Barracuda **Email Security Gateway**

Complete Protection from Email-Borne Threats in Microsoft Azure

Barracuda®

The Barracuda Email Security Gateway for Microsoft Azure offers advanced email management and layered protection that is completely cloud-based, protecting against incoming email-based threats.

☑ **Security**
☐ Data Protection
☐ Application Delivery

The Barracuda Advantage

- Free Cloud Protection Layer providing:
  – Email spooling up to 96 hours
  – Inbound email filtering
- Barracuda Real-Time Protection
- Cloud-based encryption included free of charge
- Configuration backup to the cloud
- Preconfigured for quick deployment

Product Spotlight

- Industry-leading spam and virus defense for email
- Protection from data loss and reputation damage
- Advanced Threat Protection[1] to protect against ransomware and other advanced threats
- Advanced, granular policy management
- Also available as a physical or virtual appliance

Comprehensive Protection for the Long Term

The Barracuda Email Security Gateway includes spam and virus blocking, data protection, email continuity, DoS prevention, and policy management—combined to deliver a complete solution. As new requirements emerge, it is automatically updated with new capabilities to ensure continuous protection.

Complete Email Threat Protection

The Barracuda Email Security Gateway provides multi-layer security and email continuity. Advanced Threat Protection[1] combines behavioral, heuristic, and sandboxing technologies to protect against zero-hour, targeted attacks and ransomware.

Scalable and Easy to Use

Fast, easy set-up and simple, intuitive management keep time and resource needs low. The integration of the Barracuda Cloud Protection Layer makes it easy to scale capacity as your business grows.

Barracuda Cloud Protection Layer filters and spools inbound email traffic.

Internet → Cloud Protection Layer (Spooling & Filtering) → **ESG** Barracuda Email Security Gateway on Azure → Mail Servers
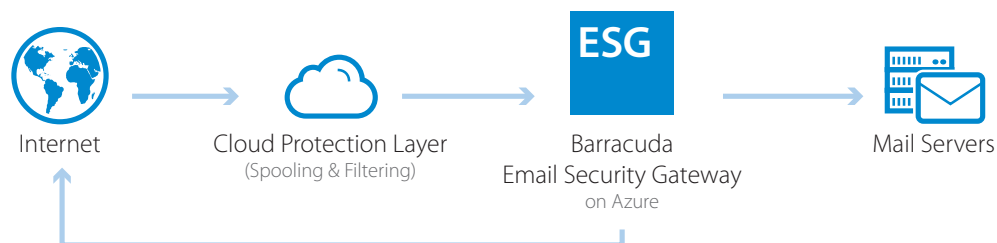
Technical Specs

Comprehensive Protection

- Spam and virus filtering
- Cloud Protection Layer
- Prevents spoofing, phishing, and malware
- Denial of Service (DoS/DDoS) protection
- Directory harvest protection

Advanced Policy Control

- IP and content-based filtering
- Bulk email categorization
- Content encryption
- Sender/recipient filtering
- RBL and DNSBL support
- Keyword blocking
- Character-set blocking
- Reverse DNS blocking
- URL pattern and category blocking
- TLS encryption policy
- Secondary authentication

Sender Authentication

- SPF and DomainKeys
- Emailreg.org
- Invalid bounce suppression

Spam Filter

- Rate control
- IP reputation analysis
- Fingerprint and image analysis
- Rules-based scoring algorithms

Virus Filter

- Triple-layer virus blocking
- Integrated Exchange AV Agent
- Decompression of archives
- File type blocking
- Barracuda Antivirus Supercomputing Grid
- Advanced Threat Protection[1] to protect against ransomware, zero hour and targeted attacks.

System Features

Administrators

- Web-based interface
- User account administration
- Reports, graphs, and statistics
- LDAP interface
- Multiple domain support
- Secure remote administration
- Delegated domain administration
- Delegated help desk role
- Email spooling
- Configure backup to cloud

End Users

- User-based filtering
- Individual spam scoring
- Personal allow and block lists
- End-user quarantine and digest emails
- Outlook add-in
- Bayesian analysis

MODEL COMPARISON	LEVEL 3	LEVEL 4	LEVEL 6
CAPACITY			
Azure Instance	D1	D2	D3
Active Email Users	3,000-10,000	8,000-22,000	15,000-30,000
Domains	5,000	5,000	5,000
FEATURES			
Advanced Threat Protection[1]	●	●	●
Cloud Protection Layer	●	●	●
MS Exchange/LDAP Accelerator	●	●	●
Per-User Settings and Quarantine	●	●	●
Delegated Help Desk Role	●	●	●
Syslog Support	●	●	●
Clustering & Remote Clustering	●	●	●
Per Domain Settings	●	●	●
Single Sign-On	●	●	●
SNMP/API	●	●	●
Customizable Branding	●	●	●
Per-User Score Settings	●	●	●
Delegated Domain Administration	●	●	●

* Also available in Vx (Virtual Edition). Specifications subject to change without notice.

[1] Advanced Threat Protection (ATP) is available as an add-on subscription.