Barracuda SecureEdge

Microsoft Azure Certified

Schützen Sie User, Standorte und Dinge - und stellen Sie eine Verbindung zu Anwendungen her, unabhängig davon, wo sie gehostet werden

SecureEdge gewährleistet sicheren Anwendungszugriff, cloudbasierte Sicherheit für Endgeräte und automatisierte SD-WAN-Konnektivität für Standorte und Industrieanlagen jeder Art und Größe. Remote-User greifen von jedem Gerätetyp aus direkt auf Anwendungen zu. Zero-Trust Enforcement, URL-Filterung und Optimierung des Datenverkehrs auf der “Last-Mile” sorgen dafür, dass der Anwendungszugriff stets sicher und für die bestmögliche Nutzung der gemeinsam genutzten Internetleitungen optimiert ist.

Schützt Benutzer, Standorte und Dinge

Barracuda SecureEdge wurde als Sicherheitsplattform entwickelt, die in der Cloud verwaltet und bereitgestellt wird und als automatisch verwaltete Edge-Services für jede Art von Gerät, Bereitstellung oder Plattform verfügbar sind.

Angetrieben durch das Barracuda Threat Intelligence Network geht die von KI abgeleitete Sicherheitsintelligenz über die simple Bereitstellung eines Standorts oder Cloud-Services hinaus und inkludiert User auf jedem Gerät und in allen Bereichen.

Verbindet jedes Gerät, jede Anwendung oder Cloud/Hybrid-Umgebung

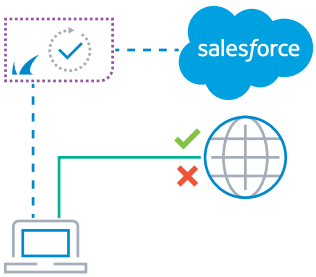
Neu aufkommende Zero-Trust-Lösungen sind nur für den sicheren Zugriff auf Cloud-basierte Ressourcen konzipiert, lassen sich aber in der Praxis oft nur schwer einrichten, verwalten und nutzen. Heutzutage erwarten User jedoch auf jedem Gerät sicheren und zuverlässigen Zugang zu jeder Anwendung, unabhängig davon, ob diese gehostet wird. Die Lösung muss außerdem einfach zu bedienen sein und die Benutzererfahrung verbessern. Barracuda SecureEdge Access bietet all dies. Es ist für jeden Gerätetyp, jede Plattform und jede Cloud oder On-Premises verfügbar, nutzt SD-WAN-Fähigkeiten und optimiert den Application Flow.

Einfacher Erwerb, Einsatz und Verwaltung

Die Barracuda SecureEdge-Plattform ist eine SASE-Lösung aus einer Hand, die ihre Komponenten geschickt integriert und automatisiert und als SaaS, in Azure Virtual WAN und sogar für private Instanzen verfügbar ist. Die Konnektivität wird durch Zero-Touch-Deployment mit automatischer SD-WAN-Optimierung hergestellt. Remote-Benutzer auf beliebigen Betriebssystemen registrieren sich selbst mit dem SecureEdge Access Agent, der in jedem App Store erhältlich ist und bis zu 5 Geräte für ZTNA und Secure Internet Access (SIA) pro User erlaubt. All dies wird über den Cloud-basierten SecureEdge Manager zentral verwaltet und durchgesetzt. Intent-based Networking und Intent-based Security Policies bieten die schnellste und intuitivste Möglichkeit zur zentralen Orchestrierung einer SASE-Lösung, einschließlich ZTNA und sicherem SD-WAN für die Konnektivität.

Alle Site Devices lassen sich per Zero-Touch schnell einrichten und verbinden sich automatisch mit Services in der Cloud. Sie optimieren den Cloud-Uplink-Verkehr durch Reduzierung von Paketverlusten und andere fortschrittliche SD-WAN-Optimierungsfunktionen, sodass Unternehmen auf teure Standleitungen verzichten können.

