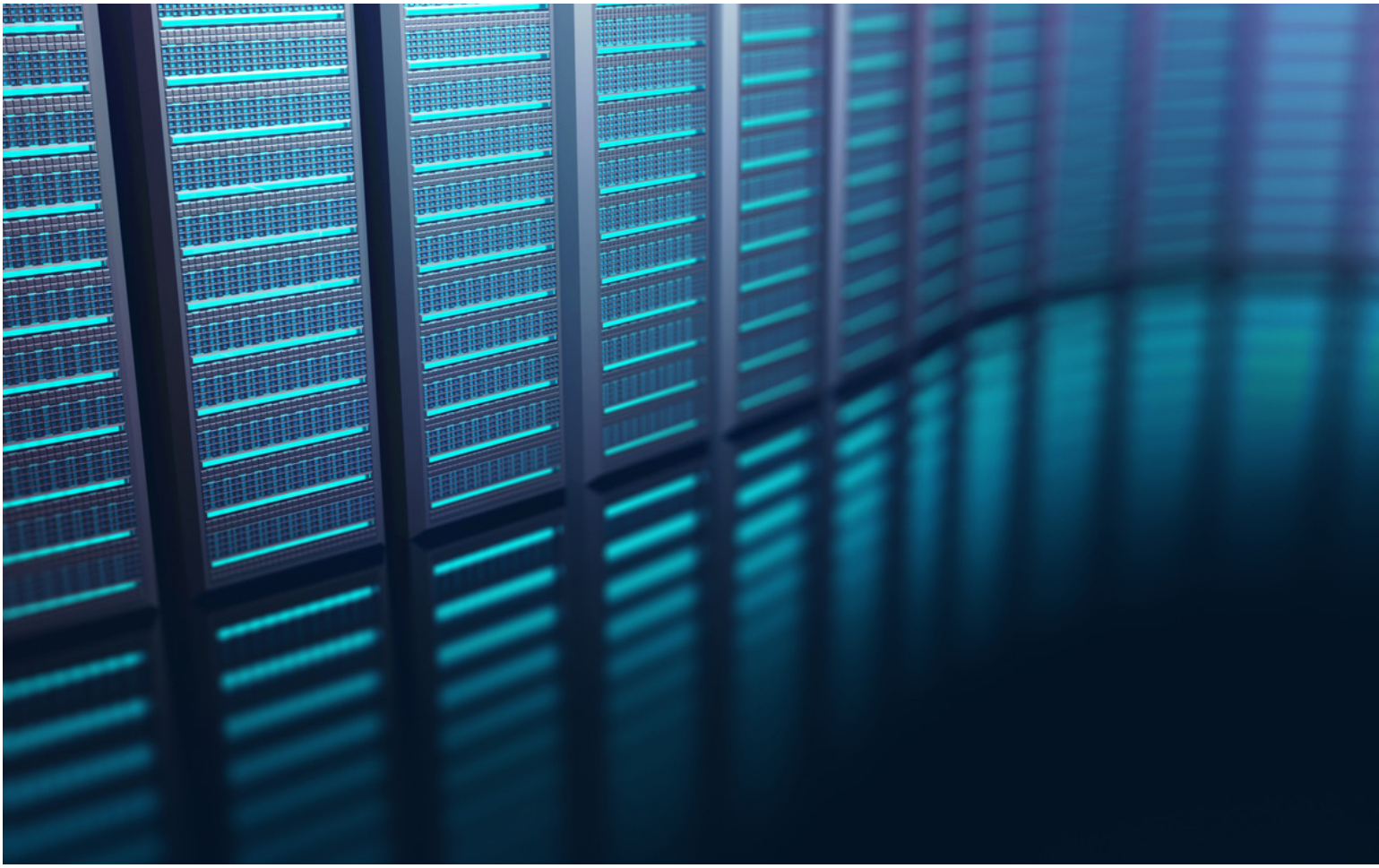
Línea de productos de SonicWall



Información general

Asegure los sistemas, usuarios y datos de su empresa con un nivel de protección profundo que no comprometa el rendimiento de la red. Más de 500.000 empresas tienen implementadas soluciones cableadas e inalámbricas SonicWall en 150 países, desde pequeñas y medianas empresas hasta grandes entornos empresariales, gobierno, punto de venta minorista, educación, profesionales de salud y proveedores de servicios.

SonicWall ofrece líneas de productos integrales y complementarias en cada una de las siguientes áreas:

- Seguridad de red
- Seguridad de acceso
- Seguridad de correo electrónico
- Análisis, informes y administración de seguridad

Productos de seguridad de red

SonicWall es uno de los proveedores líder de firewalls de próxima generación (NGFW). El comprobado firmware de SonicOS es el elemento central de cada NGFW de SonicWall. SonicOS aprovecha nuestra arquitectura de hardware escalable y multinúcleo, así como nuestro motor de inspección de memoria profunda en tiempo real (Real-Time Deep Memory Inspection, RTDMI™) con patente en trámite y nuestro motor patentado de un solo paso y latencia baja de inspección profunda de paquetes libre de reensamblaje (Reassembly-Free Deep Packet Inspection®, RFDPI) que analizan todo el tráfico independientemente del puerto o del protocolo.

