Barracuda SecureEdge

Proteja a los usuarios, los sitios web y las cosas, y conéctese a cualquier aplicación sin importar dónde esté alojada

SecureEdge proporciona acceso seguro a las aplicaciones, seguridad prestada en la nube para los terminales y conectividad SD-WAN automatizada para sitios web e instalaciones industriales de cualquier tipo o tamaño. Los usuarios remotos acceden a las aplicaciones directamente desde cualquier tipo de dispositivo. La incorporación de Zero Trust, el filtrado de URL y la optimización del tráfico en la última milla aseguran que el acceso a las aplicaciones sea siempre seguro y esté optimizado para aprovechar al

Protege a los usuarios, los sitios y las cosas

Barracuda SecureEdge se creó desde el principio como una plataforma de seguridad para gestionarse y ejecutarse en la nube y para que estuviera disponible en forma de servicios periféricos gestionados para cualquier tipo de dispositivo, implementación o plataforma.

Gracias a la amplia red de información sobre amenazas de Barracuda, la inteligencia de seguridad derivada de la IA va más allá de la implementación habitual de sitios web o servicios en la nube y lleva la seguridad avanzada a cualquier usuario, con independencia del dispositivo que utilice, y a todas las cosas.

Conecta cualquier dispositivo, aplicación o entorno híbrido o en la nube

Las nuevas soluciones de Zero Trust se han diseñado para acceder de forma segura únicamente a los recursos basados en la nube y, a menudo, son difíciles de configurar, gestionar y utilizar en entornos reales.

Hoy en día, los usuarios que utilizan cualquier dispositivo esperan poder acceder de forma segura y fiable a cualquier aplicación, tanto si está alojada en la nube como si lo está en las infraestructuras locales. La solución también debe ser fácil de usar y mejorar el acceso a las aplicaciones para lograr una experiencia de usuario óptima. Barracuda SecureEdge Access ofrece todo esto. Está disponible para cualquier tipo de dispositivo y plataforma, así como para infraestructuras locales o en la nube, utiliza las funciones de SD-WAN de los dispositivos y optimiza el flujo de las aplicaciones para ofrecer una experiencia inigualable al usuario remoto.

Fácil de adquirir, implementar y tener en propiedad

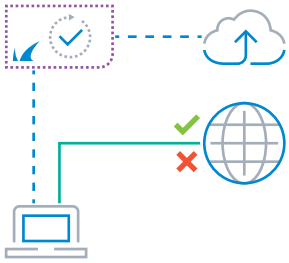
La plataforma Barracuda SecureEdge es una solución SASE de un solo proveedor que integra y automatiza sus componentes de manera inteligente. Los servicios principales están disponibles como SaaS, también para Azure Virtual WAN, e incluso como instancias privadas, todas gestionadas a través de la misma interfaz de usuario basada en la web fácil de usar.

La conectividad del sitio se crea mediante la implementación sin intervención de un dispositivo desplegado localmente con una optimización automática de SD-WAN para el servicio.

Los usuarios remotos que se encuentren en cualquier sistema operativo se autoinscriben con el agente de SecureEdge Access, que está disponible en cualquier tienda de aplicaciones y puede usarse en un máximo de 10 dispositivos por usuario simultáneamente para el acceso a la red Zero Trust (ZTNA) y el acceso seguro a Internet (SIA).

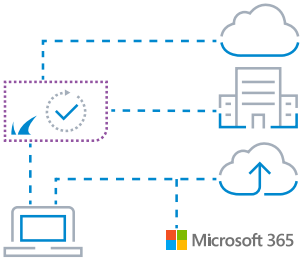
Los dispositivos desplegados localmente se implementan de forma rápida y se conectan automáticamente a los servicios en la nube. Asimismo, optimizan el tráfico de enlaces ascendentes en la nube mediante la reducción de la pérdida de paquetes y otras funciones avanzadas de optimización de SD-WAN para que las empresas puedan prescindir del gasto que suponen las líneas alquiladas.