Beispiel für den Einsatz der Barracuda SecureEdge SASE-Plattform

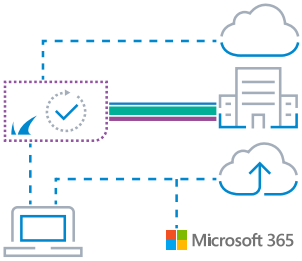


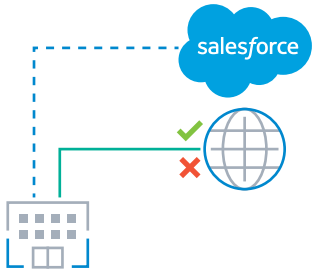
Sicherer Internetzugang (Secure Internet Access, kurz SIA) für mobile User

Heutzutage arbeiten viele Mitarbeiter an verschiedenen Orten im Unternehmen, in Zweigstellen, in Heimbüros und unterwegs. Dennoch müssen die Sicherheitsrichtlinien des Unternehmens, z. B. für den erlaubten Internetzugang, auf demselben Niveau bleiben. Der SecureEdge Access Agent, der auf dem umfangreichen Barracuda Threat Intelligence Network und einer von KI abgeleiteten Sicherheitsintelligenz basiert, erweitert die Sicherheit und die Einhaltung von Richtlinien auf jedes Gerät und jede Plattform.

Sicherer Zugriff auf private und SaaS-Anwendungen (Zero-Trust-Network-Access, kurz ZTNA)

Ermöglichen Sie einen direkten, sicheren Zugang zu allen freigegebenen Anwendungen mit kontinuierlicher Sicherheits- und Berechtigungsbewertung, unabhängig davon, wo die Anwendungen gehostet werden und für jeden Nutzer auf jedem Gerät. Optimieren Sie den Netzwerkverkehr auf der letzten Meile, um die gemeinsam genutzten Internet-Uplinks bestmöglich zu nutzen.



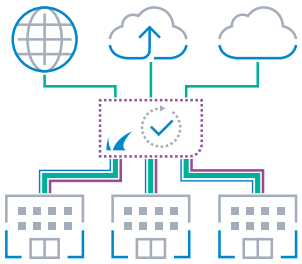


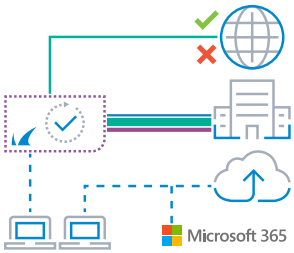
Secure Web Gateway (SWG) für Büros und Niederlassungen

SecureEdge Site Devices schützen die Büroumgebung und alle Geräte im Büro vor Malware, Spyware und anderen unerwünschten Inhalten aus dem Internet. Neben der Erkennung von bösartigem Code umfasst dies auch URL-Filterung und Anwendungskontrolle für Tausende gängiger Anwendungen (auch solche, die nicht webbasiert sind). Die Durchsetzung kann entweder auf dem Gerät oder im Service-Layer von SecureEdge erfolgen.

Cloud-basierte Konnektivität und Sicherheit

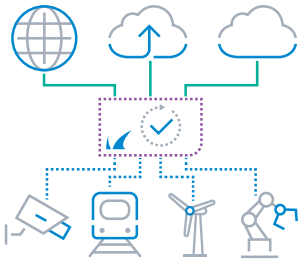
Verbinden Sie jede Niederlassung sicher mit der Cloud und stellen Sie sicher, dass sie vor Bedrohungen aus dem Internet wie Malware, Ransomware und Spyware geschützt ist. Secure SD-WAN stellt die Verbindung zur Cloud für eine optimale Anwendungsleistung her.





Firewall as a Service (FWaaS)

Bieten Sie Cloud-basierte Next-Generation Security, sicheren Internetzugang und Anwendungskontrolle für jeden Remote-User und jedes Gerät.



