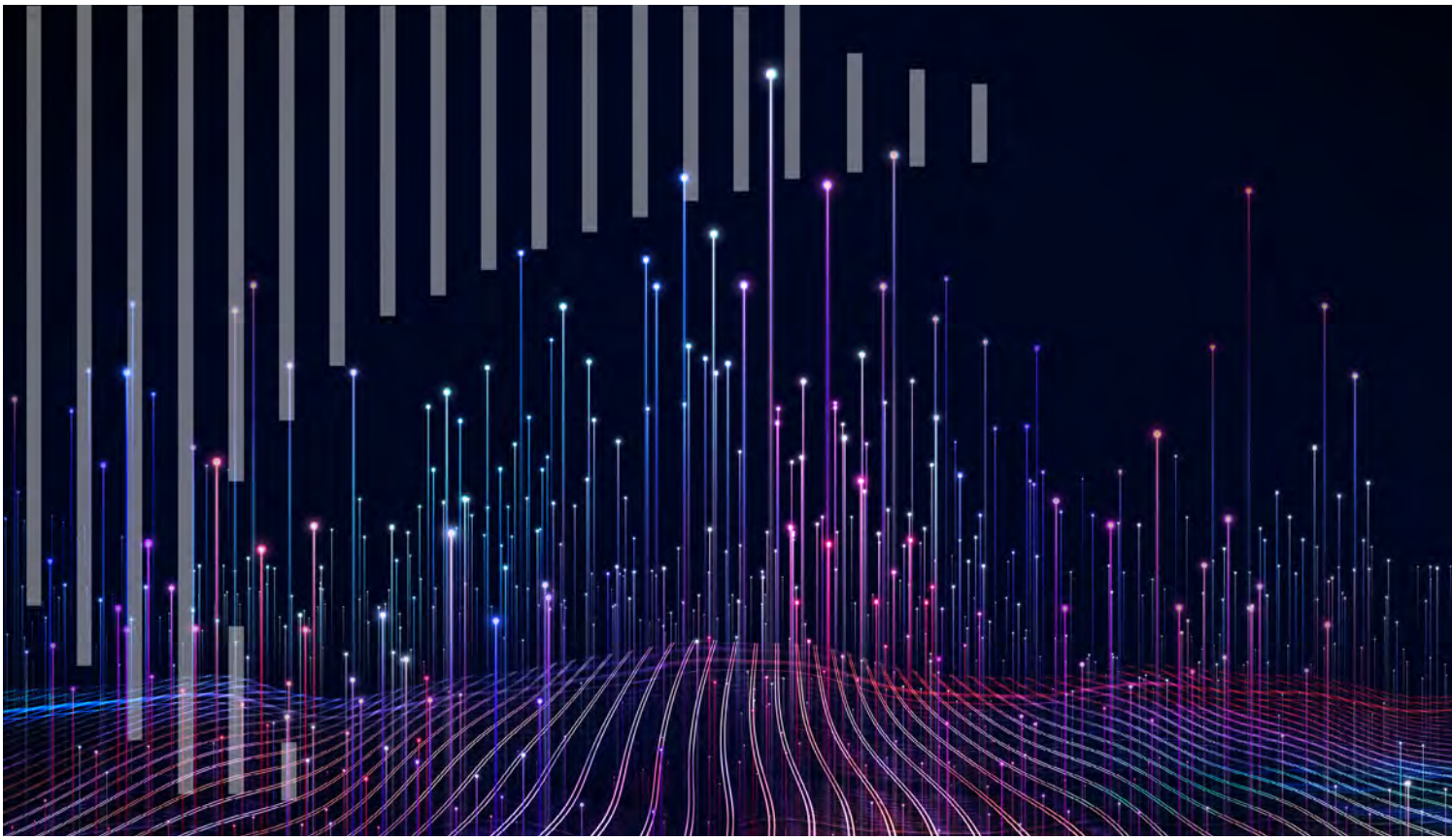
Líneas de productos SonicWall

Junio de 2022



Visión general

Proporcione un nivel profundo de protección para la nube pública/privada, las aplicaciones, los usuarios y los datos de su organización sin comprometer el rendimiento de la red. La plataforma SonicWall Capture Cloud integra estrechamente seguridad, gestión, análisis e inteligencia de amenazas en tiempo real en la cartera de productos de seguridad de red, inalámbrica, de correo electrónico, móvil y de nube de la empresa. Este enfoque permite a empresas medianas, entornos empresariales de gran tamaño, agencias gubernamentales, puntos de venta minoristas, instituciones educativas y sanitarias y proveedores de servicios disfrutar de nuestro completo ecosistema de seguridad, que se beneficia de la potencia, la agilidad y la escalabilidad de la nube.

La estrategia y la visión de futuro de la plataforma Capture Cloud son la innovación continua y el desarrollo de aplicaciones de seguridad como servicio contenedorizadas fácilmente programables y puestas a disposición a demanda. La plataforma está compuesta por los siguientes componentes y prestaciones principales:

- Seguridad de red
- Seguridad por cable
- Seguridad inalámbrica
- Seguridad de endpoints
- Aceleración WAN
- Servicios de seguridad avanzados
- Cloud App Security
- Cloud Edge Secure Access
- Secure Mobile Access
- Email Security
- Gestión, informes y análisis
- Servicios profesionales y soporte

Todos ellos combinados proporcionan una defensa cibernética multicapa de misión crítica, inteligencia de amenazas, análisis y colaboración, así como gestión, informes y análisis comunes que funcionan juntos de forma sincrónica.

Seguridad de red

SonicWall es uno de los proveedores líderes de firewalls de nueva generación (NGFW). El firmware SonicOS o SonicOSX constituyen la base de todos los NGFW de SonicWall. SonicOS utiliza nuestra arquitectura de hardware escalable, así como nuestro motor de Inspección de memoria profunda en tiempo real (RTDMI™) pendiente de patente y nuestros motores patentados* Reassembly-Free Deep Packet Inspection® (Inspección profunda de paquetes sin reensamblado, RFDPI) de paso único y baja latencia, que escanean todo el tráfico independientemente del puerto y el protocolo.

Nuestros NGFW inspeccionan todos los bytes de cada paquete manteniendo el alto nivel de rendimiento y la baja latencia que necesitan las redes concurridas. Además, a diferencia de los productos de la competencia, gracias a su motor RFDPI de paso único, permiten realizar escaneados multiamenazas y de aplicaciones de forma simultánea, así como análisis de archivos de cualquier tamaño, sin reensamblado de paquetes. Gracias a ello, los NGFW de SonicWall pueden escalarse hasta convertirse en sistemas de seguridad de última generación, capaces de responder a las necesidades de las redes empresariales y centros de datos distribuidos en continuo crecimiento.

