Plataforma SonicOS

Todos los firewalls físicos y virtuales de SonicWall, incluidos los de las series TZ, NS*a*, NSv y SuperMassive, se basan en la arquitectura de SonicOS. SonicOS utiliza nuestra tecnología patentada* Reassembly-Free Deep Packet Inspection® (RFDPI) de paso único y baja latencia y nuestra tecnología pendiente de patente Real-Time Deep Memory Inspection™ (RTDMI) para proporcionar una seguridad de alta eficacia validada por la industria, SD-WAN, visualización en tiempo real, redes privadas virtuales (VPN) de alta velocidad y otras prestaciones de seguridad eficaces.

Prestaciones de firewall

Motor de inspección profunda de paquetes sin reensamblado (Reassembly-Free Deep Packet Inspection, RFDPI)	
Prestación	Descripción
Inspección profunda de paquetes sin reensamblado (RFDPI)	Este motor de inspección de alto rendimiento patentado y propietario realiza análisis bidireccionales del tráfico basados en flujos sin almacenamiento en búfer ni proxies a fin de descubrir posibles intentos de intrusión o ataques de malware y de identificar el tráfico de aplicaciones independientemente del puerto.
Inspección bidireccional	Escanea el tráfico entrante y saliente de forma simultánea en busca de amenazas con el fin de evitar que la red se utilice para la distribución de malware o se convierta en una plataforma de lanzamiento de ataques en el caso de que se introduzca un equipo infectado.
Inspección basada en flujos	La tecnología de inspección sin proxy ni búfer proporciona un rendimiento DPI de latencia ultrabaja para millones de flujos de red simultáneos sin limitaciones de tamaño de archivos ni flujos, y puede aplicarse a protocolos comunes y a flujos de TCP sin procesar.
Altamente paralelo y escalable	El diseño único del motor RFDPI, en combinación con la arquitectura multinúcleo, proporciona un rendimiento DPI elevado y tasas de establecimiento de sesiones nuevas extremadamente altas para hacer frente a los picos de tráfico de las redes más exigentes.
Inspección de paso único	La arquitectura DPI de paso único escanea el tráfico simultáneamente para la detección de malware y de intrusiones y para la identificación de aplicaciones, reduciendo drásticamente la latencia de la DPI y garantizando la correlación de toda la información sobre las amenazas en una única arquitectura.
Firewall y redes	
Prestación	Descripción
Secure SD-WAN	Una alternativa a las tecnologías más caras, como MPLS, Secure SD-WAN permite a las empresas distribuidas crear, operar y gestionar redes seguras de alto rendimiento en emplazamientos remotos con el fin de compartir datos, aplicaciones y servicios utilizando servicios de Internet públicos, de bajo coste y fácilmente disponibles.
API REST	Permite al firewall recibir y utilizar cualquier información de inteligencia propietaria, de fabricantes de equipos originales o de terceros para combatir las amenazas avanzadas como los ataques de día cero, usuarios internos maliciosos, credenciales comprometidas, ransomware y amenazas persistentes avanzadas.
Inspección dinámica de paquetes	Todo el tráfico de la red se inspecciona, se analiza y se somete a las políticas de acceso del firewall.
Alta disponibilidad/agrupación (clústeres)	Soporta los modos de alta disponibilidad Activa/Pasiva (A/P) con sincronización de estado, DPI Activa/Activa (A/A)[2] y agrupada Activa/Activa.[2] La DPI Activa/Activa desvía la carga de la inspección profunda de paquetes al dispositivo pasivo con el fin de mejorar el rendimiento.
Protección contra ataques DDoS/DOS	La protección contra inundaciones SYN proporciona una defensa contra los ataques DoS mediante el uso de tecnologías de listas negras de nivel 3 (SYN proxy) y nivel 2 (SYN). Asimismo, ofrece protección contra ataques DoS/DDoS mediante funciones de protección contra inundaciones UDP/ICMP y de limitación de la tasa de conexión.
Opciones de implementación flexibles	El firewall puede implementarse en los modos Wire, TAP de red o puente de capa 2[2].
Equilibrio de carga WAN	Equilibra la carga de múltiples interfaces WAN mediante Round Robin o Spillover o utilizando métodos basados en porcentajes. El enrutamiento basado en políticas crea enrutamientos basados en protocolos para direccionar el tráfico a una determinada conexión WAN, con posibilidad de reconexión a una WAN secundaria en caso de fallo de la alimentación.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y remapeo del tráfico VoIP en la red.
Soporte de Gatekeeper H.323 y proxy SIP	Bloquea las llamadas spam: todas las llamadas entrantes han de ser autorizadas y autenticadas mediante Gatekeeper H.323 o proxy SIP.