Sicherheit, Konnektivität und ZTNA Remote Access für die Industrie (IoT/ICS)

Sichern und verbinden Sie Industriegeräte mit der Cloud Ihrer Wahl oder dem Büro.
Bieten Sie sicheren ZTNA-basierten Zugriff auf Industriegeräte, unabhängig vom Standort.

Highlights der Barracuda SecureEdge-Lösung

Agent Auto-Provisionierung

Remote-User können sich problemlos auf bis zu 5 Geräten selbst registrieren. Der SecureEdge Access Agent kann in jedem App-Store und auch für Linux kostenlos heruntergeladen werden. Klicken Sie einfach auf den Link, der in der Email zur Registrierung enthalten ist, um loszulegen.

Last-Mile Optimierung

Die integrierte Optimierung des Internetverkehrs vom Dienst bis zum SASE-Agenten ermöglicht es den Endpunkten, mehr von der verfügbaren Bandbreite auf gemeinsam genutzten Internetleitungen zu nutzen, um die Anwendungsleistung zu verbessern. Die zugrundeliegende Technologie zur Behebung von Paketverlusten basiert auf zufälligen linearen Netzwerkcodes (Random Linear Network Codes, kurz RLNC), einem leistungsstarken Kodierungsschema. Algorithmen, die auf RLNC-Codes basieren, reagieren viel schneller auf Verluste und beheben diese Verluste schneller im laufenden Betrieb, so dass weniger Paketübertragungen erforderlich sind und der Overhead der Geräte reduziert wird.

Intent-basiertes Networking und Richtlinienmanagement

In der Vergangenheit waren Sicherheitslösungen entweder kompliziert in der Anwendung oder unzureichend in ihren zugrunde liegenden Sicherheitsfunktionen. Firewalls und andere Sicherheitslösungen basierten auf der Zuweisung von Netzwerken, IP-Bereichen und Sicherheitsfunktionen von Einzelprodukte in diesen Netzwerken. Intent-basierte Abläufe sind von Grund auf als Teil des Konzepts des SecureEdge Managers für unsere einheitliche SASE-Plattform aufgebaut. Die SecureEdge SASE-Plattform ist streng benutzer-, gruppen- und anwendungsspezifisch. Remote-Benutzer können dadurch viel schneller auf private und Public Cloud-Anwendungen und das Internet zugreifen.

„Once-Only“ intent-basiertes Management

Zusätzlich zu Tausenden von vordefinierten Anwendungen können Sie mit der SecureEdge SASE-Plattform private Anwendungen erstellen, die überall gehostet sein können. Das geht schnell und einfach und muss nur einmal durchgeführt werden - und wird dann mit Sicherheits-, SD-WAN- und ZTNA-Richtliniendefinitionen geteilt. Alle erforderlichen Netzwerk- und Routing-Optimierungen erfolgen völlig transparent im Hintergrund und werden automatisch auf jeden Standort, Benutzer oder jede Service-Instanz angewendet.

Zero-Touch-Konnektivität für jeden Standort

Das Onboarding von Standorten und Dingen auf die Barracuda SecureEdge SASE-Plattform könnte nicht einfacher sein. Mit nur wenigen Mausklicks ist die Konfiguration im cloud-basierten Manager abgeschlossen, und die Geräte werden direkt an den gewünschten Standort gesendet. Durch das Zero-Touch-Deployment werden Standorte und IoT-Geräte automatisch mit dem nächstgelegenen SecureEdge-Einstiegspunkt verbunden.

Auto-SD-WAN

Nach dem Anschließen und Einschalten nutzt jedes Site Device automatisch alle verfügbaren Uplinks, um sich mit dem SASE-Service zu verbinden. Mit vordefinierten SD-WAN-Richtlinieneinstellungen für Tausende gängiger Geschäftsanwendungen stellen die Site Devices sicher, dass immer der beste Uplink-Pfad für die Anwendung verwendet wird.