Nuestros NGFW garantizan que se inspeccione cada byte de cada paquete, mientras se mantienen el alto rendimiento y la baja latencia que requieren las redes ocupadas. A diferencia de las ofertas de la competencia, el motor RFDPI de un solo paso permite el análisis simultáneo de aplicaciones y varias amenazas, así como el análisis de archivos de cualquier tamaño, sin reensamblaje de paquete. De esta forma, los NGFW de SonicWall se pueden escalar de forma masiva para equipar a las crecientes redes empresariales distribuidas y a los centros de datos con seguridad de vanguardia.

Los NGFW de SonicWall ofrecen una variedad de funcionalidades sólidas. Entre ellas, se incluyen las siguientes:

- Captura de espacios aislados multimotor basados en la nube
- API de amenazas
- Descifrado e inspección de tráfico cifrado
- Servicio de prevención de intrusiones (IPS)
- Protección contra software malicioso
- Inteligencia, control y visualización en tiempo real de aplicaciones
- Filtrado de sitios web/URL (filtrado de contenido)
- Redes privadas virtuales (VPN) por SSL o IPSec
- Seguridad inalámbrica
- Conmutación por error/por recuperación con estado

Además, los firewalls de SonicWall ofrecen una respuesta rápida y protección continua ante amenazas de día cero gracias al equipo de investigación de Capture Labs. Este equipo recopila, analiza y examina información de amenazas de distintos vectores provenientes de una variedad de orígenes de inteligencia de amenazas, incluido un millón de sensores ubicados en todo el mundo dentro de su red de amenazas Capture Threat Network.

Serie SonicWall SuperMassive

La plataforma de NGFW de la serie SonicWall SuperMassive 9000 está diseñada para proporcionar escalabilidad, fiabilidad y seguridad profunda a grandes redes con una velocidad de varios gigabits.

NSS Labs evaluó los firewalls de SonicWall usando una de las pruebas de rendimiento más rigurosas y reales para NGFW. SonicWall obtuvo excelentes resultados en eficacia de seguridad, rendimiento, escalabilidad, fiabilidad y costo total de propiedad. Los firewalls de SonicWall definen el nivel para evaluar el control de aplicaciones de alto rendimiento y prevención de amenazas en usos de casos de distintas implementaciones, desde pequeñas empresas hasta grandes centros de datos, operadores y proveedores de servicios.

La serie SuperMassive 9000 garantiza un servicio de alta calidad con la disponibilidad y conectividad sin interrupciones de la red que requieren las empresas, agencias gubernamentales y universidades de hoy en día con infraestructuras de 10/40 Gbps. Al ofrecer una arquitectura de núcleos de alta densidad en un eficiente dispositivo rack de 1U y 2U, los firewalls SuperMassive 9000 permiten ahorrar espacio valioso en racks y reducen los costos de energía y refrigeración.

**Patentes de EE. UU. 7.310.815; 7.600.257; 7.738.380; 7.835.361; 7.991.723*

SONICWALL®

Serie SonicWall Network Security Appliance (NS*a*)

La serie SonicWall Network Security Appliance (NS*a*) es una de las líneas de NGFW más segura y de mayor rendimiento. Brinda seguridad y rendimiento de clase empresarial sin riesgos, ya que utiliza la misma arquitectura que la línea de NGFW SuperMassive de cabecera (desarrollada en un principio para los operadores y las empresas más exigentes del mundo). Al mismo tiempo, ofrece la aclamada facilidad de uso y el gran valor de SonicWall.

Después de muchos años de investigación y desarrollo, la serie NS*a* se diseñó desde cero para empresas distribuidas, pequeñas y medianas empresas, sucursales, campus escolares y agencias gubernamentales. La serie NS*a* combina una arquitectura revolucionaria multinúcleo con tecnología Real-Time Deep Memory Inspection (RTDMI) basada en la red y un motor RFDPI patentado de un solo paso y prevención de amenazas en un diseño de gran escalabilidad. Esto ofrece protección, rendimiento y escalabilidad líderes en la industria, con la mayor cantidad de conexiones simultáneas, la menor latencia, sin limitaciones de tamaño de archivo y superiores conexiones por segundo en su clase.

Serie SonicWall TZ

La serie SonicWall TZ está compuesta de firewalls de administración unificada de amenazas (UTM) de gran seguridad y fiabilidad diseñados para pequeñas y medianas empresas (SMB), implementaciones minoristas, empresas gubernamentales y empresas distribuidas con sitios remotos y sucursales. A diferencia de los productos para consumidores, la serie TZ brinda capacidades sumamente eficaces contra software malicioso, de prevención de intrusiones, de filtrado de contenido/URL y de control de aplicaciones en redes WLAN y cableadas, junto con un amplio soporte para plataformas móviles en equipos portátiles, teléfonos inteligentes y tabletas. Ofrece una completa inspección profunda de paquetes (DPI) en niveles de muy alto rendimiento, que elimina las limitaciones en la red que provocan otros productos, y permite que las empresas obtengan ganancias en la productividad.

