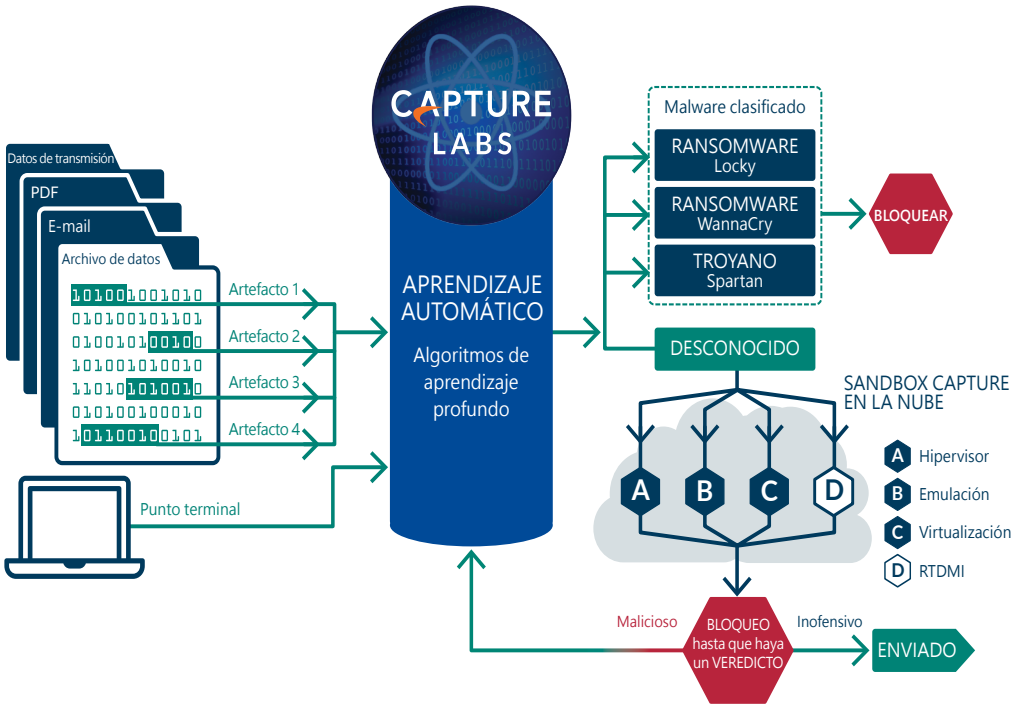
SonicOS 7 y servicios relacionados

Todos los firewalls físicos y virtuales de SonicWall, incluidos los de las series TZ, NS*a*, NS*v* y NS*sp*, se basan en la arquitectura de SonicOS. SonicOS utiliza nuestras tecnologías patentadas Reassembly-Free Deep Packet Inspection® (RFDPI), de paso único y baja latencia, y 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 eficaces prestaciones de seguridad.

Nuestra visión para la protección de las redes en el actual panorama de las amenazas cibernéticas, en continua evolución, consiste en la detección y la prevención de amenazas en tiempo real y automatizadas. Gracias a la combinación de tecnologías basadas en la nube e integradas, nuestros firewalls cuentan con una sólida protección validada en pruebas independientes y distinguida por ofrecer un nivel extremadamente alto de efectividad de la seguridad. Las amenazas desconocidas se envían para su análisis al sandbox multimotor de SonicWall basado en la nube Capture Advanced Threat Protection (ATP). Nuestra tecnología RTDMI™ aumenta la eficacia de Capture ATP. El motor RTDMI detecta y bloquea el malware y las amenazas de día cero, al inspeccionar directamente en la memoria. La tecnología RTDMI es precisa, minimiza los falsos positivos e identifica y mitiga los ataques sofisticados en los que las armas del malware se exponen durante menos de 100 nanosegundos.



FICHA TÉCNICA

En combinación con ella, nuestro motor RFDPI examina cada byte de cada paquete, inspeccionando el tráfico entrante y saliente directamente en el firewall. Al utilizar Capture ATP con la tecnología RTDMI en la plataforma SonicWall Capture Cloud junto con prestaciones integradas, como prevención de intrusiones, antimalware y filtrado Web/URL, nuestros firewalls de nueva generación detienen en la pasarela el malware, el ransomware y otras amenazas.

La introducción del sistema operativo SonicOS 7.1.1 impulsa aún más las prestaciones y la funcionalidad de los firewalls y las lleva al siguiente nivel. Además de ofrecer seguridad avanzada, gestión de políticas simplificada y prestaciones críticas de redes y de gestión —pensadas para las empresas distribuidas con oficinas pequeñas SD-Branch y empresas pequeñas y medianas—, SonicOS 7.1.1 incorpora prestaciones nuevas o mejoradas relacionadas con soporte de Wi-Fi 6, seguridad DNS, filtrado de contenido basado en la reputación e integración de control de acceso de red (NAC).