Los NGFW de SonicWall ofrecen diversas prestaciones robustas, entre las que se encuentran las siguientes:

- Sandboxing multimotor basado en la nube Capture ATP
- SD-WAN
- APIs REST
- Descifrado e inspección de tráfico cifrado
- Servicio de prevención de intrusiones (IPS)
- Protección contra malware
- Inteligencia, control y visualización de aplicaciones en tiempo real
- Filtrado de páginas Web/URL (filtrado de contenido)
- Redes privadas virtuales (VPN) mediante SSL o IPSec
- Seguridad inalámbrica
- Seguridad híbrida y multinube
- Reconexión/recuperación dinámica

Además, los firewalls de SonicWall proporcionan una respuesta rápida y protección continua contra las amenazas de día cero a través del equipo de investigación de amenazas de Capture Labs. Este equipo recopila, analiza y comprueba información multivector sobre amenazas de diversas fuentes de inteligencia de amenazas, incluidos más de un millón de sensores distribuidos por todo el mundo en su red Capture Threat Network.

Serie de la plataforma de servicios SonicWall Network Security (NS*sp*)

La plataforma de NGFW de la serie NS*sp* de SonicWall está diseñada para ofrecer a las redes grandes escalabilidad, fiabilidad y un nivel profundo de seguridad a velocidades multi-gigabit.

ICSA Labs ha puesto a prueba repetidamente los firewalls de SonicWall durante los últimos cinco trimestres y ha descubierto que destacan por su efectividad de la seguridad con una tasa de detección del 100% sin falsos positivos. Los firewalls de SonicWall han marcado la pauta en el control de aplicaciones y la prevención de amenazas de alto rendimiento en varios casos de uso, desde empresas pequeñas hasta grandes centros de datos, operadoras y proveedores de servicios.

Por ejemplo, nuestro firewall multiinstancia de alta gama NS*sp* garantiza un alto nivel de calidad de servicio con la conectividad y la disponibilidad de red ininterrumpidas que requieren hoy en día las empresas, las agencias gubernamentales, los proveedores de servicios y las universidades con infraestructuras de 100/40/10 Gbps. Mediante el uso de innovadoras tecnologías de seguridad de aprendizaje profundo en la plataforma SonicWall Capture Cloud, la serie NS*sp* ofrece protección probada contra las más avanzadas amenazas sin ranlentizar el rendimiento.

Políticas unificadas con SonicOSX 7

La prestación de políticas unificadas de SonicOSX 7 ofrece gestión integrada de las políticas de acceso y seguridad en determinados firewalls de alta gama NS*sp* y virtuales Ns*v* de SonicWall.

Viene con una nueva interfaz Web diseñada con un enfoque radicalmente diferente. El énfasis recae sobre su diseño, que da prioridad al usuario. Gracias a ello, se pueden establecer políticas de seguridad contextuales de forma más intuitiva utilizando alertas accionables y funciones sencillas de señalar y hacer clic.

Además, visualmente es más atractiva que la interfaz clásica. En una visión centralizada de un firewall, la interfaz presenta al usuario información sobre la efectividad de varias normas de seguridad. El usuario puede modificar fácilmente las normas predefinidas de antivirus en pasarela, anti-spyware, filtrado de contenido, prevención de intrusiones, filtrado Geo-IP e inspección profunda de paquetes del tráfico cifrado.

Con esta nueva interfaz de políticas unificadas, SonicWall proporciona una experiencia optimizada para controlar con mayor rapidez los cambios dinámicos en el tráfico y mejorar la seguridad en general.

*Patentes en EE UU 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Serie SonicWall Network Security appliance (NS*a*)

La serie SonicWall Network Security appliance (NS*a*) es uno de los NGFW más seguros y de más alto rendimiento disponibles en su categoría. Proporciona seguridad de clase empresarial sin comprometer el rendimiento y utiliza la misma arquitectura que nuestra línea estrella de NGFW NS*sp*, desarrollada para las redes empresariales más exigentes del mundo.

Tras años de investigación y desarrollo, la serie NS*a* ha sido diseñada desde cero para empresas distribuidas, empresas medianas, oficinas pequeñas, campus escolares y agencias gubernamentales. La serie NS*a* combina una arquitectura multinúcleo revolucionaria con tecnología de Inspección de memoria profunda en tiempo real (RTDMI) basada en la nube, un motor patentado de prevención de amenazas con un diseño altamente escalable. Gracias a ello, ofrece una protección, un rendimiento y una escalabilidad líderes en la industria, con una gran cantidad de conexiones simultáneas, baja latencia, sin limitaciones del tamaño de los archivos y un número elevado de conexiones por segundo en comparación con otros proveedores líderes de firewalls.

Serie SonicWall TZ

La serie SonicWall TZ está compuesta por firewalls de Gestión unificada de amenazas (UTM) altamente fiables y seguros, diseñados para empresas pequeñas y medianas (pymes), implementaciones minoristas, organizaciones gubernamentales y empresas distribuidas con emplazamientos remotos y oficinas pequeñas. A diferencia de los productos de consumo, la serie TZ consolida funciones altamente eficaces de prevención de intrusiones, antimalware, filtrado de contenido/URL y control de aplicaciones a través de redes por cable e inalámbricas, y ofrece soporte para las más diversas plataformas móviles de portátiles, teléfonos inteligentes y tablets. Al proporcionar inspección profunda de paquetes (DPI) completa a niveles de rendimiento muy elevados, elimina los cuellos de botella provocados por otros productos y contribuye a aumentar la productividad de las organizaciones.

Al igual que ocurre con todos los firewalls de SonicWall, la serie TZ inspecciona todo el archivo, incluidos aquellos cifrados mediante TLS/SSL, a fin de ofrecer una protección completa. Asimismo, la serie TZ ofrece funciones de inteligencia y control de aplicaciones, análisis e informes avanzados del tráfico de aplicaciones, Seguridad de protocolo de Internet (IPSec), SSL-VPN, reconexión ISP múltiple, equilibrio de carga y SD-WAN. Las funciones opcionales integradas de alimentación por Ethernet (PoE) y conectividad inalámbrica 802.11ac de alta velocidad permiten a las organizaciones ampliar los límites de sus redes de forma fácil y segura. En combinación con los switches de SonicWall, los firewalls de la serie TZ ofrecen una fácil Implementación sin necesidad de intervención y sin añadir complejidad, proporcionando la flexibilidad necesaria para hacer crecer el negocio de forma segura.

La serie TZ de última generación es el primer firewall en factor de forma de escritorio que ofrece interfaces multi-gigabit (2,5/5/10G) o gigabit, SD-WAN segura, almacenamiento ampliable integrado y soporte para TLS 1.3 y 5G con un rendimiento sin precedentes. Las fuentes de alimentación redundantes y el soporte para 802.11ac Wave 2 mejoran aún más las prestaciones de estos dispositivos. Diseñados para organizaciones medianas y empresas grandes distribuidas con ubicaciones SD-Branch, los firewalls de la serie TZ de nueva generación proporcionan efectividad de la seguridad validada por la industria con la mejor relación precio/rendimiento de su categoría.

