Protecting the expanded network

Hybrid workforce, direct-to-app architectures, and cloud migration has created new security requirements that go beyond the traditional on-premises network security needs. Secure customers’ distributed network with the purpose-built Barracuda SecureEdge platform that can expand with customers’ evolving requirements.

Connect any device, app, or cloud/hybrid environment

Provide seamless user experience for remote workers with Barracuda SecureEdge Access. 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.

Expand your business

Like all Barracuda MSP offerings, Barracuda SecureEdge is available on an affordable monthly fixed-price basis. This extends the Barracuda MSP difference; helping MSPs expand security service offerings and revenue potential with no added complexity or capital cost.

Zero-touch management

With the Barracuda SecureEdge Manager, the cloud-based management portal, MSPs can deploy and manage Barracuda SecureEdge site devices without any onsite visits. Barracuda SecureEdge Manager allows MSPs to easily deploy a site device via its out-of-the-box configurations, gain access to all the information about security deployments in real time, and easily generate reports on one or all Barracuda SecureEdge site devices.
Barracuda SecureEdge Feature Highlights

General & central management
• All features centrally managed via cloud-based SecureEdge Manager
• Management languages available: English, German, French, Japanese
• Azure AD support for user-based operation
• 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 Manager

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

Web Security
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
• Alarms on:
  - Suspicious keywords
  - Cyber-bullying keywords
  - Terrorism keywords

Secure Internet Access, remote filtering
• SecureEdge Access Agent for Windows, macOS, iOS, Android, and Linux
• Local DNS filtering
• Client security posture enforcement
• Application risk enforcement
• Device status
• IDS/IPS
• User-identity awareness
• Site-specific and service-specific ACLs
• Stateful packet inspection and forwarding

Connectivity & SD-WAN
• Zero-touch deployment for site devices
• Zero-touch self-enrollment for SecureEdge 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
• Uplink types supported:
  - Dynamic
  - Static
  - Express Route
  - Bridge
  - LAN (LTE modem, PPPoE)
• Encryption protocols:
  - IPSec v2, TINA
• Point-to-Site user connectivity (VPN)

Universal ZTNA
• Tamper proof SecureEdge Access Agent for Windows, macOS, iOS, Android, and Linux platforms
• Consistent usability, look and feel across all platforms
• Integrated secure internet access across all platforms
• Integrated role-based access based on user/group permissions
• 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

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

### SecureEdge Access Agent

<table>
<thead>
<tr>
<th>OS</th>
<th>Windows</th>
<th>macOS 12 (Monterey) or higher</th>
<th>Android 12 or higher</th>
<th>iOS / iPadOS 15 or higher</th>
<th>Current Ubuntu and Fedora distributions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported OS versions</td>
<td>Windows 10 or higher</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mass enrollment per user group, deployment via MDM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-provisioning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Client health enforcement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>App support</td>
<td>HTTP/HTTPS &amp; TCP/UDP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Last-mile optimization</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>URL filtering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Selective security inspection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tamper proof</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Max. concurrent devices/user</td>
<td>10 devices per user (across all platforms)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### SD-WAN Connector

<table>
<thead>
<tr>
<th>OS</th>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported OS versions</td>
<td>Windows 10 (Pro, Server, Intel architecture)</td>
<td>✓</td>
</tr>
<tr>
<td>Single click self-provisioning</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Encryption to service</td>
<td>Proprietary (TINA encryption)</td>
<td>✓</td>
</tr>
<tr>
<td>Max. throughput</td>
<td>100 Mbps-1 Gbps (depending on server hardware)</td>
<td>✓</td>
</tr>
<tr>
<td>Supported cloud platform</td>
<td>Any cloud provider offering IaaS or container services for Windows and Linux</td>
<td>✓</td>
</tr>
</tbody>
</table>

### SecureEdge Edge Service, provided by Barracuda

<table>
<thead>
<tr>
<th>Americas</th>
<th>EMEA</th>
<th>APAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available for following regions</td>
<td>Europe (North, West), France, Germany, Norway, South Africa, Switzerland, UAE, UK (South, West)</td>
<td>Asia (East, Southeast), Australia (Central, East, Southeast), India (Central, South), Japan (East, West), Korea</td>
</tr>
</tbody>
</table>

- **Barracuda Networks** - **DATASHEET** - **Barracuda SecureEdge**
<table>
<thead>
<tr>
<th>Hardware Site Devices</th>
<th>Hardware Site Devices</th>
<th>Virtual Site Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>T100B</td>
<td>T200C</td>
<td>T400C</td>
</tr>
<tr>
<td><strong>Edge Service capabilities</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>RECOMMENDED NUMBER OF USERS</strong> (please refer to Specifications brochure for detailed performance information)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Protection</td>
<td>50-100</td>
<td>150-300</td>
</tr>
<tr>
<td>Web Security Only</td>
<td>300</td>
<td>1,000</td>
</tr>
<tr>
<td><strong>HARDWARE</strong> (please refer to Specifications brochure for detailed hardware information)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rugged hardware version</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Licensed vCPUs (virtual)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Copper NICs (1 GbE)</td>
<td>5x</td>
<td>12x</td>
</tr>
<tr>
<td>Fiber NICs (SFP) (1 GbE)</td>
<td>-</td>
<td>4x</td>
</tr>
<tr>
<td>Fiber NICs (SFP+) (10 GbE)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Fiber NICs (QSFP+) (40 GbE)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Virtual NICs</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>WiFi (AP / Client)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GSM / UTMS</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4G / LTE</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

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.
9. Sub-models FSC31 and FSC35.
10. Sub-models FSC34 and FSC35.