Paquetes de servicios de seguridad

Los servicios de seguridad SonicWall convierten el firewall en una solución de seguridad completa. Los servicios de seguridad están disponibles en tres paquetes que se activan por suscripción: Threat Protection, Essential Protection y Advanced Protection (protección contra amenazas, esencial y avanzada). (I) La suite de servicios SonicWall Threat Protection incluye en un paquete económico los servicios de seguridad básicos necesarios para garantizar que la red esté protegida frente a amenazas. (II) La suite de servicios SonicWall Essential Protection proporciona todos los servicios de seguridad necesarios para la protección frente a amenazas conocidas y desconocidas. (III) La suite de servicios SonicWall Advanced Protection ofrece prestaciones avanzadas para ampliar la seguridad de su red con servicios de seguridad esenciales en la nube.

Prestación	Protección contra amenazas	Essential Protection	Advanced Protection
Antivirus en pasarela, prevención de intrusiones, control de aplicaciones	✓	✓	✓
Content Filtering Service	✓	✓	✓
Antispam	!	✓	✓
Soporte 24x7	✓	✓	✓
Visibilidad de red	✓	✓	✓
Sandboxing multimotor Capture ATP	!	✓	✓
Tecnología RTDMI	!	✓	✓
Seguridad DNS	✓	✓	✓
Gestión en la nube	!	!	✓
Informes basados en la nube (7 días)	!	!	✓

✓ Forma parte del paquete. ! No está disponible con el paquete, pero se puede comprar por separado.

DASHBOARD MEJORADO

Dashboard mejorado	
Prestación	**Descripción**
Seguridad DNS	Utiliza el sistema de nombres de dominio (DNS) para bloquear las páginas web o las aplicaciones maliciosas, así como para filtrar el contenido peligroso o inadecuado.
Integración del control de acceso de red (NAC)	Proporciona a los clientes de SonicWall control de acceso a la red, mediante la integración con ClearPass de Aruba. Esta arquitectura convierte la seguridad estática en seguridad contextual para proporcionar una protección más flexible y de seguridad avanzada.
Integración de Wi-Fi 6	Integre y gestione los puntos de acceso SonicWave con Wi-Fi 6.
Mejoras de almacenamiento secundario PCS	Soporta captura de paquetes, TSR y datos de correlación de amenazas en el almacenamiento. Guarde en el almacenamiento los registros de amenazas y de auditoría, el flujo de aplicaciones, pcap.
Registro basado en token	Se trata de una cadena de texto que sustituirá en el archivo de bootstrap los datos de usuario y contraseña de MySonicWall utilizados para el proceso de bootstrapping en NS*v*, con el fin de automatizar las implementaciones masivas con información básica sobre la configuración y la licencia.
Bootstrapping NS*v*	Simplifique las implementaciones masivas en NS*v*; soporte en VMware, Hyper-V, AWS y Azure; licencia basada en token para un registro de producto simplificado; el archivo INIT incluye una configuración básica para que la instancia esté lista con un mínimo de preparación.
Dashboard mejorado	Dashboard con alertas útiles.
Vista de dispositivos mejorada con pantalla de vista frontal y trasera y estadísticas de almacenamiento del hardware	Ahora, el usuario puede ver desde la pestaña de inicio de la UI el estado en tiempo real del panel frontal, del panel trasero y de las estadísticas de uso del módulo de almacenamiento. Proporciona una experiencia similar a la obtenida físicamente delante del hardware.
Uso en tiempo real del sistema y del ancho de banda	Ahora, el usuario puede ver en tiempo real el uso que hace el sistema de los recursos principales y del ancho de banda en la red.
Resumen de la distribución del tráfico	Uso de la distribución del tráfico en el firewall del usuario, con actualización en tiempo real de las aplicaciones más utilizadas.
Resumen de los principales usuarios.	El resumen de los principales usuarios basado en sesiones permitidas o bloqueadas; por datos enviados y recibidos.
Resumen de las amenazas observadas	Resumen en tiempo real de las amenazas vistas dentro de la red del cliente, como virus, malware de día cero, spyware, vulnerabilidades y aplicaciones peligrosas.
Resumen de los servicios	Estado en tiempo real de los servicios de seguridad activados o desactivados, como IPS, GAV, Anti-Spyware, Capture ATP o DPI-SSL.
Información sobre los hosts infectados	Muestra en tiempo real el número total de hosts de la red que están infectados.
Información sobre ataques de misión crítica	Muestra en tiempo real el número total de ataques de misión crítica encontrados en la red.
Información sobre el tráfico cifrado	Muestra en tiempo real el total de tráfico cifrado que hay en la red.
Resumen de las aplicaciones más utilizadas	Muestra las aplicaciones más utilizadas en la red, con opciones adicionales para ordenarlas por sesión, bytes, bloques de regla de acceso, virus, spyware e intrusiones.
Resumen de las direcciones más usadas	Muestra los objetos de dirección más utilizados en la red, con opciones adicionales para ordenarlos por sesión, bytes, bloques de regla de acceso, virus, spyware e intrusiones.
Resumen de los principales usuarios	Muestra a los principales usuarios de la red, con opciones adicionales para ordenarlos por sesión, bytes, bloques de regla de acceso, virus, spyware e intrusiones.
Resumen de los sitios web con mejores calificaciones	Muestra los sitios web con mejor calificación, por sesión.
Resumen de las estadísticas de los principales países	Muestra las estadísticas de los principales países por sesión, tráfico rechazado, bytes enviados o bytes recibidos.
Resumen en tiempo real de las amenazas	Muestra las principales amenazas, con estadísticas separadas para virus, intrusiones, spyware y botnets.
Instantánea mejorada de punto de acceso	Muestra las estadísticas sobre el estado de los puntos de acceso de la red y estadísticas en tiempo real de clientes asociados.
Tasa de tráfico por punto de acceso	Proporciona el uso por parte de los puntos de acceso del ancho de banda en tiempo real.
Informes de clientes Wi-Fi	Proporciona un informe de clientes Wi-Fi en tiempo real basado en tipo de SO, frecuencia y un gráfico con principales clientes.
Supervisión de clientes Wi-Fi en tiempo real	Determina el equipo host, el tipo de SO, la frecuencia, la información sobre el punto de acceso y la transferencia de datos.
Información sobre los veredictos de Capture ATP	Muestra los veredictos de análisis de archivo emitidos por Capture ATP.
Información sobre tipos de archivos	Muestra los tipos de archivos, basándose en el informe de Capture ATP.
Información sobre la dirección de destino	Muestra los principales destinos que utilizan los archivos maliciosos.
Estadísticas de análisis de malware	Muestra estadísticas detalladas del análisis dinámico/estático por archivo.
Análisis de ubicación basado en el origen del ataque de día cero	Muestra el origen del ataque según los países.
Estadísticas de Capture ATP	Muestra información obtenida mediante Capture ATP sobre el total de archivos enviados, archivos analizados dinámicamente, archivos maliciosos y tiempo promedio de procesamiento.