Ausgereifte Web-Sicherheit

Der Schutz Ihres Netzwerks und Ihrer Remote-User vor Online-Bedrohungen war noch nie so einfach. Ob Mitarbeiter im Büro hinter einem Site-Device, bei der Arbeit von zu Hause aus oder anderswo - SecureEdge prüft den Datenverkehr und blockiert den Zugriff auf schädliche Websites. Richtlinien für das Surfen im Internet werden bis zu einer sehr granularen Ebene durchgesetzt. Die Einsicht in den SSL/TLS-verschlüsselten Webverkehr und die Filter für verdächtige Schlüsselwörter bieten einen unverstellten Einblick in die Vorgänge in Ihrem Unternehmen.

Optimierte Konnektivität, jederzeit und überall

Jedes Site-Device von SecureEdge und jeder SecureEdge Access Agent optimieren den Netzwerkverkehr, um die bestmögliche Latenz und Bandbreite für in der Cloud gehostete Anwendungen bereitzustellen. Die verfügbare physische Bandbreite der Uplinks liegt oft auf einem gemeinsam genutzten Medium. Eingebaute Forward-Error-Correction-Methoden, die auf RLNC-Codecs basieren, sorgen dafür, dass die verfügbare Bandbreite gegenüber anderen Komponenten auf dem gemeinsamen Medium optimal genutzt wird. SecureEdge erweitert die Vorteile von SD-WAN effektiv auf Standorte mit einzelnen Uplinks und Remote-Usern.

Flexibles Service Edge

Der SASE-Service ist sowohl als SaaS verfügbar, der direkt von Barracuda Networks verwaltet wird, als SecureEdge for Virtual WAN in Microsoft Azure, das von Microsoft verwaltet wird, oder als virtuelle und Hardware-Appliances, die vom Kunden oder einem Dienstleister verwaltet und gehostet werden. Unabhängig von der Bereitstellungsart erfolgt das gesamte intent-basierte Konfigurationsmanagement über das SecureEdge Manager Cloud-Portal. Der Service sorgt dann für die Weitergabe und Durchsetzung der Änderungen an jedem Service-Edge, Standort, User oder Ding.

Alles aus einer Hand

Die Barracuda SecureEdge-Plattform ist die einzige Lösung, die Sicherheit und Konnektivität von Usern, Standorten und Dingen in einem benutzerfreundlichen, cloudbasierten Format bietet, das unterschiedliche Technologien - wie SD-WAN für den Standortzugang und Sicherheit und Konnektivität für Dinge und industrielle Sicherheit - in einer Plattform integriert.

Barracuda SecureEdge Feature Highlights

Allgemeine und zentrale Verwaltung

- Alle Funktionen werden zentral über den Cloud-basierten SecureEdge Manager verwaltet
- Management verfügbar in: Englisch, Französisch, Japanisch
- Azure AD-Unterstützung für user-basierten Einsatz
- Zero-Touch Deployment für Site Devices
- Self-Provisionierung (Onboarding) für SecureEdge Access Agent
- Einfach einzurichtende Hochverfügbarkeit
- Einfache Integration von industriellen IoT-Umgebungen mit Hilfe von Barracuda Secure Connector Appliances
- Multi-Tenant-Funktionen
- Mehrere Workspaces pro Mandant
- Public SecureEdge Edge Service Subscription verfügbar über Barracuda Networks in 26 Regionen weltweit
- Private SecureEdge Edge Services verfügbar über SecureEdge Site Device oder CloudGen Firewall, administriert via SecureEdge Manager
- Private SecureEdge Edge Service verfügbar über Azure Virtual WAN, administriert via SecureEdge Manager