Como el resto de los firewalls de SonicWall, la serie TZ analiza todo el archivo, incluidos los archivos cifrados por TLS/SSL, para obtener una protección completa. Asimismo, la serie TZ ofrece inteligencia y control de aplicaciones, generación de informes y análisis de tráfico de aplicaciones avanzados, VPN con Internet Protocol Security (IPsec) y SSL, conmutación múltiple por error de ISP, equilibrio de carga, conexión inalámbrica 802.11ac integrada y opcional de alta velocidad y segmentación de red; también permite cumplir con PCI. Si se combinan con los conmutadores de la serie Dell X, los firewalls de la serie TZ proveen la flexibilidad para hacer que la empresa crezca de forma segura sin agregar complejidad.

Serie SonicWall Network Security virtual (NS*v*)

Los firewalls SonicWall Network Security virtual (NS*v*) amplían la detección y prevención automatizadas de vulnerabilidades en entornos de redes públicas, privadas e híbridas mediante versiones virtualizadas de los firewalls SonicWall de próxima generación. Con herramientas y servicios integrales equivalentes al firewall SonicWall NS*a*, los NS*v* defienden con eficacia sus entornos virtuales y en la nube contra uso malintencionado de recursos, ataques entre máquinas virtuales, ataques de canal lateral, y todas las vulnerabilidades y amenazas más frecuentes basadas en la nube.

NS*v* se puede implementar y aprovisionar fácilmente en entornos virtuales de usuarios múltiples; por lo general, entre redes virtuales (VN). Establece medidas de control de acceso para proteger los datos y la seguridad de las máquinas virtuales. Al mismo tiempo, captura el tráfico virtual entre las máquinas virtuales y las redes para evitar vulnerabilidades de forma automática. Con infraestructura y soporte para implementación de alta disponibilidad (HA), NS*v* satisface las necesidades de escalabilidad y disponibilidad de los centros de datos definidos por software (SDDC). NS*v* se puede implementar con flexibilidad como un dispositivo virtual en nubes privadas que utilicen VMWare o Microsoft Hyper-V, o en entornos de nubes públicas que utilicen AWS o Microsoft Azure. Además, les ofrece a las empresas todas las ventajas de seguridad de un firewall físico, pero con los beneficios operativos y económicos de la virtualización.

Serie SonicWave Wireless Network Security

SonicWall permite que las redes WLAN sean seguras, simples y asequibles gracias a la solución innovadora SonicWall Wireless Network Security. La solución combina wireless access points de alto rendimiento serie SonicWave 802.11ac Wave 2 y firewalls SonicWall líderes en la industria para obtener rendimiento y seguridad de red cableada en su red WLAN, que incluye la prevención de intrusiones, el descifrado y la inspección TLS/SSL, el control de aplicaciones y el filtrado de contenido para obtener un rendimiento y una protección de nivel empresarial.

Nuestra solución ofrece más que meras soluciones inalámbricas seguras, ya que asegura las redes WLAN con tecnologías RTDMI y RFDPI. Además, proporciona protección dual mediante el cifrado de tráfico inalámbrico y la eliminación de amenazas de red, mientras protege a la red contra ataques inalámbricos. SonicWall reduce el costo total de propiedad (TCO), ya que permite a los administradores evitar la implementación y la administración por separado de una costosa solución específicamente inalámbrica que se ejecuta en paralelo a su red cableada existente.

Serie SonicWall Web Application Firewall (WAF)

La serie SonicWall Web Application Firewall (WAF) protege a las aplicaciones web que se ejecuten en un entorno de nube privada, pública o híbrida. Ofrece herramientas y servicios de seguridad web avanzada para no exponer los datos de cumplimiento y para que las propiedades web estén a salvo, no tengan interrupciones y trabajen al máximo rendimiento. WAF utiliza capacidades de entrega de aplicaciones de siete capas que habilitan el equilibrio de carga con reconocimiento de aplicaciones, la descarga de SSL y la aceleración para obtener resiliencia y una mejor experiencia digital.

WAF emplea una combinación de motores de inspección profunda de paquetes basados en firmas y de perfiles de aplicación para proteger contra los ataques de aplicaciones web más frecuentes, como los descritos en Open Web Application Security Project (OWASP), además de amenazas de aplicaciones web más avanzadas, como los ataques por denegación de servicio (DoS) y las vulnerabilidades con reconocimiento del contexto. Además de proteger a las aplicaciones web, WAF también previene la pérdida de datos mediante el uso de técnicas para el ocultamiento de datos y el bloqueo de páginas en patrones especificados de datos sensibles, como la información de pagos con tarjeta (PCI) e identificaciones emitidas por el gobierno.

Gracias a la virtualización, WAF ofrece beneficios de economía de escala y se puede implementar como un dispositivo virtual en nubes privadas que utilicen VMWare ESXi o Microsoft Hyper-V, o en entornos de nubes públicas que utilicen AWS o Microsoft Azure.

