SONICWALL

Cloud Edge Secure Access de SonicWall

Implemente seguridad de confianza cero en unos minutos

Cloud Edge Secure Access de SonicWall es un potente servicio en la nube que proporciona una sencilla red como servicio para conectividad en la nube de sitio a sitio e híbrida a AWS, Azure o Google Cloud, entre otros. De paso, combina enfoques de seguridad de confianza cero y de mínimo privilegio en una oferta integrada.

El enfoque de acceso de mínimo privilegio restringe el acceso de un usuario concreto únicamente a lo que necesita y nada más, de forma similar al concepto de «según su necesidad de conocer». Al limitar la exposición a otras áreas sensibles de la red, las organizaciones pueden proteger sus recursos sin sacrificar su flexibilidad operativa.

Cloud Edge Secure Access de SonicWall aplica seguridad de confianza cero basada en cuatro medidas de seguridad fundamentales:

- Comprobar las credenciales del usuario y del dispositivo, incluso para el tráfico interno
- Contextualizar la solicitud para garantizar la autenticidad y el cumplimiento de las directrices corporativas
- Microsegmentar el acceso a la red para evitar que las amenazas se desplacen lateralmente
- Conceder acceso a las aplicaciones solicitadas y nada más

La moderna arquitectura de parámetros definidos por software (SDP) segura desde el diseño constituye el núcleo de la infraestructura de Cloud Edge Secure Access.

SDP desvincula el controlador que autentica a los usuarios y dispositivos de las *gateways* que actúan como agentes de confianza. Al distribuir las *gateways* cerca de las ubicaciones de los usuarios finales, el servicio Cloud Edge Secure Access puede ampliarse rápidamente para mantener un alto rendimiento y ofrecer la mejor experiencia en la nube.

Además, la separación de las funciones detiene eficazmente las ciberamenazas comunes, como los ataques DDoS, el secuestro de WiFi públicas, las inundaciones SYN y Slowloris, y permite a SonicWall ofrecer una plataforma de seguridad de confianza cero altamente integrada.

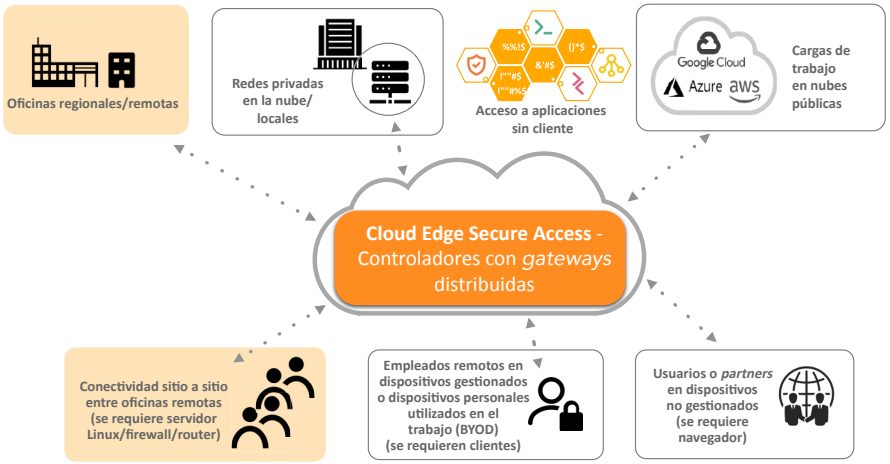

Figura 1 – Cloud Edge Secure Access de SonicWall

Ventajas:

- Protege a las empresas distribuidas y a los teletrabajadores
- Acceso instantáneo y seguro a cualquier sitio y recurso de las nubes híbridas
- Políticas de confianza cero por redes, aplicaciones, perfiles de usuarios y dispositivos
- Microsegmentación integrada para evitar movimientos laterales no autorizados
- Posibilidad de ampliación de 100 a miles de usuarios
- El responsable de TI puede configurarlo en 15 minutos
- El usuario final puede realizar la instalación en 5 minutos
- Sin límite de uso y ancho de banda
- Seguridad de Wi-Fi pública
- Cifrado WireGuard de alto rendimiento
- Integración con proveedores de identidad en la nube
- Integración moderna de SSO y MFA
- Detiene los ataques DDoS, Slowloris y las inundaciones SYN
- Múltiples clientes para los MSSP
- Completa supervisión e informes para las auditorías de cumplimiento
- *Gateways* en la nube y direcciones IP dedicadas por cliente
- Servicio disponible en EE. UU., Europa, Oriente Medio y Asia

La evolución de la VPN tradicional a la seguridad de confianza cero

En la era de la transformación digital, en la que los empleados pueden trabajar desde cualquier lugar y los recursos están en las nubes, la solución VPN tradicional es demasiado complicada de implementar y tiene demasiadas limitaciones.

