

LÍNEA DE PRODUCTOS SONICWALL DESCRIPCIÓN RESUMIDA



Firewalls de próxima generación

Gama alta: NSp 15700

Firewall de múltiples instancias diseñado para grandes empresas distribuidas, centros de datos y MSP que ofrece protección de alta velocidad, alta densidad de puertos y verdadero aislamiento de clientes (*tenants*) con Política Unificada



Gama media: Serie SMA

NSa 9650/9450/9250/ 66505650, 46503650, 1492650

Eficacia y rendimiento de la seguridad validados por el sector para redes medianas, oficinas remotas y empresas distribuidas



Nivel básico: Serie TZ

TZ670/TZ570/TZ400/TZ350

Prevención de amenazas integrada y plataforma SD-WAN para pequeñas y medianas empresas e implementaciones de SD-Branch



Virtual: Serie NSv

Firewalls virtuales con modelos de licencias flexibles para proteger todos los componentes críticos de su infraestructura de nube pública y privada



Seguridad inalámbrica

Serie SonicWave

SonicWave 432e/432i/432o/ 231c/224w/231o

Seguridad y rendimiento preparados para la próxima ola de dispositivos inalámbricos, gestionados a través de la nube o el firewall



Acceso móvil seguro

Serie SMA SMA 8200v/7210/ 6210/5 (+), 410/210 (-)

Acceso a los recursos de la red y la nube de forma sencilla, segura y mediante políticas



Switch de acceso

SWS12-8/SWS12-8POE/SWS12-10FPOE/ SWS14-24/SWS14-24FPOE/SWS14-48/ SWS14-48FPOE

Proporciona conmutación inteligente para conectividad segura de última generación para pymes e implementaciones de SD-Branch



Serie Email Security

ESA 9000/7000/5000/ Software VM/Servicio en la nube

Una solución multicapa que protege su red contra las amenazas de correo electrónico avanzadas



Gestión y análisis

Capture Security Center

Global Management System (GMS)

Network Security Manager

Máximo control y visibilidad sobre su red



CAPTURE SECURITY appliance (CSa)

Comprobación de archivos *in situ* y prevención de *malware*.



Capture Client

Una plataforma cliente unificada que ofrece múltiples funciones de protección de *endpoints*, como protección frente al *malware* avanzado, entorno aislado o

sandboxing, inteligencia sobre vulnerabilidades de aplicaciones y restauración en caso de infección



Cloud App Security

Una solución CASB que ofrece seguridad de última generación para aplicaciones SaaS, como Office 365 y G Suite, para proteger el correo electrónico, los datos y las credenciales de los usuarios frente a las amenazas avanzadas y, al mismo tiempo, cumplir las normativas en la nube

Servicios de suscripción de firewall de próxima generación

Essential Protection Services Suite

proporciona todos los servicios esenciales de seguridad necesarios para protegerse de amenazas conocidas y desconocidas. Esto incluye Capture Advanced Threat Protection con tecnología RTDMI, antivirus para *gateways*, prevención de intrusiones y control de aplicaciones, servicio de filtrado de contenido, servicio *antispam* integral, visibilidad de la red y soporte 24x7.

Advanced Gateway Security Suite (AGSS) está disponible como servicio complementario para todos los firewalls SonicWall físicos y virtuales para proteger de las amenazas más avanzadas y desconocidas.

Incluidos en Advanced Gateway Security Suite (AGSS); en combinación con un firewall de próxima generación en TotalSecure Advanced Edition

- *Sandboxing* multimotor basado en la nube Capture Advanced Threat Protection (ATP)
- Antivirus y antispymware en pasarela
- Servicio de prevención de intrusiones
- Control de aplicaciones
- Servicio de filtrado de contenido/Web
- Soporte 24x7

Seguridad como servicio (SECaaS)

Externalice su seguridad de red con nuestra solución de llave en mano

Preguntas de evaluación

Firewalls de próxima generación

- ¿Puede seguir el ritmo del aumento del ancho de banda, que exige un rendimiento de varios gigabits?
- ¿Puede su firewall actual realizar inspecciones de amenazas a la velocidad de las amenazas entrantes?
- ¿Cuáles son sus criterios de requisitos de rendimiento?
- ¿Cuál es el número total de usuarios/redes tras el firewall?
- ¿Cuál es el número total de sesiones/conexiones a máximo rendimiento?
- ¿Cuántos sitios y usuarios remotos se conectarán al firewall?
- ¿Cómo mide la efectividad de sus controles de seguridad?
- ¿Qué tipo de conexión a Internet tiene? ¿De qué velocidad?
- ¿Qué hace para protegerse contra las nuevas amenazas, como los ataques de día cero?
- ¿Su *sandbox* es capaz de detectar y bloquear amenazas ocultas en la memoria profunda?
- ¿Cuántos motores incorpora su *sandbox*?
- ¿Su *sandbox* puede retener los archivos en la pasarela antes de liberarlos?
- ¿Sabe si el firewall de su organización inspecciona o no el tráfico HTTPS?
- ¿Ha sufrido interrupciones del servicio de red o periodos de inactividad a causa de la inspección del tráfico HTTPS?
- ¿Su firewall virtual es tan robusto como su firewall físico?
- ¿Cómo protege sus entornos de nube pública o privada?
- ¿Puede implementar funciones apropiadas de zonas de seguridad y microsegmentación en su red virtual?
- ¿Tiene visibilidad y control completos sobre su tráfico virtual?
- ¿Le interesaría reducir costes sustituyendo la tecnología MPLS por SD-WAN para disfrutar de redes privadas seguras?