Vista de topología de red	Muestra la topología de red, con hosts, puntos de acceso conectados en la red del usuario según el nombre del dispositivo, dirección mac y dirección IP.
Gestión basada en API	La gestión del firewall se basa en la API.
Asistente de usabilidad de SD-WAN	El asistente configura automáticamente en el firewall la política de SD-WAN.
Centro de notificaciones	Nuevo centro de notificaciones con resumen de amenazas, registros de eventos y alertas del sistema.
Ayuda en línea mejorada	Ayuda en línea con enlaces a la documentación técnica en todos los modelos.
Monitorización mediante SD-WAN	Muestra el rendimiento de los sondeos y las principales conexiones de la SD-WAN.
Utilidad Packet Monitor mejorada	Packet Monitor mejorada para incluir reglas de acceso, reglas NAT e información de enrutamiento.
Configuración del dispositivo de almacenamiento	Soporte para la configuración de módulos, incluyendo los módulos ampliados. Estadísticas de uso por módulos.
Capture Threat Assessment (CTA) 2.0	El nuevo informe CTA 2.0 soporta una nueva plantilla de informes con opciones personalizadas, como logo, nombre y secciones. Soporta el análisis de archivos y de malware. Estadísticas de la compañía por sección con el promedio global y del sector. Plantilla ejecutiva separada con recomendaciones.
Descarga de registros del sistema	Los registros del sistema, incluidos los registros de consola, se pueden descargar desde la sección de diagnósticos sin que el usuario necesite conectar el equipo al puerto de la consola para capturar los registros de esta. Así se simplifican los métodos de depuración y el tiempo necesario para la resolución de problemas.
Terminal SSH en IU	Se puede acceder a la terminal SSH desde la UI Web.
Utilidad de comprobación en GRID.	Esta utilidad permite comprobar las direcciones IP en GRID.
Utilidad de depuración	El usuario puede activar el modo de depuración dentro del propio firmware y ejecutar los comandos correspondientes desde la terminal SSH dentro de la UI.
Herramientas de diagnóstico del sistema	Más herramientas de diagnóstico, como GDB, HTOP y Linux Perf Tool.
Visión general de la red con Switch	SonicWall Switch permite obtener una vista física, una vista de lista y una vista de VLAN.
Uso de ancho de banda por SwitchPort	La información de SonicWall Switch muestra el uso de ancho de banda por puerto.
Estado WWAN	Muestra el estado WWAN del módem y de la red.