Capture Client

En el entorno comercial actual, es fundamental administrar y asegurar los endpoints. Los usuarios finales usan sus dispositivos para entrar y salir de la red, y las amenazas cifradas tienen rienda suelta para llegar a los endpoints: es necesario tomar medidas para proteger estos dispositivos. Con el aumento de ransomware y el constante robo de credenciales, los endpoints son el campo de batalla del actual entorno de amenazas.

Además, los administradores tienen más y más dificultades para ver y administrar su postura en cuanto a seguridad. También cuentan con el desafío de garantizar constantemente la seguridad del cliente, y ofrecer inteligencia e informes fáciles de usar y aptos para tomar decisiones.

Los productos para seguridad de los endpoints se comercializan desde hace años, pero los administradores siguen teniendo dificultades para lo siguiente:

- Mantener actualizados los productos de seguridad
- Imponer políticas y cumplimiento
- Obtener informes
- Enfrentar amenazas que provengan de canales cifrados
- Comprender las alertas y los pasos para remediarlas
- Administrar licencias
- Detener amenazas, como ransomware

SonicWall Capture Client es una plataforma de cliente unificada que proporciona distintas capacidades para proteger múltiples endpoints. Esta solución cuenta con una consola de administración basada en la nube y se integra completamente en los firewalls de próxima generación de SonicWall para ofrecerles a los clientes de SonicWall una experiencia de seguridad unificada. SonicWall Capture Client se combina con capacidades de

cumplimiento normativo para garantizar que los endpoints ejecuten software de seguridad o cuenten con un certificado SSL incorporado que permitan inspeccionar el tráfico cifrado. Asimismo, para facilitar la inspección de tráfico SSL (DPI-SSL) con una mejor experiencia de usuario, Capture Client permite que los administradores implementen certificados de SSL en los endpoints con mucha más facilidad que antes.

Además, en Capture Client, se puede elegir entre dos motores de antivirus según sea necesario. En primer lugar, el motor de próxima generación de SentinelOne está diseñado para detener los softwares maliciosos más ingeniosos y ofrece la posibilidad de reversión para regresar a un estado anterior que no esté infectado. En segundo lugar, el motor tradicional de McAfee ofrece eliminación de amenazas basada en firmas además de análisis de discos completos.

Los beneficios de integración de SentinelOne incluyen lo siguiente:

- Cumplimiento de la seguridad
- Administración de certificados DPI-SSL
- Monitoreo de comportamiento continuo
- Decisiones muy precisas a través de aprendizaje de máquina
- Técnicas heurísticas multicapa
- Capacidades de reversión únicas (solo en Capture Client Advanced)

Los beneficios de integración de McAfee incluyen lo siguiente:

- Cumplimiento de la seguridad
- Administración de certificados DPI-SSL
- Eliminación de amenazas basada en firmas
- Análisis de discos completos

Serie SonicWall WAN Acceleration Appliance (WXA)

La serie SonicWall WAN Acceleration Appliance (WXA) reduce la latencia de las aplicaciones y conserva el ancho de banda; de esta forma, aumenta significativamente el rendimiento de las aplicaciones WAN y mejora la experiencia de usuario en pequeñas y medianas empresas con sucursales y oficinas remotas. Después de la transferencia inicial de datos, la serie WXA reduce significativamente todo tráfico posterior porque transmite a la red únicamente los datos nuevos o modificados. WXA deduplica datos que atraviesan la WAN, recuerda datos transferidos previamente y reemplaza las secuencias de bytes repetidas con un identificador, lo que permite reducir la latencia de las aplicaciones y conservar el ancho de banda. Otras funciones de aceleración incluyen el almacenamiento de datos en caché, la deduplicación de archivos, el almacenamiento de metadatos en caché, el almacenamiento de HTTP (web) en caché y la compresión de datos que se encuentran en transferencia.

A diferencia de los productos de aceleración de WAN independientes, las soluciones WXA son complementos integrados en los firewalls SonicWall de las series SuperMassive 9000, NSa y TZ. Esta solución integrada optimiza la colocación, la implementación, la configuración, el enrutamiento, la administración y la integración de WXA en otros componentes, como las VPN. Cuando se implementa junto con un NGFW SonicWall que ejecuta el servicio de control e inteligencia de aplicaciones, WXA ofrece el particular beneficio combinado de priorizar el tráfico de aplicaciones y minimizar el tráfico entre los sitios, lo que genera un rendimiento de red óptimo.

Obtenga más información sobre los productos SonicWall para seguridad de la red en www.sonicwall.com/en-us/products.

Servicios de seguridad de red y productos complementarios

Los servicios y complementos de firewall para la seguridad de redes que ofrece SonicWall proporcionan una protección avanzada y altamente eficaz a empresas de todos los tamaños, para ayudarlas a defenderse de amenazas de seguridad, obtener mayor control de seguridad, mejorar la productividad y reducir los costos.