Capture Client

- ¿Sus *endpoints* necesitan protección avanzada coherente contra el *ransomware* y las amenazas cifradas?
- ¿Con qué facilidad puede reforzar el cumplimiento de las políticas y la gestión de licencias en todos los *endpoints*?
- ¿Tiene dificultades con la visibilidad de sus *endpoints* y la gestión de su sistema de seguridad?
- ¿Su producto de seguridad de *endpoints* se conecta a un entorno de *sandbox*?
- ¿Puede catalogar las aplicaciones instaladas en los *endpoints* y saber cuántas vulnerabilidades contienen?
- ¿Su solución actual monitoriza continuamente el estado de salud de su sistema?
- ¿Puede revertir el daño causado por el *ransomware* a un estado limpio anteriormente conocido?
- ¿Tiene la capacidad de bloquear la conexión de dispositivos desconocidos y potencialmente infectados con los *endpoints*?

Cloud App Security

- ¿Utiliza O365 o G Suite?
- ¿Está utilizando Proofpoint o Mimecast para proteger O365/G Suite?
- ¿Está analizando el correo electrónico interno de O365?
- ¿Cuántas aplicaciones SaaS autorizadas utiliza su organización?
- ¿Tiene dificultades para cumplir las normativas de los datos almacenados en las aplicaciones SaaS?
- ¿Cómo sabrá si las credenciales de sus usuarios están comprometidas?
- ¿Tiene visibilidad de quién accede a los datos, desde dónde y cuándo? (BYOD)

Inspección de memoria profunda

El motor de Inspección de memoria profunda en tiempo real de SonicWall (RTDMI™), pendiente de patente, utiliza la Inspección de memoria profunda en tiempo real para detectar y bloquear de forma proactiva el malware de masas desconocido. Ahora disponible con el servicio de *sandbox* en la nube SonicWall Capture Advanced Threat Protection (ATP), el motor identifica y mitiga incluso las amenazas más modernas y dañinas, incluidos los futuros exploits Meltdown.

Seguridad inalámbrica

- ¿Sus empleados/*partners*/clientes se quejan de que la conexión Wi-Fi es lenta?
- ¿Cuál sería la máxima cantidad de usuarios inalámbricos simultáneos que podría soportar en un momento determinado?
- ¿Le preocupa el coste de añadir una solución inalámbrica segura a su red?
- ¿Hasta qué punto está familiarizado con el estándar inalámbrico 802.11ac Wave 2?
- ¿Necesita flexibilidad para administrar los puntos de acceso, la nube o la administración de firewalls?
- ¿Ha planificado su red WiFi de manera eficaz?
- ¿Necesitaría que los servidores de seguridad desengancharan los servidores de seguridad?
- ¿Le preocupa ofrecer funcionalidades de seguridad avanzadas en su red WiFi?
- ¿Son importantes para usted los servicios para usuarios invitados?
- ¿Necesitaría un portal con inicio de sesión personalizado para la incorporación de invitados?

Switch de acceso

- ¿Necesita *switches* de acceso con capacidad de gigabits para alimentar dispositivos con tecnología PoE?
- ¿Es importante para usted una postura de seguridad unificada con visibilidad y administración unificadas?
- ¿Se enfrenta al desafío de hallar soluciones con *switches* de terceros que funcionan con el ecosistema de SonicWall?

Acceso móvil seguro

- ¿Cuál es su actual estrategia de acceso para sus teletrabajadores?
- ¿Qué le parece aplica un enfoque de acceso a la red de confianza cero?
- ¿Cómo proporciona a los usuarios un acceso seguro a los recursos y las aplicaciones de la empresa alojados localmente y en la nube?
- ¿Puede ver a todos los usuarios y dispositivos que acceden a su red?
- ¿Cómo protege actualmente sus propiedades y servidores Web críticos de negocio?

Seguridad de correo electrónico

- ¿Le preocupan las amenazas avanzadas de correo electrónico, como el *ransomware*, el *spear-phishing* y el Business Email Compromise?
- ¿Su solución de seguridad del correo electrónico ofrece prestaciones de protección contra amenazas avanzadas?
- ¿Le preocupa que los mensajes de correo electrónico que contienen información confidencial puedan sufrir filtraciones?
- ¿Cómo cumple las normas, como GDPR, Sarbanes-Oxley, GLBA o HIPAA?
- ¿Le interesa ofrecer servicios de seguridad de correo electrónico gestionados a sus clientes? (MSSPs)

Gestión y análisis

- ¿Qué problemas podría resolver unificando sus soluciones de seguridad bajo una plataforma de gestión común que ofrezca una experiencia desde una sola consola?
- ¿A qué retos económicos y operativos se enfrenta a la hora de gestionar su infraestructura de seguridad?
- ¿Hasta qué punto cree que está en condiciones de demostrar el cumplimiento normativo en materia de seguridad cibernética, como PCI, HIPAA y el RGPD?
- ¿Cómo se vería afectada su seguridad si fuera capaz de detectar y responder mejor a las amenazas y los riesgos con velocidad y precisión?
- ¿Qué valor obtendrían usted y su equipo directivo si tuvieran visibilidad total de las amenazas y los riesgos cibernéticos que acechan a su negocio?

Obtenga más información en sonicwall.com