Serie SonicWall Network Security virtual (NS*v*)

Los firewalls SonicWall Network Security virtual (NS*v*) amplían la detección y la prevención automatizadas de brechas a entornos híbridos y multinube con versiones virtualizadas de los firewalls de nueva generación de SonicWall. Gracias a sus herramientas y servicios de seguridad equipados con todas las prestaciones y equivalentes a un firewall SonicWall, NS*v* defiende de forma efectiva sus entornos virtuales y de nube contra los ataques de uso indebido de los recursos, ataques entre equipos virtuales, ataques de canal lateral y todos los exploits y las amenazas comunes basados en la red.

NS*v* puede implementarse y ponerse a disposición fácilmente en un entorno virtual multiempresa, normalmente entre redes virtuales. Establece medidas de control del acceso para preservar la seguridad de los datos y de los equipos virtuales, al tiempo que captura el tráfico virtual entre los equipos virtuales y las redes para ofrecer prevención de brechas automatizada.

Con soporte de infraestructura para implementación de alta disponibilidad, NS*v* cumple los requisitos de escalabilidad y disponibilidad del Centro de datos definidos por software (SDDC). Estos firewalls pueden implementarse fácilmente como dispositivos virtuales en plataformas de nube privada, como VMWare ESXi, Linux KVM, Nutanix o Microsoft Hyper-V, o en entornos de nube pública de AWS o Microsoft Azure. Benefíciese de los modelos de licencias flexibles BYOL y PAYG con NS*v* y proporcione a las organizaciones todas las ventajas de seguridad de un firewall físico, más las ventajas operativas y económicas de la virtualización.

Ciertos modelos de firewall NS*v* incluyen SonicOSX con Políticas unificadas, ofreciendo así una experiencia optimizada para controlar con mayor rapidez los cambios dinámicos del tráfico, y proporcionar una mejor seguridad en general.

Obtenga más información sobre los productos de firewall de SonicWall en: www.sonicwall.com/products/firewalls/

Capture Security appliance 1000 (CSa 1000)

Para cumplir la normativa y los estándares de privacidad, necesita una plataforma de análisis de amenazas que se adapte a su presupuesto y que no pueda ser detectada y evadida por el código malicioso. SonicWall Capture Security appliance (CS*a*) es una solución local de análisis de archivos y detección de malware que incluye la tecnología de Inspección de memoria profunda en tiempo real (RTDMI) de SonicWall. La RTDMI permite a CS*a* detectar más malware de forma más rápida y efectiva. Su baja tasa de falsos positivos mejora la seguridad y la experiencia del usuario final.

Con CS*a,* puede analizar malware oculto en una amplia variedad de tipos de archivos, tamaños de archivos y entornos operativos, para disfrutar de funciones completas de detección de amenazas de día cero. Detecta y detiene ataques de canal lateral mediante la inspección basada en la memoria en tiempo real. Al forzar al malware a revelar sus armas en la memoria, CS*a* bloquea de forma proactiva las amenazas del mercado de masas, de día cero y desconocidas. CS*a* soporta las redes cerradas y puede utilizarse con los últimos firewalls de nueva generación de SonicWall.

La implementación de SonicWall CS*a* es rápida y sencilla. Su puesta en funcionamiento solo requiere la configuración básica de las redes, los informes y el acceso de los dispositivos autorizados. CS*a* está diseñada para que se le pueda asignar una dirección IP y por tanto es posible implementarla en cualquier lugar, siempre que pueda ser localizada por los dispositivos que envían archivos para su análisis. CS*a* también puede implementarse en redes cerradas o aisladas.

Seguridad por cable

Los switches de SonicWall ofrecen switching de red de alta velocidad con un rendimiento y una gestionabilidad sin precedentes. Ofrecen alta densidad de puertos, alimentación por Ethernet (PoE) opcional y rendimiento de 1 ó 10 gigabits. Ideales para pymes y redes de oficinas pequeñas definidas por software (SD-Branch), permiten a empresas de cualquier tamaño someterse a la transformación digital y seguir el ritmo del cambiante panorama de las redes y la seguridad.

Los switches de SonicWall pueden gestionarse mediante los firewalls de SonicWall o SonicWall Wireless Network Manager (WNM). WNM integra de forma fluida la seguridad por cable e inalámbrica de extremo a extremo para ofrecer un sistema de seguridad unificado. Esto simplifica la implementación, la gestión y la resolución de problemas, a la vez que elimina las brechas que pueden aparecer con switches de terceros. Los switches de SonicWall pueden implementarse rápidamente en oficinas pequeñas distribuidas utilizando la Implementación sin necesidad de intervención.

Seguridad inalámbrica

La innovadora solución de seguridad de red inalámbrica de SonicWall hace que las redes inalámbricas sean seguras, sencillas y asequibles. Los puntos de acceso inalámbricos de alto rendimiento de la serie SonicWave 802.11ax pueden gestionarse fácilmente con Wireless Network Manager.

Además de los puntos de acceso inalámbricos de alta velocidad y del dashboard gestionado en la nube, la solución de seguridad inalámbrica de SonicWall incluye Wi-Fi Planner, una herramienta avanzada de análisis del emplazamiento para ayudar a los administradores a planificar e implementar las redes WiFi de forma efectiva. La solución también ofrece la aplicación móvil SonicExpress para la fácil incorporación y monitorización de puntos de acceso a fin de proporcionar a los administradores información en tiempo real sobre el estado y la seguridad de la red.

SonicWall ofrece más que una mera solución de seguridad inalámbrica. Nuestra solución protege las redes

inalámbricas con las tecnologías RTDMI y RFDPI y proporciona prestaciones de seguridad avanzadas, como sandboxing multimotor, filtrado de contenido y antivirus en la nube directamente en el punto de acceso, sin necesidad de un firewall. Mejore aún más la seguridad y el rendimiento de su red con prestaciones como la prevención de intrusiones, el descifrado y la inspección TLS/SSL y el control de aplicaciones, y disfrute de un rendimiento y una protección de nivel empresarial.

Los puntos de acceso SonicWave soportan la itinerancia rápida para que los usuarios puedan itinerar de una ubicación a otra de forma fluida. La solución ofrece gran cantidad de prestaciones, entre las que se incluyen un portal cautivo, la selección automática de canal, análisis de espectros, air-time fairness, band steering y herramientas de análisis de la señal para la monitorización y la resolución de problemas.

