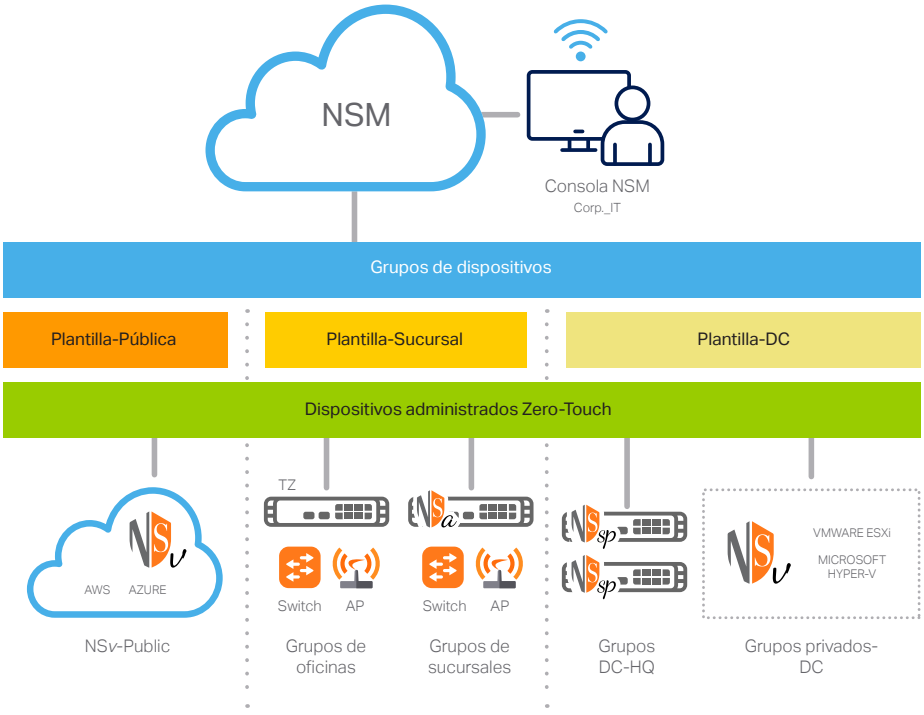
SONICWALL

Network Security Manager

Sistema unificado de gestión de firewalls que se adapta a cualquier entorno

Tanto si lo que quiere proteger es una pequeña empresa, una empresa distribuida o varias empresas, la seguridad de la red puede verse sobrepasada por el desorden operativo, los riesgos invisibles o los requisitos legales. Hasta ahora las buenas prácticas de gestión de firewalls se basaban principalmente en medidas de control operativo y de sistema sólidas y fiables. Sin embargo, los errores comunes, las malas configuraciones e incluso las violaciones de esos controles siguen siendo retos habituales de los Centros de Operación de Seguridad (SOC) bien dirigidos.

SonicWall Network Security Manager (abreviado NSM) es un gestor de firewalls multicliente centralizado que le permite administrar de manera centralizada todas las operaciones de firewall sin errores siguiendo flujos de trabajo auditables. Su motor analítico nativo proporciona visibilidad en un solo panel y le permite monitorizar y detectar amenazas unificando y correlacionando registros en todos los firewalls. NSM también le ayuda a cumplir en todo momento con la legislación, ya que proporciona una pista de auditoría completa de cada cambio de configuración e informes detallados. NSM se adapta a las redes de gestión de organizaciones de todos los tamaños con hasta miles de dispositivos de firewall desplegados en muchas ubicaciones, y lo hace con menos esfuerzo y tiempo.



Ventajas:

Negocio

- Menos gastos de gestión de la seguridad
- Conocimiento del panorama de amenazas y de la posición de seguridad
- Menos CAPEX con SaaS

Operatividad

- Sin necesidad de instalar software ni hardware
- Elimina los silos de administración de firewalls
- Integra fácilmente cualquier cantidad de firewalls de forma remota
- Visibilidad en todas las operaciones de seguridad

Seguridad

- Audite, asigne y aplique políticas de seguridad coherentes en todos los entornos
- Busque y responda rápidamente a problemas y riesgos
- Disponga de información correcta para tomar decisiones de ciberseguridad

Asuma el control: dirija todas las operaciones de firewalls desde un solo lugar

NSM tiene todo lo que debe tener un sistema unificado de administración de firewalls. Le proporciona visibilidad a nivel de cliente (*tenant*), control de dispositivos en grupo y una escalabilidad ilimitada para gestionar centralmente sus operaciones de seguridad de red de SonicWall. Esto incluye implementar y gestionar todos los dispositivos de firewall, grupos de dispositivos y clientes (*tenants*); sincronizar y aplicar políticas de seguridad unificadas en todos sus entornos con controles locales flexibles; y monitorizarlo todo desde un solo panel de control dinámico con informes detallados y análisis. NSM le permite hacer todo esto desde una única consola nativa en la nube fácil de usar a la que se puede acceder desde cualquier lugar utilizando un dispositivo con navegador.