Reporting und Visualisierung

- Anpassbare Dashboards mit Detail-Widgets für:
  - Advanced Threat Protection
  - Appliance Configuration Status
  - Application Risk
  - Edge Service Status
  - Geo Destinations, Geo Sources
  - IPS Incidents
  - Device Status
  - SD-WAN Map
  - Recent Events
  - Top Allowed/Blocked (User, Apps, URL, Domain)
  - SD-WAN Tunnel Status
- Live Connections: Visualisierung des Datenverkehrs für jeden Standort und SecureEdge Edge Service mit Advanced Filtering
- Recent Connections: Visualisierung von abgelaufenem Datenverkehr für jeden Standort und SecureEdge Edge Service mit Advanced Filtering für schnelles Troubleshooting
- Firewall Report Creator (inkludiert) für unbegrenzte benutzerdefinierte Berichte über mehrere Standorte und Dienste
- Integration mit Barracuda XDR
- Integration mit Azure Log analytics für alle Site Devices und Edge Services

Web Security und Secure Internet Access

Content Filtering

- SSL/TLS Inspection
- URL-Filtering nach Kategorie, benutzerdefinierter Kategorie, Domain
- benutzerdefinierte Kategorien
- Safe Search Enforcement
- Ad-Blocking
- Application Control und Blocken tausender gängiger Webanwendungen

Advanced policy creation

- Anpassbare Standardrichtlinien für alle Benutzer und Standorte
- Ausnahmen für Benutzer-, Gruppen-, Netzwerk- und Site-Richtlinien
- Benutzerdefinierte Kategorien und Blockseiten
- Richtlinien:
  - Sperren (Block)
  - Erlauben (Allow)
  - Warnen (Warn)
  - Benachrichtigen (Notify)

Advanced Threat Protection

- Integration mit Barracuda ATP Service
- Schutz gegen:
  - Ransomware
  - Advanced Persistent Threats
  - Polymorphe Viren
  - Zero-Hour-Malware

Web Monitoring

- Überwachung sozialer Medien
- Überwachung von benutzerdefinierten Schlüsselwörter
- Warnungen bei
  - Verdächtigen Schlüsselwörter
  - Schlüsselwörter zu Cyber-Mobbing
  - Schlüsselwörter mit Terrorismusbezug

Secure Internet Access, Remote Filtering

- SecureEdge Access Agent für Windows, macOS, iOS, Android und Linux
- Lokales DNS-Filtering
- Durchsetzung der Sicherheitsstandards auf SecureEdge Access Agents
- Benutzerdefinierte, selektive Sicherheitsüberprüfung durch jede Art von SecureEdge Edge Service (SaaS, Azure, Private oder bestehende CloudGen Firewall-Installationen)

Konnektivität & SD-WAN

- Zero-Touch Deployment für Site Devices
- Zero-Touch Registrierung für Access Agents
- Automatische SD-WAN-Richtlinien für Hunderte von Anwendungen
- Optimierte Auswahl des direkten Internet-Uplinks
- Internet-Uplink Optimierung (Forward Error Correction) für Site Devices und Access Agents
- Gleichzeitige Nutzung von mehreren Uplinks (bis zu 16 Transporte) pro SD-WAN-Verbindung
- Dynamische Bandbreitenerkennung
- Leistungsbasierte Transportauswahl
- Applikationsorientiertes Traffic-Routing
- Adaptives Session-Balancing über multiple Uplinks
- Applikationsbasierte Providerauswahl
- Provider-Pinning
- Uplink Health Check
- Unterstützte Uplink Varianten:
  - Dynamic
  - Static
  - Express Route
  - Bridge
  - WWAN (LTE Modem)
  - PPPoE

Konnektivität & SD-WAN (fortsetzung)

- Verschlüsselungsprotokolle: IPsec v2, TINA
- Point-to-Site-Benutzerkonnektivität (VPN)

