Barracuda SecureEdge

Secure users, sites, and things—and connect to any application no matter where it's hosted

SecureEdge provides secure application access, cloud-based security for endpoints, and automated SD-WAN connectivity for sites and industrial facilities of any type or size. Remote users access applications directly from any type of device. Zero-trust enforcement, URL filtering, and last-mile traffic optimization all ensure that application access is always secure and optimized to make the most of shared internet lines.

Secures users, sites and things

A hybrid workforce, direct-to-app architectures, and cloud migration have largely made legacy security architectures obsolete. New cloud-based security solutions have emerged, but their "cloud only" approach targeted at large enterprises often results in inconsistent security protection or poor user experience, especially when accessing hybrid apps. Barracuda SecureEdge was built from the ground up as a security platform to be cloud managed, cloud delivered, and available as auto-managed edge services for any type of device, deployment, or platform.

Powered by the vast Barracuda Threat Intelligence Network, A.I. derived security intelligence extends beyond the typical site or cloud service deployment, extending advanced security to any user on any device and all things.

Connects any device, app, or cloud/hybrid environment

Traditional VPN solutions have proven to be inherently insecure, lack scaling options, and fail to meet the needs for cybersecurity resilience as required by many regulating bodies. Newly emerging zero-trust solutions have been designed for secure access to cloud-based resources only, and are often hard to set up manage, and use in the real world. Today, users on any device expect secure and reliable access to any app, whether it's hosted in the cloud or on-premises. The solution should also be easy to use and enhance application access for optimal user experience. Barracuda SecureEdge Access provides all of this. Available for any type of device, any platform, and any cloud or on-premises, it utilizes the SD-WAN capabilities of site devices and optimizes application flow for an unparalleled remote-user experience.

Easy to acquire, deploy, and manage

The Barracuda SecureEdge platform is a single-vendor SASE solution that cleverly integrates and automates its components. The core services are available as SaaS, in Azure Virtual WAN, and even as private instances. Connectivity is created by zero-touch deployment of a site device with automatic SD-WAN optimization to the service. Remote users on any operating system self-enroll with the SecureEdge Access Agent, which is available from any app store and includes up to 5 devices for ZTNA and Secure Internet Access (SIA). All of this is centrally managed and enforced via the cloud-based SecureEdge Manager. Intent-based networking and intent-based security policies provide the quickest and most intuitive way to centrally orchestrate a SASE solution, including ZTNA and secure SD-WAN for connectivity.

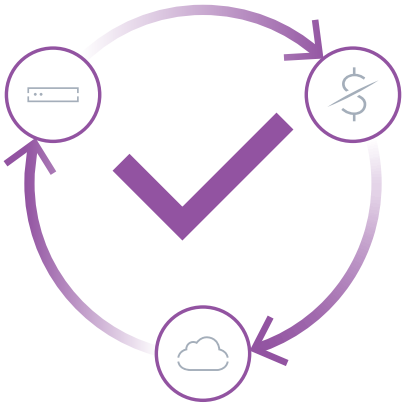
Barracuda SecureEdge business benefits

Consistent security posture across sites, users, and things

Security policies are first defined in the cloud-based management portal and then extended to each user, site, and IoT device or factory floor equipment. Powered by the vast Barracuda Threat Intelligence Network, our A.I.-derived security intelligence extends beyond the typical site or cloud service deployment, and offers advanced security to any user on any device and to all things.

Secure anytime, anywhere connectivity to any application

Today, many organizations need their users to access applications as SaaS, hosted in their cloud environment and on-premises. As if this was not challenging enough, organizations also need to support a model where the majority of employees can work fluidly between corporate offices, branch offices, home offices, and on the road. Barracuda SecureEdge Access provides zero-trust secure access to any application, no matter where it is hosted and from any type of device.