Con esta solución, SonicWall reduce el coste total de propiedad (TCO), ya que las empresas ya no tienen que implementar ni gestionar soluciones inalámbricas caras que funcionen como sistemas adicionales a la red por cable existente.

Seguridad de endpoints

En el clima empresarial de hoy en día, la gestión y la seguridad de los endpoints son críticas. Dado que los usuarios entran y salen de la red con sus dispositivos, y que las amenazas cifradas acceden a los endpoints de forma desapercibida, es necesario hacer algo para proteger estos dispositivos. Con el crecimiento del ransomware y de las vulnerabilidades de las aplicaciones, los endpoints son el campo de batalla del panorama actual de las amenazas.

Asimismo, los administradores tienen problemas de visibilidad de sus endpoints y a la hora de gestionar su sistema de seguridad. Además, se enfrentan al reto de tener que garantizar una seguridad coherente del cliente, y al mismo tiempo proporcionar funciones de inteligencia e informes fáciles de usar y accionables.

Si bien los productos de seguridad de endpoints llevan años en el mercado, los administradores se enfrentan a los siguientes retos:

- Mantener los productos de seguridad al día
- Reforzar las políticas a escala global
- Obtener informes y ver el estado de los tenants
- Las amenazas ocultas que llegan a través de, y crean, canales cifrados
- Entender las alertas y los pasos de resolución
- Catalogar las aplicaciones y sus vulnerabilidades
- Detener las amenazas como el ransomware
- Ataques sin archivos y dispositivos USB infectados que burlan las defensas del perímetro

SonicWall Capture Client es una plataforma de cliente unificada que proporciona múltiples prestaciones de protección de endpoints. Esta solución incluye una consola de gestión basada en la nube y una integración completa opcional con los firewalls de nueva generación de SonicWall para ofrecer a los clientes de SonicWall una experiencia de seguridad unificada. En combinación con las prestaciones de refuerzo, SonicWall Capture Client puede asegurar que los endpoints estén ejecutando software de seguridad y/o utilizando un certificado SSL embebido para la inspección del tráfico cifrado. Además, para simplificar la inspección del tráfico SSL (DPI-SSL) y mejorar la experiencia del usuario final, Capture Client permite a los administradores transferir los certificados SSL a los endpoints mucho más fácilmente que antes.

Asimismo, Capture Client ofrece un motor antivirus avanzado diseñado para detener el malware más ingenioso con una opción de reversión que permite regresar al estado previo a la infección. Por otra parte, Capture Client Advanced se integra con SonicWall Capture Advanced Threat Protection (ATP) para examinar archivos sospechosos con el fin de detener mejor los ataques antes de que se activen.

Ahora, los administradores pueden catalogar todas las aplicaciones en cada endpoint protegido por Capture Client con informes sobre las vulnerabilidades conocidas del ecosistema.

El Dashboard global está diseñado para permitir a los MSSPs ver el número de infecciones, las vulnerabilidades presentes y la versión de Capture Client instalada por cada tenant.

Pueden ver qué contenidos y que usuarios están siendo bloqueados más frecuentemente por el Filtrado de contenido y qué dispositivos están conectados y operativos. La Política global permite a los administradores aplicar una única política básica a todos los tenants. Esto hace que sea más sencillo poner en marcha nuevos tenants y crear protecciones rápidamente para nuevas amenazas en todos los tenants bajo esta política.

Las prestaciones de SonicWall Capture Client incluyen:

- Refuerzo de la seguridad
- Gestión de certificados DPI-SSL
- Monitorización continua del comportamiento
- Determinaciones altamente precisas gracias al aprendizaje automático
- Múltiples técnicas multicapa basadas en la heurística
- Inteligencia de vulnerabilidades de aplicaciones
- Prestaciones únicas de reversión
- Integración del sandbox de red Capture Advanced Threat Protection
- Dashboard global y Política global con herencia
- Búsqueda de archivos sospechosos mediante un solo clic con ayuda de la base de datos de inteligencia de Capture ATP de amenazas peligrosas y supuestas
- Filtrado de contenido para reforzar las políticas Web y bloquear las direcciones IP, las URLs y los dominios maliciosos en dispositivos que no se encuentran en la red
- Control de dispositivos basado en políticas para bloquear dispositivos de almacenamiento potencialmente infectados

Servicios de seguridad avanzados

Los servicios de firewall de seguridad de red de SonicWall ofrecen una protección avanzada y altamente efectiva para organizaciones de todos los tamaños con el fin de ayudarlas a defenderse contra las amenazas de seguridad, aumentar el control sobre la seguridad, mejorar la productividad y reducir los costes.

SonicWall ofrece tres paquetes de suscripción en los firewalls de las series de 7ª generación: Threat Protection Services Suite, Essential Protection Services Suite y Advanced Protection Services Suite. Threat Protection Services Suite ofrece un paquete económico que incluye los servicios de seguridad básicos necesarios para asegurar que la red esté protegida contra las amenazas. Se puede añadir el paquete SonicWall Essential, que brinda los servicios de seguridad básicos necesarios para ofrecer protección contra las amenazas conocidas y desconocidas, u optar por el nivel Advanced, que proporciona seguridad avanzada para ampliar la seguridad de su red con servicios añadidos de seguridad esenciales basados en la nube.

Threat Protection Services Suite, disponible solo en las series TZ270/370/470, incluye Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Inspección profunda de paquetes del tráfico cifrado mediante TLS/SSLc (DPI-SSL) y soporte 24x7.

Essential Protection Services Suite incluye Capture Advanced Threat Protection con tecnología RTDMI, Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Comprehensive Anti-Spam Service, Inspección profunda de paquetes del

tráfico cifrado mediante TLS/SSL (DPI-SSL) y soporte 24x7.

Advanced Protection Services Suite incluye Capture Advanced Threat Protection con tecnología RTDMI, Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Comprehensive Anti-Spam Service, Inspección profunda de paquetes del tráfico cifrado mediante TLS/SSL (DPI-SSL), soporte 24x7, gestión en la nube, informes basados en la nube para 7 días y soporte Premier opcional.

Inspeccione la memoria profunda

La tecnología pendiente de patente del motor de Inspección de memoria profunda en tiempo real de SonicWall (RTDMI) detecta y bloquea de forma proactiva el malware desconocido del mercado de masas mediante la Inspección de memoria profunda en tiempo real. Ahora disponible con el servicio de sandbox en la nube SonicWall Capture Advanced Threat Protection (ATP), el motor identifica y mitiga incluso las amenazas más modernas y dañinas, incluidos los futuros exploits Meltdown.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Cloud App Security

La solución SonicWall Cloud App Security protege aplicaciones SaaS de correo electrónico, colaboración y productividad populares, como Office 365 email, SharePoint, OneDrive, G-Suite, Dropbox y Box.
Su protección incluye:

- Compromiso del correo electrónico de negocio (BEC)
- Prevención de pérdida de datos (DPL)
- Hackeo de cuentas (ATO)
- Malware avanzado y amenazas de día cero en archivos adjuntos y almacenados maliciosos
- Phishing específico
- Intentos de fraude

Cloud App Security utiliza funciones avanzadas de creación de perfiles y análisis de comportamiento con más de 300 indicadores de amenazas para determinar si hay cuentas legítimas que están siendo explotadas por cibercriminales. Gracias a sus prestaciones de aprendizaje automático e inteligencia artificial, incluido el escaneo retroactivo de actividades, la solución bloquea los ataques de suplantación.