Gestión multicliente
A medida que su entorno de firewalls crezca con complejos clientes (*tenants*) multinube y multiubicación, con diferentes necesidades de seguridad para cada segmento de red, necesitará un sistema de gestión de firewalls capaz de adaptarse a ese entorno. NSM proporciona una completa gestión multicliente y un aislamiento independiente con control de políticas en todos los clientes administrados. Esta separación abarca todas las características y funciones de administración de NSM que determinan el funcionamiento de firewall de cada cliente. Puede configurar cada cliente para que tenga su propio conjunto de usuarios, grupos y funciones; de esta forma podrá gestionar grupos de dispositivos, organizar políticas y realizar todas las demás tareas administrativas dentro de los límites de la cuenta de cliente asignada.

Gestión de grupos de dispositivos
Device Group le ofrece un método eficaz de crear y administrar dispositivos de firewall como grupo o grupos jerárquicos y de asignar e implementar plantillas de configuración en grupos de firewalls. De esta forma podrá sincronizar y hacer cumplir las mismas políticas, objetos o requisitos de configuración en cualquier grupo de firewall seleccionado de manera coherente y fiable. Todos los cambios de política que se aprueben en la plantilla se aplican automáticamente a todos los grupos de dispositivos vinculados a dicha plantilla. La agrupación de dispositivos se puede definir de manera detallada por características como el tipo de red, la ubicación, la unidad de negocios, la estructura organizativa o una combinación de atributos relativos para facilitar la administración, la identificación y la asociación.

Gestión, asignación y despliegue de plantillas
NSM cuenta con flujos de trabajo simplificados que le permiten diseñar, validar, auditar y asignar plantillas de configuración de manera fácil y rápida para administrar uno o miles de dispositivos de firewall en numerosas localizaciones geográficas. Las plantillas con diversas políticas de firewall, configuraciones y objetos relacionados se crean independientemente del dispositivo y el NSM las aplica de forma centralizada y automática a los dispositivos o grupos de dispositivos que trabajan con configuraciones similares.

Sea más eficaz: Trabaje de manera más inteligente y adopte medidas de seguridad más rápido y con menos esfuerzo

NSM es una herramienta de gestión de la productividad que le permite trabajar de manera más inteligente y adoptar medidas de seguridad más rápido y con menos esfuerzo. Su diseño se basa en procesos empresariales y se rige por el principio de la simplificación y, en algunos casos, automatización de flujos de trabajo para lograr una mejor coordinación de la seguridad y, a la vez, reducir la complejidad, el tiempo y los gastos generales de las operaciones de seguridad y tareas de administración cotidianas.

Implementación Zero-Touch fácil
NSM incorpora Implementación Zero-Touch, un servicio que permite instalar y poner en funcionamiento firewalls, *switches* y *access points* de SonicWall en ubicaciones y oficinas remotas sin esfuerzo. El proceso requiere una intervención mínima del usuario y está totalmente automatizado. Los dispositivos Zero-Touch se envían directamente al lugar de instalación. Una vez desembalados, registrados, conectados a la red y encendidos, todos los dispositivos funcionan al instante, con una seguridad y una conectividad impecables. Una vez establecidos los enlaces de comunicación con NSM, las plantillas de dispositivos preasignadas se aplican automáticamente a todos los dispositivos Zero-Touch. De este modo, elimina el tiempo, el coste y la complejidad del tradicional proceso de integración *in situ*.

Gestión de cambios infalible
NSM proporciona acceso inmediato a poderosos flujos de trabajo automatizados que cumplen con los requisitos de auditoría y gestión de cambios de las políticas de firewall de los Centros de Operación de Seguridad. Permite introducir cambios de las políticas sin errores mediante la aplicación de una serie de procesos de configuración, comparación, validación, revisión y aprobación de políticas de firewall antes de la implementación. Los grupos de aprobación tienen flexibilidad para cumplir con los diversos procedimientos de autorización y auditoría de distintos tipos de organizaciones. NSM implementa de forma programática políticas de seguridad plenamente validadas y auditadas para mejorar la eficiencia operativa, mitigar riesgos y eliminar errores humanos y de configuración.