Los servicios y complementos incluyen:

- Paquete TotalSecure: firewall más el paquete Advanced Gateway Security Suite (espacios aislados multimotor, antivirus, antispyware, prevención de intrusiones, inteligencia de aplicaciones, filtrado de contenido/web y soporte las 24 horas, todos los días)
- Paquete Advanced Gateway Security Suite: Capture Advanced Threat Protection, antivirus de gateway, antispyware, prevención de intrusiones, filtrado de contenido/web y soporte las 24 horas, todos los días
- Servicios de seguridad de gateway: antivirus de gateway, antispyware, prevención de intrusiones, y control e inteligencia de aplicaciones
- Capture Advanced Threat Protection (ATP)
- Servicios de filtrado de contenido
- Software antispyware y antivirus de clientes implementado
- Servicio integral contra correos no deseados
- Inspección profunda de paquetes para tráfico cifrado TLS/SSL (DPI-SSL)
- Inteligencia y control de aplicaciones
- Sistema de prevención de intrusiones (IPS)

Obtenga más información sobre los servicios y complementos para la seguridad de redes en www.sonicwall.com/en-us/products/firewalls/security-services.

Inspeccione la memoria profunda

El motor Real-Time Deep Memory Inspection (RTDMI) de SonicWall (tecnología con patente en trámite) detecta y bloquea, de forma proactiva, software malicioso desconocido de mercado masivo a través de la inspección de la memoria profunda en tiempo real. El motor, disponible actualmente con el servicio de sandbox en la nube Capture Advanced Threat Protection (ATP) de SonicWall, identifica y aplaca hasta las amenazas modernas más insidiosas, como las futuras vulnerabilidades de Meltdown.

Productos de seguridad de acceso

SonicWall SMA es el gateway de acceso seguro unificado para empresas que enfrenten desafíos en movilidad, BYOD y migración a la nube. La solución les permite a las empresas ofrecer acceso a recursos empresariales fundamentales en cualquier momento, en cualquier lugar y a cualquier dispositivo. El motor de políticas para el control de acceso granular, la autorización de dispositivos con reconocimiento del contexto, la VPN a nivel de aplicación y la autenticación avanzada con inicio de sesión único que ofrece SMA permiten que las empresas adopten BYOD y movilidad en un entorno de TI híbrido.

Además, SMA disminuye el área de amenazas, ya que ofrece funciones como detección de Geo IP y Botnet, firewalls de aplicaciones web e integración de sandbox de Capture ATP.

Movilidad y BYOD

En empresas que deseen adoptar BYOD, tareas flexibles o desarrollo en el extranjero, SMA se convierte en el punto central de control. SMA ofrece la mejor seguridad para minimizar amenazas de superficie y, al mismo tiempo, permite que las empresas sean más seguras, ya que soporta los últimos algoritmos y cifrados. SonicWall SMA les permite a los administradores aprovisionar acceso móvil seguro y privilegios basados en los roles para que los usuarios finales obtengan acceso rápido y simple a las aplicaciones, los datos y los recursos empresariales que necesiten. Al mismo tiempo, las empresas pueden establecer políticas de BYOD seguras para proteger sus datos y redes corporativas contra accesos no autorizados y softwares maliciosos.

Migración a la nube

En empresas que comiencen a migrar a la nube, SMA ofrece una infraestructura de inicio de sesión único (SSO) que utiliza un único portal web para autenticar usuarios en un entorno de TI híbrido. No importa si el recurso empresarial se encuentra en el edificio, en la web o en la nube; el acceso será constante y dinámico. No hace falta que los usuarios recuerden todas las URL de cada aplicación y guarden marcadores extensos. Gracias a Workplace, un portal de acceso centralizado, los usuarios obtienen una sola URL para acceder a todas las aplicaciones fundamentales desde un navegador web convencional. SMA ofrece SSO federado tanto a aplicaciones SaaS alojadas en la nube que utilicen SAML 2.0 como a aplicaciones alojadas en los campus que utilicen RADIUS o Kerberos. SMA se integra a múltiples servidores de autenticación, autorización y contabilidad, y a tecnologías líderes de autenticación multifactor (MFA) para mayor seguridad. El SSO seguro se suministra únicamente a dispositivos endpoints autorizados después de comprobar el estado de salud y el nivel de cumplimiento.

Proveedores de servicios administrados

En empresas con centros de datos o en proveedores de servicios administrados, SMA ofrece una solución lista para usar que proporciona un alto nivel de continuidad y escalabilidad empresarial. SonicWall SMA soporta hasta 20.000 conexiones simultáneas en un único dispositivo y se puede escalar hasta cientos de miles de usuarios con clústeres inteligentes. Disminuya los costos en los centros de datos con clústeres de alta disponibilidad activos-activos (Global High Availability) y un equilibrador dinámico de cargas integrado (Global Traffic Optimizer), que reasigna el tráfico global al centro de datos más optimizado en tiempo real según la demanda de usuarios. A través de una variedad de herramientas, SMA permite que los propietarios de servicios proporcionen un servicio sin tiempos de inactividad y permite el cumplimiento de SLA muy agresivos.

