FICHA TÉCNICA

Cloud Secure Edge

Acceso remoto y mayor seguridad

SonicWall Cloud Secure Edge™ es una solución de Security Service Edge (SSE), moderna y nativa de la nube, que resuelve las limitaciones de los dispositivos de red antiguos, gracias a un enfoque unificado y escalable que protege el acceso. Permite a organizaciones compuestas por una gran variedad de usuarios (empleados, proveedores y otros usuarios externos, etc.) conectarse de forma segura y fluida a recursos privados y de Internet desde cualquier dispositivo y ubicación.

Al consolidar en una única plataforma de nube funciones clave de red y seguridad, como VPN de acceso remoto, proxy web y firewalls, Cloud Secure Edge refuerza la seguridad de su organización y le permite adoptar una estrategia de seguridad proactiva, sin que eso afecte a la experiencia del usuario final.

Nota: Los clientes que ya utilizan firewalls SonicWall Gen 7 y más recientes pueden conectarse a Cloud Secure Edge directamente y gestionar las políticas de acceso fácilmente desde un dashboard unificado.

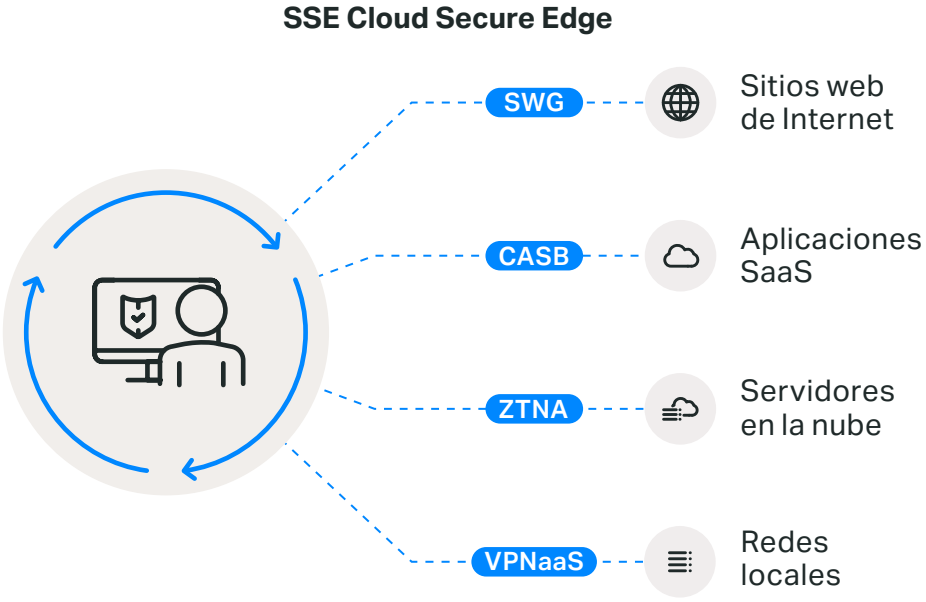


Figura 1: SonicWall Cloud Secure Edge protege el acceso a cualquier recurso desde cualquier dispositivo.

SONICWALL®

¿Por qué utilizar SonicWall Cloud Secure Edge?

Facilidad de gestión e implementación
Puede utilizar Cloud Secure Edge de forma individual o añadirla a sus firewalls SonicWall Gen 7 o más recientes existentes como suscripción mensual. Es ideal para MSPs y organizaciones que se ocupan de su propia seguridad, cuyos recursos se encuentran sobreexplotados, y que buscan un TCO reducido y un ROI rápido. Al iniciar sesión en Cloud Secure Edge por primera vez, los administradores pueden seguir un asistente guiado de tres pasos para establecer su primer túnel VPNaaS seguro, acelerando así la amortización.

Protección contra amenazas
Cloud Secure Edge incluye controles de seguridad Zero Trust necesarios para plantillas híbridas y remotas que requieren acceso a recursos sensibles privados y de Internet para realizar su trabajo desde cualquier lugar. Utiliza una tecnología única basada en la puntuación de la fiabilidad centrada en los dispositivos y las identidades y en criptografía de corta duración para proporcionar una seguridad líder en el sector y una excelente experiencia de usuario.