Para las aplicaciones SaaS y de compartición de archivos, como OneDrive, Cloud App Security aplica el sandbox multimotor de SonicWall Capture ATP a fin de detectar malware nunca antes visto. Realiza escaneos tanto históricos como en tiempo real de los archivos y los datos, ya estén en reposo o atravesando un entorno SaaS, internamente o de nube a nube. Además, la prestación de DPL de la solución protege los datos en reposo limitando el acceso a las aplicaciones autorizadas y previniendo las cargas de datos no autorizadas.

Como servicio SaaS, Cloud App Security puede activarse y estar operativo en cuestión de minutos.

Con escalabilidad ilimitada, la solución ayuda a organizaciones de cualquier tamaño a añadir protección inmediatamente para sus usuarios de aplicaciones SaaS, ya sean unos cientos o miles de ellos distribuidos por todo el mundo. Cada aplicación SaaS tiene un motor de políticas separado, cada uno de ellos con sus propias normas y funciones de refuerzo. De este modo, puede asignar una política específica para cada aplicación SaaS en base a sus requisitos de seguridad para cada una de ellas.

Sin necesidad de instalar ni gestionar hardware ni software, Cloud App Security elimina los gastos de capital, la instalación compleja y los costes continuos de mantenimiento relacionados con la implementación de una solución local alternativa.

Obtenga más información sobre SonicWall Cloud App Security en www.sonicwall.com/cloud-security

Cloud Edge Secure Access

La evolución de la VPN tradicional a la seguridad de confianza cero

Los empleados de hoy en día quieren flexibilidad para trabajar desde cualquier lugar — y las organizaciones quieren beneficiarse del ahorro de costes y de las eficiencias operativas que ofrece la nube.

Sin embargo, las soluciones VPN tradicionales no están diseñadas para esta nueva realidad. Su implementación puede llevar días, o incluso semanas. Los problemas de disponibilidad de suministro implican que pueden estar disponibles o no, y que una vez que tiene una instalada, puede resultar difícil programar periodos de inactividad.

Y lo que es peor, pueden ofrecer una puerta trasera a su red, ya que cualquier inicio de sesión con éxito brinda un amplio acceso a la red y permite el movimiento lateral dentro de la subred.

Además, puesto que el tráfico de usuarios pasa por el concentrador VPN local en lugar de ir directamente a la nube, la VPN genera una latencia que disminuye la eficiencia y degrada la experiencia en la nube del usuario.

Gartner predice que en 2023, el 60% de las empresas eliminará la mayoría de sus redes privadas virtuales de acceso remoto (VPNs) en favor del Acceso de red de confianza cero (ZTNA).

Seguridad de red de confianza cero para proteger los recursos valiosos

Con Cloud Edge Secure Access, SonicWall ofrece una solución ZTNA que resuelve estos problemas y además ofrece muchas ventajas más. SonicWall Cloud Edge Secure Access se basa en tres prestaciones esenciales:

- Acceso de mínimo privilegio para proteger los recursos corporativos
- Implementación rápida de autoservicio
- Acceso fiable directo a la nube desde cualquier lugar

Como servicio nativo de nube, proporciona una Red como servicio (NaaS) sencilla para una conectividad entre emplazamientos y de nube híbrida con seguridad de confianza cero y de mínimo privilegio.

- La comprobación del estado de seguridad de los dispositivos (DPC) brinda acceso a la red únicamente a los dispositivos autenticados y que cumplen las normas
- Las políticas de microsegmentación definidas por software previenen de forma efectiva la propagación de filtraciones
- El Control del tráfico de red (NTC) es un firewall como servicio (FwaaS) dinámico que proporciona protección basada en políticas definiendo quién puede acceder a qué recurso y desde dónde

Ahora, las organizaciones pueden empoderar a los teletrabajadores y al mismo tiempo proteger los recursos de negocio valiosos.

Servicio nativo de nube a nivel mundial que se implementa en cuestión de minutos

Más de 30 puntos de presencia (PoPs) en todo el mundo soportan SonicWall Cloud Edge.

El servicio global permite a los administradores de TI conectar una oficina pequeña e implementar el servicio en 15 minutos. Además, los usuarios finales pueden instalar el cliente de SonicWall Cloud Edge y ser productivos en 5 minutos.

La infraestructura está basada en la arquitectura de Perímetro definido por software (SPD). Esta separa el controlador centralizado de las pasarelas, que por su parte actúan como intermediarios de confianza.

Al distribuir las pasarelas de SDP, Cloud Edge Secure Access puede escalarse rápidamente, mantener un alto nivel de rendimiento y proporcionar la mejor experiencia en la nube posible.

Además, la separación de funciones también hace que Cloud Edge Secure Access sea resistente a ciberamenazas comunes, como DDoS, exploits de Log4j, secuestro de Wi-Fi pública, SYN flood y Slowloris.

Ventajas adicionales:

- Solución de seguridad para empresas distribuidas y teletrabajadores
- Acceso instantáneo seguro a sitios físicos y recursos en nubes híbridas
- Escalable desde 10 hasta miles de usuarios
- Soporta acceso Web sin clientes con cualquier dispositivo público
- Cifrado WireGuard de alto rendimiento
- Proveedor de identidades en la nube e integraciones SIEM
- SSO moderno e integración con MFA
- Integración con SIEM
- Tecnología multiempresa para MSSPs
- El Control del tráfico de red (NTC) permite ofrecer una protección a nivel de firewall definiendo quién puede acceder a servicios de red específicos y desde dónde
- La comprobación del estado de seguridad de los dispositivos (DPC) concede acceso a la red únicamente a los dispositivos autenticados y que cumplen las normas.
- Disponible en EE. UU., Europa, Oriente Medio y Asia

Obtenga más información sobre SonicWall Cloud Edge Secure Access en www.sonicwall.com/products/cloud-edge-secure-access

Secure Mobile Access

La serie SonicWall Secure Mobile Access (SMA) es una pasarela de acceso seguro unificado para organizaciones que se enfrentan a retos en materia de movilidad, trabajo desde casa, BYOD y migración a la nube. Se trata de una solución que permite a las organizaciones proporcionar acceso en cualquier momento, desde cualquier lugar y utilizando cualquier dispositivo, a los recursos corporativos de misión crítica. El motor de políticas de control granular del acceso, la autorización de dispositivos con sensibilidad contextual, la VPN a nivel de aplicación y la autenticación avanzada con inicio de sesión único de SMA permiten a las organizaciones adoptar enfoques BYOD y de movilidad en un entorno de TI híbrido.

