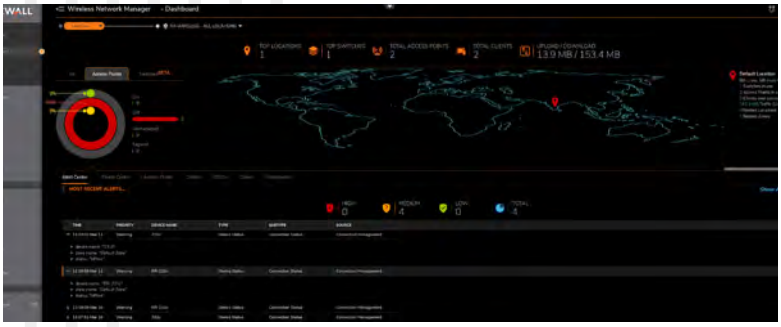
Wireless Network Manager

Consola unificada basada en la nube para la gestión de puntos de acceso y switches

Escalable para organizaciones de cualquier tamaño, SonicWall Wireless Network Manager (WNM) es un sistema intuitivo de gestión de red centralizada para conexiones inalámbricas y switches. Proporciona análisis exhaustivos, potentes funciones y fácil incorporación, desde una única consola.

Su infraestructura basada en la nube simplifica el acceso, el control y la resolución de problemas, al unificar múltiples tenants, ubicaciones y zonas. WNM da soporte a miles de puntos de acceso SonicWave y switches de SonicWall, sin el coste de complejos sistemas de gestión superpuestos.



PRESTACIONES DESTACADAS

- Permite Private Pre-Shared Keys (PPSK).
- Autenticación SAML.
- Identificación DHCP.
- Permite Content Filtering Service (CFS).
- Gestión integrada de puntos de acceso SonicWave y switches SonicWall.
- Visibilidad y control unificados a través de una única consola basada en la nube.
- Integración fluida con Capture Security Center.
- Configuración de política unificada para redes por cable e inalámbricas.
- Implementación sin necesidad de intervención para una incorporación y un aprovisionamiento rápidos.
- Actualizaciones automáticas de firmware y de seguridad.
- Analíticas exhaustivas y en tiempo real.
- Informes, registros y alertas detallados.
- Operación fiable, estabilidad en la nube y seguridad.
- Potentes mapas de topología de red.
- Herramienta avanzada integrada de análisis de emplazamientos.
- Interfaz intuitiva.
- Menor TCO.

Obtenga una solución de gestión de red segura e integrada para entornos por cable e inalámbricos:

sonicwall.com/wnm

FICHA TÉCNICA

Cree una política unificada y gestione desde cualquier parte, desde unos cuantos a miles de puntos de acceso, todo desde una única consola basada en la nube.

Gestión desde una única consola

WNM le permite gestionar fácilmente redes globales desde una única consola. Como parte del ecosistema Capture Security Center de SonicWall, su consola intuitiva ofrece visibilidad y control unificados. La jerarquía de red le permite ver las políticas individuales creadas a nivel de tenant que se aplican en diversas ubicaciones y zonas. Desglose los dispositivos gestionados para obtener datos granulares. WNM es muy escalable, desde un único emplazamiento hasta redes corporativas con decenas de miles de dispositivos gestionados que dan soporte a varios tenants.

La incorporación y la implementación son automáticas. Su red estará funcionando en unos minutos.

Clave previamente compartida

Las claves privadas previamente compartidas (PPSK) son una herramienta importante para proteger las redes. Cada una consiste en una larga serie aleatoria de números y letras combinados que se genera cuando un dispositivo se conecta a una red. Como cada dispositivo tiene su propia clave previamente compartida exclusiva, PPSK es una forma efectiva de proteger la red anfitriona o de desactivar un acceso individual a la red, cuando alguien se va de la organización. PPSK permite simplificar el uso y la gestión de la red, la compatibilidad para los clientes antiguos y el soporte para distintas VLAN.

Compatibilidad con autenticación SAML

El Lenguaje de Marcado para Confirmaciones de Seguridad (SAML) es una forma de autenticar los datos entre dos partes, especialmente, entre un proveedor de identidades y un proveedor de servicios. Permite a un usuario acceder a varias aplicaciones web mediante un único conjunto de credenciales de inicio. En resumen, SAML es una forma de indicar a las aplicaciones externas que un usuario es quien dice ser. Este inicio de sesión único proporciona al usuario una mejor experiencia y, además, puede aumentar la seguridad, ya que el proveedor de identidades —no el proveedor de servicios— es el responsable de almacenar las credenciales de los usuarios.

Identificación DHCP

Con la proliferación del BYOD («traiga su propio dispositivo») en los lugares de trabajo actuales, los administradores de redes se enfrentan al desafío de detectar e identificar esos dispositivos para asegurarse del cumplimiento. La identificación DHCP es una técnica para la verificación de la identidad que permite rastrear a los dispositivos y, lo más importante, bloquear aquellos que no estén permitidos.

Content Filtering Service

Mantener su red protegida del malware, los virus y las infecciones es crucial. El servicio de filtrado de contenido (CFS) hacen eso al inspeccionar el acceso a la página web y pasar a la acción cuando detectan una amenaza. CFS proporciona a los administradores las herramientas necesarias para crear y aplicar 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, para más de 56 categorías predefinidas.

Una operación fiable

WNM proporciona la estabilidad y fiabilidad de la nube. En caso de que falle el servicio de internet, los puntos de acceso y los switches pueden seguir trabajando sin WNM, con lo que se garantiza la continuidad de la actividad del negocio. La autenticación de dos factores y el cifrado de paquetes refuerzan la seguridad, mientras que las actualizaciones de firmware y de seguridad mantienen al día los dispositivos gestionados. WNM permite a los administradores aplicar de forma selectiva versiones de producción, beta o parches al firmware de cada dispositivo gestionado, según la necesidad, y permite el envío automático de informes a varios destinatarios a la vez.