Dispositivos SMA

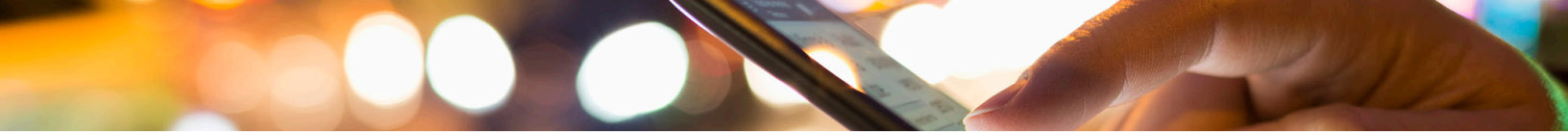
Puede implementar SonicWall SMA como un dispositivo reforzado y de alto rendimiento o como un dispositivo virtual que aproveche los recursos informáticos compartidos, a fin de optimizar el uso, facilitar la migración y reducir los costos de capital. Los dispositivos de hardware se incorporan a una arquitectura multinúcleo capaz de ofrecer un alto rendimiento con aceleración de SSL, rendimiento de VPN y proxis potentes que proporcionen un acceso seguro y sólido. Las empresas reguladas y federales disponen de SMA con certificación FIPS 140-2 nivel 2. Los dispositivos virtuales de SMA ofrecen las mismas capacidades sólido de acceso seguro en las plataformas virtuales más importantes, como Hyper-V y VMware. Si decide implementar dispositivos físicos, virtuales o una combinación de ambos, SMA se adaptará perfectamente a su actual infraestructura del área de TI.

Administración y generación de informes

SonicWall proporciona una intuitiva plataforma de administración basada en la web para optimizar la administración de dispositivos y ofrecer grandes capacidades de generación de informes. La interfaz de usuario gráfica es fácil de usar y brinda claridad a la administración de múltiples equipos. La administración de políticas unificada ayuda a crear y monitorear políticas y configuraciones de acceso. Una sola política se encarga de administrar a los usuarios, los dispositivos, las aplicaciones, los datos y las redes. Automatice las tareas rutinarias y programe actividades; de esta forma, los equipos de seguridad estarán disponibles para encargarse de las tareas de seguridad estratégica, como la respuesta ante incidentes, y no se preocuparán por las tareas repetitivas.

Permita que su departamento de TI ofrezca la mejor experiencia y los accesos más seguros según el escenario del usuario. Elija entre una variedad de accesos seguros basados en la web completamente sin clientes para proveedores y contratistas externos, o un acceso VPN más tradicional de túnel completo basado en el cliente para ejecutivos. No importa si necesita proporcionar accesos seguros a cinco usuarios de un solo centro de datos o a miles de usuarios de centros de datos distribuidos en todo el mundo, SonicWall SMA tiene la solución ideal para usted.

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



Productos de seguridad de correo electrónico

El correo electrónico es fundamental para la comunicación de la empresa, pero también pueden exponer a la empresa a ataques y mermas de productividad si las amenazas basadas en correos electrónicos, como ransomware, suplantación de identidad, riesgos de correo electrónico empresarial (BEC), suplantación de IP, correo no deseado y virus, ingresan a los servidores de correo electrónico y a las bandejas de entrada de los usuarios. Asimismo, actualmente, las reglas gubernamentales determinan que la misma empresa se responsabiliza por la protección de los datos confidenciales y debe garantizar que no haya fugas de datos, y que exista un intercambio seguro de los correos electrónicos que contienen datos de clientes o información confidencial. No importa si se trata de una pequeña o mediana empresa en crecimiento, una empresa grande y distribuida, o un proveedor de servicio administrado (MSP), necesita un modo rentable de implementar la seguridad y el cifrado de correos electrónicos, además de la escalabilidad para aumentar fácilmente la capacidad de unidades y dominios organizativos y delegar la administración en estos.

Además, para administrar los costos y recursos, las empresas comienzan a adoptar Microsoft Office 365. Si bien Office 365 ofrece funcionalidades de seguridad incorporadas, las empresas necesitan una solución de seguridad de correos electrónicos de próxima generación que sea capaz de integrarse dinámicamente en Office 365 para combatir las amenazas avanzadas de correo electrónico y protegerse contra las amenazas avanzadas de hoy en día.

Dispositivos SonicWall Email Security

SonicWall Email Security es fácil de configurar y administrar, y está diseñado para escalar de 10 a 100.000 casillas de correo de forma económica. Se puede implementar como un dispositivo de hardware, un dispositivo virtual que aproveche los recursos informáticos compartidos o como software (incluso software optimizado para servidores de Microsoft Windows o servidores de pequeñas empresas). Los dispositivos físicos de SonicWall Email Security son ideales para empresas que necesiten una solución dedicada en las instalaciones. Nuestra solución multicapa ofrece una protección entrante y saliente integral, y está disponible en una variedad de opciones de hardware, que se puede escalar hasta a 10.000 usuarios por dispositivo. SonicWall Email Security también está disponible como un dispositivo virtual o una aplicación de software, ideal para empresas que requieran la flexibilidad y la agilidad propias de la virtualización. La solución se puede configurar para obtener alta disponibilidad en modo dividido con el fin de administrar, de manera central y confiable, las implementaciones a gran escala.

La solución SonicWall Email Security usa tecnologías como Advanced Reputation Management, Advanced Content Management, filtros Adversarial Bayesian y un algoritmo de Support Vector Machine para ofrecer una protección integral en datos de entrada y de salida.

