DESCRIPCIÓN DEL PRODUCTO SONICWALL DE UN VISTAZO

Firewalls de próxima generación

Gama alta: NS*sp* 12000
Serie NS*sp* 12800/12400
Seguridad ampliable y de vanguardia para grandes empresas distribuidas, centros de datos y proveedores de servicios y se apoya en la potencia de la inteligencia en el cloud

Gama media: Serie NS*a*
NS*a* 9650/9450/9250/ 6650/5650/4650/3650/2650
Eficacia y rendimiento de la seguridad validados por el sector para redes medianas, sucursales y empresas distribuidas

Nivel básico: Serie TZ
TZ600/TZ500/TZ400/TZ350/ TZ300/ SOHO 250/SOHO
Prevención de amenazas integrada y plataforma SD-WAN para pequeñas y medianas empresas y empresas distribuidas

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

Obtenga más información en: www.sonicwall.com/es-mx/products

Acceso móvil seguro

SMA Series SMA
EX9000/8200v/7200/ 6200/500v/400/200
Acceso sencillo, seguro y reforzado mediante políticas a los recursos de la red y de la nube

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)
Análisis
Máximo control y visibilidad sobre su red

Serie de aceleración WAN

WXA 6000 (SW)
WXA 5000 (VM)/500 (SW)
Mejore considerablemente el rendimiento de la transferencia de aplicaciones y aumente la productividad de los empleados

Capture Client

Una plataforma cliente unificada que ofrece múltiples funciones de protección de endpoints, como protección frente al malware avanzado, entorno aislado, control de dispositivos y restauración en caso de infección

Web Application Firewall (WAF)

Seguridad de aplicaciones Web, prevención de filtración de datos y cumplimiento normativo, de forma local o en la nube

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

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 antispyware 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

Inspeccione la memoria profunda

El motor de Inspección de memoria profunda en tiempo real de SonciWall (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.

Preguntas de evaluación

Firewalls de próxima generación

- ¿Cómo mide la efectividad de sus controles de seguridad?
- ¿Cuál es su plan para remediar las brechas de seguridad identificadas?
- ¿Cómo reduce el riesgo de las aplicaciones Web vulnerables a las que podrían acceder sus usuarios?
- ¿Qué tipo de conexión a Internet tiene? ¿De qué velocidad?
- ¿Debe sacrificar el rendimiento para disfrutar de un mayor nivel de seguridad de su red?
- ¿Qué hace para protegerse contra las nuevas amenazas, como los ataques de día cero?
- ¿En qué medida es capaz su equipo de poner parches a las vulnerabilidades en el transcurso de 12 horas desde la publicación de los parches?
- ¿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 que la mayoría de las sesiones Web están cifradas? ¿Su firewall puede descifrarlas e inspeccionarlas?
- ¿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?
- ¿Su firewall actual integra soporte de PoE/PoE+? ¿O necesita un switch para alimentar los dispositivos con tecnología PoE?
- ¿Le interesaría reducir costes sustituyendo la tecnología MPLS por SD-WAN para disfrutar de redes privadas seguras?
- ¿Necesita licencias basadas en suscripciones para los firewalls virtuales?

Capture Client

- ¿Sus puntos terminales 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 puntos terminales?
- ¿Tiene dificultades con la visibilidad de sus puntos terminales y la gestión de su sistema de seguridad?
- ¿Su producto de seguridad de puntos terminales se conecta a un entorno de sandbox?
- ¿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?

Web Application Firewall

- ¿Cómo protege actualmente sus propiedades y servidores Web críticos de negocio?
- ¿Qué medidas de seguridad implementa para ayudar a cumplir los requisitos de seguridad de la PCI?

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)

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?

Acceso móvil seguro

- Actualmente, ¿su organización está trasladando o tiene previsto trasladar sus aplicaciones y recursos de negocio a la nube?
- ¿Está proporcionando a sus usuarios un inicio de sesión único unificado para aplicaciones in situ y en la nube?
- ¿Sus empleados utilizan Dropbox o su correo electrónico personal para compartir archivos?
- ¿Sus empleados gestionan múltiples URLs y contraseñas?
- ¿Cuál es su estrategia de movilidad/BYOD actual?
- ¿Puede ver todos los dispositivos que acceden a su red?

Seguridad de correo electrónico

- ¿Le preocupan las amenazas avanzadas de correo electrónico, como el ransomware, el spear-phishing y el compromiso del correo electrónico de negocio?
- ¿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, HIPPA y el RGPD?
- ¿Cómo se vería afectada su seguridad si fuera capaz de detectar y responder mejor a las amenazas y los riegos 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?

Aceleración WAN

- ¿Su organización tiene múltiples ubicaciones de oficinas remotas? ¿Cuántas?
- ¿Las oficinas están interconectadas mediante una conexión VPN o WAN dedicada (MPLS)?
- ¿Sus empleados utilizan aplicaciones como Microsoft Windows File Sharing, SharePoint, Office o FTP?
- ¿Le gustaría reducir el consumo y el coste del ancho de banda sin necesidad de pagar por aumentar la capacidad?

Obtenga más información en: www.sonicwall.com/es-mx/products

Datasheet-SonicWallProductLineAtAGlance-US-VG-MKTG5159

SONICWALL®