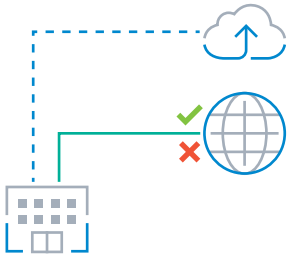
Ejemplos de casos prácticos de la plataforma SASE de Barracuda SecureEdge



Acceso seguro a Internet para usuarios de dispositivos móviles
Hoy en día, muchos empleados trabajan con fluidez entre oficinas corporativas, sucursales, oficinas en casa y en los medios de transporte. Sin embargo, el nivel de las políticas de seguridad corporativas, por ejemplo, para un acceso aceptable a la web, debe ser el mismo sea cual sea su ubicación. Gracias a la amplia red de información sobre amenazas de Barracuda y a una inteligencia de seguridad derivada de la IA, el agente de SecureEdge Access extiende la seguridad y el cumplimiento de las políticas a cualquier dispositivo de cualquier plataforma.

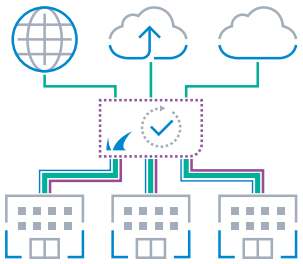
Acceso seguro a aplicaciones privadas y de SaaS (ZTNA)
Proporcione un acceso directo y seguro a todas las aplicaciones autorizadas con una evaluación continua de la seguridad y la idoneidad, independientemente de dónde estén alojadas y del dispositivo que utilicen los usuarios. Optimice el tráfico de red de última milla para aprovechar al máximo los enlaces de Internet compartidos.

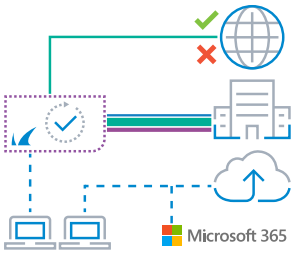




Secure Web Gateway (SWG) para oficinas y sucursales
Los dispositivos del sitio web de SecureEdge protegen el perímetro de la oficina y cualquier dispositivo que se encuentre en esta contra el malware, el spyware y otros contenidos no deseados de Internet. Además de la detección de códigos maliciosos, también se lleva a cabo el filtrado de URL y el control de miles de aplicaciones populares (incluso las que no están basadas en web). Todo ello se puede ejecutar en el dispositivo o en los servicios de SecureEdge.

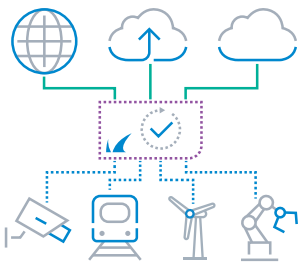
Seguridad y conectividad de la oficina en la nube
Conecte de forma segura cualquier sucursal a la nube y asegúrese de que esté protegida contra las amenazas de Internet, como el malware, el ransomware y el spyware. La SD-WAN segura constituye la vía de acceso a la nube para lograr un rendimiento óptimo de las aplicaciones.





Firewall como servicio (FWaaS)
Las funciones de los firewall de nueva generación se distribuyen a cualquier sitio o cliente mediante un servicio en la nube. Esto incluye controles de acceso a la red, control de aplicaciones, filtrado web, prevención de amenazas avanzadas, sistema de prevención de intrusiones (IPS) e inspección profunda de SSL/TLS.

Seguridad, conectividad y acceso remoto ZTNA para las cosas (IoT/ICS)
Proteja y conecte los dispositivos industriales a la nube de su elección o a la oficina. Proporcione acceso seguro basado en ZTNA a dispositivos industriales, independientemente de su ubicación.