PRESTACIONES Y SERVICIOS DEL 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 e interconexión

Prestación	Descripción
Secure SD-WAN	Secure SD-WAN ofrece una alternativa a las tecnologías más caras, como MPLS, y permite a las organizaciones empresariales distribuidas crear, operar y gestionar redes seguras de alto rendimiento en emplazamientos remotos con el fin de compartir datos, aplicaciones y servicios, mediante 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, DPI2 Activa/Activa (A/A) y agrupada (clústeres) Activa/Activa. 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.

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 rutas basadas 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.
Integración con SonicWall Switch	Los primeros switches de SonicWall proporcionan una integración sin fisuras con los firewalls para la gestión y visibilidad de su red a través de una única consola.
Gestión de switches individuales y en cascada de las series N y X de Dell	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 desde redes sociales	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.
Soporte completo de API	Soporte completo de API para todas las secciones de la UI del firewall.
Escalabilidad de SD-WAN	Interfaces de túnel escalables para empresas distribuidas.

Gestión, informes y soporte

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.
Detección de malware orientada al cumplimiento	Analice los archivos sospechosos en su propio entorno, sin tener que enviar archivos o resultados a una nube de terceros.

Red privada virtual (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 WAN, 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.
Inspección de memoria profunda en tiempo real (RTDMI™)	SonicWall RTDMI es una tecnología y un proceso patentados utilizados por SonicWall Capture Cloud para identificar y mitigar hasta las amenazas más modernas y dañinas, incluidos los futuros exploits de Meltdown. Incluso detecta y bloquea el malware que no exhibe ningún comportamiento malicioso y que oculta sus armas mediante el cifrado.
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, PDF, 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.

Seguridad de endpoints

Prestación	Descripción
Protección de endpoints	Mediante las prestaciones de EDR SentinelOne de nueva generación, Capture Client aplica protección avanzada contra las amenazas en base al comportamiento. Integración de Capture ATP para una mayor efectividad de la seguridad, tiempos de respuesta más rápidos y un menor coste total de propiedad
Refuerzo DPI-SSL	Implementa certificados DPI SSL y permite el refuerzo de la inspección profunda de paquetes de tráfico cifrado (DPI-SSL) en los endpoints.
Refuerzo de endpoints	Dirige a los usuarios no protegidos a una página de descarga de Capture Client antes de que accedan a Internet, siempre que se encuentren detrás de un firewall.
Inicio de sesión SSO	Permite el uso de información del usuario a partir de los endpoints para las políticas SSO.

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.
Soporte para TLS 1.3	Soporte para TLS 1.3 para mejorar la seguridad general del firewall. Esto se implementa en la gestión del firewall, SSL VPN y DPI.

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 IP 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 resulten esenciales.
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 basado en reputación	Restringe y controla el contenido web al que puede acceder un usuario de internet. El filtrado de contenido basado en reputación proporciona una clasificación de reputación que prevé el riesgo de seguridad de una URL.
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 URL 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	Se asegura de que todos los equipos que accedan a la red tengan instalado y activo el software antivirus y/o el 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.
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.

Seguridad avanzada

Prestación	Descripción
Visibilidad de red	Proporciona una visibilidad granular sobre la topología de la red, además de información sobre los hosts.
Gestión en la nube	Gestiona los firewalls desde la nube, a través de la sección Network Security Manager de Capture Security Center.
Informes basados en la nube	Incluye informes a siete días basados en la nube.

[1] Requiere una suscripción adicional.

SERVICIOS HABILITADOS POR PARTNERS

¿Necesita ayuda para planificar, implementar u optimizar su solución de SonicWall? Los SonicWall Advanced Services Partners están formados para proporcionarle servicios profesionales de clase mundial.

Obtenga más información en **www.sonicwall.com/PES.**

Acerca de SonicWall

SonicWall proporciona una ciberseguridad estable, escalable y fluida para la era hiperdistribuida, así como 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 ciberseguridad para empresas, gobiernos y pymes en todo el mundo. Si desea obtener más información, visite www.sonicwall.com.

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

SONICWALL