Además, SMA reduce la superficie de ataque para las amenazas al proporcionar prestaciones como Geo IP, detección de botnets, Web Application Firewall e integración con sandbox Capture ATP.

Movilidad y BYOD

Para las organizaciones que desean adoptar políticas BYOD o modelos de trabajo flexible o de desarrollo externo, SMA se convierte en el principal punto de refuerzo para todos ellos. SMA proporciona la mejor seguridad de su categoría para minimizar la superficie de ataque de las amenazas y aumenta la seguridad de las organizaciones al soportar los últimos algoritmos de cifrado. SonicWall SMA permite a los administradores proporcionar acceso móvil seguro y privilegios basados en roles para que los usuarios finales puedan acceder de forma rápida y sencilla a las aplicaciones, los datos y los recursos de negocio que necesiten. Al mismo tiempo, las organizaciones pueden establecer políticas BYOD seguras para proteger sus redes y sus datos corporativos contra el acceso no autorizado y los ataques de malware.

El traslado a la nube

Para aquellas organizaciones que emprenden el viaje a la nube, SMA ofrece una infraestructura de inicio de sesión único (SSO) que utiliza un único portal Web para autenticar a los usuarios en un entorno de TI híbrido. Tanto si el recurso corporativo está en una ubicación local, como en la Web o en una nube hospedada, la experiencia de acceso es coherente y fluida. Los usuarios no necesitan recordar las URLs de cada una de las aplicaciones ni mantener marcadores exhaustivos. Con Workplace, un portal de acceso centralizado, los usuarios pueden acceder a todas las aplicaciones críticas de negocio con una sola URL desde un navegador Web estándar. SMA proporciona un inicio de sesión único combinado tanto para las aplicaciones SaaS hospedadas en la nube que utilizan SAML 2.0 como para las aplicaciones hospedadas en campus que utilizan RADIUS o Kerberos. SMA se integra con múltiples servidores de autenticación, autorización y contabilidad, así como con tecnologías de autenticación multifactor (MFA) líderes para ofrecer un mayor nivel de seguridad. Solo se proporciona inicio de sesión único seguro a los endpoints autorizados después de que se haya comprobado el estado y la conformidad con las normas.

Proveedores de servicios gestionados

Tanto para organizaciones con centros de datos como para proveedores de servicios gestionados, SMA proporciona una solución de llave en mano para garantizar un alto nivel de continuidad de negocio y escalabilidad. SonicWall SMA puede soportar hasta 20.000 conexiones simultáneas en un solo dispositivo, y ofrece escalabilidad para soportar a un millón de usuarios a través de la agrupación inteligente (clústeres). Reduzca los costes de los centros de datos gracias a la agrupación (clústeres) activa-activa de alta disponibilidad y a un equilibrador de carga dinámico integrado que reasigna el tráfico global al centro de datos más optimizado en tiempo real en base a la demanda de los usuarios. SMA proporciona al propietario del servicio una serie de herramientas que le permiten ofrecer un servicio sin interrupciones, así como la capacidad de cumplir SLAs muy agresivos.

Dispositivos SMA

SonicWall SMA puede implementarse como dispositivo reforzado de alto rendimiento o como dispositivo virtual utilizando recursos informáticos compartidos para optimizar el uso, facilitar la migración y reducir los costes de capital. Los dispositivos de hardware se basan en una arquitectura multinúcleo de alto rendimiento con aceleración SSL, rendimiento VPN y proxies potentes para ofrecer un acceso seguro y eficaz. Para las organizaciones reguladas y gubernamentales, SMA está disponible con certificación FIPS 140-2 de nivel 2. Los dispositivos virtuales SMA ofrecen las mismas prestaciones de acceso seguro y eficaz en las principales plataformas virtuales y en la nube, como Hyper-V, VMWare ESX/ ESXi, KVM, AWS y Azure. Tanto si opta por implementar dispositivos físicos como virtuales, o una combinación de ambos, SMA encaja a la perfección en su infraestructura de TI existente.

SMA Web Application Firewall

El Web Application Firewall (WAF) de la serie SonicWall SMA100 permite implementar una estrategia de defensa en profundidad aumentando la seguridad del perímetro para proteger sus aplicaciones Web ejecutadas en entornos de nube privada, pública o híbrida. El WAF de la serie SMA100 ofrece protección de aplicaciones Web y protección contra fugas de información al tiempo que acelera las prestaciones de entrega de aplicaciones Web que permiten el equilibrio de carga con inteligencia de aplicaciones, la descarga SSL para proporcionar resiliencia y mejorar la interacción y la experiencia digitales.

Las ventajas adicionales también incluyen:

- Protección contra las vulnerabilidades conocidas y de día cero con parches virtuales y normas personalizadas
- Defensa contra las últimas vulnerabilidades y amenazas mencionadas por el OWASP, incluidas la inyección SQL y el cross-site scripting (XSS)
- Soporta el acceso de confianza cero sin clientes a través de un navegador Web para que pueda utilizarse cómodamente con cualquier dispositivo público
- Estrictos requisitos de gestión de sesiones y de autenticación, como OTP, 2FA y SSO
- Protección de servidores de alta disponibilidad contra ataques DoS/DDoS que acechan a las aplicaciones

Gestión e informes

SonicWall proporciona una plataforma de gestión intuitiva basada en Web para optimizar la gestión de los dispositivos, así como amplias funciones de informes. La GUI fácil de usar permite gestionar múltiples equipos de forma clara y sencilla. La gestión unificada de políticas le ayuda a crear y monitorizar políticas de acceso y configuraciones. Una única configuración de políticas puede gestionar sus usuarios, dispositivos, aplicaciones, datos y redes. Automatice las tareas rutinarias y planifique actividades, liberando a los equipos de seguridad de las tareas repetitivas para que puedan centrarse en las tareas de seguridad estratégicas, como en la respuesta a posibles incidentes.

Permita al departamento de TI proporcionar la mejor experiencia y el acceso más seguro en función del escenario de los usuarios. Elija entre diversas posibilidades que abarcan desde un acceso seguro basado en Web sin clientes para proveedores y contratistas externos a un acceso más tradicional mediante túnel VPN y basado en cliente para ejecutivos. Tanto si necesita proporcionar acceso seguro fiable a 5 usuarios desde un único centro de datos, como si debe escalar su solución para miles de usuarios en centros de datos distribuidos por todo el mundo, SonicWall SMA tiene una solución para usted.