Aspectos destacados de la solución Barracuda SecureEdge

Fácil de implementar: Los agentes de acceso SecureEdge, disponibles para un máximo de 10 dispositivos simultáneamente por usuario, se pueden implementar fácilmente a través de la inscripción automática o masiva y la gestión de dispositivos móviles. Los agentes de acceso están disponibles para Windows, macOS, iOS, Android y Linux.

Optimización de último kilómetro: La optimización integrada del tráfico de Internet desde el servicio hasta el agente de SASE permite que los terminales aprovechen una mayor parte del ancho de banda disponible en las líneas de Internet compartidas para mejorar el rendimiento de las aplicaciones. La tecnología subyacente que se usa para solucionar la pérdida de paquetes se basa en códigos de red lineales aleatorios (RLNC, por sus siglas en inglés), un potente esquema de codificación. Los algoritmos basados en los códigos RLNC reaccionan mucho más rápido ante las pérdidas y las corrigen más deprisa sobre la marcha, lo que requiere menos retransmisiones de paquetes y reduce la sobrecarga de los dispositivos.

Gestión de políticas y redes basadas en la intención: En el pasado, las soluciones de seguridad eran complicadas de usar, o bien presentaban carencias en sus funciones de seguridad subyacentes. Los firewalls y otras soluciones de seguridad se basaban en la asignación de redes, rangos de IP y funciones de seguridad de productos concretas para estas redes. Las operaciones basadas en la intención se crean desde cero como parte del concepto del SecureEdge Manager para nuestra plataforma SASE unificada. La plataforma SASE de Barracuda SecureEdge es estrictamente específica para el usuario, el grupo y la aplicación. De este modo, los usuarios remotos pueden acceder a aplicaciones de nube pública y privada, e Internet mucho más rápido.

“Una única” administración basada en intenciones: La plataforma SASE de SecureEdge le permite crear miles de aplicaciones predefinidas, así como otras privadas que se pueden alojar en cualquier lugar. Constituye un procedimiento rápido, sencillo y que solo hay que seguir una vez para, a continuación, compartirlo con las definiciones de políticas de seguridad, SD-WAN y ZTNA. Todas las optimizaciones de redes y enrutamiento necesarias se llevan a cabo de forma completamente transparente en segundo plano y se aplican de forma automática a cada sitio web, usuario o instancia de servicio.

Conectividad sin intervención para cualquier sitio web: Incorporar sitios web y cosas a la plataforma SASE de Barracuda SecureEdge no puede ser más sencillo. Con tan solo un par de clics del ratón, podrá completar la configuración en el administrador basado en la nube, y los dispositivos a desplegar localmente se enviarán directamente a la ubicación remota. La implementación sin intervención conecta automáticamente dispositivos desplegados localmente y los dispositivos de IoT al punto de entrada de SecureEdge más cercano.

SD-WAN automática: Tras conectar y encender los dispositivos del sitio, cada uno utiliza automáticamente todos los enlaces ascendentes disponibles para conectarse al servicio SASE. Gracias a la configuración de políticas de SD-WAN predefinida para miles de aplicaciones empresariales frecuentes, se asegura que los dispositivos utilicen siempre la mejor ruta de enlace ascendente para la aplicación.

Seguridad web avanzada: Proteger su red y a los usuarios remotos de las amenazas en línea nunca ha sido tan fácil. Independientemente de que los empleados estén en la oficina sentados detrás de sus dispositivos, trabajando desde casa o en cualquier otro lugar, SecureEdge examina el tráfico web y bloquea el acceso a sitios web dañinos. Las políticas de la empresa para la navegación web se aplican a niveles muy granulares. La visibilidad del tráfico web cifrado SSL/TLS y los filtros de palabras clave sospechosas ofrecen una visibilidad que no representa lo que está sucediendo en su organización.