ZTNA

- SecureEdge Access Agent für Windows, macOS, iOS, Android und Linux
- Konsistente Bedienung und einheitliches Erscheinungsbild in allen Betriebssystemen
- Integrierter Secure Internet Access für alle Betriebssysteme
- Integrierter Rollenbasierter Zugang unter Einbeziehung von User/Gruppen Berechtigungen
- Integrierte Device-Health-Check basierend auf ZTNA Richtlinien
- ZTNA Zugang auf TCP/UDP-basierte Applikationen, unabhängig vom Host
- Unterstützung für Anwendungen in jeder Public Cloud und lokal mit der SD-WAN Connector App
- Inbound-Unterstützung für lokal gehostete Anwendungen hinter SecureEdge Site Devices
- Inbound-Unterstützung für lokal gehostete Anwendungen hinter Barracuda CloudGen Firewall
- Unterstützte Richtlinien für Device-Health: Blockieren von Jailbreak-Geräten, Erfordernis einer Bildschirmsperre, Erfordernis einer Firewall, Erfordernis eines Virenschutzes, Erfordernis von Betriebssystem-Updates, Erfordernis von SecureEdge Access Agent-Updates, Erfordernis einer Festplattenverschlüsselung
- Beschränkung des Zugriffs auf Anwendungen basierend auf dem Betriebssystem Pre-Logon-Konnektivität für das zentrale Management von unternehmenseigenen Geräten
- Verwaltung zugelassener Geräte
- Verwaltung zugelassener Benutzer

Sicherheit der Standorte und Firewall-as-a-Service

- Stateful Packet Inspection und Forwarding
- Standortbezogene ACLs
- Servicebezogene ACLs
- Benutzererkennung
- IDS/IPS
- Ingress NAT
- Applikationskontrolle und granulare Applikationsdurchsetzung
- Abfangen und Prüfen von SSL/TLS-verschlüsselten Anwendungen
- ATP, IPS, Applikationskontrolle und Web-Filtering im Single-Pass-Modus
- DHCP-Server
- Dynamische und statische Routen
- Netzwerk-Bridge Modus
- VLAN-Unterstützung
- Benutzerdefinierte weitergeleitete Domänen

Weitere Informationen über den Funktionsumfang von Barracuda SecureEdge finden Sie unter barracuda.com.

Technische Angaben

SecureEdge Access Agent

BETRIEBSSYSTEM	Windows	macOS [1]	Android	iOS / iPadOS	Linux
Unterstützte Betriebssysteme	Windows 10 Windows 11	macOS 11 (Big Sur) macOS 12 (Monterey) macOS 13 (Ventura)	Android 10 (oder höher)	iOS/iPadOS 15 iOS/iPadOS 16	Aktuelle Ubuntu- und Fedora-Distributionen
Self-Provisioning	✓	✓	✓	✓	✓
Client Health Enforcement	✓	✓	✓	✓	✓
App unterstützt	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP
Last-Mile Optimierung	✓	✓	✓	✓	✓
URL Filterung	✓	✓	✓	✓	✓
Selektive Sicherheitsüberprüfung	✓	✓	✓	✓	✓
Max. gleichzeitige Geräte/User	5 Geräte pro User (plattformübergreifend)				

SD-WAN Connector

BETRIEBSSYSTEM	Windows	Linux
Unterstützte Betriebssysteme	Windows 10 (Pro, Server, Intel Architektur) Windows 11 (Pro, Server, Intel Architektur)	Aktuelle Ubuntu- und Fedora-Distributionen (Desktop, Server, Cloud Editions) Generic x86_64 Linux
Single-Click Self-Provisioning [2]	✓	✓
Verschlüsselung zum Service	Proprietär (TINA Verschlüsselung)	Proprietär (TINA Verschlüsselung)
Max. Durchsatz [3]	100 Mbps-1 Gbps (abhängig von Server-Hardware)	100 Mbps-1 Gbps (abhängig von Server-Hardware)
Unterstützte Cloud Plattformen	Alle Cloud-Anbieter, die IaaS- oder Container-Dienste für Windows und Linux anbieten	

SecureEdge Service gemanaged von Barracuda

	Americas	EMEA	APAC
Verfügbar für folgende Regionen	Brasilien (Süd), Kanada (Mitte, Ost), USA (Mitte, Ost, West)	Europa (Nord, West), Frankreich, Deutschland, Norwegen, Südafrika, Schweiz, VAE, UK (Süd, West)	Asien (Ost, Südost), Australien (Mitte, Ost, Südost), Indien (Mitte, Süd), Japan (Ost, West), Korea

