Barracuda
Your business, secured.

Barracuda SecureEdge

Microsoft Azure
Certified

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

SecureEdge provides secure application access, cloud-delivered 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

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, endpoint, 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

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 must 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 own

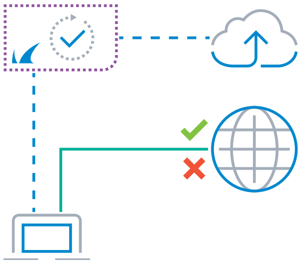
The Barracuda SecureEdge platform is a single-vendor SASE solution that cleverly integrates and automates its components. The core services are available as SaaS, in Azure Virtual WAN, and even as private instances, all managed via the same easy-to-use web-based user interface.

Site 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 on all app stores and can be used on up to 10 devices per user simultaneously for Zero Trust Network Access (ZTNA) and Secure Internet Access (SIA).

All 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.

Example use cases for the Barracuda SecureEdge SASE platform

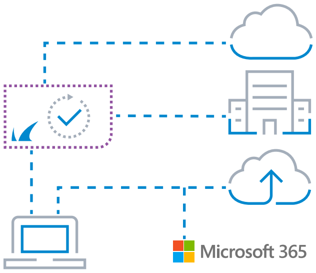


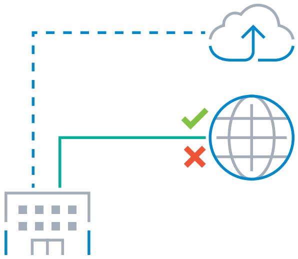
Secure Internet Access (SIA) for mobile users

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.



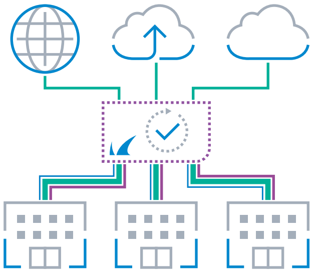


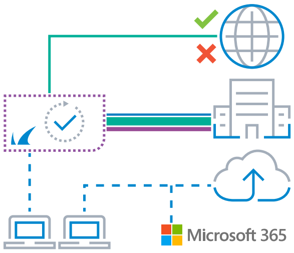
Secure Web Gateway (SWG) for office and branch edges

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.



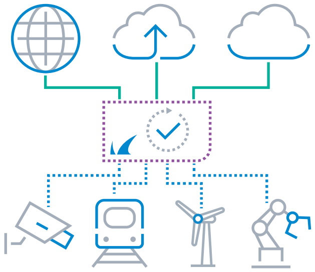


Firewall as a Service (FWaaS)

Next-generation firewall capabilities are delivered to any site or any client by a cloud service. This includes network access controls, application control, web filtering, Advanced Threat Prevention, Intrusion Prevention System (IPS), and deep SSL/TLS inspection.

Security, connectivity, and ZTNA remote access for things (IoT/ICS)

Secure and connect industrial devices to the cloud of your choice or the office.
Provide secure ZTNA based access to industrial devices, regardless of location.



Barracuda SecureEdge solution highlights

Easily deployed

SecureEdge Access Agents, available for up to 10 devices simultaneously per user, can easily be deployed via self- or mass-enrollment and mobile device management. Access Agents are available for Windows, macOS, iOS, Android, and Linux.

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.

Advanced Web Security

Protecting your network and remote users from online threats has never been easier. Whether employees are in the office behind a site device, work-from-home or anywhere else - SecureEdge examines web traffic and blocks access to harmful websites. Company policies for web-surfing are enforced down to very granular levels. Visibility into SSL/TLS encrypted web traffic and suspicious keyword filters provides unrepresented visibility on what is happening in your organization.

Optimized connectivity, anytime, and anywhere

Every SecureEdge site device and SecureEdge Access Agent optimize network traffic to provide the best possible latency and bandwidth to cloud hosted applications. The available physical bandwidth of the uplinks is often on a shared medium. Built-in forward error correction methods based on RLNC codecs effectively make sure that the available bandwidth is used to the best extend over other constituents on the shared medium. SecureEdge effectively expands the benefits of SD-WAN to sites with single uplinks remote users.