- Integración en espacios aislados Capture ATP multimotor
- Múltiples motores antivirus
- Ajustes configurables de Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) y Domain-based Message Authentication, Reporting & Conformance (DMARC)
- Análisis de reputación de la IP del emisor y del asunto, el contenido, los enlaces incorporados y los archivos adjuntos del mensaje
- Integración optimizada en Office 365
- Complemento de cifrado y cumplimiento

La administración de la solución de seguridad del correo electrónico es intuitiva, rápida y sencilla. Puede delegar de forma segura la administración de correo no deseado a los usuarios finales, al tiempo que retiene el control final sobre el cumplimiento de la seguridad. Puede administrar cuentas de usuarios y grupos con facilidad a través de la sincronización perfecta con varios LDAP. La solución también permite integrarse fácilmente en Office 365 para protegerse contra amenazas avanzadas de correo electrónico.

En los entornos grandes y distribuidos, la compatibilidad con múltiples usuarios le permite delegar subadministradores para administrar la configuración de diversas unidades organizativas (como divisiones empresariales o clientes de proveedores de servicios administrados) dentro de una sola implementación de Email Security.

Servicio SonicWall Hosted Email Security

Confíe en servicios alojados fáciles de administrar y rápidos de implementar para proteger a su empresa contra amenazas provenientes de correos electrónicos, como ransomware, amenazas de día cero, spear phishing y BEC, sin comprometer el cumplimiento normativo ni las disposiciones reglamentarias de los correos electrónicos. Obtenga el mismo nivel de protección avanzada para correo electrónico con nuestra solución alojada, que ofrece las mismas características que los dispositivos físicos y virtuales. La solución también ofrece la continuidad de los correos electrónicos para garantizar que siempre se entreguen y que la productividad no se vea afectada durante interrupciones planeadas y no planeadas en servidores de correo electrónico dentro de las instalaciones y de proveedores en la nube, como Office 365.

SonicWall Hosted Email Security brinda protección de alta calidad basada en la nube contra amenazas entrantes y salientes a un precio de suscripción mensual o anual accesible, predecible y flexible. Puede minimizar el tiempo y los costos de la implementación inicial además de los gastos administrativos constantes sin comprometer la seguridad.

SonicWall les ofrece a los VAR y a los MSP mejores oportunidades para competir y aumentar los ingresos, y minimizar el riesgo y los costos iniciales y constantes. SonicWall Hosted Email Security incluye funciones adecuadas para MSP, como servicios de múltiples clientes, administración central para múltiples suscriptores, integración en Office 365, opciones flexibles de compra y aprovisionamiento automatizado.

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

SONICWALL®

Análisis, generación de informes y administración

Para SonicWall, un método conectado para la administración de la seguridad es fundamental en prácticas de seguridad preventiva, pero además, forma parte de la base necesaria para una estrategia de seguridad unificada para la administración de control, cumplimiento y riesgos. Con las soluciones de administración, generación de informes y análisis de SonicWall, las empresas obtienen una plataforma integrada, segura y extensible para establecer una estrategia de defensa y respuesta de seguridad que sea sólida y uniforme en todas sus redes cableadas, inalámbricas y móviles. La adopción total de esta plataforma común les proporciona a las empresas datos detallados sobre la seguridad para tomar decisiones informadas en cuanto a la seguridad y operar rápidamente para incorporar colaboración, comunicación y conocimientos a todo el marco de seguridad compartido.

SonicWall Global Management System

Con la posibilidad de implementarse en las instalaciones como software o dispositivo virtual, SonicWall Global Management System (GMS) administra, de forma cohesiva, las operaciones de seguridad de la red por procesos comerciales y niveles de servicio en lugar de hacerlo dispositivo a dispositivo, que es un método menos eficaz y aislado. GMS permite que empresas de distintos tamaños y tipos consoliden fácilmente la administración de dispositivos de seguridad, disminuyan las complejidades de la administración y de la solución de problemas, y puedan federar todos los aspectos operativos de la infraestructura de seguridad. Esto incluye administración y cumplimiento de políticas centralizadas, monitoreo de eventos en tiempo real, análisis e informes de datos granulares, seguimientos de auditoría y más desde una plataforma empresarial unificada.

GMS también cumple con los requisitos de la administración de firewalls de las empresas gracias a la automatización de flujos de trabajo. Este proceso intrínseco y automatizado garantiza la precisión y el cumplimiento de cambios en las políticas mediante la implementación de un proceso riguroso para configurar, comparar, validar, revisar y aprobar las políticas de administración de seguridad antes de la implementación. Los grupos de aprobación son flexibles. Esto permite adherirse a las políticas de seguridad de la empresa y garantizar que se implementen las adecuadas políticas de firewall en el momento adecuado y de conformidad con las disposiciones normativas.