Gestión automatizada con la API RESTful
Las API RESTful de NSM ofrecen a sus especialistas en seguridad un método estándar de administrar funciones específicas de NSM programáticamente sin una interfaz web de gestión. Facilita la interoperabilidad entre NSM y las consolas de gestión de terceros para que su equipo interno de seguridad sea más eficiente. Los servicios API sirven para automatizar las operaciones de firewall de cualquier dispositivo administrado. Esto incluye tareas cotidianas comunes como la administración de clientes, grupos de dispositivos, configuraciones de auditoría y controles de estado del sistema, entre otras.

Sea más consciente: detecte riesgos ocultos gracias a la monitorización, los informes y los análisis activos

NSM cuenta con un panel de control interactivo repleto de datos de monitorización, informes y análisis en tiempo real para ayudar a diagnosticar problemas, analizar riesgos y tomar decisiones inteligentes sobre políticas de seguridad y medidas estratégicas para una posición de seguridad adaptativa más sólida.

Verlo todo desde cualquier lugar
El panel de control de informes, análisis y control de riesgos de NSM le ofrece hasta 7 días de visibilidad continua 360° de todo su sistema de seguridad SonicWall a nivel de cliente, grupo o dispositivo. Proporciona análisis estático

y casi en tiempo real de todo el tráfico de red y la comunicación de datos que pasan a través del ecosistema de firewalls. Todos los datos de registro se guardan, agregan, contextualizan y presentan automáticamente de una manera significativa, procesable y fácilmente consumible que le permite descubrir, interpretar, priorizar y tomar las medidas defensivas y correctivas adecuadas basadas en la percepción de los datos y el conocimiento de la situación. Con los informes programados puede personalizar completamente sus informes con cualquier combinación de datos auditables. Muestra hasta 365 días de registros obtenidos a nivel de dispositivo con fines de análisis históricos, detección de anomalías, descubrimiento de brechas de seguridad, etc. De esta forma podrá rastrear, medir y ejecutar operaciones eficaces de red y seguridad.

Conozca sus riesgos
Gracias a las capacidades añadidas de desglose y giro, puede seguir investigando y correlacionando datos para examinar y descubrir amenazas y problemas ocultos con más precisión y fiabilidad. Mediante la combinación de informes históricos, análisis basados en usuarios y aplicaciones y visibilidad de *endpoints*, puede analizar exhaustivamente diversos patrones y tendencias asociados al tráfico de entrada/salida, uso de aplicaciones, acceso a usuarios y dispositivos, amenazas y mucho más. Conocerá mejor la situación y dispondrá de conocimientos valiosos no solo para descubrir riesgos de seguridad, también para organizar la solución, mientras controla y hace un seguimiento de los resultados para potenciar e impulsar una seguridad coherente en todo su entorno.

Resumen de características

Gestión

- Gestión a nivel de cliente (*tenant*) y grupo de dispositivos
- Plantillas de configuración
- Agrupación de dispositivos
- Asistente de asignación y aplicación
- Auditorías de configuración
- Configuración – Dif.
- Gestión y programación *offline*
- Gestión de políticas de firewalls de seguridad
- Gestión de políticas de VPN de seguridad
- Gestión de SD-WAN
- Gestión de servicios de seguridad con valor añadido
- Redundancia y alta disponibilidad
- Copia de seguridad de los archivos de preferencia del dispositivo de firewall
- API RESTful
- Actualización de firmware
- Administración basada en roles
- Gestión de *access points* y *switches*

Monitorización

- Estado e integridad de dispositivos
- Estado de licencia y asistencia
- Resumen de redes/amenazas
- Centro de alertas y notificaciones
- Registros de eventos
- Vista de topología

Análisis

- Actividades basadas en los usuarios
- Uso de las aplicaciones
- Visibilidad entre productos con Capture Client
- Visualización dinámica en tiempo real
- Capacidades de desglose y giro

Generación de informes

- Informes PDF programados: a nivel de cliente, grupo y dispositivo
- Informes personalizables
- Registro centralizado
- Informe multiamenaza
- Informe centrado en el usuario
- Informe de uso de aplicaciones
- Informes de ancho de banda y servicios
- Generación de informes de ancho de banda por usuario