Conectividad optimizada, en cualquier momento y en cualquier lugar: Cada dispositivo de sitio SecureEdge y de agente de SecureEdge Access optimizan el tráfico de red para ofrecer la mejor latencia y ancho de banda posibles a las aplicaciones alojadas en la nube. El ancho de banda físico disponible de los enlaces ascendentes suele estar en un medio compartido. Los métodos de corrección de errores de reenvío incorporados basados en códecs RLNC garantizan de manera efectiva que el ancho de banda disponible se utilice de la mejor manera posible frente a otros componentes en el medio compartido. SecureEdge amplía de manera efectiva los beneficios de SD-WAN a sitios con usuarios remotos de enlaces ascendentes únicos.

Service Edge flexible: El servicio SASE de Barracuda SecureEdge está disponible como SaaS administrado directamente por Barracuda Networks, como SecureEdge para Microsoft Azure Virtual WAN administrado por Microsoft, o como dispositivos virtuales y de hardware que el cliente o el socio de confianza pueden administrar y alojar. Independientemente del tipo de implementación, toda la administración de la configuración basada en la intención se lleva a cabo desde el portal en la nube del administrador de SecureEdge. A continuación, el servicio se encarga de propagar y aplicar los cambios en cada extremo del servicio, sede local, usuario o cosa.

Proveedor único: La plataforma de Barracuda SecureEdge es la única solución que ofrece seguridad y conectividad a los usuarios, los sitios web y las cosas en un formato basado en la nube fácil de usar que integra tecnologías que de otro modo serían dispares, como la SD-WAN para acceder a los sitios, la seguridad y la conectividad para las cosas y la seguridad industrial, y todo ello en una misma plataforma.

Características destacadas de Barracuda SecureEdge

Gestión general y central

- Todas las funciones se gestionan de forma centralizada a través de SecureEdge Manager basado en la nube
- Idiomas de gestión disponibles: Inglés, Alemán, Francés, Japonés
- Implementación sin intervención para dispositivos del sitio
- Autoaprovisionamiento (incorporación) para el agente de SecureEdge Access
- Implementaciones de alta disponibilidad fáciles de configurar
- Entornos de IoT industrial de fácil integración a través de los dispositivos Secure Connector
- Funciones multiinquilino
- Varios espacios de trabajo por inquilino
- La suscripción pública al servicio perimetral SecureEdge está disponible a través de Barracuda en 26 regiones de todos los continentes
- Los servicios perimetrales privados de SecureEdge están disponibles con el dispositivo del sitio SecureEdge o CloudGen Firewall, gestionados a través de SecureEdge Manager
- El servicio perimetral privado SecureEdge está disponible con Azure Virtual WAN, gestionado a través de SecureEdge Manager

Autenticación y compatibilidad con proveedores de identidad

- Compatibilidad con autenticación basada en SAML e integración perfecta con proveedores de identidad de terceros como Microsoft Entra ID, Okta, Google Workspace, OpenID, MSAD y LDAP.
- Compatibilidad con autenticación basada en correo electrónico

Informes y visibilidad

- Paneles personalizables con widgets de detalle para (extracto):
  - Protección frente a amenazas avanzadas
  - Estado de configuración del dispositivo
  - Riesgo de aplicaciones
  - Estado del dispositivo perimetral
  - Destinos y fuentes geográficas
  - Incidentes de IPS y eventos recientes
  - Estado del dispositivo
  - Estado del túnel y del mapa SD-WAN
  - ZTNA permitido/bloqueado (usuario, aplicación, URL, dominio)
  - Mapa de dispositivos ZTNA
- Conexiones en tiempo real: visibilidad del tráfico para cada sitio y servicio perimetral SecureEdge con filtrado avanzado
- Conexiones recientes: visibilidad del tráfico histórico de la sesión para cada sitio y servicio perimetral SecureEdge con filtrado avanzado para una rápida resolución de problemas
- Firewall Report Creator (incluido) para informes personalizados ilimitados en múltiples sitios y servicios
- Integración con Barracuda XDR
- Integración con Azure Log Analytics para todos los dispositivos del sitio y servicios perimetrales

Para obtener más información sobre el conjunto de funciones de Barracuda SecureEdge, visite barracuda.com.

