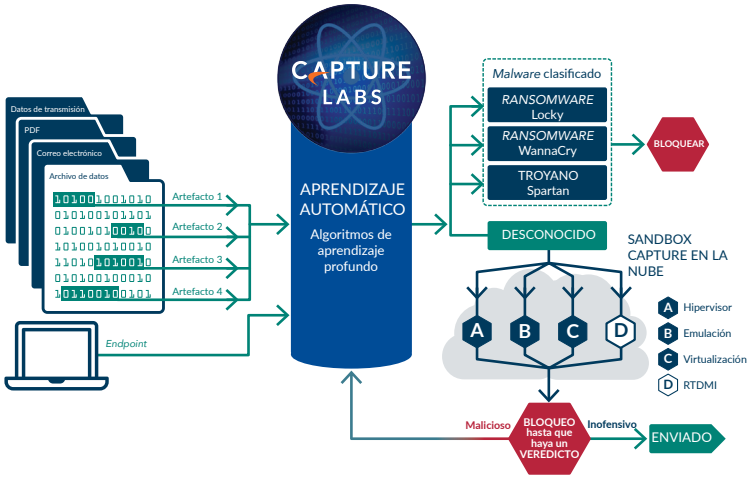
Ficha técnica de SonicOSX 7.0 y servicios

La arquitectura de SonicOSX constituye el núcleo de los firewalls físicos y virtuales de categoría empresarial de SonicWall, como los de las series NSa, NSv y NSsp. SonicOSX aprovecha nuestras tecnologías patentadas, de paso único y baja latencia, Reassembly-Free Deep Packet Inspection® (RFDPI) y Real-Time Deep Memory Inspection™ (RTDMI), pendiente de patente, para ofrecer una alta efectividad de seguridad validada por la industria, Secure SD-WAN, visualización en tiempo real, redes privadas virtuales (VPN) de alta velocidad y otras características de seguridad de gran solidez.

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 por pruebas independientes y distinguida por ofrecer un nivel extremadamente alto de efectividad de la seguridad. Las amenazas desconocidas se envían al *sandbox* multimotor basado en la nube Capture Advanced Threat Protection (ATP) de SonicWall para su análisis. Para mejorar Capture ATP está nuestra tecnología RTDMI™. El motor RTDMI detecta y bloquea el malware y las amenazas de día cero inspeccionando 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.

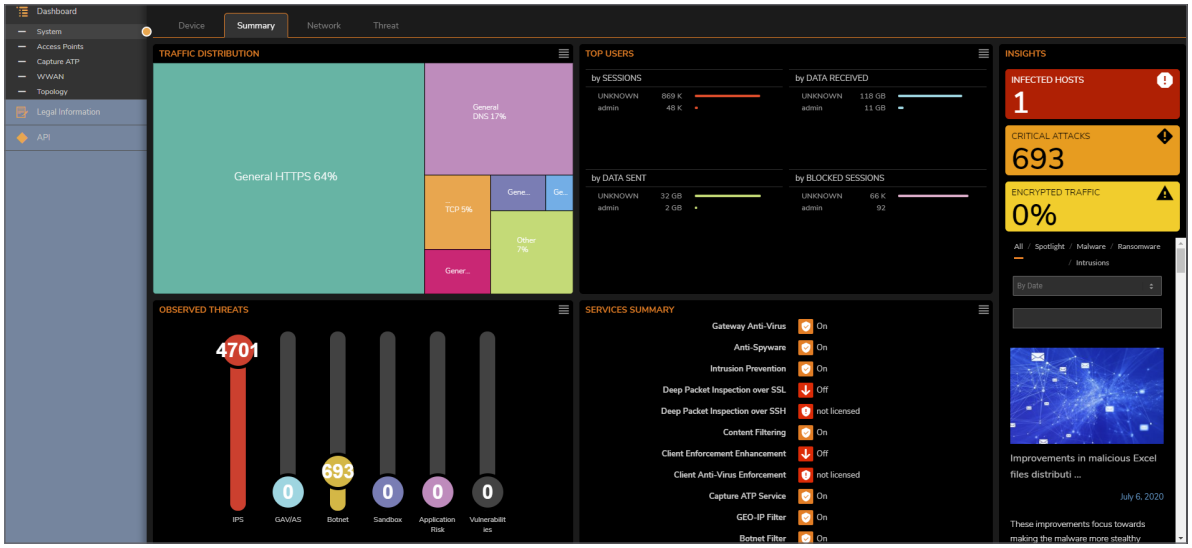
En combinación con ella, nuestro motor RFDPI examina cada byte de cada paquete, inspeccionando el tráfico entrante y saliente directamente en el firewall. Al utilizar Capture ATP con la tecnología RTDMI en la plataforma SonicWall Capture Cloud junto con prestaciones integradas, como prevención de intrusiones,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