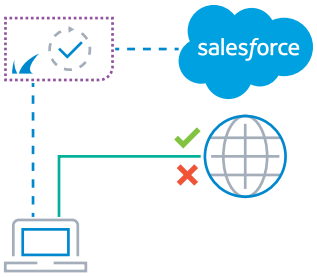
Save costs with a cloud on-ramp

SecureEdge site devices, fully integrate into the SASE concept of SecureEdge, include secure SD-WAN capabilities to enable fast access to apps hosted in the cloud. SecureEdge site devices deploy quickly via zero-touch and connect to services in the cloud automatically. They optimize cloud uplink traffic via packet loss reduction and other advanced SD-WAN optimizing functions so businesses can forego expensive leased lines.

Operational efficiency with single-vendor consolidation

By tightly integrating multiple components, businesses can consolidate multiple vendor solutions into one., reduce their trained IT staff, consolidate and decrease their ongoing subscriptions, and yet still benefit from improved security coverage, faster application access, better site connectivity, and greater agility in the IT functions of their business.

Example use cases for the Barracuda SecureEdge SASE platform

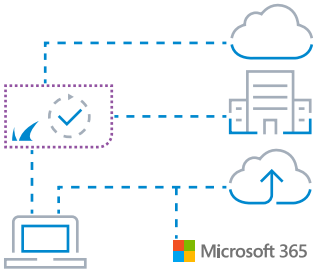


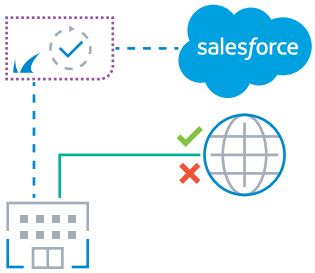
Secure Internet Access (SIA) for mobile users

Today, many employees work fluidly between corporate offices, branch offices, home offices, and on the road. And yet the level of corporate security policies, for example, for acceptable web access, needs to be the same. Powered by the vast Barracuda Threat Intelligence Network and an A.I.-derived security intelligence, the SecureEdge Access Agent extends security and policy compliance to any device on any platform.

Secure access to private and SaaS apps (ZTNA)

Provide direct, secure access to all sanctioned applications with continuous security and eligibility valuation, no matter where the apps are hosted and for any user on any device. Optimize last-mile network traffic to make the best use of shared internet uplinks.



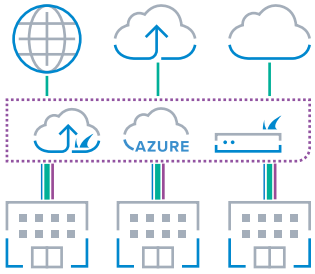


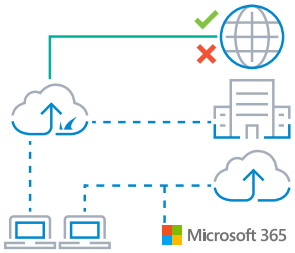
Secure Web Gateway (SWG) for office and branch edges

SecureEdge site devices protect the office edge and any device in the office from internet-borne malware, spyware, and other unwanted content. In addition to malicious-code detection, this includes URL filtering and application control for thousands of popular applications (even ones that are not web based). Enforcement can be done either on the device or in the SecureEdge service layer.

Cloud-delivered office connectivity and security

Securely connect any branch office to the cloud and ensure it is protected against internet-borne threats like malware, ransomware, and spyware. Secure SD-WAN provides the on ramp to the cloud for optimal application performance.



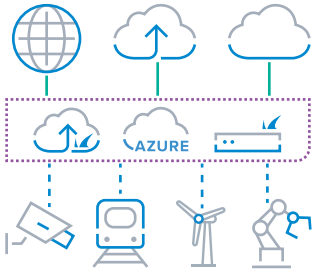


Firewall as a Service (FWaaS)

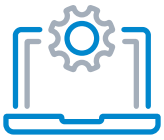
Provide cloud-delivered, next-generation security, secure internet access, and application control to any remote user on any device.

