Cloud Secure Edge

Acceso remoto y mayor seguridad

SonicWall Cloud Secure Edge™, antes conocida como Banyan Security, es una solución SSE (Security Service Edge) altamente efectiva y de fácil adopción que permite a su personal acceder de forma segura a cualquier recurso desde cualquier dispositivo. Proporciona acceso zero trust sencillo y seguro a recursos privados y de Internet para todos sus empleados y usuarios externos, independientemente de la ubicación de su red. Combina la funcionalidad de múltiples dispositivos de red tradicionales — VPN de acceso remoto, proxy web, firewall, etc. — en una solución unificada basada en la nube, mejorando la seguridad y la experiencia de usuario de todo el personal.

Nota: Los clientes con firewalls SonicWall Gen 7 ya implementados pueden conectarlos a Cloud Secure Edge directamente y gestionar las políticas de acceso a través de un dashboard unificado.

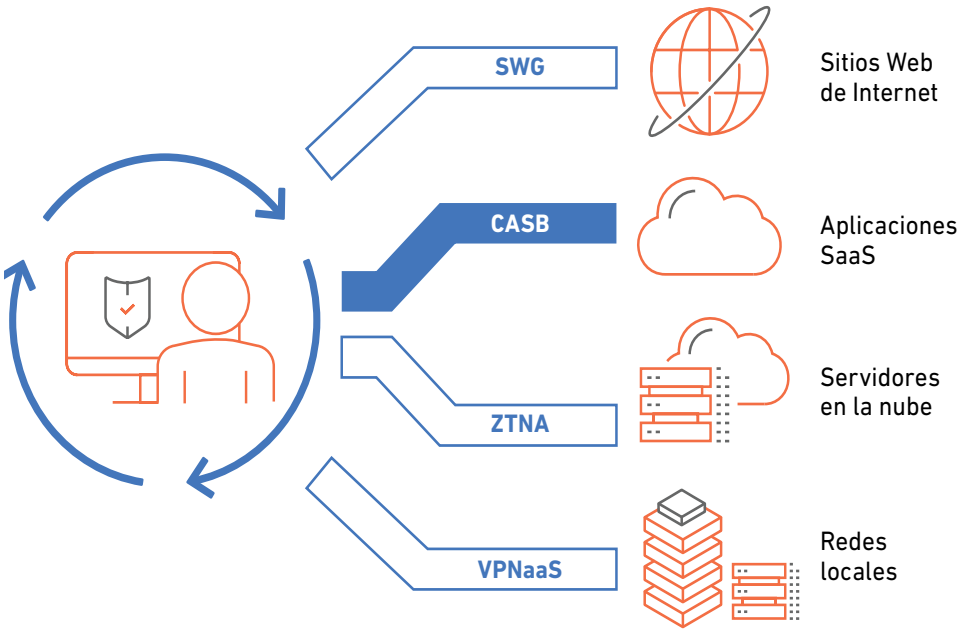

Figura 1: SonicWall Cloud Secure Edge protegiendo el acceso a cualquier recurso desde cualquier dispositivo

FICHA TÉCNICA

¿Por qué SonicWall Cloud Secure Edge?

FACILIDAD DE IMPLEMENTACIÓN Y GESTIÓN

Puede utilizar Cloud Secure Edge de forma individual o añadirla a sus firewalls SonicWall Gen 7 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.

PROTECCIÓN CONTRA AMENAZAS MODERNAS

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 VPNs/FWs 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.

Se trata de una solución basada en la nube que 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 / M&A)

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 tres prestaciones fundamentales:
   - Seguridad de capa de DNS (DNS): Protección contra amenazas a nivel de dominio mediante el bloqueo de dominios maliciosos y el refuerzo de políticas de uso aceptables.
   - 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 CSE 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 Banyan 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**
Prestaciones fundamentales				
Túnel ZTNA (VPNaaS) para permitir el acceso a redes específicas	✓	✓		
Proxy ZTNA para una conexión segura a aplicaciones HTTP internas y servicios TCP		✓		
Seguridad de capa de DNS para ofrecer protección contra las amenazas de Internet			✓	✓
Broker de seguridad de acceso a la nube (CASB) para reforzar las políticas de fiabilidad de los dispositivos para las aplicaciones SaaS				✓
Pasarela web segura (SWG) avanzada para eliminar el malware y otras amenazas ocultas en el tráfico web cifrado				✓
Acceso seguro a la red				
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	✓	✓		
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				
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				
Filtrado URL				✓
Protección contra malware				✓
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)		✓		✓

SONICWALL

Usuarios y dispositivos (Continuación)				
Integración de SCIM para gestionar las asignaciones de los usuarios		✓		✓
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

SonicWall Cloud Secure Edge es una solución Security Service Edge que combina un TCO líder en el sector con seguridad zero trust de clase empresarial. Proporciona acceso zero trust sencillo y seguro a recursos privados y de Internet para empleados y usuarios externos, independientemente de su ubicación física o del dispositivo que utilicen. Cloud Secure Edge combina la funcionalidad de múltiples dispositivos de red tradicionales — VPN de acceso remoto, proxy web, firewall, etc. — en una solución multi-tenant unificada y basada en la nube que es fácil de implementar y de gestionar, maximizando el ROI para organizaciones de todos los tamaños y sus clientes.

¿Desea obtener más información sobre SonicWall Cloud Secure Edge? Empiece aquí.

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

Acerca de SonicWall

SonicWall es una empresa pionera en ciberseguridad, con más de 30 años de experiencia y un enfoque firmemente centrado en sus partners. Gracias a su capacidad de crear, escalar y gestionar la seguridad en tiempo real en entornos de nube, híbridos y tradicionales, SonicWall puede proporcionar de forma rápida y económica soluciones de seguridad creadas específicamente para respaldar a cualquier organización de cualquier parte del mundo. Basándose en datos de su propio centro de investigación de amenazas, SonicWall ofrece protección sin fisuras contra los ciberataques más evasivos y proporciona inteligencia de amenazas accionable a sus partners, a sus clientes y a la comunidad de la ciberseguridad.

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