Una implementación VPN típica puede tardar días o incluso semanas, verse obstaculizada por la disponibilidad del suministro y la dificultad para programar el tiempo de inactividad.

Una VPN tradicional también puede abrir la puerta trasera a una posible violación, ya que todo inicio de sesión satisfactorio proporciona al usuario un acceso amplio a la red y permite el movimiento lateral dentro de la subred.

Por último, la VPN induce una latencia adicional que degrada la experiencia en la nube de los usuarios, ya que el tráfico del usuario pasa por el concentrador VPN local en lugar de ir directamente a la nube.

Gartner estima que en 2023, el 60 % de las empresas eliminarán gradualmente la mayoría de sus redes privadas virtuales (VPN) de acceso remoto en favor de un acceso a la red de confianza cero (ZTNA).

Cloud Edge Secure Access de SonicWall supera los problemas descritos anteriormente y ofrece ZTNA con estas tres funcionalidades esenciales:

Acceso de mínimo privilegio para proteger los activos corporativos

Implementación rápida y autoservicio

Acceso directo y fiable a la nube desde cualquier lugar

Figura 2 – Funciones de Cloud Edge Secure Access de SonicWall

Casos de uso principales

Implementación rápida y autoservicio

- **Implementación rápida**: en menos de 15 minutos, el responsable de TI puede registrarse, crear una *gateway* y configurar políticas pormenorizadas en función de las redes y el contexto de los usuarios.
- **Incorporación rápida de usuarios**: los usuarios finales tienen la opción de conectarse a través de una aplicación cliente móvil o de escritorio u omitir por completo la instalación de un cliente cuando utilizan un ordenador público, siempre que haya un navegador disponible. Con el modelo de implementación de autoservicio, un usuario puede ponerlo en funcionamiento en 5 minutos.
- **Acceso fiable a la nube híbrida**: al finalizar, los usuarios tendrán un acceso rápido, fácil y seguro a los recursos locales y de la nube pública, desde cualquier lugar del mundo.

Protección para trabajar desde cualquier lugar en zonas con puntos de acceso públicos y de confianza

- **Seguridad automática de Wi-Fi:** las aplicaciones del agente Cloud Edge Secure Access para Windows y mac OS supervisan el entorno de forma proactiva y activan automáticamente una conexión de acceso seguro en los puntos de acceso públicos. De esta forma, se protege a los usuarios de las interceptaciones Wi-Fi demasiado comunes que pueden dar lugar a robos de datos e infracciones de cumplimiento.
- **Interruptor de emergencia:** para interrumpir cualquier posible infracción cibernética, cuando se interrumpe una conexión de acceso seguro, la conexión a Internet del dispositivo se detiene al instante para evitar que los datos salgan del dispositivo.
- **Redes Wi-Fi de confianza:** cuando un SSID se especifica como de confianza, no se activa la función de seguridad Wi-Fi automática.
- **VPN/aplicaciones siempre activas:** esta cómoda función vuelve a conectar automáticamente a un usuario o dispositivo a la aplicación o conjunto de aplicaciones sin necesidad de volver a iniciar sesión o volver a autenticarse.