Security and connectivity for “things” (IoT/ICS)

Easily and quickly connect almost any IoT device or heavy machinery on the factory floor to the cloud of your choice or the office you need. Centrally provide the security you need.



Barracuda SecureEdge solution highlights



Agent auto-provisioning

Remote users easily self-enroll on up to 5 devices. The SecureEdge Access Agent is available for free download on any app store and even for Linux. Just click on the link that is sent out via the enrollment email to get started.

Last-mile optimization

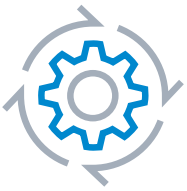
Built-in internet traffic optimization from the service to the SASE agent enables endpoints to grab more of the available bandwidth on shared internet lines for improved application performance. The underlying technology to remediate packet loss is based on random linear network codes (RLNC), a powerful encoding scheme. Algorithms based on RLNC codes react much faster to losses and remediate these losses faster on the fly, thereby requiring fewer packet retransmissions and reducing overhead on the devices.

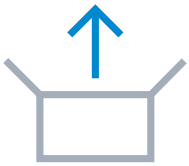
Intent-based networking & policy management

In the past, security solutions were either complicated to use or lacking in their underlying security capabilities. Firewalls and other security solutions were based on assigning networks, IP ranges, and point product security capabilities to these networks. Intent-based operations are built from the ground up as part of the concept of the SecureEdge Manager for our unified SASE platform. The Barracuda SecureEdge SASE platform is strictly user-, group-, and application-specific. Remote users can thereby access private and public cloud applications, and the internet much faster.

"Once-only" intent-based management

In addition to thousands of predefined applications, the SecureEdge SASE platform lets you create private applications that can be hosted anywhere. It's quick, easy, and has to be done only once—and is then shared with security, SD-WAN, and ZTNA policy definitions. All necessary networking and routing optimizations are done completely transparently in the background and automatically applied to each site, user, or service instance.



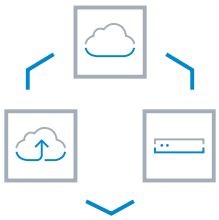


Zero-Touch connectivity for any site

Onboarding sites and things to the Barracuda SecureEdge SASE platform could not be easier. With just a couple of mouse clicks, your configuration in the cloud-based manager is complete, and site devices are drop-shipped to the remote location. Zero-touch deployment automatically connects sites and IoT devices to the nearest SecureEdge entry point.

Auto-SD-WAN

Once plugged in and turned on, each site device automatically makes use of all available uplinks to connect to the SASE service. With SD-WAN policy settings predefined for thousands of common business applications, the devices ensure that the best uplink path is always used for the application.



Flexible Service Edge

The Barracuda SecureEdge SASE service is available either as SaaS directly managed by Barracuda Networks, as SecureEdge for Virtual WAN in Microsoft Azure and managed by Microsoft, or as virtual and hardware appliances to be managed and hosted by the customer or trusted partner. Regardless of deployment type, all intent-based configuration management is done from the SecureEdge Manager cloud portal. The service then takes care of propagating and enforcing the changes to each service edge, site, user, or thing.

Single vendor

The Barracuda SecureEdge platform is the only solution that delivers security and connectivity of users, sites, and things in an easy-to-use cloud-based format that integrates otherwise disparate technologies—like SD-WAN for site access and security and connectivity for things and industrial security—into one platform.

Technical specifications

SecureEdge Access Agent

OS	Windows	macOS [1]	Android	iOS / iPadOS	Linux
Supported OS versions	Windows 10 Windows 11	macOS 11 (Big Sur) macOS 12 (Monterey) macOS 13 (Ventura)	Android 10 (or later)	iOS/iPadOS 15 iOS/iPadOS 16	Current Ubuntu and Fedora distributions
Self-provisioning	✓	✓	✓	✓	✓
Client health enforcement	✓	✓	✓	✓	✓
App support	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP	HTTP/HTTPS & TCP/UDP
Last-mile optimization	✓	✓	✓	✓	✓
URL filtering	✓	✓	✓	✓	✓
Selective security inspection	✓	✓	✓	✓	✓
Max. concurrent devices/user	5 devices per user (across all platforms)				