Rendimiento y privacidad
Cloud Secure Edge está diseñada desde cero para proporcionar un elevado nivel de rendimiento al tiempo que garantiza la privacidad. El administrador tiene el control total de sus datos y se asegura de que los usuarios disfruten de la conexión más natural y eficiente posible para maximizar la productividad, la protección de los datos y la privacidad.

Casos de uso comunes

Modernización de VPN/FW con ZTNA
En lugar de utilizar herramientas básicas, como firewalls y VPNs antiguas, para proteger los recursos corporativos, Cloud Secure Edge permite el acceso de mínimo privilegio a aplicaciones y servidores específicos basándose en dos factores contextuales en tiempo real combinados: la fiabilidad de los usuarios y dispositivos y la sensibilidad de los recursos.

Cloud Secure Edge está basada en la nube y puede aplicarse tanto de forma independiente como en combinación con infraestructuras de seguridad preexistentes.

Defensa contra las amenazas de Internet y el compromiso de credenciales
SonicWall ha implementado POPs de alto rendimiento en el borde global para garantizar el enrutamiento más eficiente y directo y al mismo tiempo aplicar controles de refuerzo coherentes con el fin de ofrecer protección contra todos los tipos de ataques o exposición a riesgos. Gracias a ello, nuestra solución no solo brinda una protección sencilla y efectiva contra los ataques de phishing y los sitios web maliciosos, sino que además permite aplicar funciones de filtrado de contenido según se desee. Asimismo, verifica — tal y como debería ser — la seguridad de los dispositivos antes de conceder el acceso.

Protección de usuarios de alto riesgo (usuarios externos / BYOD / contratistas)
Proporcione a los usuarios externos un acceso sencillo y seguro únicamente a los recursos específicos que necesitan, evitando así el sobreaprovisionamiento. Cloud Secure Edge garantiza el acceso no solo en función de la seguridad del usuario y el dispositivo, sino también según su rol y su nivel de autorización. Ofrece una gestión sencilla con grupos y roles que pueden ser preidentificados y aplicados según sea necesario desde una consola central. No es necesario aplicar parches ni configurar el hardware— nunca.

Licencias

Cloud Secure Edge está disponible para su compra como Secure Private Access (acceso a recursos en redes internas) y Secure Internet Access (acceso a recursos del Internet público).

1. **Secure Private Access proporciona dos prestaciones fundamentales:**
   - ZTNA basado en túneles (también llamado VPN de nube o VPNaaS): Acceso seguro a segmentos específicos de la red.
     ZTNA basado en proxy: Acceso seguro a recursos privados, como aplicaciones HTTP internas y servicios TCP.

2. **Secure Internet Access proporciona las siguientes prestaciones fundamentales:**
   - Broker de seguridad de acceso a la nube (CASB): Refuerzo de políticas de fiabilidad de los dispositivos para acceder a las aplicaciones SaaS.
   - Pasarela web segura (SWG): Filtrado de contenido web para bloquear el malware y otras amenazas ocultas en el tráfico web cifrado.

Hay disponibles SKUs de Secure Private Access (SPA) y Secure Internet Access (SIA) en dos categorías: Básico y avanzado. Las licencias se venden por usuario.

Prestaciones comunes

Plano de datos de alto rendimiento
Arquitectura de borde dinámica para proporcionar conexiones rápidas y fiables a usuarios de todo el mundo

Soporte nativo para todos los sistemas operativos de cliente
Escritorio (Windows, macOS, Linux) y móvil (iOS, Android, ChromeOS)

Interfaz de gestión en la nube
Para que los administradores de TI y de seguridad configuren la conectividad Zero Trust

Puntuación de la fiabilidad
Cuantifique el nivel de fiabilidad y riesgo asociados a sus usuarios y dispositivos

Visibilidad accionable
Una visión completa del riesgo del usuario/dispositivo y de la aplicación/el recurso

Refuerzo continuo de las políticas
En base a la sensibilidad de los recursos, independientemente de la ubicación del usuario

Integraciones
Se integra con las herramientas existentes (IDP, EDR, MDM, SIEM)

Conector de firewalls SonicWall
Integración lista para usar con los firewalls Gen 7 en modo global con 7.1.2+

Gestión multi-tenant
Políticas basadas en la nube para la gestión multi-tenant

Usuario y dispositivos

Inicio de sesión único
Utilice el SSO corporativo con creación de usuarios justo a tiempo

Gestión de la seguridad
Analice la seguridad de un dispositivo, como el firewall, el cifrado del disco, el bloqueo de pantalla, la versión del sistema operativo, etc.