1 Disponible sólo para Site Devices y Private Edge Service.

Seguridad web y acceso seguro a Internet

Filtrado de contenido

- Inspección SSL/TLS
- Filtrado de URL por categoría, categoría personalizada, dominio
- Categorías personalizadas
- Aplicación segura de la búsqueda
- Bloqueo de anuncios
- Control y bloqueo de aplicaciones para miles de aplicaciones web comunes

Creación avanzada de políticas

- Política predeterminada personalizable para todos los usuarios y sitios
- Excepciones de políticas de usuario, grupo, red y sitio
- Categorías personalizadas y páginas de bloqueo
- Bloquear, permitir, advertir y notificar políticas

Protección frente a amenazas avanzadas

- Integración con el servicio Barracuda ATP
- Protección frente a ransomware, amenazas persistentes avanzadas, virus polimórficos y malware de hora cero

Seguimiento web

- Supervisión de redes sociales
- Supervisión de palabras clave personalizadas
- Alertas sobre
  - Palabras clave sospechosas
  - Palabras clave de ciberacoso
  - Palabras clave de terrorismo

Métodos de despliegue disponibles

- Proxy web[1]
- Modo en línea con escaneado de una sola pasada

Acceso seguro a Internet, filtrado remoto

- SecureEdge Access Agents para Windows, macOS, iOS, Android y Linux
- Filtrado de DNS local
- Aplicación de la posición de seguridad del cliente
- Inspección de seguridad selectiva definida por el usuario mediante cualquier tipo de servicio perimetral de SecureEdge (SaaS, Azure, privado o implementaciones existentes de CloudGen Firewall)

CASB

- Compatibilidad de CASB basado en proxy para cientos de aplicaciones empresariales (por ejemplo, Microsoft Office365, Netsuite, SAP, etc.)

Conectividad y SD-WAN

- Implementación sin intervención para dispositivos del sitio
- Self-enrollment sin intervención para el agente de SecureEdge Access
- Políticas SD-WAN automáticas para cientos de aplicaciones
- Selección optimizada de enlace ascendente directo a Internet
- Optimización del vínculo ascendente de Internet (corrección de errores de reenvío) para dispositivos y clientes del sitio
- Uso simultáneo de varios enlaces ascendentes (hasta 16 transportes) por conexión SD-WAN
- Detección dinámica de ancho de banda
- Selección de transporte basada en el rendimiento
- Enrutamiento de tráfico con reconocimiento de aplicaciones
- Equilibrio de sesión adaptativo a través de múltiples enlaces ascendentes
- Selección de proveedores basada en aplicaciones

Conectividad y SD-WAN (continuación)

- Fijación de proveedores
- Comprobación del estado de vínculos superiores
- Protocolos de cifrado: IPsec v2, TINA
- Tipos de vínculos superiores compatibles: námico, estático, Express Route, Bridge, WAN (módem LTE), PPPoE
- Conectividad de usuario (VPN) de punto a sitio

ZTNA universal basada en la nube

- Agente de SecureEdge Access a prueba de manipulaciones para plataformas Windows, macOS, iOS, Android y Linux
- Acceso integrado basado en roles basado en permisos de usuario/grupo
- Comprobación del estado del dispositivo integrada basada en los requisitos de la política ZTNA
- Acceso ZTNA a cualquier aplicación basada en TCP/UDP, independientemente de dónde esté alojada
- Compatibilidad con aplicaciones en cualquier nube pública y en las instalaciones con la aplicación SD-WAN Connector
- Compatibilidad de entrada para aplicaciones alojadas en las instalaciones detrás de los dispositivos del sitio SecureEdge o implementaciones de CloudGen Firewall
- Políticas de estado de dispositivos compatibles: bloquear dispositivos con jailbreak, requerir bloqueo de pantalla, requerir firewall, requerir antivirus, requerir actualizaciones del sistema operativo, requerir actualizaciones del agente de SecureEdge Access, requerir cifrado de disco
- Limitación del acceso a las aplicaciones en función del tipo de sistema operativo
- Conectividad previa al inicio de sesión para la gestión centralizada de los dispositivos propiedad de la empresa
- Gestión de dispositivos y usuarios inscritos
- Catálogo de aplicaciones para un acceso rápido a aplicaciones predefinidas directamente a través de los agentes de SecureEdge Access
- Amplíe la aplicación de la política de ZTNA a las ubicaciones de campus, sucursales y sitios
- Servicios ZTNA fáciles de proporcionar como complemento para implementaciones existentes de CloudGen Firewall
- En todas las plataformas
  - Usabilidad, aspecto y funcionamiento coherentes
  - Acceso seguro a Internet integrado