La introducción del nuevo sistema operativo (SO) OSX 7.0 catapulta aún más las prestaciones y funciones de los firewalls de última generación al siguiente nivel. Desarrollada desde cero, la arquitectura de SonicOSX 7.0 incorpora una Política Unificada, que ofrece administración integrada de diversas políticas de seguridad para firewalls de categoría empresarial.



La Política Unificada permite proporcionar controles de capa 3 a 7 en una base única de reglas en cada firewall, ofreciendo así a los administradores una ubicación centralizada para configurar políticas. Viene con una nueva interfaz web nacida de un enfoque radicalmente diferente: se da relevancia al diseño pensando primero en el usuario. La interfaz basada en la web de SonicOSX presenta visualizaciones significativas de información sobre amenazas y muestra alertas factibles que le indican configurar políticas de seguridad contextual con simplicidad de "point-and-click".

Además de ser más fácil de usar, la nueva interfaz también es más atractiva que la versión clásica. En una vista de panel único de firewall, la interfaz presenta al usuario información sobre la efectividad de las diferentes reglas de seguridad. Esto permite al usuario modificar las reglas predefinidas para antivirus de puerta de enlace, *antispyware*, filtrado de contenido, prevención de intrusiones, filtrado de geo-IP e inspección profunda de paquetes del tráfico cifrado sin contratiempos. Con la Política Unificada, SonicWall ofrece una experiencia más optimizada que reduce los errores de configuración y el tiempo de implementación para lograr una mejor posición general de seguridad.



La Política Unificada brinda a las organizaciones la capacidad de controlar el tráfico dinámico que pasa por el firewall y ofrece visibilidad y perspectiva sobre las políticas dispares que afectan al antivirus de gateway, *antispyware*, filtrado de contenidos, prevención de intrusiones, filtrado de geoIP, inspección profunda de paquetes de tráfico cifrado, entre otros. Ayuda a simplificar las tareas de administración, reducir los errores de configuración y acelerar el tiempo de implementación, lo que contribuye a una mejora general del nivel de seguridad.

Esta actualización del SO admite múltiples instancias en firewalls de la serie NSsp. MultiInstancia es la siguiente generación de multi-tenancy, donde cada tenant está aislado con recursos informáticos dedicados para evitar la falta de recursos.

Paquetes de servicios de seguridad

Los servicios de seguridad de SonicWall convierten el firewall en una solución de seguridad completa. Los servicios de seguridad se ofrecen en tres paquetes de suscripción: Essential, Advanced y Premier.

- **SonicWall Essential Protection Service Suite** proporciona todos los servicios esenciales de seguridad necesarios para protegerse contra amenazas conocidas y desconocidas.
- **SonicWall Advanced Protection Service Suite** ofrece seguridad avanzada para ampliar la seguridad de su red con otros servicios de seguridad esenciales en la nube.
- **SonicWall Premier Protection Service Suite*** ofrece seguridad total con otros servicios de seguridad, visibilidad de la nube, análisis y servicios de *endpoints* para disfrutar de la protección definitiva.

FUNCIÓN	ESSENTIAL	ADVANCED	PREMIER*
Antivirus de gateway, prevención de intrusiones y control de aplicaciones	√	√	√
Servicio de filtrado de contenido	√	√	√
Antispam	√	√	√
Soporte 24x7	√	√	√
Visibilidad de la red	√	√	√
Sandboxing Capture ATP (multimotor)	√	√	√
Tecnología RTDMI	√	√	√
Seguridad básica de DNS	√	√	√
Gestión en la nube	!	√	√
Informes basados en la nube: 7 días	!	√	√
Análisis avanzados de la nube: informes virtuales de 365 días	!	!	√
Seguridad avanzada de DNS	!	!	√
Herramienta de comprobación del sistema de firewall	X	X	√
Paquete inicial de Cloud App Security	X	X	√
Paquete inicial de Capture Client	X	X	√
Soporte Premier	X	!	!

