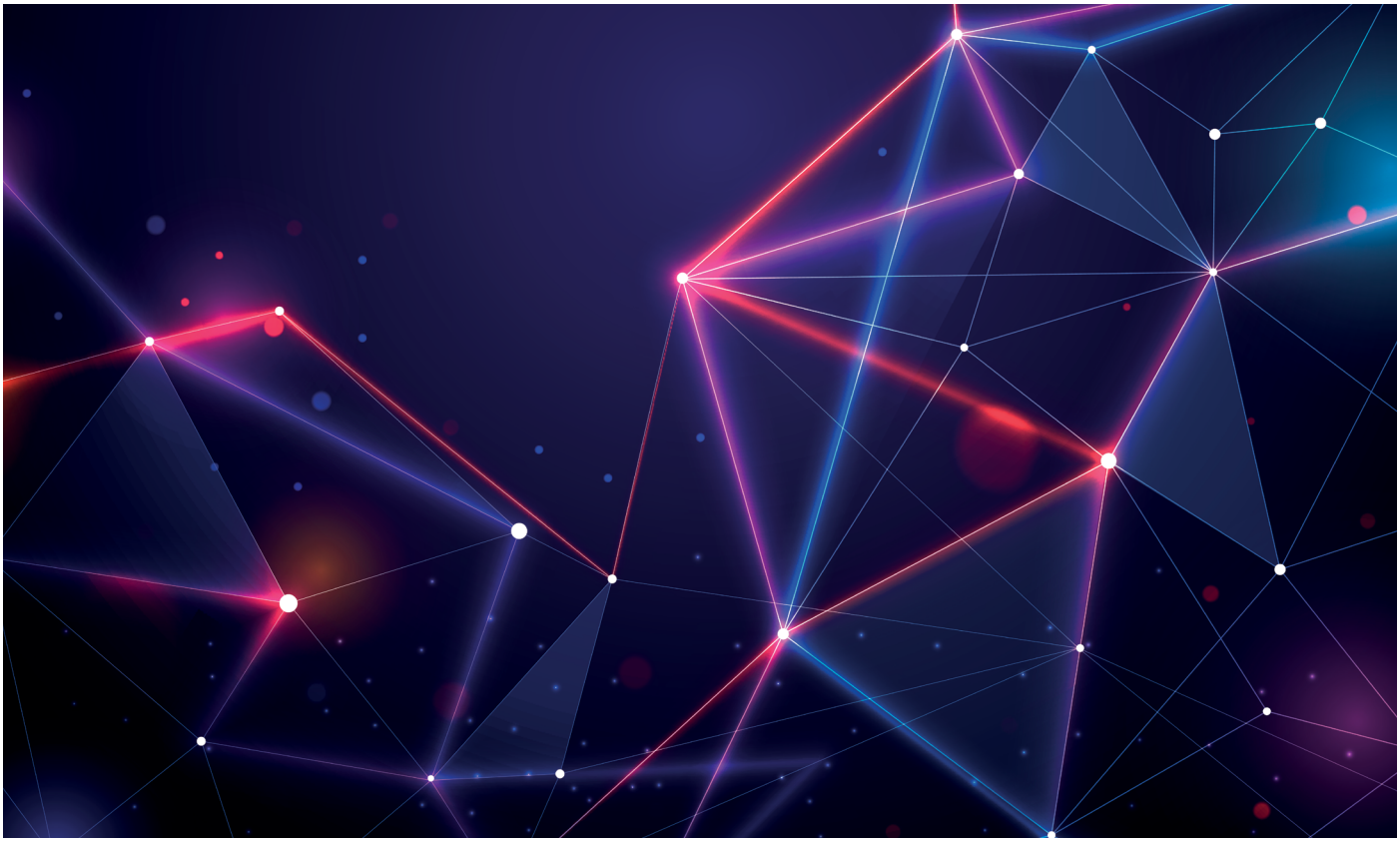
Requisitos del sistema de NSM On-Prem

- Hipervisor: ESXi 7.0, 6.7 y Hyper-V 2016, 2019, KVM
- Nube pública: Azure
- Recursos informáticos mínimos: 4 vCPUs, 24 GB de memoria para gestionar 1-500 firewalls, almacenamiento de 250GB

Dispositivos gestionados

- NS*sp* 15700, NS*sp* 13700, serie NS*sp* 12000[4], serie SuperMassive 9000[4], serie NSA, serie NS*a*, serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Dispositivos y firmware de 5ª generación incluidos dispositivos SOHO no inalámbricos con SonicOS 5.9 no soportados
- Dispositivos virtuales de seguridad de red de SonicWall: Serie NS*v*
- SonicWall SonicWave[6], SonicPoint
- El soporte de SonicWave incluye puntos de acceso equipados con tecnología Wi-Fi6
- SonicWall Switch

[1] NSM SaaS incluye prestaciones de informes y análisis.
[2] NSM On-Prem requiere una instalación y una licencia de SonicWall Analytics On-Prem separadas para las prestaciones de informes y análisis.
[3] Disponible solo en NSM On-Prem.
[4] 365 días de informes y 30 días de análisis no soportados.
[5] Requiere licencia AGSS/CGSS en firewalls de generación 6/6.5, licencia Essential Protection en firewalls de 7ª generación.
[6] El soporte de SonicWave incluye puntos de acceso equipados con tecnología Wi-Fi6



Implemente y gestione todos sus firewalls, switches conectados y puntos de acceso mediante una interfaz fácil de usar.

www.sonicwall.com/nsm

Acerca de SonicWall

SonicWall proporciona una Ciberseguridad sin límites, sin perímetro, para la era hiperdistribuida y 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

Datasheet-NSM-A4-JK-10177