Firewall y redes (cont.)	
Prestación	Descripción
Gestión de switches individuales y en cascada de las series N y X de Dell[2]	Gestione los ajustes de seguridad de los puertos adicionales, incluidos Portshield, HA, PoE y PoE+, desde una única consola utilizando el dashboard de gestión del firewall para los switches de red de las series Dell N y Dell X.
Autenticación biométrica	Soporta la autenticación de dispositivos móviles, como el reconocimiento de huellas dactilares, que no pueden ser fácilmente duplicadas ni compartidas, con el fin de autenticar la identidad del usuario de forma segura para que pueda acceder a la red.
Autenticación abierta e inicio de sesión social	Permite a los usuarios invitados utilizar sus credenciales de servicios de redes sociales, como Facebook, Twitter o Google+, para iniciar sesión y acceder a Internet y a otros servicios para usuarios invitados mediante una conexión inalámbrica de un host, una LAN o zonas DMZ, utilizando una autenticación de paso a través.
Autenticación multidominio	Ofrece una forma rápida y sencilla de administrar las políticas de seguridad en todos los dominios de la red. Gestione una política individual para un dominio individual o un grupo de dominios.
Gestión e informes	
Prestación	Descripción
Gestión basada en la nube y local	Funciones de configuración y gestión de los dispositivos SonicWall disponibles en la nube a través del SonicWall Capture Security Center y localmente utilizando el Sistema de gestión global (GMS) de SonicWall.
Potente gestión de dispositivos individuales	Ofrece una interfaz intuitiva basada en Web que puede configurarse de forma rápida y sencilla, una interfaz de línea de comandos completa y soporte para SNMPv2/3.
Informes IPFIX/Netflow de flujos de aplicaciones	Exporta análisis del tráfico de aplicaciones y datos de uso mediante protocolos IPFIX o NetFlow para supervisar y elaborar informes en tiempo real y de datos antiguos con herramientas como SonicWall Analytics u otras compatibles con IPFIX y NetFlow con extensiones.
Redes privadas virtuales (VPN)	
Prestación	Descripción
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewall distribuidas automatizando el aprovisionamiento inicial de la pasarela VPN de extremo a extremo entre los firewalls de SonicWall, mientras que los sistemas de seguridad y conectividad funcionan de forma instantánea y automática.
VPN IPSec para conectividad entre emplazamientos	La VPN IPSec de alto rendimiento permite al firewall actuar como un concentrador VPN para miles de emplazamientos grandes, sucursales u oficinas domésticas.
Acceso remoto mediante SSL VPN o cliente IPSec	Permite utilizar la tecnología SSL VPN sin clientes o un cliente IPSec de fácil gestión para el acceso sencillo a e-mails, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.
Pasarela VPN redundante	Cuando se utilizan múltiples WANs, se pueden configurar una VPN primaria y otra secundaria para permitir la reconexión y la recuperación automáticas de todas las sesiones VPN.
VPN basada en enrutamiento	El enrutamiento dinámico a través de enlaces VPN garantiza un servicio sin interrupciones en caso de fallo temporal del túnel VPN, ya que el tráfico entre los puntos terminales puede reenrutarse fácilmente a través de rutas alternativas.
Reconocimiento de contenido/contextual	
Prestación	Descripción
Seguimiento de la actividad de los usuarios	Gracias a la integración fluida de las funciones de SSO con AD/LDAP/Citrix/Terminal Services, en combinación con la amplia información proporcionada por la DPI, es posible identificar a los usuarios y sus actividades.
GeoIP – Identificación del tráfico en base al país	Identifica y controla el tráfico de red dirigido a, o procedente de, países determinados para ofrecer protección contra ataques de amenazas de origen conocido o sospechoso, o para investigar el tráfico sospechoso originado en la red. Permite crear listas personalizadas de países y Botnets para anular etiquetas de país o Botnet erróneas asociadas con una dirección IP. Elimina el filtrado de direcciones IP no deseado debido a errores de clasificación.
Coincidencia y filtrado de expresiones regulares	Previene la filtración de datos gracias a que identifica y controla el contenido que atraviesa la red mediante la coincidencia de expresiones regulares.