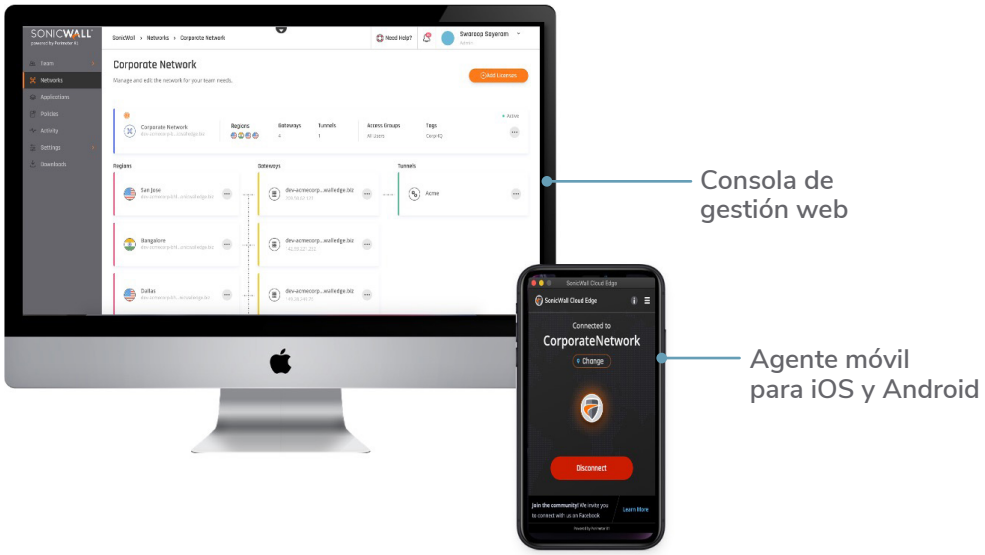

Figura 3 – Consola de gestión de Cloud Edge Secure Access de SonicWall y aplicación de agente móvil para Apple iOS

Acceso a aplicaciones de confianza cero

Cloud Edge Secure Access proporciona a las organizaciones digitales una herramienta muy necesaria para proteger los recursos corporativos y, al mismo tiempo, habilitar y capacitar a los teletrabajadores.

Con las políticas de confianza cero de Secure Access, los usuarios externos con un conjunto adecuado de contexto pueden acceder de manera segura a una gran cantidad de aplicaciones web y de escritorio remotas sin exponer la red corporativa a ciberamenazas.

- **El control de acceso de mínimo privilegio se aplica de manera estricta:** las organizaciones pueden controlar las interacciones con recursos en función de atributos relevantes, como la identidad del usuario y del grupo y la sensibilidad de los datos a los que se accede.
- **Contextual:** la solución garantiza un acceso centrado en el usuario y basado en políticas a los recursos locales y alojados en la nube.
- **Se integra con los principales proveedores de gestión de identidades basados en la nube:** las organizaciones pueden ampliar la vida útil de los activos locales heredados o migrar a los modernos servicios de gestión de identidades basados en la nube de proveedores como Azure AD, Google Authenticator y Okta.
- **Microsegmentación:** al segmentar con precisión todo el tráfico entrante, la microsegmentación impide que el *malware* o los usuarios no autorizados se desplacen lateralmente, lo que reduce la superficie de ataque y la exposición general a las ciberamenazas.
- **Autenticación de inicio de sesión único federado y multifactor:** esta combinación proporciona un único portal para autenticar a los usuarios en un entorno de TI híbrido con una experiencia coherente y fluida.
- **Función de auditoría de cumplimiento:** todas las actividades de acceso de confianza cero se supervisan y registran exhaustivamente para las auditorías futuras.

Figura 4 – Proceso ZTNA de Cloud Edge Secure Access de SonicWall

Interconectividad entre sitios o red como servicio (NaaS)

Cloud Edge Secure Access ofrece servicio de conectividad entre sitios o red como servicio (NaaS) para incorporar rápidamente oficinas remotas en lugares geográficamente dispersos.

Con NaaS, el responsable de TI puede conectar de forma rápida y segura quioscos móviles, tiendas minoristas y puntos de venta a recursos alojados en la nube sin depender del costoso MPLS.

- **Servicio de interconexión sitio a sitio o sitio a nube:** la solución se conecta fácilmente a entornos de nube populares, como AWS, Azure y Google Cloud, o crea un enlace de comunicación seguro entre dos redes diferentes ubicadas en distintos sitios.
- **Implementación multirregional:** los administradores pueden implementar *gateways* Cloud Edge dedicadas en diferentes ubicaciones para prestar el mejor servicio a oficinas remotas y empleados internacionales con una velocidad óptima.
- **Estructura global de alto rendimiento:** el servicio Cloud Edge de SonicWall está disponible en todo el mundo. La infraestructura ofrece una latencia mínima al distribuir las *gateways* cerca de las ubicaciones de los clientes y equilibrar la carga del tráfico entre los servidores.
- **Túnel WireGuard de última generación:** el responsable de TI puede aprovechar cualquier router o firewall con IPsec de la oficina para conectarse a la *gateway* de Cloud Edge más cercana.

