Barracuda SecureEdge

Zero Trust Network Access (ZTNA) made easy

Microsoft Azure Certified

A hybrid workforce, accelerated cloud migration, and SaaS adoption have expanded security perimeters and attack surfaces. As a result, the implicit trust security model is no longer suitable for modern cybersecurity threats.

The Zero Trust Network Access (ZTNA) model ensures data and resources are inaccessible by default, and access is only be granted by identifying and authenticating every user, device, and request. Furthermore, the tight integration into the web filtering functionality of SecureEdge protects your users, organization, and brand reputation.

Ensure conditional, application-specific access

SecureEdge grants least privileged access to authorized apps without exposing your private network. Even authenticated users won't be able to scan or sweep the internal network, since they will only be able to observe apps and servers that are explicitly granted access to.

Secure SaaS applications

Secure access to SaaS applications with certificate-based authentication, which prevents advanced MFA bypass attacks, and mitigate breach risk for your employees and contractors. Enforce granular access policies and gain valuable insights and full visibility into your SaaS resource access flows, to mitigate security and compliance risks.

Easy to deploy and manage

Gain visibility and control over access to corporate applications for employees, contractors, and partners with unmatched speed. Manage, track, and verify the who, what, and when of privileged access in one product. 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).

Corporate Compliance

Securing traffic to and from the web is critical, but not all web security solutions are designed for the era of cloud-connected services, remote work force, and widely-distributed networks.

SecureEdge combines robust content filtering, granular policy enforcement and reporting, simple centralized management, and real-time threat intelligence to protect your users, your organization, and your brand.

Secure third-party access

Mitigate the risks associated with third-party access to your business with Zero Trust. SecureEdge enables secure, reliable and fast access to authorized apps and workloads in your network from any device, network, and location. SecureEdge enforces continuous device identity and security posture checks.

See other SecureEdge use cases:

Overview

Secure Web Gateway

Barracuda SecureEdge ZTNA Feature Highlights

General & central management

- On-premises, hybrid-cloud, and fully managed data-plane options
- All features centrally managed via cloud-based SecureEdge Manager
- Management languages available: English, German, French, Japanese
- Self-provisioning (onboarding) for SecureEdge Access Agent
- Multi-tenant capabilities
- Multiple workspaces per tenant

Authentication & Identity Provider Support

- Support for Identity Providers:
  - Google Workspace
  - OpenID
- Support for SCIM:
  - Microsoft Entra ID
  - Okta
- Support for authentication directories:
  - MSAD
  - LDAP
- Support for email-based authentication

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

Web Security & Corporate Compliance

Content filtering

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

Advanced Policies

- 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

Protection against

- Ransomware
- Advanced persistent threats
- Polymorphic viruses
- Zero-hour malware

Corporate Compliance - 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)

Cloud-based universal ZTNA

- Tamper proof SecureEdge Access Agent for all platforms
- Max. 10 devices per user in simultaneous use
- IPsec connectivity to third-party firewalls
- IPsec and BGP connectivity to cloud gateways
- 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 included Connector app for Windows and Linux servers (no routing)
- 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
- 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

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)				

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 (optional)

	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

Supported SecureEdge models - hardware and virtual (optional)

SecureEdge Site Device hardware	T100B	T200C	T400C	T600D	T900C
SecureEdge Site Device virtual	VT100	VT500	VT1500	VT3000	VT5000

Supported CloudGenFirewall models - hardware and virtual (optional)

CloudGen Firewall hardware	F12A	F18B	F80B	F180B	F280C	F380B	F400C	F600D	F800D	F900C	F1000B
CloudGen Firewall virtual	VFC1	VFC2	VFC4	VFC8	VFC16	VFC48					

For licensing details, please see the Licensing brochure.

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.

Barracuda
Your business, secured.