Servicios de suscripción de prevención de brechas

Capture Advanced Threat Protection[1]	
Prestación	Descripción
Sandboxing multimotor	La plataforma de sandbox multimotor, que incluye sandboxing virtualizado, emulación de sistema completo y tecnología de análisis de nivel de hipervisor, ejecuta el código sospechoso y analiza su comportamiento, proporcionando una visibilidad completa de la actividad maliciosa.
Bloqueo hasta que haya un veredicto	A fin de evitar el acceso a la red de archivos potencialmente peligrosos, los archivos enviados a la nube para su análisis pueden retenerse en la pasarela hasta que se emita un veredicto.
Análisis de gran variedad de tipos de archivos	Soporta análisis de una amplia variedad de tipos de archivos, como los programas ejecutables (PE), DLL, PDFs, documentos MS Office, archivos, JAR y APK, así como múltiples sistemas operativos, como Windows, Android, Mac OS y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, inmediatamente se pone una definición a disposición de los firewalls con suscripción a SonicWall Capture y se envía a las bases de datos de definiciones de Gateway Anti-Virus e IPS y a las bases de datos de reputación de URL, IP y dominios en el transcurso de 48 horas.
Capture Client	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
Prevención de amenazas cifradas	
Prestación	Descripción
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/SSL sobre la marcha, sin necesidad de proxies, en busca de malware, intrusiones y filtraciones de datos, y aplica políticas de control de aplicaciones, URL y contenido para ofrecer protección contra las amenazas ocultas en el tráfico cifrado mediante SSL. Incluido con las suscripciones de seguridad para todos los modelos excepto SOHO. Para los modelos SOHO, se vende como una licencia independiente.
Inspección SSH	La inspección profunda de paquetes de SSH (DPI-SSH) descifra e inspecciona los datos que atraviesan los túneles SSH para prevenir ataques que utilicen SSH.
Prevención de intrusiones[1]	
Prestación	Descripción
Protección basada en contramedidas	El sistema de prevención de intrusiones (IPS) estrechamente integrado utiliza definiciones y otras contramedidas para escanear los datos útiles de los paquetes en busca de vulnerabilidades y exploits, cubriendo de este modo un amplio abanico de ataques y vulnerabilidades.
Actualizaciones automáticas de las definiciones	El equipo de investigación de amenazas de SonicWall investiga e implementa contramedidas IPS, actualizando continuamente una larga lista que cubre más de 50 categorías de ataques. Las nuevas actualizaciones se hacen efectivas en el acto, sin que sea necesario reiniciar los sistemas ni interrumpir su servicio.
Protección IPS entre zonas	Refuerza la seguridad interna al segmentar la red en múltiples zonas de seguridad con prevención de intrusiones para evitar la propagación de las amenazas de unas zonas a otras.
Detección y bloqueo de actividades de comando y control (CnC) procedente de ataques botnets	Identifica y bloquea el tráfico de comando y control originado en bots de la red local y dirigido a IPs y dominios identificados como propagadores de malware o conocidos como puntos de CnC.
Abuso/anomalía de protocolo	Identifica y bloquea ataques que abusan de los protocolos para intentar eludir el IPS.
Protección de día cero	Protege la red ante los ataques de día cero con actualizaciones constantes contra los últimos métodos y técnicas de exploits, que cubren miles de exploits individuales.
Tecnología antievasión	La amplia normalización de flujos, la descodificación y otras técnicas impiden que las amenazas puedan penetrar la red sin ser detectadas utilizando técnicas de evasión en las capas 2-7.
Prevención de amenazas[1]	
Prestación	Descripción
Antimalware en pasarela	El motor RFDPI analiza todo el tráfico entrante, saliente y dentro de una misma zona en busca de virus, troyanos, registradores de pulsaciones de teclas y otros tipos de malware en archivos de una longitud y un tamaño ilimitados en todos los puertos y flujos de TCP.
Protección antimalware de Capture Cloud	Los servidores de la nube de SonicWall disponen de una base de datos de decenas de millones de definiciones de amenazas que se actualiza continuamente y se utiliza para aumentar las capacidades de la base de datos de definiciones integrada, lo que proporciona a la tecnología RFDPI una amplia cobertura de amenazas.
Actualizaciones de seguridad las 24 horas	Las nuevas actualizaciones de amenazas se transfieren automáticamente a los firewalls con servicios de seguridad activos, donde se hacen efectivas inmediatamente sin necesidad de reiniciar el sistema ni interrumpir el servicio.
Inspección TCP bidireccional (sin procesar)	El motor RFDPI escanea flujos de TCP sin procesar en cualquier puerto y bidireccionalmente para detectar y prevenir las amenazas tanto entrantes como salientes.
Amplio soporte de protocolos	Identifica protocolos comunes, como HTTP/S, FTP, SMTP, SMBv1/v2, etc., que no envían datos en TCP sin procesar. Descodifica datos útiles para su inspección antimalware, incluso si no se ejecutan en puertos estándar bien conocidos.