Perfiles de fiabilidad
Personalice los factores y los efectos de las políticas en base a grupos de usuarios y dispositivos

Resolución personalizada
Configure las instrucciones para la resolución de la seguridad de los dispositivos, como los mensajes y enlaces, que se muestran a sus usuarios finales

Visibilidad y cumplimiento normativo

Flujo de eventos en tiempo real
Monitorice un flujo en tiempo real de actividades de los usuarios y dispositivos

Informes sobre la seguridad de los dispositivos
Haga un seguimiento de todos los dispositivos— gestionados y no gestionados — que acceden a los recursos corporativos, así como de su seguridad

Informes sobre las actividades del administrador
Registre toda la actividad del administrador en el Centro de comandos en la nube

Operaciones y automatización

API RESTful
Endpoint RESTful para configurar objetos Cloud Secure Edge en el plano de control

Clientes API—Pybanyan, Terraform
Biblioteca de Python y Terraform para la automatización y la gestión

Registro de dispositivos sin necesidad de intervención
Implemente la aplicación de Cloud Secure Edge en su flota de dispositivos sin necesidad de intervención por parte de los usuarios finales

	Secure Private Access		Secure Internet Access	
PRESTACIÓN	BÁSICO	AVANZADO	BÁSICO	AVANZADO
Acceso seguro a la red				
Túnel ZTNA (VPNaaS) para permitir el acceso a redes específicas	●	●		
Proxy ZTNA para una conexión segura a aplicaciones HTTP internas y servicios TCP		●		
Redes (rangos RFC-1918) y dominios (servidores DNS internos) privados	●	●		
Tunelización dividida a subredes y dominios específicos (privados o públicos)	●	●		
Tunelización completa para todo el tráfico gracias a Private Edge		●		
Políticas de red / capa 4 basadas en CIDRs y FQDNs	●	●		
Acceso seguro a recursos privados				
Acceso a sitios web internos utilizando flujos de OpenID Connect solo con navegador		●		
SSH a servidores Linux		●		
RDP a equipos Windows		●		
Clientes nativos para acceder a servidores de bases de datos como PostgreSQL y MySQL		●		
Cliente Kubernetes para acceder a un clúster		●		
Autenticación basada en certificados SSH, autorización de responsables y registros de auditoría		●		
Políticas de capa 7 para acceder a APIs, páginas web		●		
Protección contra las amenazas de Internet				
Seguridad de capa de DNS mediante el bloqueo de los dominios con malware, phishing, botnet y otros riesgos			●	●
Categorización de contenidos			●	●
Bloqueo personalizado			●	●
Seguridad de las aplicaciones SaaS				
Broker de seguridad de acceso a la nube (CASB) para reforzar las políticas de fiabilidad de los dispositivos para las aplicaciones SaaS				●
Visibilidad de las aplicaciones en la nube / TI en la sombra				●
Listas de IPs permitidas para aplicaciones en la nube mediante SonicWall Edge	●	●		●
Fiabilidad de los dispositivos para Okta				●
Fiabilidad de los dispositivos para Azure AD				●
Fiabilidad de los dispositivos para otros IDPs, como OneLogin, Jumpcloud				●
Servicio de filtrado de contenido web				
Pasarela web segura (SWG) | Filtrado de contenido mediante DNS			●	●
Pasarela web segura (SWG) | Filtrado de amenazas mediante DNS			●	●
Pasarela web segura (SWG) | Filtrado de riesgos mediante URL				●
Pasarela web segura (SWG) | Filtrado Geo-IP				●
Usuarios y dispositivos				
Autenticación sin contraseña mediante la federación de IDPs		●		●
Acceso reforzado mediante políticas desde dispositivos no registrados con un certificado de dispositivo de confianza		●		●
Acceso sin clientes		●		●
Cuentas de servicios (tokens API para el acceso programático, como scripting y automatización a través del plano de datos)		●		
Integración de SCIM para gestionar las asignaciones de los usuarios		●		●