Licencias y paquetes

Prestaciones	Essential	Advanced
Administrar cientos de dispositivos por cliente	Sí	Sí
Gestión multicliente	Sí	Sí
Inventario de dispositivos	Sí	Sí
Imponer políticas a nivel de grupo	Sí	Sí
Grupo de dispositivos	Sí	Sí
Plantillas	Sí	Sí
Asignar y aplicar	Sí	Sí
Auditoría de configuración	Sí	Sí
Dif. configuración	Sí	Sí
Automatización de flujos de trabajo	Sí	Sí
API	Sí	Sí
Implementación Zero-Touch	Sí	Sí
Planificación de tareas	Sí	Sí

Prestaciones	Essential	Advanced
Copia de seguridad/Restauración	Sí	Sí
Actualizaciones de firmware	Sí	Sí
Gestión de access points y switches	Sí	Sí
Días de informes de datos	7 días	365 días
Panel de control a nivel de grupo/cliente	Sí	Sí
Capture ATP (a nivel de dispositivo)	Sí	Sí
Capture Threat Assessment (a nivel de dispositivo)	Sí	Sí
Visibilidad e informes a nivel de grupo	Sí	Sí
Informes programados (a nivel de grupo de dispositivos)	Sí	Sí
Análisis basados en usuarios	No	Sí
Análisis de aplicaciones	No	Sí
Análisis de amenazas	No	Sí
Desglose y pivots	No	Sí

Producto	SKU
NSM ESSENTIAL PARA SOHO 250 1 AÑO	02-SSC-5219
NSM ADVANCED PARA SOHO 250 1 AÑO	02-SSC-5213
NSM ESSENTIAL PARA TZ 350 1 AÑO	02-SSC-5239
NSM ADVANCED PARA TZ 350 1 AÑO	02-SSC-5231
NSM ESSENTIAL PARA TZ 400 1 AÑO	02-SSC-5263
NSM ADVANCED PARA TZ 400 1 AÑO	02-SSC-5257
NSM ESSENTIAL PARA TZ 500 1 AÑO	02-SSC-5183
NSM ADVANCED PARA TZ 500 1 AÑO	02-SSC-5177
NSM ESSENTIAL PARA TZ 570 1 AÑO	02-SSC-4975
NSM ADVANCED PARA TZ 570 1 AÑO	02-SSC-4963
NSM ESSENTIAL PARA TZ 600 1 AÑO	02-SSC-5201
NSM ADVANCED PARA TZ 600 1 AÑO	02-SSC-5195
NSM ESSENTIAL PARA TZ 670 1 AÑO	02-SSC-5011
NSM ADVANCED PARA TZ 670 1 AÑO	02-SSC-4999
NSM ESSENTIAL PARA NS*a* 2600/NS*a* 2650 1 AÑO	02-SSC-5281
NSM ADVANCED PARA NS*a* 2600/NS*a* 2650 1 AÑO	02-SSC-5275
NSM ESSENTIAL PARA NS*a* 3600/NS*a* 3650 1 AÑO	02-SSC-5299
NSM ADVANCED PARA NS*a* 3600/NS*a* 3650 1 AÑO	02-SSC-5293
NSM ESSENTIAL PARA NS*a* 4600/NS*a* 4650 1 AÑO	02-SSC-5325
NSM ADVANCED PARA NS*a* 4600/NS*a* 4650 1 AÑO	02-SSC-5319
NSM ESSENTIAL PARA NS*a* 5600/NS*a* 5650 1 AÑO	02-SSC-5347
NSM ADVANCED PARA NS*a* 5600/NS*a* 5650 1 AÑO	02-SSC-5341
NSM ESSENTIAL PARA NS*a* 6600/NS*a* 6650 1 AÑO	02-SSC-5365
NSM ADVANCED PARA NS*a* 6600/NS*a* 6650 1 AÑO	02-SSC-5359

También hay disponibles contratos de soporte y SKU para varios años. Para acceder a la lista completa, diríjase a su distribuidor habitual o a Ventas de SonicWall.

Navegadores de Internet

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

Dispositivos administrados de NSM[1]

- Soluciones de seguridad de red SonicWall: Serie SuperMassive 9000[2], E-Class NSA, serie NS*sp* 12000[2], serie NS*a*, serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Dispositivos virtuales de seguridad de red SonicWall: NS*v*Series
- SonicWall SonicWave, SonicPoint
- SonicWall Switch

[1] Compatible con firewalls que funcionan con SonicOS versión 6.x o 7.x.
[2] No incluye los 365 días de informes ni los 30 días de análisis.

Acerca de SonicWall

SonicWall ofrece Boundless Cybersecurity (Ciberseguridad sin Límites, sin Perímetro) para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para obtener más información, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Ficha de datos-NSM-US-COG-2114