Inteligencia y control de aplicaciones[1]	
Prestación	Descripción
Control de aplicaciones	Controla aplicaciones, o funciones de aplicaciones individuales, identificadas por el motor RFDPI mediante su cotejo con una base de datos en continuo crecimiento de más de miles de definiciones de aplicaciones. De este modo se aumentan la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controla las aplicaciones personalizadas creando definiciones basadas en parámetros o patrones específicos únicos de una aplicación en sus comunicaciones de red. Esto proporciona un mayor control sobre la red.
Gestión del ancho de banda de las aplicaciones	La gestión del ancho de banda de las aplicaciones asigna y regula de forma detallada el ancho de banda disponible para aplicaciones (o categorías de aplicaciones) críticas, a la vez que limita el tráfico de aplicaciones que no resulta esencial.
Control granular	Controla aplicaciones (o componentes específicos de una aplicación) basándose en programaciones, grupos de usuarios, listas de exclusión y una gama de acciones con una completa identificación de usuario mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.
Filtrado de contenido[1]	
Prestación	Descripción
Filtrado de contenido dentro y fuera	Aplique políticas de usos aceptables y bloquee el acceso a sitios Web HTTP/HTTPS que contengan información o imágenes inaceptables o improductivas con Content Filtering Service y Content Filtering Client.
Cliente de filtrado de contenido reforzado	Amplía el refuerzo de políticas para bloquear contenido de Internet para dispositivos Windows, Mac OS, Android y Chrome situados fuera del perímetro del firewall.
Controles granulares	Bloquean el contenido utilizando cualquier combinación de categorías. El filtrado puede programarse por hora del día, por ejemplo, durante el horario laboral o escolar, y aplicarse a usuarios individuales o grupos.
Almacenamiento en caché Web	Las clasificaciones de URL se almacenan en caché en el firewall de SonicWall, con lo que se reduce el tiempo de respuesta para el posterior acceso a sitios que se visitan con frecuencia a solo una fracción de segundo.
Respondedor CFS local	El respondedor CFS local puede implementarse como dispositivo virtual en nubes privadas con VMWare o Microsoft Hyper-V. De este modo, proporciona una opción de implementación flexible (equipo virtual ligero) de la base de datos de clasificaciones de CFS en varios casos de uso de redes de clientes que requieran una solución local dedicada capaz de acelerar la solicitud de clasificaciones de CFS y las correspondientes respuestas, que soporte una amplia lista de URLs permitidas/bloqueadas (+100.000 elementos), y que añada hasta 1000 firewalls SonicWall para búsquedas de clasificaciones de CFS.
Antivirus y antispyware reforzados[1]	
Prestación	Descripción
Protección en varios niveles	Utiliza las funciones del firewall, como la primera capa de defensa en el perímetro, junto con la protección de puntos terminales, a fin de bloquear los virus que penetran en la red por medio de portátiles, unidades de memoria flash y otros sistemas no protegidos.
Opción de aplicación automatizada	Asegúrese de que todos los equipos que accedan a la red tengan instalado y activo el software antivirus y/o certificado DPI-SSL apropiado. De este modo, eliminará los costes asociados habitualmente a la gestión de soluciones antivirus para equipos de escritorio.
Opción de instalación e implementación automatizadas	La implementación y la instalación máquina a máquina de clientes antivirus y antispyware se realiza de forma automática en toda la red, con lo que se minimiza la sobrecarga administrativa.
Antivirus de próxima generación	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar a un estado previo a la infección.
Protección antispyware	La potente función de protección antispyware analiza y bloquea la instalación de un completo conjunto de programas de spyware en equipos de escritorio y portátiles antes de que éstos transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.