SD-WAN Connector

OS	Windows	Linux
Supported OS versions	Windows 10 (Pro, Server, Intel architecture) Windows 11 (Pro, Server, Intel architecture)	Current Ubuntu and Fedora distributions (Desktop, Server, Cloud editions) Generic x86_64 Linux
Single click self-provisioning [2]	✓	✓
Encryption to service	Proprietary (TINA encryption)	Proprietary (TINA encryption)
Max. throughput [3]	100 Mbps-1 Gbps (depending on server hardware)	100 Mbps-1 Gbps (depending on server hardware)
Supported cloud platform	Any cloud provider offering IaaS or container services for Windows and Linux	

SecureEdge Service managed by Barracuda

	Americas	EMEA	APAC
Available for following regions	Brazil, Canada Central, Canada East, US Central, US East, US West	Europe North, Europe West, France, Germany, Norway, South Africa, UAE, UK South, UK West	Asia East, Asia Southeast, Australia Central, Australia East, Australia Southeast, India Central, India South, Japan East, Japan West, Korea

SecureEdge Service for Microsoft Azure Virtual WAN

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

SecureEdge site devices

	HARDWARE SITE DEVICES									VIRTUAL SITE DEVICES				
	DESKTOP		1U RACK MOUNT			DIN RAIL COMPATIBLE								
	T100B	T200C	T400C	T600D	T900B	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
PERFORMANCE														
Site performance up to	300 Mbps	1.3 Gbps	3.0 Gbps	6.0 Gbps	9.3 Gbps	30 Mpbs	30 Mpbs	200 Mpbs	240 Mbps	300 Mbps	700 Mbps	1.5 Gbps	3.8 Gbps	9.3 Gbps
Recommended no. of users	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
Concurrent sessions	80,000	300,000	500,000	2,100,000	4,000,000	n/a	n/a	80,000	250,000	80,000	250,000	500,000	2,100,000	4,000,000
New session/s	8,000	12,000	20,000	115,000	190,000	n/a	n/a	8,000	12,000	8,000	12,000	20,000	115,000	190,000
Edge Service capabilities	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
HARDWARE														
Rugged hardware version	-	-	-	-	-	-	✓[4]	✓[5]	✓[5]	-	-	-	-	-
Licensed vCPUs (virtual)	-	-	-	-	-	-	-	-	-	2	4	8	10	up to 32
Copper NICs (1 GbE)	5x	12x	8x	10x	8x	4x	4x	2x	5x	-	-	-	-	-
Fiber NICs (SFP) (1 GbE)	-	4x	-	8x	8x	-	-	1x	2x	-	-	-	-	-
Fiber NICs (SFP+) (10 GbE)	-	-	2x	2x	4x	-		-	-	-	-	-	-	-
Fiber NICs (QSFP+) (40 GbE)	-	-	-	-	2x	-	-	-	-	-	-	-	-	-
Virtual NICs	-	-	-	-	-	-	-	-	-	5-16x	5-16x	5-16x	5-16x	5-16x

1— SecureEdge Access Agent is supported on officially Apple Inc. supported & maintained operating systems. As of the creation of this document, this included the OS version mentioned above. Older versions or devices that are defined as "vintage" or "obsolete" according to https://support.apple.com/en-us/HT201624 may work, but are not officially supported with Barracuda SecureEdge Access Agent.

2— Just requires internet connectivity and a token generated via SecureEdge Manager.

3— Depending on hardware installed on and memory assignment; utilizes a single CPU thread.

4— Fanless site devices with extended operating temperature range (-4 to +158 °F) purpose-built for harsh environments.

5— Fanless site devices with extended operating temperature range (-40 to +167 °F) purpose-built for harsh environments.

Barracuda
Your journey, secured.