SONICWALL

Integraciones de EDR (p.ej. CrowdStrike, SentinelOne, Microsoft Defender)		●		●
Integraciones de MDM/UEM (p.ej. JAMF, Kandji, Jumpcloud, Intune, Workspace One)		●		●
Visibilidad y cumplimiento normativo				
Integración de SIEM (p.ej. Splunk, Elastic, Sumo Logic)	●			●
Descubrimiento de redes privadas (aplicaciones no aprobadas a las que acceden los usuarios o dispositivos)	●			N/D
Descubrimiento de recursos de IaaS	●			N/D
Descubrimiento de aplicaciones de SaaS	N/D			●
Operaciones y automatización				
Implementación Private Edge: hospede la pasarela de SonicWall con reconocimiento de identidad en su infraestructura		●	N/D	N/D
Servicios y soporte				
Soporte 24x7	●	●	●	●
Soporte Premier		Adicional		Adicional
Servicios de implementación remota		Adicional		Adicional

Resumen

Como solución SSE revolucionaria basada en la nube, SonicWall Cloud Secure Edge es mucho más que una simple forma de sustituir los dispositivos perimetrales anticuados y obsoletos. Constituye un enfoque escalable y moderno para proteger la conectividad entre los usuarios, Internet y los recursos internos. Al verificar continuamente a los usuarios, los dispositivos, las aplicaciones y los recursos, ofrece un auténtico acceso Zero Trust a los empleados y usuarios externos, estén donde estén.

Cloud Secure Edge, que se implementa fácilmente a través de los firewalls SonicWall, también ofrece servicios de gestión multitenant que se adaptan a organizaciones de todos los tamaños y a los MSPs que les prestan servicio. Con Cloud Secure Edge, las organizaciones pueden hacer frente de forma eficaz a las brechas de seguridad, ofrecer una experiencia superior al usuario final y adoptar un enfoque proactivo y de limitación de riesgos para las redes y la seguridad. ¿Está preparado para mejorar y proteger el acceso en toda su organización? Hable con nuestro equipo hoy o solicite una demostración.

Si desea añadir Cloud Secure Edge a sus firewalls SonicWall Gen 7 existentes, póngase en contacto con su ejecutivo de cuenta.

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | Si desea obtener más información, consulte nuestra página web.

© 2025 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.
SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. y/o sus filiales en EE. UU. y/u otros países. Las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos propietarios. La información incluida en este documento se proporciona en relación con los productos de SonicWall Inc. y/o sus filiales. No se otorga mediante este documento, ni en relación con la venta de productos SonicWall, ninguna licencia, expresa ni implícita, por doctrina de los propios actos ni de ningún otro modo, sobre ningún derecho de propiedad intelectual. A excepción de lo establecido en los términos y condiciones tal y como se especifican en el contrato de licencia de este producto, SonicWall y/o sus filiales no asumen ninguna responsabilidad y rechazan cualquier garantía expresa, implícita o legal en relación con sus productos, incluidas, entre otras, las garantías implícitas de comercialización, adecuación para un determinado propósito o no violación de derechos de terceros. SonicWall y/o sus filiales no se harán responsables en ningún caso de daños directos, indirectos, consecuentes, punitivos, especiales ni incidentales (incluidos, sin limitación, los daños relacionados con la pérdida de beneficios, la interrupción del negocio o la pérdida de información) derivados del uso o de la incapacidad de utilizar el presente documento, incluso si se ha advertido a SonicWall y/o sus filiales de la posibilidad de que se produzcan tales daños. SonicWall y/o sus filiales no ofrecen declaración ni garantía alguna con respecto a la precisión ni a la integridad de la información contenida en el presente documento y se reservan el derecho de modificar las especificaciones y las descripciones de productos en cualquier momento y sin previo aviso. SonicWall Inc. y/o sus filiales no se comprometen a actualizar la información contenida en el presente documento.

Solution Brief - SonicPlatform

sonicwall.com

SONICWALL®