√ *Parte del paquete*
! *No disponible con el paquete, pero se puede adquirir por separado*
X *No compatible con el paquete*
* *Disponibilidad pendiente*

Funciones y servicios del firewall

PANEL MEJORADO	
Función	**Descripción**
Panel mejorado	Panel con alertas procesables.
Vista mejorada de dispositivos con visualización de vista frontal, vista posterior y estadísticas de almacenamiento del hardware	Ahora el usuario puede averiguar en la pestaña principal de la interfaz de usuario el estado en tiempo real del panel frontal, el panel posterior y las estadísticas de uso del módulo de almacenamiento. Esto le proporciona una experiencia similar a la de estar físicamente delante del hardware.
Uso del sistema en tiempo real y uso del ancho de banda	Ahora el usuario puede ver el uso en tiempo real del sistema del núcleo y el ancho de banda de la red.
Distribución resumida del tráfico	Uso de la distribución del tráfico en el firewall del usuario con actualización en tiempo real de la aplicación más utilizada.
Resumen de los principales usuarios	Resumen de los principales usuarios según sesiones permitidas o bloqueadas; por datos enviados y recibidos.
Resumen de amenazas observadas	Resumen en tiempo real de las amenazas observadas en la red del cliente, como virus, *malware* de día cero, *spyware*, vulnerabilidades y aplicaciones peligrosas.
Resumen de servicios	Estado en tiempo real de los servicios de seguridad habilitados o deshabilitados como IPS, GAV, Anti-Spyware, Capture ATP o DPI-SSL.
Información sobre hosts infectados	Muestra en tiempo real el número total de máquinas host infectadas en la red.
Información sobre ataques críticos	Muestra en tiempo real el número total de ataques de misión crítica en la red.
Información sobre el tráfico cifrado	Muestra en tiempo real el número total de tráfico cifrado en la red.
Resumen de las principales aplicaciones	Muestra las principales aplicaciones utilizadas en la red con opciones adicionales de clasificación por sesiones, bytes, bloques de reglas de acceso, virus, *spyware* e intrusiones.
Resumen de las principales direcciones	Muestra los principales objetos de direcciones utilizados en la red con opciones adicionales de clasificación por sesiones, bytes, bloques de reglas de acceso, virus, *spyware* e intrusiones.
Resumen de los principales usuarios	Muestra los principales usuarios utilizados en la red con opciones adicionales de clasificación por sesiones, bytes, bloques de reglas de acceso, virus, *spyware* e intrusiones.
Resumen de clasificaciones de los principales sitios web	Muestra las clasificaciones de los principales sitios web por sesión.
Resumen de las estadísticas de los principales países	Muestra las estadísticas de los principales países por sesión, tráfico reducido, bytes enviados o recibidos.
Resumen de amenazas en tiempo real	Muestra las principales amenazas con estadísticas independientes de virus, intrusiones, *spyware* y *botnet* por sesión.
Información para los veredictos de Capture ATP	Muestra los veredictos dados en el análisis de archivos por Capture ATP.
Información sobre tipos de archivos	Muestra el tipo de archivos según el informe de Capture ATP.
Información sobre direcciones de destino	Muestra los principales destinos utilizados por los archivos maliciosos.
Estadísticas del análisis de *malware*	Muestra datos estadísticos detallados sobre análisis de *malware* dinámico frente a estático por archivo.
Análisis del origen del ataque de día cero basado en la ubicación	Muestra el origen del ataque por países.
Estadísticas de Capture ATP	Muestra información del total de archivos enviados, archivos analizados dinámicamente, archivos maliciosos y tiempo medio de procesamiento utilizando Capture ATP.
Gestión basada en API	La gestión del firewall está basada en API.
Asistente de SD-WAN	Asistente para configurar automáticamente la política de SDWAN en el firewall
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 documentación técnica sobre todos y cada uno de los modelos.
Monitorización de SD-WAN	Muestra sondeos de rendimiento de SD-WAN y las principales conexiones.
Utilidad mejorada de supervisión de paquetes	Supervisión mejorada de paquetes que incluye información de firmas de aplicaciones y seguridad, política de seguridad, política de descifrado, política de rutas.
Capture Threat Assessment (CTA) 2.0	El nuevo informe CTA 2.0 admite la nueva plantilla de informes con opciones de personalización como el logotipo, el nombre y las secciones. Admite análisis de archivos y análisis de *malware*. Estadísticas de la empresa con la media del sector y global para cada sección. Plantilla ejecutiva independiente con recomendaciones.
Descargas de registros del sistema	Los registros del sistema incluyen registros de la consola que se pueden descargar desde la sección de diagnóstico sin que el usuario deba conectar el equipo al puerto de la consola para capturar sus registros. De este modo, se simplifican los métodos de depuración y tiempo para resolver problemas.
Terminal SSH en la interfaz de usuario	Se puede acceder al terminal SSH desde la interfaz de usuario web.
Herramientas útiles de diagnóstico del sistema	Compatibilidad con más herramientas de diagnóstico como GDB, HTOP y Linux Perf Tool.