SonicWall Capture Cloud Security Center

Capture Cloud Security Center forma parte de la plataforma SonicWall Capture Cloud y es una plataforma abierta y escalable para la administración de seguridad en la nube, el monitoreo, la generación de informes y los análisis que se entrega en el formato económico de software como servicio (SaaS). Está diseñada para empresas de distintos tamaños y casos de uso, incluso empresas distribuidas y proveedores de servicios, que estén en proceso de adoptar servicios informáticos en la nube por sus ventajas económicas. Capture Cloud Security Center es la plataforma de administración de seguridad en la nube ideal para establecer un método de seguridad sostenible y completamente coordinado en cualquier red.

Para los clientes, Capture Cloud Security Center ofrece lo último en visibilidad, agilidad y capacidad para gestionar todo el ecosistema de seguridad de red SonicWall con mayor claridad, precisión y velocidad. Y todo desde un único lugar, independientemente de la ubicación. Con una visibilidad del entorno de seguridad que abarca a toda la empresa y una inteligencia de seguridad en tiempo real que alcanza a las personas adecuadas de la empresa, se pueden tomar las decisiones apropiadas sobre las políticas y los controles de seguridad para reforzar la postura en cuanto a la seguridad.

Para los proveedores de servicio, Capture Cloud Security Center simplifica la administración discreta de las operaciones de seguridad de múltiples clientes. Desarrolla oportunidades para que los MSP/MSSP aumenten la agilidad de sus servicios de seguridad mientras reducen los gastos operativos y las complejidades propias de una infraestructura exclusiva.

SonicWall Analyzer

Analyzer es una herramienta de generación de informes y análisis de tráfico basada en la web que es fácil de usar y brinda datos históricos y en tiempo real del estado, el rendimiento y la seguridad de la red. Analyzer soporta los firewalls de SonicWall y los dispositivos de acceso móvil seguro; al mismo tiempo, aprovecha el análisis de tráfico de las aplicaciones para los informes de eventos de seguridad. Las empresas de todos los tamaños obtienen como beneficio una mayor productividad laboral, ancho de banda de red óptimo y mayor conciencia sobre la seguridad. Analyzer está disponible como una aplicación de Windows y un dispositivo virtual.

Obtenga más información sobre los productos de administración y generación de informes de SonicWall en www.sonicwall.com/en-us/products/firewalls/management-and-reporting.

Servicios empresariales de SonicWall

Obtenga más de su solución de seguridad para redes de SonicWall y reciba la ayuda que necesite, cuando la necesite. Gracias al soporte para empresas y a los servicios profesionales de SonicWall, obtendrá un valor a largo plazo y de alta calidad con su solución.

Servicios de soporte globales

Obtenga el soporte adecuado para que su empresa se mantenga en funcionamiento sin problemas:

Soporte técnico

- **8 a 17**: lunes a viernes, de 8:00 a 17 horas. para entornos no críticos
- **24 horas, todos los días**: soporte las 24 horas, incluidos los fines de semana y los feriados, para entornos empresariales críticos

Soporte de valor agregado

- **Soporte Premier** proporciona a los entornos empresariales un responsable técnico de cuenta (TAM) dedicado. Su TAM actúa en representación suya como un asesor confiable que trabaja con su personal para ayudar a minimizar el tiempo de inactividad no planificado, optimizar los procesos del área de TI y proveer informes operativos para impulsar la eficiencia. Además, es su único punto de responsabilidad para una experiencia de soporte sin interrupciones.
- **Ingeniero de asistencia dedicado (DSE)** brinda un recurso de ingeniería con nombre para brindar soporte a su cuenta empresarial. Su DSE conocerá y comprenderá su entorno, sus políticas y sus objetivos del área de TI para brindarle una resolución técnica rápida cuando necesite soporte.

Servicios profesionales globales

¿Necesita ayuda para determinar cuál es la mejor solución de seguridad para su empresa, así como para implementarla en su infraestructura existente? Deje que nosotros nos ocupemos. Con los Servicios profesionales globales, usted obtiene un único punto de contacto para todas sus necesidades de implementación e integración. Recibirá servicios personalizados para su entorno en particular además de asistencia para lo siguiente:

- **Planificación:** determinación del alcance y comprensión de los requisitos de su firewall.
- **Implementación:** evaluación e implementación de su solución.
- **Transferencia de conocimiento:** utilización, administración y mantenimiento de su dispositivo.
- **Migración:** minimización de interrupciones y garantía de continuidad de la empresa.

Los servicios empresariales de SonicWall están disponibles con SuperMassive/NSa/serie TZ/SRA/SMA/Email Security/GMS.

Obtenga más información enhttps://support.software.com/essentials/support-offerings.

Conclusión

Descubra los productos de seguridad de SonicWall

Integre su hardware, software y servicios para una seguridad más conveniente. Obtenga más información en www.sonicwall.com. Obtenga información sobre las opciones de compra y actualización en www.sonicwall.com/how-to-buy. Y pruebe las soluciones de SonicWall en www.sonicwall.com/trials.

Acerca de nosotros

SonicWall ha luchado contra la delincuencia cibernética durante más de 25 años, defendiendo a las pequeñas y medianas empresas en todo el mundo. Nuestra combinación de productos y socios ha permitido ofrecer una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 empresas en más de 150 países, para que pueda hacer más negocios con menos temor.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Visite nuestro sitio web para obtener más información.
www.sonicwall.com