Seguridad del sitio y Firewall como servicio

- Inspección y reenvío de paquetes con estado
- ACL específicas del sitio y del servicio
- Concienciación de la identidad de los usuarios
- IDS/IPS
- NAT de entrada
- Control de aplicaciones y aplicación granular
- Interceptación e inspección de aplicaciones cifradas SSL/TLS
- ATP, IPS y control de aplicaciones en modo de un solo paso
- Servidor DHCP, Retransmisión DHCP
- Rutas dinámicas y estáticas
- Puente de red
- Compatibilidad con VLAN
- Dominios reenviados personalizados

Conectividad de red global

- Microsoft Global Network
- Teridion Connect & Teridion China

Especificaciones técnicas

SecureEdge Access Agent

SISTEMA OPERATIVO	Windows	macOS	Android	iOS / iPadOS	Linux
Versiones de sistema operativo compatibles [1]	Windows 10 o superior	macOS 12 (Monterey) o superior	Android 10 o superior	iOS/iPadOS 15 o superior	Distribuciones actuales de Ubuntu y Fedora
Inscripción masiva por usuario grupo, implementación a través de MDM	✓	✓	✓	✓	✓
Autoaprovisionamiento	✓	✓	✓	✓	✓
Control de la salud de los clientes	✓	✓	✓	✓	✓
Soporte de aplicaciones	HTTP/HTTPS y TCP/UDP	HTTP/HTTPS y TCP/UDP	HTTP/HTTPS y TCP/UDP	HTTP/HTTPS y TCP/UDP	HTTP/HTTPS y TCP/UDP
Optimización de último kilómetro	✓	✓	✓	✓	✓
Filtrado de URL	✓	✓	✓	✓	✓
Inspección de seguridad selectiva	✓	✓	✓	✓	✓
Inalterable	✓	✓ [2]	✓ [2]	✓ [2]	✓
Cantidad máxima de dispositivos simultáneos por usuario	10 dispositivos por usuario (en todas las plataformas)				

SD-WAN Connector

SISTEMA OPERATIVO	Windows	Linux
Versiones de sistema operativo compatibles	Windows 10 (arquitecturas Pro, Server e Intel) Windows 11 (arquitecturas Pro, Server e Intel)	Distribuciones actuales de Ubuntu y Fedora (versiones Desktop, Server y Cloud) Linux x86_64 genérico
Autoaprovisionamiento en un clic [3]	✓	✓
Cifrado del servicio	Propietario (cifrado TINA)	Propietario (cifrado TINA)
Rendimiento máx. [4]	100 Mbps-1 Gbps (según el hardware del servidor)	100 Mbps-1 Gbps (según el hardware del servidor)
Plataforma en la nube compatible	Cualquier proveedor de nube que ofrezca IaaS o contenedores como servicio para Windows y Linux	

SecureEdge Edge Service , proporcionado por Barracuda

	América	EMEA	APAC
Disponible para las siguientes regiones	Brasil (Sur), Canadá (Centro, Este), EE. UU. (Centro, Este, Oeste)	Europa (Norte, Oeste), Francia, Alemania, Noruega, Sudáfrica, Emiratos Árabes Unidos, Reino Unido (Sur, Oeste)	Asia (Este, Sudeste), Australia (Centro, Este, Sudeste), India (Centro, Sur), Japón (Este, Oeste), Corea