POLÍTICA UNIFICADA

Función	Descripción
Resumen de políticas	Vista gráfica de las estadísticas utilizadas, no utilizadas, permitidas o denegadas sobre seguridad, NAT, ruta, descifrado o política DoS.
Resumen de objetos	Vista gráfica de objetos personalizados o predeterminados de dirección, zona, servicio, programas, coincidencia personalizada, aplicación, país, URI, sitio web o categoría web.
Resumen de grupos	Vista gráfica de objetos personalizados o predeterminados de dirección, zona, servicio, coincidencia personalizada, aplicación, país, URI, sitio web o categoría web.
Resumen de perfiles y firmas	Vista gráfica de perfiles personalizados o predeterminados como IPS, seguridad, DoS o página de bloqueo y resumen de firmas GAV o *antispyware*.
Búsqueda de políticas	Muestra la política de seguridad correspondiente introduciendo los parámetros de flujo necesarios como dirección IP, puerto, aplicación y sitio web.
Perfil de acciones de seguridad	El perfil de acciones de seguridad son las acciones adicionales que el usuario puede realizar tras la autorización o denegación de paquetes, como la aplicación de servicios de seguridad y gestión del ancho de banda.
Perfil de acciones de DoS	El perfil de acciones de DoS son las acciones adicionales que el usuario puede realizar tras la protección o la omisión de paquetes, como la aplicación de umbral de ataque y limitación de conexión.
Objeto de firmas antivirus	Firmas antivirus con más detalles sobre cada firma.
Objeto de firmas *antispyware*	Firmas antispyware con más detalles sobre cada firma.
Grupo de aplicaciones intuitivo	Grupo de aplicaciones que debe incluir múltiples firmas de aplicaciones con una experiencia de usuario mejorada.
Contador en vivo sobre política de seguridad	Permite capturar estadísticas en vivo sobre política de seguridad.
Concordancia de aplicaciones basada en políticas	Identificación de concordancias personalizadas y de aplicaciones basadas en directivas individuales.
Clonación	Clona la regla de seguridad existente en una nueva regla.
Edición selectiva de celdas	Capacidad para realizar la edición selectiva de celdas sobre la regla de seguridad sin abrirla. Reduce el número de clics del usuario.
En la sombra	Muestra reglas duplicadas y en la sombra dentro de cada directiva.
Agrupación de directivas por secciones	Agrupación de directivas por secciones para ayudar a los usuarios de las empresas que tienen miles de reglas de seguridad.
Agrupación personalizada de directivas	Agrupación de directivas por opciones personalizadas como zona, etiqueta, etc. para ayudar a los usuarios de las empresas que tienen miles de reglas de seguridad.
Política de descifrado	Política para inspeccionar el tráfico SSL/TLS.
Política sobre DoS	Política para proteger contra ataques DoS/DDoD, como inundaciones, Smurf.

MOTOR DE INSPECCIÓN PROFUNDA DE PAQUETES SIN REENSAMBLADO (RFDPI)

Función	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 proxys 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 para evitar que la red se utilice para distribuir *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

Función	Descripción
Compatibilidad total con API	Compatibilidad completa con API para todas y cada una de las secciones de la interfaz de usuario del firewall.
Escalabilidad SD-WAN	Interfaces de túnel escalables para empresas distribuidas.
Multi-Tenancy[2]	Habilite la asistencia de múltiples instancias en el firewall NSsp.
Vista de clientes de Multi-Tenancy[2]	Vea el uso de cada instancia y otras estadísticas relacionadas.