Obtenga más información sobre los productos de seguridad móvil de SonicWall en: www.sonicwall.com/products/remote-access/

Email Security

Si bien es cierto que el correo electrónico es una herramienta de comunicación imprescindible en las empresas, también es el vector número 1 para amenazas como el ransomware, el phishing, el compromiso del correo electrónico de negocio (BEC), el spoofing, el spam y los virus. Además, hoy en día la legislación hace responsable a las empresas de la protección de la información confidencial, de prevenir su filtración y de que los mensajes de correo electrónico que contengan datos sensibles de clientes o información confidencial se intercambien de forma segura. Tanto si su organización es una pyme en crecimiento, como una empresa grande distribuida o un proveedor de servicios gestionados (MSP), lo que usted necesita es una solución económica de seguridad y cifrado del correo electrónico que ofrezca suficiente escalabilidad para aumentar fácilmente la capacidad a través de unidades y dominios organizativos, y para delegar en ellos las tareas de gestión.

Además, para gestionar los costes y los recursos, las organizaciones están adoptando Microsoft Office 365 y Google G Suite. Mientras que estos productos ofrecen funciones de

seguridad integradas, para combatir las amenazas de correo electrónico avanzadas, las organizaciones necesitan una solución de seguridad de correo electrónico de nueva generación que se integre de forma fluida con Office 365 y G Suite a fin de protegerlas contra las amenazas avanzadas de hoy en día.

Dispositivos Email Security de SonicWall

Fácil de instalar y administrar, SonicWall Email Security está diseñado para escalarse de forma económica de 10 a 100.000 buzones. Puede implementarse como dispositivo de hardware, como dispositivo virtual utilizando recursos informáticos compartidos, o como software — incluido software optimizado para Microsoft Windows Server o Small Business Server. Los dispositivos físicos SonicWall Email Security son ideales para organizaciones que necesitan una solución local dedicada. Nuestra solución multicapa ofrece protección completa entrante y saliente. Está disponible en diversas opciones de dispositivos de hardware que se escalan hasta 10.000 usuarios por dispositivo. SonicWall Email Security también está disponible como dispositivo virtual o como aplicación de software. Esto es ideal para organizaciones que requieren la flexibilidad y la agilidad que ofrece la virtualización. La solución puede configurarse en modo distribuido de alta disponibilidad para gestionar sus implementaciones de gran tamaño de forma centralizada y fiable.

La solución de seguridad del correo electrónico de SonicWall utiliza tecnologías como el aprendizaje automático, la heurística, el análisis de la reputación y del contenido, protección de URL "time-of-click" y el sandboxing para archivos adjuntos y URLs a fin de proporcionar protección completa tanto entrante como saliente.

Asimismo, la solución incluye potentes estándares de autenticación de correo electrónico para detener los ataques spoofing y el fraude de correo electrónico. Estos incluyen el Marco de directivas de remitente (SPF), el Correo identificado por claves de dominio (DKIM) y la Autenticación de mensajes, informes y conformidad basada en dominios (DMARC)

- Detenga las amenazas maliciosas antes de que lleguen a su bandeja de entrada
- Proteja contra el fraude de correo electrónico y los ataques de phishing específicos
- Disfrute de seguridad actualizada con nuestra inteligencia de amenazas en tiempo real
- Garantice la seguridad de su servicio de correo electrónico en la nube (Office 365, G Suite)
- Permita la prevención de la pérdida de datos de correo electrónico y el cumplimiento normativo
- Gestión e informes sencillos
- Opciones de implementación flexibles

La administración de Email Security es intuitiva, rápida y sencilla. Con Email Security, además, puede delegar la gestión del spam en los usuarios finales sin perder el control sobre la seguridad. Por otra parte, puede gestionar fácilmente las cuentas de usuarios y grupos gracias a las sencillas funciones de sincronización multi-LDAP.

La solución también proporciona integración sencilla para Office 365 y G Suite a fin de ofrecer protección contra las amenazas de correo electrónico avanzadas.

En entornos distribuidos de gran envergadura, el soporte multiempresa permite delegar la gestión de configuraciones en subadministradores de otras unidades (como divisiones empresariales o clientes MSP) dentro de una única implementación de Email Security.

Servicio SonicWall Hosted Email Security

Confíe en nuestros servicios hospedados de implementación rápida y administración sencilla para proteger su organización contra las amenazas basadas en el correo electrónico, como el ransomware, las amenazas de día cero, el spear phishing y el BEC, cumpliendo al mismo tiempo las normas de correo electrónico y las leyes vigentes. Disfrute del mismo nivel de protección avanzada del correo electrónico con nuestra solución hospedada, que viene con las mismas prestaciones que los dispositivos físicos y virtuales. La solución también ofrece continuidad del correo electrónico para garantizar que los e-mails siempre se entreguen y que la productividad no se vea afectada en caso de caída, ya sea planeada o imprevista, de los servidores de correo electrónico locales o de un proveedor en la nube como Office 365 y G Suite.

SonicWal Hosted Email Security ofrece una protección superior basada en la nube contra amenazas entrantes y salientes por un precio de suscripción asequible, predecible y flexible (mensual o anual). Le permite minimizar el tiempo y los costes de implementación iniciales, así como los gastos corrientes de administración, sin comprometer la seguridad.

SonicWall ofrece a los VARs y MSPs una gran oportunidad para mejorar en términos de competitividad e ingresos y minimizar al mismo tiempo el riesgo, los gastos generales y los costes corrientes. SonicWall Hosted Email Security incluye prestaciones favorables para los MSPs, como la gestión centralizada, robusta y multiempresa de múltiples suscriptores, la integración con Office 365, opciones de compra flexibles y el aprovisionamiento automático.

Obtenga más información sobre los productos SonicWall Email Security en www.sonicwall.com/en-us/products/secure-email.

Gestión, informes y análisis

En SonicWall, creemos que un enfoque de gestión de la seguridad conectado es fundamental para una buena práctica de seguridad preventiva. Además, sienta la base para una estrategia unificada de control de la seguridad, cumplimiento normativo y gestión de riesgos. Con las soluciones de gestión, informes y análisis de SonicWall, las organizaciones disponen de una plataforma integrada, segura y ampliable para establecer una estrategia sólida y uniforme de defensa de seguridad y de respuesta en sus redes por cable, inalámbricas y multinube. Asimismo, la adopción total de esta plataforma común proporciona a las organizaciones una visión profunda de la seguridad que les permite tomar decisiones informadas en materia de seguridad, así como actuar rápidamente para fomentar la colaboración, la comunicación y el conocimiento en el marco de seguridad compartido.

Gestión de la seguridad de red de SonicWall

SonicWall Network Security Manager (NSM) ofrece a su organización 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.