SecureEdge Edge Service para Microsoft Azure Virtual WAN (Opcional)

	UNIDAD DE ESCALADO PARA LA WAN VIRTUAL DE MICROSOFT AZURE							
	2	4	10	20	30	40	60	80
Ancho de banda disponible	1 Gbps	2 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps	30 Gbps	40 Gbps

Dispositivos del sitio de SecureEdge

	DISPOSITIVOS DE HARDWARE									DISPOSITIVOS VIRTUALES				
	ESCRITORIO		MONTAJE EN BASTIDOR DE 1 U			COMPATIBILIDAD CON CARRIL DIN								
	T100B	T200C	T400C	T600D	T900C	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
Funciones de Edge Service	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
NÚMERO RECOMENDADO DE USUARIOS (consulte el folleto de especificaciones (Ingles) para obtener información más detallada sobre las prestaciones)														
Protección contra amenazas	130	300	1,000	4,000	9,000	10 [5]	1-10 [5]	100	300	100	300	1000	4000	9000
Solo seguridad web	400	1,000	5,000	10,000	20,000	10 [5]	1-10 [5]	100	150	400	1,000	5,000	10,000	20,000
HARDWARE (consulte el folleto de especificaciones (Ingles) para obtener información más detallada sobre el hardware)														
Versión de hardware resistente	-	-	-	-	-	-	✓ [6]	✓ [6]	✓ [6]	-	-	-	-	-
Licencias de vCPU (virtuales)	-	-	-	-	-	-	-	-	-	2	4	8	10	hasta 32
NIC de cobre (1 GbE)	5x	12x	8x	10x	8x	4x	4x	2x	5x	-	-	-	-	-
NIC de fibra (SFP) (1 GbE)	-	4x	-	8x	8x	-	-	1x	2x	-	-	-	-	-
NIC de fibra (SFP+) (10 GbE)	-	-	2x	2x	4x	-		-	-	-	-	-	-	-
NIC de fibra (QSFP+) (40 GbE)	-	-	-	-	2x	-	-	-	-	-	-	-	-	-
NIC virtuales	-	-	-	-	-	-	-	-	-	5-16x	5-16x	5-16x	5-16x	5-16x
WiFi (AP / Cliente)	-	-	-	-	-	✓ [7]	✓ [9]	-	-	-	-	-	-	-
GSM / UTMS	-	-	-	-	-	✓ [8]	✓ [10]	-	-	-	-	-	-	-
4G / LTE	-	-	-	-	-	✓ [8]	✓ [10]	-	-	-	-	-	-	-

Para obtener más información sobre las licencias, consulte el folleto de licencias (Ingles).

1 Por lo general, el agente de SecureEdge Access de Barracuda funcionará bien en versiones anteriores del sistema operativo, pero no se ha probado ni se admite oficialmente. No se recomienda la ejecución en versiones no compatibles para implementaciones de producción.
2 Necesita MDM.
3 Solo requiere conectividad a Internet y un token generado a través del administrador de SecureEdge.
4 Depende del hardware instalado y de la asignación de memoria; utiliza un único hilo de CPU.
5 La seguridad se aplica en el componente del servicio perimetral SecureEdge al que está conectado el dispositivo SC.
6 Sin ventilador con un rango de temperatura de funcionamiento ampliado (de -20 to +70 °C) diseñados específicamente para entornos difíciles.
7 Submodelos FSC21 y FSC25.
8 Submodelos FSC24 y FSC25.
9 Submodelos FSC31 y FSC35.
10 Submodelos FSC34 y FSC35.

Barracuda
Your business, secured.

Barracuda Networks y el logotipo de Barracuda Networks son marcas registradas de Barracuda Networks, Inc. en Estados Unidos. El resto de los nombres pertenecen a sus respectivos propietarios.