Barracuda SecureEdge

Microsoft Azure
Certified

Secure Web Gateway

Traditional web security and firewall solutions haven't been designed to combat against modern cyberthreats. Today's use of cloud-based apps and services offer your organization greater agility, scalability, and cost savings. But this also expands your attack surface, exposing your organization to a massive volume of sophisticated cyber-threats that easily evade traditional security measures.

Internet security provided by the Secure Edge platform provides advanced security at scale with cloud-based sandboxing and full visibility into encrypted TLS/SSL traffic, as well as full transparency into user-to-app connections based on identity, context, and business policies. As part of the SecureEdge SASE platform it is easy to deploy and integrates into the zero-touch workflow and managed XDR service for peace of mind around the clock.

Constantly evolving capabilities

SecureEdge and its Secure Web Gateway component is continually updated with the latest malware signatures, suspicious URL listings, and online application functionality.

Knowledge is power

SecureEdge' intuitive management interface delivers detailed, real-time visibility into network activity and web interactions. This lets you identify users and applications that waste bandwidth and harm productivity, and enforce granular policies to regulate access without impacting legitimate business uses.

Advanced Web Security

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.

Advanced Threat Protection

Secure Web Gateways with SecureEdge Site Devices include cloud-based sandboxing to protect against targeted threats, zero-day malware, and other spyware that cannot be detected otherwise.

Deep SSL Inspection

Visibility into SSL/TLS encrypted web traffic and suspicious keyword filters provides unrepresented visibility on what is happening in your organization.

Security without boundaries.

Enforcing access policies on remote devices that are used off-network is critical for preventing malware intrusions into the network, and for preventing data loss. SecureEdge Access and its Secure Web Gateway capabilites include protection of up to 10 devices per user to make sure that protection ensured - whenever and from whatever device users access resources or the internet.

Barracuda SecureEdge SWG 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
- 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 Manager

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

See other SecureEdge use cases:

Overview

Zero Trust Network Access

Reporting and visibility

- Search, analyze, and categorize logs for up to 30 days included with Energize Updates
- Ad-hoc as well as scheduled reporting
- Create and export graphical reports on
  - web usage
  - network
  - threat data
  - detailed user reports
- 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
  - 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 & Company Compliance

Content filtering

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

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

Protection against

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

Social Media Control (Web monitoring)

- Web application control
- Social media monitoring
- Custom keyword monitoring
- Alerts on (excerpt)
  - Suspicious keywords
  - Cyber-bullying keywords
  - Terrorism keywords

Application control

- Internet application blocking, including proxy applications (e.g., hotspot shield)
- IP and port blocking
- Google Apps controls

Remote Filtering (i.e., corporate compliance)

- Requires licensed SecureEdge Access Agent
- SecureEdge Access Agent ensuring secure internet access; available for all platforms
- Local DNS filtering
- Client security posture enforcement
- User-defined selective security inspection by any type of SecureEdge Service (SaaS, Azure, Private, or existing CloudGen Firewall deployments)

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 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.

[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.*

Barracuda®
Your business, secured.