SecureEdge Service for Microsoft Azure Virtual WAN

	MICROSOFT AZURE VIRTUAL WAN SCALE UNIT							
	2	4	10	20	30	40	60	80
Verfügbare Bandbreite	1 Gbps	2 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps	30 Gbps	40 Gbps

SecureEdge Site Devices

	HARDWARE SITE DEVICES									VIRTUELLE SITE DEVICES				
	DESKTOP		1U RACK MONTAGE			TRAGSCHIENEN KOMPATIBEL								
	T100B	T200C	T400C	T600D	T900B	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
Edge Service Funktionen	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
EMPFOHLENE ANZAHL AN USER (Detailliertere Informationen zur Leistung finden Sie in der Broschüre Specifications)														
Threat Protection	50-100	150-300	300-1,000	1,000-4,000	6,000-9,000	n/a	n/a	50-100	150-300	50-100	150-300	300-1,000	1,000-4,000	6,000-9,000
Nur Web Security	300	1,000	5,000	10,000	20,000	n/a	n/a	100	150	300	1,000	5,000	10,000	20,000
HARDWARE (Detailliertere Informationen zur Hardware finden Sie in der Broschüre Specifications)														
Rugged Hardware	-	-	-	-	-	-	✓ [4]	✓ [5]	✓ [5]	-	-	-	-	-
Lizensierte vCPUs (virtuell)	-	-	-	-	-	-	-	-	-	2	4	8	10	bis zu 32
Kupfer NICs (1 GbE)	5x	12x	8x	10x	8x	4x	4x	2x	5x	-	-	-	-	-
Glasfaser NICs (1 GbE)	-	4x	-	8x	8x	-	-	1x	2x	-	-	-	-	-
Glasfaser NICs (10 GbE)	-	-	2x	2x	4x	-		-	-	-	-	-	-	-
Glasfaser NICs (40 GbE)	-	-	-	-	2x	-	-	-	-	-	-	-	-	-
Virtuelle NICs	-	-	-	-	-	-	-	-	-	5-16x	5-16x	5-16x	5-16x	5-16x
WiFi (AP / Client)	-	-	-	-	-	✓ [6]	✓ [8]	-	-	-	-	-	-	-
GSM / UTMS	-	-	-	-	-	✓ [7]	✓ [9]	-	-	-	-	-	-	-
4G / LTE	-	-	-	-	-	✓ [7]	✓ [9]	-	-	-	-	-	-	-

1 *SecureEdge Access Agent wird auf offiziell von Apple Inc. unterstützten und gewarteten Betriebssystemen unterstützt. Zum Zeitpunkt der Erstellung dieses Dokuments umfasste dies die oben genannte Betriebssystemversion. Ältere Versionen oder Geräte, die gemäß https://support.apple.com/en-us/HT201624 als "vintage" oder "obsolete" definiert sind, können funktionieren, werden aber nicht offiziell von Barracuda SecureEdge Access Agent unterstützt.*

2 *Erfordert lediglich eine Internetverbindung und ein über SecureEdge Manager generiertes Token.*

3 *Abhängig von der installierten Hardware und der Speicherbelegung; nutzt einen einzigen CPU-Thread.*

4 *Lüfterlos, mit erweitertem Betriebstemperaturbereich (-20 bis +70 °C), die speziell für raue Umgebungen entwickelt wurden.*

5 *Lüfterlos, mit erweitertem Betriebstemperaturbereich (-40 bis +75 °C), die speziell für raue Umgebungen entwickelt wurden.*

6 *Submodelle FSC21 und FSC25.*

7 *Submodelle FSC24 und FSC25.*

8 *Submodelle FSC31 und FSC35.*

9 *Submodelle FSC34 und FSC35.*

Barracuda
Your journey, secured.