FIREWALL Y REDES (CONTINUACIÓN)	
Firmware independiente según cliente[2]	Capacidad para ejecutar firmware por separado en cada instancia y raíz.
Licencias de clientes desde la raíz[2]	Licencia de instancias secundarias desde la instancia raíz. Muestra la clave para cada instancia.
Secure SD-WAN	Secure SD-WAN es una alternativa a las tecnologías más caras, como MPLS, que 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)	Admite los modos[2] de alta disponibilidad Activa/Pasiva (A/P) con sincronización de estado, DPI[2] Activa/Activa (A/A) y agrupación (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 creación 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 desplegarse en modos Wire, Tap de red NAT 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 rutas basadas en un protocolo para dirigir el tráfico a la conexión WAN preferida con posibilidad de relevar a una WAN secundaria en caso de interrupción.
Calidad de Servicio (QoS) avanzada	Garantiza las comunicaciones críticas con etiquetado 802.1p y DSCP y reasignación 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 de switch de SonicWall	Los primeros *switches* de SonicWall que ofrecen una integración perfecta con los firewalls para una gestión desde una única consola y visibilidad de la red
Gestión de switches individuales y en cascada de las series N y X de Dell	Gestiona los ajustes de seguridad de los puertos adicionales, como Portshield, HA, PoE y PoE+, desde una única consola utilizando el panel de gestión del firewall para *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 simple y rápida de administrar las políticas de seguridad en todos los dominios de la red. Administre la política individual a un solo dominio o grupo de dominios.

GESTIÓN, INFORMES Y SOPORTE	
Función	**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* centrada en las normas	Analice los archivos sospechosos en su propio entorno sin enviar archivos ni resultados a una nube de terceros.
Match Object mejorado	Match Object admite la incorporación de aplicaciones con una experiencia de usuario mejorada.
Objetos basados en perfiles	Objetos de perfiles para seguridad de *endpoints*, gestión del ancho de banda, marcado QoS, filtro de contenido, opción DHCP y VPN AWS.
Reglas de seguridad mejoradas	Visualización de reglas mejorada para una experiencia de usuario intuitiva.
Ajustes de cuadrícula personalizables	Columnas personalizables y móviles dentro de la Política de seguridad, la Política NAT, la Política de rutas, la Política de descifrado y la Política de DoS.
Visualización de reglas activas e inactivas	Muestra las reglas que están activadas o desactivadas.

GESTIÓN, INFORMES Y SOPORTE (CONTINUACIÓN)	
Visualización de reglas usadas y no usadas	Muestra las reglas que se usan activamente o que no se usan.
Exportación de reglas de acceso	Exporta todas las reglas de acceso a un archivo CSV.
Contador en vivo sobre política de seguridad	Permite capturar estadísticas en vivo sobre política de seguridad.
Diagrama de reglas	Vista gráfica de una determinada política de seguridad, regla NAT y de enrutamiento que ayuda a encontrar estadísticas en tiempo real.
Reglas de seguridad para *endpoints*	Posibilidad de agregar reglas de seguridad para *endpoints* utilizando Capture Client.

REDES PRIVADAS VIRTUALES (VPN)	
Función	**Descripción**
VPN con aprovisionamiento automático	Simplifica y reduce al máximo la complejidad de las implementaciones de firewalls distribuidas automatizando el aprovisionamiento inicial de la gateway 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 a la serie TZ 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 correos electrónicos, archivos, ordenadores, sitios Intranet y aplicaciones desde una variedad de plataformas.
Gateway VPN redundante	Al utilizarse múltiples WANs, pueden configurarse 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 *endpoints* puede redireccionarse fácilmente a través de rutas alternativas.

RECONOCIMIENTO DE CONTENIDO/CONTEXTUAL	
Función	**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.
Correspondencia 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 violaciones de seguridad

CAPTURE ADVANCED THREAT PROTECTION[1]	
Función	**Descripción**
Sandbox 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 proceso pendiente de patente utilizado por SonicWall Capture Cloud para identificar y mitigar incluso las amenazas modernas más insidiosas, como los futuros *exploits* Meltdown. Incluso detecta y bloquea el *malware* que no presenta ningún comportamiento malicioso y oculta su armamento mediante 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 gateway hasta que se emita un veredicto.
Análisis de gran variedad de tipos de archivos	Permite el 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 X y entornos multinavegador.
Rápida implementación de definiciones	Cuando se detecta un archivo malicioso, se envía inmediatamente una definición a los firewalls con suscripciones a SonicWall Capture y 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.
Capture Client	Capture Client utiliza un motor de inteligencia artificial estático para determinar las amenazas antes de que puedan ejecutarse y regresar al estado previo a la infección.