[1] Requiere suscripción adicional
[2] Prestación no soportada en los firewalls de la serie NSv

Acerca de nosotros

SonicWall lleva más de 27 años combatiendo la industria del crimen cibernético y defendiendo a las empresas pequeñas, medianas y grandes de todo el mundo. Nuestra combinación de productos y partners nos ha permitido crear una solución automatizada de detección y prevención de brechas en tiempo real adaptada a las necesidades específicas de más de 500.000 organizaciones en más de 215 países y territorios, para que usted pueda centrarse por completo en su negocio sin tener que preocuparse por las amenazas. Para más información, visite **www.sonicwall.com** o síganos en Twitter, LinkedIn, Facebook e Instagram.

Partner Enabled Services
¿Necesita ayuda para planificar, implementar u optimizar su solución SonicWall? Los Partners de servicios avanzados de SonicWall están cualificados para proporcionarle servicios profesionales de clase mundial. Si desea obtener más información, visite www.sonicwall.com/PES.

Visión de conjunto de las prestaciones de SonicOS

Firewall

- Inspección dinámica de paquetes
- Inspección profunda de paquetes sin reensamblado
- Protección contra ataques DDoS (inundaciones UDP/ICMP/SYN)
- Soporte para IPv4/IPv6
- Autenticación biométrica para el acceso remoto
- Proxy DNS
- APIs REST

Descifrado e inspección TLS/SSL/SSH[2]

- Inspección profunda de paquetes para TLS/SSL/SSH
- Inclusión/exclusión de objetos, grupos o nombres de host
- Control SSL
- Controles DPI SSL granulares por zona o norma

Capture Advanced Threat Protection[2]

- Inspección de memoria profunda en tiempo real
- Análisis multimotor basado en la nube
- Sandboxing virtualizado
- Análisis de nivel de hipervisor
- Emulación de sistema completo
- Análisis de gran variedad de tipos de archivos
- Envío automatizado y manual
- Actualizaciones de inteligencia de amenazas en tiempo real
- Bloqueo hasta que haya un veredicto
- Capture Client

Prevención de intrusiones[2]

- Análisis basado en definiciones
- Actualizaciones automáticas de las definiciones
- Motor de inspección bidireccional en tiempo real
- Capacidad para reglas de IPS detalladas
- Refuerzo de GeoIP
- Filtrado de botnets con lista dinámica
- Coincidencia de expresiones regulares

Antimalware[2]

- Escaneo antimalware basado en flujos
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Inspección bidireccional
- Tamaño de archivo ilimitado
- Base de datos de malware en la nube

Identificación de aplicaciones[2]

