Barracuda SecureEdge
Our SASE, easy to deploy and manage firewall for MSPs

Protecting the expanded network
Hybrid workforce, direct-to-app architectures, and cloud migration has created new security requirements that goes beyond the traditional on-premises network security needs. Secure customers’ expanded network with the purpose-built Barracuda SecureEdge platform, multi-tenant, SASE firewall that is easy to deploy and use.

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, a web 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, access to all the information about security deployments in real time, and easily generate reports on one or all Barracuda SecureEdge site devices.
Technical specs

Security

Advanced multi-layered security
• Stateful packet inspection
• Single-pass architecture
• Advanced threat protection
• Intrusion detection and prevention
• Malware protection
• SSL inspection and interception
• URL filtering
• Application-base access control list
• Azure Active Directory two-factored authentication

Supported Microsoft Azure specifics
• Deployment directly via Azure Marketplace
• Native SaaS service in Azure
• Automates access to Microsoft Global Network
• Azure Log Analytics and Azure Sentinel support for optional data analysis
• Azure Secured Hub compatible
• Licensing via PAYG per user per hour

Management and automation

Zero-touch deployment
• No in-house pre-configuration
• No manual configuration on-site
• Site device installation without special-trained IT personnel onsite
• USB LTE modern support

Simple to deploy
• Smart default configurations
• Run either as pure-play SD-WAN solution next to existing security devices or as Secure SD-WAN solution replacing existing security devices

Simple to manage
• Predefined SD-WAN optimization policies for all common cloud applications
• Single web management portal with multi-tenant capabilities
• Continuous monitoring and optimizing
• Highest level of automation for superior Quality-of-Service and uninterrupted always-on connectivity for business-critical traffic and applications
• User and group-based security policies for URL filtering, malware protection, SSL inspection, and IPS/firewall rules

<table>
<thead>
<tr>
<th>HARDWARE SITE DEVICES</th>
<th>VIRTUAL SITE DEVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESKTOP</td>
<td>1U RACK MOUNT</td>
</tr>
<tr>
<td>PERFORMANCE</td>
<td></td>
</tr>
<tr>
<td>Site performance up to</td>
<td>300 Mbps</td>
</tr>
<tr>
<td>Recommended n. of users</td>
<td>50-100</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>80,000</td>
</tr>
<tr>
<td>New session(s)</td>
<td>8,000</td>
</tr>
<tr>
<td>HARDWARE</td>
<td></td>
</tr>
<tr>
<td>Rugged hardware version</td>
<td>-</td>
</tr>
<tr>
<td>Licensed vCPUs (virtual)</td>
<td>-</td>
</tr>
<tr>
<td>Copper NICs (1 GbE)</td>
<td>5x</td>
</tr>
<tr>
<td>Fiber NICs (SFP) (1 GbE)</td>
<td>-</td>
</tr>
<tr>
<td>Fiber NICs (SFP+) (10 GbE)</td>
<td>-</td>
</tr>
<tr>
<td>Fiber NICs (QSFP+) (40 GbE)</td>
<td>-</td>
</tr>
<tr>
<td>Virtual NICs</td>
<td>-</td>
</tr>
</tbody>
</table>

1—Fanless site devices with extended operating temperature range (-4 to +158 °F) purpose-built for harsh environments.
2—Fanless site devices with extended operating temperature range (-40 to +167 °F) purpose-built for harsh environments.