PREVENCIÓN DE AMENAZAS CIFRADAS

Función	Descripción
Compatibilidad con TLS 1.3	Compatibilidad con TLS 1.3 para mejorar la seguridad general del firewall. Esto se implementa en la gestión del firewall, SSL VPN y DPI.
Descifrado e inspección TLS/SSL	Descifra e inspecciona el tráfico cifrado mediante TLS/SSL sobre la marcha, sin necesidad de proxys, 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 dentro del tráfico cifrado. 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]

Función	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]

Función	Descripción
Antimalware en gateway	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 analiza los flujos de TCP sin procesar en cualquier puerto y bidireccionalmente para detectar y prevenir amenazas entrantes y superarlas.
Amplio soporte de protocolos	Identifica protocolos comunes como HTTP/S, FTP, SMTP, SMBv1/v2 y otros, que no envían datos en TCP sin procesar. Descodifica las cargas útiles para la inspección de malware, incluso si no se ejecutan en puertos estándar conocidos.

INTELIGENCIA Y CONTROL DE APLICACIONES[1]

Función	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 miles de definiciones de aplicaciones. Esto aumenta la seguridad y la productividad de la red.
Identificación personalizada de aplicaciones	Controla las aplicaciones personalizadas creando definiciones basadas en parámetros específicos o patrones exclusivos de una aplicación en sus comunicaciones de red. Esto contribuye a tener un mayor control de 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 no esenciales.
Control granular	Controla las 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 usuarios mediante SSO a través de la integración de LDAP/AD/Terminal Services/Citrix.

FILTRADO DE CONTENIDO[1]

Función	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 la aplicación de políticas para bloquear contenido de Internet para dispositivos Windows, Mac OS, Android y Chrome situados fuera del perímetro del firewall.
Controles granulares	Bloquea 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.
Local CFS Responder	Local CFS Responder puede desplegarse como dispositivo virtual en nubes privadas basadas en VMWare o Microsoft Hyper-V. Esto proporciona flexibilidad de despliegue (VM ligera) de la base de datos de calificaciones de CFS en varios casos de uso de redes de clientes que requieran una solución específica *in situ* que acelere los tiempos de solicitud y respuesta de las calificaciones de CFS, admite un gran número de listas de URL permitidas/bloqueadas (+100 K) y agrega hasta 1000 firewalls de SonicWall para búsquedas de calificación de CFS.

ANTIVIRUS Y ANTISPYWARE OBLIGATORIOS[1]

Función	Descripción
Protección en varios niveles	Utiliza las funciones del firewall como la primera capa de defensa en el perímetro, junto con la protección de *endpoints*, para 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 transmitan datos confidenciales, lo que contribuye a aumentar la seguridad y el rendimiento de los equipos de escritorio.

SEGURIDAD AVANZADA

Función	Descripción
Seguridad avanzada de DNS	La seguridad de DNS proporciona mejor TTD (tiempo de detección) y mejora el TCO (coste total de propiedad). La seguridad de DNS inspecciona los campos de DNS para identificar dominios maliciosos y bloquear así la conexión en las primeras etapas del establecimiento de la conexión. SonicWall cuenta con petabytes de datos sobre amenazas que ayudan a clasificar los dominios como maliciosos y a reducir los falsos positivos.
Herramienta de comprobación del sistema de firewall	Identifique los riesgos y mejore el cumplimiento de normativas y la seguridad. Disponible en la interfaz de usuario del firewall, la herramienta Heath Check Tool supervisa constantemente la infraestructura de seguridad, las gateways, las tecnologías, las directivas y los ajustes de configuración en tiempo real.
Visibilidad de la red	Proporciona visibilidad granular de la topología de la red junto con información del host.
Gestión en la nube	Gestione los firewalls a través de la nube mediante el mosaico Network Security Manager de Capture Security Center.
Informes basados en la nube	Incluye informes de siete días basados en la nube

[1] *Requiere suscripción adicional*
[2] *Disponible solo en NSsp*

Acerca de SonicWall

SonicWall ofrece Ciberseguridad sin Límites, sin Perímetro para la era hiperdistribuida y una realidad laboral en la que todo el mundo usa tecnología móvil, a distancia y poco segura. Al conocer lo desconocido, proporcionar visibilidad en tiempo real y posibilitar una economía revolucionaria, SonicWall cierra la brecha comercial en materia de ciberseguridad para empresas, gobiernos y pymes de todo el mundo. Para más información, visite www.sonicwall.com

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 (Estados Unidos)
Encontrará más información en nuestro sitio web.
www.sonicwall.com

Datasheet-SonicOSX-COG-2758