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.

Barracuda SecureEdge Feature Highlights

General & central management

- All features centrally managed via cloud-based SecureEdge Manager
- Management languages available: English, German, French, Japanese
- Zero-touch deployment for site devices
- Self-provisioning (onboarding) for SecureEdge Access Agent
- Easy-to-setup high availability deployments
- Easy-to-integrate Industrial IoT environments via Barracuda Secure Connector appliances
- Multi-tenant capabilities
- Multiple workspaces per tenant
- Public SecureEdge Edge Service subscription available via Barracuda Networks in 26 regions across all continents
- Private SecureEdge Edge Services available provided with SecureEdge Site device or CloudGen Firewall, managed via SecureEdge Manager
- Private SecureEdge Edge Service available with Azure Virtual WAN, managed via SecureEdge Manage

Authentication & Identity Provider Support

- Support for SAML-based authentication and seamless integration with third party identity providers Microsoft Entra ID, Okta, Google Workspace, OpenID, MSAD, and LDAP.
- Support for email-based authentication

Reporting and visibility

- Customizable dashboards with detail widgets for (excerpt):
  - Advanced Threat Protection
  - Appliance Configuration Status
  - Application Risk
  - Edge Service Status
  - Geo destinations and sources
  - IPS incidents and recent events
  - Device status
  - SD-WAN map and tunnel status
  - ZTNA allowed / blocked (user, app, URL, domain)
  - ZTNA device map
- Live connections: traffic visibility for every site and SecureEdge Edge Service with advanced filtering
- Recent connections: historical session traffic visibility for every site and SecureEdge Edge Service with advanced filtering for quick troubleshooting
- Firewall Report Creator (included) for unlimited custom reports across multiple sites and services
- Integration with Barracuda XDR
- Integration with Azure Log analytics for all site devices and Edge Services

> For more information on the feature set of Barracuda SecureEdge, please visit barracuda.com.

Web Security & Secure Internet Access

Content filtering

- SSL/TLS inspection
- URL filtering by category, custom category, domain
- Custom categories
- Safe search enforcement
- Ad-blocking
- Application control and blocking for thousands of common web apps

Advanced policy creation

- Customizable default policy for all users and sites
- User, group, network, and site policy exceptions
- Custom categories and block pages
- Block, allow, warn, and notify policies

Advanced Threat Protection

- Integration with Barracuda ATP service
- Protection against:
  - Ransomware
  - Advanced persistent threats
  - Polymorphic viruses
  - Zero-hour malware

Web monitoring

- Social media monitoring
- Custom keyword monitoring
- Alerts on
  - Suspicious keywords
  - Cyber-bullying keywords
  - Terrorism keywords

Available deployment methods

- Web proxy[1]
- Inline mode with single-pass scanning

Secure Internet Access, remote filtering

- SecureEdge Access Agent for Windows, macOS, iOS, Android, and Linux
- Local DNS filtering
- Client security posture enforcement
- User-defined selective security inspection by any type of SecureEdge Edge Service (SaaS, Azure, Private, or existing CloudGen Firewall deployments)

CASB

- Proxy-based CASB support for hundreds of business applications (e.g., Microsoft Office365, Netsuite, SAP, etc.)

Connectivity & SD-WAN

- Zero-touch deployment for site devices
- Zero-touch self-enrollment for Access Agent
- Automatic SD-WAN policies for hundreds apps
- Optimized direct internet uplink selection
- Internet uplink optimization (forward error correction) for site devices and clients
- Simultaneous use of multiple uplinks (up to 16 transports) per SD-WAN connection
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing
- Adaptive session balancing across multiple uplinks
- Application-based provider selection
- Provider pinning
- Uplink health check

Connectivity & SD-WAN (continued)

- Uplink types supported: Dynamic, static, Express Route, Bridge, WAN (LTE modem), PPPoE
- Encryption protocols: IPsec v2, TINA
- Point-to-Site user connectivity (VPN)