  Para lograr el máximo rendimiento, SonicWall recomienda la función de conector WireGuard, que requiere un servidor Linux en la oficina para ejecutar el servicio de túnel WireGuard en la *gateway* más cercana.
- **Auditoría y supervisión de red:** obtenga más información sobre el estado, la actividad y la seguridad de su red, como la visibilidad sobre la creación de grupos y servidores, la autenticación de los miembros del equipo, los cambios de contraseñas, entre otros.

Especificaciones

Categoría	Función	Ventajas
Escala y rendimiento	Usuarios	Entre 100 y más de 10 000
	Desempeño	1 Gbps por *gateway* de cliente; escalado horizontal de la nube con más *gateways*
Plataforma en la nube	Plataforma de gestión en la nube	Plataforma de gestión en la nube para crear fácilmente la red de su organización. Tanto localmente como en la nube
	Implementación de red rápida y fácil	Implementación automática de red en menos de 15 minutos
	Disponibilidad y tiempo de actividad	Gestionado automáticamente por el servicio. El estado actual del servicio Cloud Edge se puede consultar en https://status.sonicwall.com/
	Equilibrio de carga	Proporcionado por *gateways* compartidas/dedicadas en más de 30 POP globales, alojados y gestionados por SonicWall
	Interconectividad entre sitios	Conectividad entre dos sitios (localmente, fuera de las instalaciones o basada en la nube). Compatible con IPsec y WireGuard
	DNS personalizado	Para usar sus servidores DNS internos, una vez definido un túnel, también puede definir un servidor DNS personalizado en lugar de usar el DNS predeterminado
	Acceso a la aplicación sin cliente	Acceso de aplicaciones de confianza cero a HTTP, HTTPS, RDP, VNC, SSH
	Acceso basado en el cliente	Disponible para plataformas Windows, Mac, iOS y Android
	Aplicaciones y entorno	Ideal para entornos híbridos y cargas de trabajo en la nube
Funciones de confianza cero	Aplicaciones siempre activas	Las aplicaciones siempre activas proporcionan acceso seguro a Internet cuando se conectan a una red que no es de confianza, lo que le protege de las amenazas de seguridad.
	Segmentación basada en políticas	Políticas aplicadas por usuario y aplicación
	Políticas de control de acceso pormenorizadas	Basadas en usuario, aplicación, Geo IP, geolocalización (país), tipo de navegador, SO, fecha y hora
	Túnel dividido	Le permite decidir a través de qué subred pasará su tráfico
	Interruptor de emergencia	Para interrumpir una posible infracción cibernética, cuando se interrumpe una conexión de acceso seguro, la conexión a Internet del dispositivo se detiene al instante para evitar que los datos salgan del dispositivo.
	Seguridad Wi-Fi automática	Nuestra función patentada protege automáticamente los dispositivos de los empleados cuando se conectan a una Wi-Fi pública no segura
	Filtrado de DNS	Impida que los usuarios de su red accedan a determinados sitios web, categorías de sitios y direcciones IP con un navegador de Internet
Autenticación	Función de inicio de sesión único	Implemente un inicio de sesión unificado a través de proveedores de inicio de sesión único como Okta, G Suite, Azure AD y Active Directory LDAP.
	Autenticación de dos factores	Evite ataques remotos con la integración 2FA incorporada de SMS, DUO Security y Google Authenticator
Supervisión, registro y soporte	Soporte 24X7	Solución en la nube totalmente gestionada con soporte incluido
	Auditorías e informes de actividad	Supervisión de inicios de sesión, despliegues de *gateway* y conexiones de aplicaciones
	Integración de SIEM	Captura, retención y entrega de información de seguridad y eventos en tiempo real a todas las aplicaciones SIEM, incluida una fácil integración con Splunk mediante clic
	Estado del servicio en la nube	Compruébelo en https://www.sonicwall.com/support
Interoperabilidad	Firewall empresarial	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco y Untangle
Integraciones personalizadas	API disponible	Nuestra completa API basada en REST permite una integración rápida y fácil con herramientas de gestión, automatización y orquestación de terceros, lo que garantiza la protección de las aplicaciones virtualizadas recientemente suministradas o reubicadas.
Conformidad	ISO 27001 y 27002, SOC-2 tipo 2	Infraestructura en la nube conforme a SOC 2 tipo 2
Pedidos	Suscripción	Póngase en contacto con su MSSP o su distribuidor para suscribirse a Cloud Edge Secure Access

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 obtener 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-CloudEdge-US-VG-2807

SONICWALL®