Barracuda Email Security Gateway

Defend your AWS deployment against email-borne threats.

Get comprehensive email gateway security in your Amazon Web Services infrastructure, along with advanced capabilities that help you ensure business continuity and prevent data loss.

Barracuda Email Security Gateway for AWS gives you industry-leading protection against spam, viruses, and advanced malware—including zero-day ransomware and other threats when Advanced Threat Protection is enabled. Outbound filtering prevents data loss, and 96-hour email spooling in the Barracuda Cloud ensures continuity in case of email server downtime.

Email Security Gateway for AWS is available directly in the AWS Marketplace, or on a bring-your-own-license (BYOL) basis.

Comprehensive, long-term protection

Barracuda Email Security Gateway for AWS includes spam and virus blocking, data protection, email continuity, DoS prevention, encryption, 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

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

Scalability and ease of use

Fast, easy set-up and simple, intuitive management keep time and resource needs low. The integration of the Barracuda Cloud Protection Layer[2] makes it easy to scale capacity as your business grows.

1 *Advanced Threat Protection (ATP) is available as an add-on subscription.*
2 *Available with ATP only.*

Comprehensive application security

OWASP Top-10 Attacks
XML and JSON protection
Application layer DDoS

Proactive defense

Geo-IP Control
Reputation lists
Advanced Bot Protection

Data loss prevention

Credit card numbers (PII)
Social Security Number (PII)
Custom policies (IP)

Barracuda Cloud Protection Layer filters and spools inbound email traffic.

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
- Outbound email filtering

DLP and reputation loss

- Maintain compliance
- Prevents reputation loss and block-listing
- Pre-defined filters (e.g., HIPAA, credit card, and U.S. Social Security Numbers)

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 Protection1 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

Models

	LEVEL 3	LEVEL 4	LEVEL 6
CAPACITY			
AWS container size	M3.medium/T2.medium	M3.large/M4.large/C4.large/T2.large	M3.xlarge/M4.xlarge/C4.xlarge
Active email users	3,000-10,000	8,000-22,000	15,000-30,000
FEATURES			
Advanced Threat Protection[1]	•	•	•
Outbound email filtering	•	•	•
Email encryption	•	•	•
Cloud Protection Layer[2]	•	•	•
MS Exchange/LDAP Accelerator	•	•	•
Per-user settings and quarantine	•	•	•
Delegated help desk roles	•	•	•
Syslog support	•	•	•
Clustering and remote clustering	•	•	•
Per domain settings	•	•	•
Single sign-on	•	•	•
SNMP/API	•	•	•
Customizable branding	•	•	•
Per-user score settings	•	•	•
Delegated domain administration	•	•	•

1 Advanced Threat Protection (ATP) is available as an add-on subscription.
2 Available with ATP only.

Barracuda
Your journey, secured.