- Control de aplicaciones
- Gestión del ancho de banda de las aplicaciones
- Creación de definiciones de aplicaciones personalizadas
- Prevención de filtración de datos
- Informes de aplicaciones mediante NetFlow/IPFIX
- Completa base de datos de definiciones de aplicaciones

Visualización y análisis del tráfico

- Actividad de los usuarios
- Aplicación/ancho de banda/amenaza
- Análisis basados en la nube

Filtrado de contenido HTTP/HTTPS Web[2]

- Filtrado de URL
- Puenteo de proxys
- Bloqueo según palabras clave
- Filtrado basado en políticas (exclusión/inclusión)
- Inserción de encabezado HTTP
- Gestión del ancho de banda según categorías de clasificación CFS
- Modelo de políticas unificadas con control de aplicaciones
- Content Filtering Client

VPN

- Secure SD-WAN
- VPN con aprovisionamiento automático
- VPN IPSec para conectividad entre emplazamientos
- Acceso remoto mediante VPN SSL y cliente IPSec
- Pasarela VPN redundante
- Mobile Connect para iOS, Mac OS X, Windows, Chrome, Android y Kindle Fire
- VPN basada en enrutamiento (RIP/OSPF/BGP)

Redes

- PortShield
- Jumbo frames
- Descubrimiento de rutas MTU
- Protocolización mejorada
- VLAN trunking
- Duplicación de puertos (NS*a* 2650 y superior)
- QoS de nivel 2
- Seguridad de puertos
- Enrutamiento dinámico (RIP/OSPF/BGP)
- Controlador inalámbrico SonicWall [1]
- Enrutamiento basado en políticas(ToS/metric y ECMP)
- NAT
- Servidor DHCP
- Gestión del ancho de banda
- Agregación de enlaces[1] (estática y dinámica)
- Redundancia de puertos[1]
- Alta disponibilidad A/P con state sync
- Agrupación (clústeres) A/A[1]
- Equilibrio de carga entrante/saliente
- Modo puente de capa 2[1], modo wire/virtual wire, modo tap, modo NAT
- Reconexión 3G/4G WAN[1]
- Enrutamiento asimétrico
- Compatibilidad con tarjetas Common Access Card (CAC)

VoIP

- Control QoS granular
- Gestión del ancho de banda
- DPI para tráfico VoIP
- Soporte de Gatekeeper H.323 y proxy SIP

Gestión y supervisión

- GUI Web
- Interfaz de línea de comandos (CLI)
- SNMPv2/v3
- Gestión e informes centralizados con SonicWall Global Management System (GMS)[2]
- Protocolización
- Exportaciones NetFlow/IPFIX
- Backup de configuración basado en la nube
- Plataforma de análisis de seguridad de BlueCoat
- Visualización de aplicaciones y ancho de banda
- Gestión de IPv4 e IPv6
- Informes externos (Scrutinizer)
- Pantalla de gestión LCD[1]
- Gestión de switches de las series Dell N y Dell X, incluidos switches en cascada[1]

Conectividad inalámbrica[1]

- WIDS/WIPS
- Prevención de puntos de acceso no autorizados
- Itinerancia rápida (802.11k/r/v)
- Selección de autocanal
- Análisis de espectro de radiofrecuencia
- Vista de planta
- Vista de topología
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Acceso limitado para usuarios invitados
- Portal para invitados LHM

Conectividad inalámbrica integrada (solo serie TZ)

- Banda dual (2,4 GHz y 5,0 GHz)
- Estándares inalámbricos 802.11 a/b/g/n/ac
- Detección y prevención de intrusiones inalámbricas
- Servicios inalámbricos para usuarios invitados
- Mensajería ligera en puntos de conexión
- Segmentación mediante puntos de acceso virtuales
- Portal cautivo
- ACL para la nube

[1] Prestación no soportada en los firewalls de la serie NSv
[2] Requiere suscripción adicional.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Si desea obtener más información, consulte nuestra página Web.
www.sonicwall.com

Datasheet-SonicOSplatform-US-VG-MKTG4136

SONICWALL®