Implementación sin necesidad de intervención

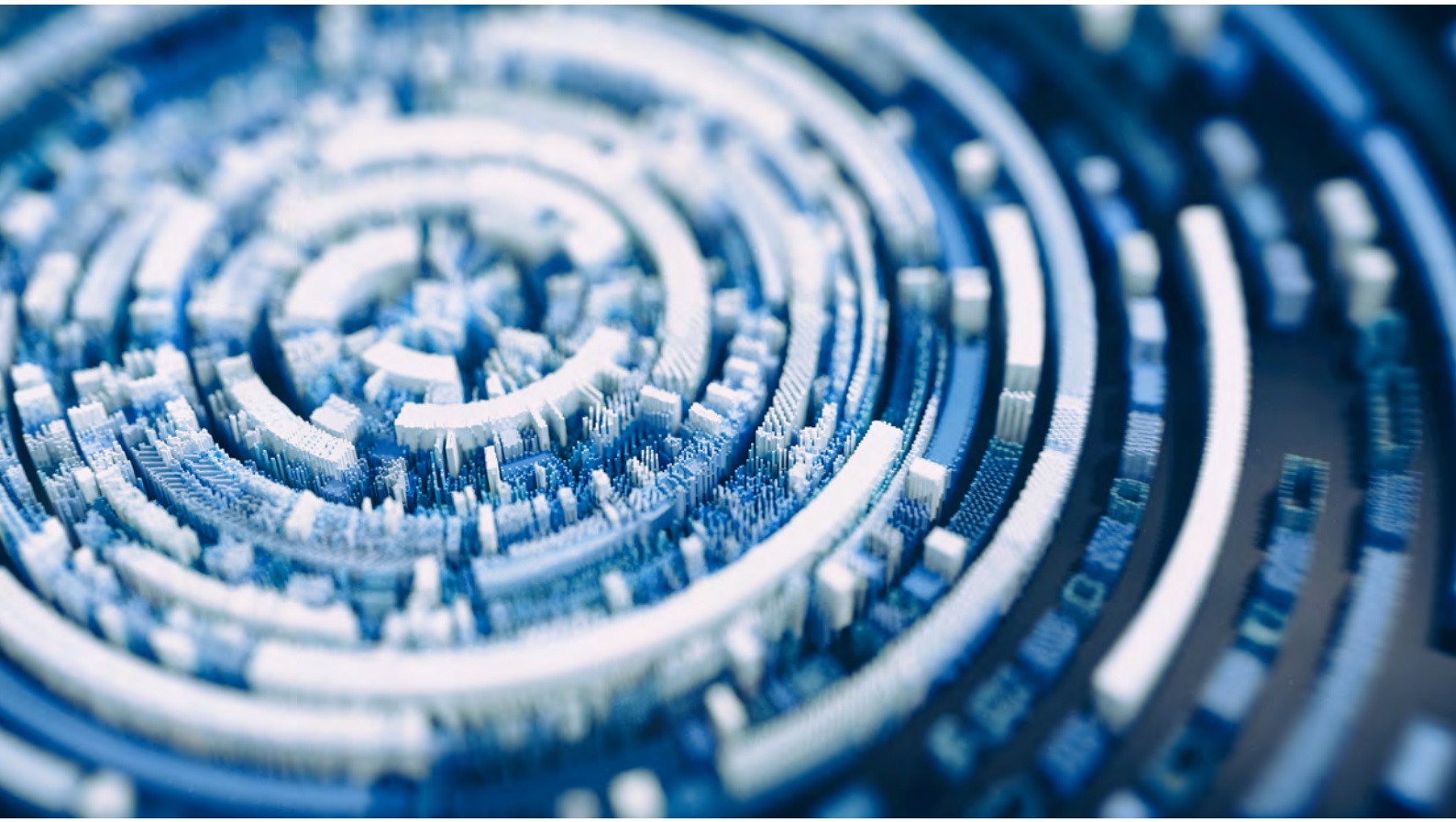
Con la implementación sin necesidad de intervención, sus puntos de acceso y switches SonicWall estarán instalados y funcionando en cuestión de minutos. Además puede registrarlos e incorporarlos desde cualquier parte, con la app móvil SonicExpress.

Herramientas de análisis avanzadas

Realizar un análisis inalámbrico de emplazamientos antes de implementar los puntos de acceso puede mejorar el rendimiento y la productividad. La herramienta WiFi Planner de WNM le ayuda a implementar de forma estratégica los puntos de acceso para optimizar la experiencia Wi-Fi del usuario y evitar costosos errores. WiFi Planner analiza la ubicación, los materiales de construcción, la potencia, la fuerza de la señal, el ancho del canal y las bandas de radio. Eso le permite optimizar la cobertura en redes nuevas o existentes, al utilizar el menor número posible de puntos de acceso. La asignación automática de canal evita las interferencias. La herramienta Topology de WNM proporciona mapas topológicos de la red y estadísticas de los dispositivos gestionados.

Menor TCO

El producto WNM basado en la nube reduce el coste total de propiedad (TCO) al convertir los gastos iniciales (CAPEX) en gastos operativos (OPEX). WNM reduce el coste y el mantenimiento de controladores hardware redundantes y optimiza el espacio en rack del centro de datos. Su interfaz intuitiva reduce la formación y los gastos administrativos.



Para obtener más información sobre la escalabilidad y la fiabilidad definitivas de esta plataforma de gestión basada en la nube, visite:

SonicWall Wireless Network Manager

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 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-WirelessNetworkManager-JK-US-6800