Cloud-based universal ZTNA

- Tamper proof SecureEdge Access Agent for Windows, macOS, iOS, Android, and Linux platforms
- Integrated role-based access based on user/group permissions
- Integrated device health check based on ZTNA policy requirements
- ZTNA access to any TCP/UDP-based application, regardless where hosted
- Support for applications in any public cloud and on-premises with the SD-WAN Connector app
- Inbound support for applications hosted on-premises behind SecureEdge site devices and/ or CloudGen Firewall deployments
- Supported device health policies: Block jailbroken devices, require screen lock, require firewall, require antivirus, require OS updates, require SecureEdge Access Agent updates, require disk encryption
- Limitation of access to applications based on OS type
- Pre-logon connectivity for central management of company owned devices
- Management for enrolled devices and users
- Application Catalog for quick access to pre-defined apps directly via SecureEdge Access Agents
- Extend ZTNA policy enforcement to campus, branch, and site locations
- Easy-to-provide ZTNA services as add-on for existing CloudGen Firewall deployments
- Across all platforms
  - Consistent usability, look and feel
  - Integrated secure internet access

Site security and Firewall-as-a-service

- Stateful packet inspection and forwarding
- Site-specific and service-specific ACLs
- User-identity awareness
- IDS/IPS
- Ingress NAT
- Application control and granular enforcement
- Interception and inspection of SSL/TLS-encrypted applications
- ATP, IPS, and application control in single-pass mode
- DHCP Server, DHCP Relay
- Dynamic and static routes
- Network bridge
- VLAN Support
- Custom forwarded domains

Global Network Connectivity

- Microsoft Global Network
- Teridion Connect & Teridion China

[1] Available for site devices and private edge services only.

Technical specifications

SecureEdge Access Agent

OS	Windows	macOS	Android	iOS / iPadOS	Linux
Supported OS versions[1]	Windows 10 or higher	macOS 12 (Monterey) or higher	Android 12 or higher	iOS/iPadOS 15 or higher	Current Ubuntu and Fedora distributions
Mass enrollment per user group, deployment via MDM	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓
Tamper proof	✓	✓[2]	✓[2]	✓[2]	✓
Max. concurrent devices/user	10 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[3]	✓	✓
Encryption to service	Proprietary (TINA encryption)	Proprietary (TINA encryption)
Max. throughput[4]	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 Edge Service, provided by Barracuda

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

SecureEdge Edge 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	T900C	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
Edge Service capabilities	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
RECOMMENDED NUMBER OF USERS (please refer to Specifications brochure for detailed performance information)														
Threat Protection	50-100	150-300	300-1,000	1,000-4,000	6,000-9,000	1-10[5]	1-10[5]	50-100	150-300	50-100	150-300	300-1,000	1,000-4,000	6,000-9,000
Web Security Only	300	1,000	5,000	10,000	20,000	1-10[5]	1-10[5]	100	150	300	1,000	5,000	10,000	20,000
HARDWARE (please refer to Specifications brochure for detailed hardware information)														
Rugged hardware version	-	-	-	-	-	-	✓[6]	✓[6]	✓[6]	-	-	-	-	-
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
WiFi (AP / Client)	-	-	-	-	-	✓[7]	✓[9]	-	-	-	-	-	-	-
GSM / UTMS	-	-	-	-	-	✓[8]	✓[10]	-	-	-	-	-	-	-
4G / LTE	-	-	-	-	-	✓[8]	✓[10]	-	-	-	-	-	-	-

For licensing details, please see the Licensing brochure.

Barracuda

Your business, secured.

[1] The Barracuda SecureEdge Access Agent will generally work fine on older operating system releases but is not officially tested nor supported. Running on unsupported releases is not recommended for production deployments.

[2] Requires MDM.

[3] Just requires internet connectivity and a token generated via SecureEdge Manager.

[4] Depending on hardware installed on and memory assignment; utilizes a single CPU thread.

[5] Security is applied at the SecureEdge Edge Service component the SC appliance is connected to.

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

[7] Sub-models FSC21 and FSC25.

[8] Sub-models FSC24 and FSC25.

[9] Sub-models FSC31 and FSC35.

[10] Sub-models FSC34 and FSC35.