Estas operaciones incluyen la implementación y la gestión de todos los dispositivos de firewall, grupos de dispositivos y tenants, la orquestación y el refuerzo de políticas de configuración y seguridad coherentes en sus entornos SD-Branch y SD-WAN, y la monitorización de todo el sistema desde un dashboard dinámico con informes y análisis detallados. NSM le permite hacer todo esto desde una única consola nativa de nube fácil de usar y accesible desde cualquier ubicación mediante cualquier dispositivo habilitado para navegador.

Para los proveedores de servicios, 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. Como resultado, 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.

SonicWall Analytics

SonicWall Analytics transforma los datos en decisiones y las decisiones en acciones que resuelven los problemas de seguridad y evitan que se repitan.

Se trata de un servicio robusto de monitorización y análisis del tráfico, que proporciona una visión global y detallada de todo lo que hay dentro del entorno de seguridad de red. El motor de análisis basado en inteligencia agrega, normaliza y contextualiza los datos de seguridad, incluido el tráfico de red y las actividades de los usuarios que pasan por el firewall y los puntos de acceso inalámbricos, proporcionando a los administradores una visión directa de la inteligencia de amenazas de sus redes y usuarios casi en tiempo real.

[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.

Armadas con análisis e informes detallados, las organizaciones cuentan con la inteligencia y la capacidad necesarias para encontrar y abordar los problemas de seguridad y operativos de forma más eficiente. Las funciones de desglose permiten a los equipos de seguridad investigar, analizar y tomar medidas basadas en hechos contra las actividades y los comportamientos sospechosos o peligrosos de los usuarios con mayor visibilidad, precisión y velocidad. Asimismo, pueden dedicar su valioso tiempo y sus esfuerzos a orquestar acciones rápidas de respuesta y resolución de los riesgos de seguridad importantes en lugar de reaccionar a todos los eventos.

Además, incorporar Analytics en el proceso de negocio ayuda a operacionalizar los análisis automatizando alertas accionables en tiempo real; a orquestar las políticas y los controles de seguridad de forma proactiva y automatizada; y a monitorizar los resultados para garantizar la seguridad.

SonicWall Wireless Network Manager

SonicWall Wireless Network Manager (WNM) integra la gestión de los puntos de acceso SonicWave y los switches de SonicWall a nivel global. Como parte del ecosistema de SonicWall Capture Security Center, ofrece visibilidad unificada y gestión de redes por cable e inalámbricas.

Basado en la nube y fácil de usar, WNM simplifica en acceso, el control y la resolución de problemas en un único dashboard. Mediante admins WNM, puede crearCree políticas individuales a nivel de tenant y transfiéralastransferirlas a varias ubicaciones y zonas o desglosar. Desglose los dispositivos gestionados para obtener datos granulares. WNM es altamente escalable, capaz de gestionar desde un solo emplazamiento hasta redes empresariales globales con decenas de miles de dispositivos gestionados.

Antes de implementar los puntos de acceso, un análisis del emplazamiento inalámbrico puede ayudar a garantizar el rendimiento y la productividad. La herramienta Wi-Fi Planner integrada en WNM ayuda a implementar los puntos de acceso de forma estratégica para optimizar la experiencia de usuario de WiFi y evitar errores costosos.

Los puntos de acceso SonicWave y los switches de SonicWall utilizan la implementación sin necesidad de intervención para disfrutar de una incorporación automática en cuestión de minutos con la aplicación móvil SonicExpress. El aprovisionamiento es sencillo y puede realizarse de forma remota, lo cual permite ahorrar tiempo y dinero.

Las actualizaciones automáticas de firmware y de seguridad mantienen actualizados los dispositivos gestionados. En caso de que se produzca una caída de Internet, los puntos de acceso y los switches continúan funcionando sin WNM, garantizando así la continuidad del negocio.

Obtenga más información sobre los productos de gestión e informes de SonicWall en www.sonicwall.com/en-us/productsfirewalls/management-and-reporting.

Servicios profesionales y soporte

Sáquele más partido a su solución de seguridad de red de SonicWall y reciba el soporte que necesite, en el momento en que lo necesite. Con los servicios de soporte y profesionales de nivel empresarial de SonicWall, verá aumentado el valor de su solución a largo plazo.

Servicios de soporte globales

Obtenga soporte de forma cómoda para garantizar el funcionamiento fluido de su negocio:

Soporte técnico

- **8x5** – De lunes a viernes, de 8:00 h a 17:00 h para entornos no críticos.
- **24x7** – Soporte las 24 horas, incluidos fines de semana y festivos, para entornos críticos de negocio.

Soporte de valor añadido

- **Soporte Premier:** proporciona a los entornos empresariales un Responsable técnico de cuenta (TAM) dedicado. Su TAM actúa en su nombre como asesor de confianza y trabaja con sus empleados para ayudarles a minimizar los periodos de inactividad imprevistos, optimizar los procesos de TI y proporcionar informes operacionales para aumentar la eficiencia. Constituye su único punto de responsabilidad a fin de que pueda disfrutar de una experiencia de soporte fluida.
- **Ingeniero de soporte dedicado (DSE):** Se asigna un ingeniero para que soporte la cuenta de su empresa. Su DSE conocerá y entenderá su entorno, sus políticas y sus objetivos de TI a fin de resolver rápidamente los asuntos técnicos cuando necesite soporte.

Servicios profesionales globales

¿Necesita ayuda para determinar cuál es la solución que más se ajusta a las necesidades de su empresa y para instalarla en su infraestructura existente? Deje que nos ocupemos nosotros. Con nuestros Servicios profesionales globales, tendrá un solo punto de contacto para todas sus necesidades de implementación e integración. Recibirá servicios hechos a medida para su entorno único, así como asistencia con los siguientes procesos:

- **Planificación:** Estudio y comprensión de sus requisitos de firewall.
- **Implementación/despliegue:** Valoración y despliegue de su solución.
- **Transferencia de conocimientos:** Uso, gestión y mantenimiento de su dispositivo.
- **Migración:** Minimización de las interrupciones y garantía de continuidad del negocio.

Los servicios empresariales de SonicWall están disponibles con NS*sp*/NS*a*/Serie TZ/SMA/Email Security/GMS.

Más información:
www.sonicwall.com/en-us/support

Conclusión

Descubra los productos de seguridad de SonicWall

Integre su hardware, su software y sus servicios para disfrutar de la mejor seguridad posible. Obtenga más información en www.sonicwall.com. Infórmese sobre las opciones de compra y actualización enwww.sonicwall.com/how-to-buy. Y pruebe las soluciones de SonicWall en www.sonicwall.com/trials.

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 seguridad cibernética para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

Si tiene alguna pregunta sobre el posible uso de este material, póngase en contacto con:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Para más información, consulte nuestra página Web.
www.sonicwall.com