Protecting your email infrastructure with the Barracuda Spam Firewall for Amazon Web Services

Today, many organizations are looking to the cloud to take advantage of the economic gains and operational efficiencies inherent to non-hardware-based solutions. A key barrier for many, however, is the limited feature set in most cloud-based solutions when compared to their more mature on-premises counterparts.

The Barracuda Spam Firewall for Amazon Web Services offers advanced email management and layered protection that is completely cloud-based, guarding against both inbound and outbound email-based threats.

Email servers that reside in the cloud deserve the same level of comprehensive security as email servers that reside on premises, especially since cloud-based email servers are no longer wholly within a network space that you control. However, most cloud-based email servers usually offer only basic spam protection if at all, and lack the functionalities found in an on-premises email protection solution.

The Barracuda Spam Firewall for Amazon Web Services is a proven email security solution that will fully secure your cloud-based email server using the same technology and the same suite of features available in our award-winning hardware appliance, without giving up any of the convenience and benefits of the cloud.

Integrating just as easily with Exchange in AWS (or any other cloud-based email server) as it does with any on-premises email server, the Barracuda Spam Firewall for Amazon Web Services protects both your inbound and outbound email traffic with advanced email security and threat detection features that utilize Barracuda's real-time threat intelligence framework to guard against zero-hour malware, Denial-of-Service attacks and other threats. Among the types of analyses performed are:

- **Multi-level intent analysis:** Recursively follows links and performs analysis of various domain attributes on the target pages
- **Behavioral analysis:** Use of heavyweight virtualization and sandboxing technology to provide real-time protection against zero-hour threats
- **Real-time fingerprint analysis:** Polymorphic virus detection to catch new variants of continuously morphing viruses

Along with best-of-breed email threat protection, the advanced email management policies in the Barracuda Spam Firewall for Amazon Web Services offers:

- **Data loss prevention (DLP):** Scanning of outbound emails and attachments, to block confidential or sensitive information from being leaked outside an organization.
- **Email encryption:** Ensures secure communication and regulatory compliance.
- **Bulk Email Management:** Our Email Categories feature gives YOU control over the types of solicited and unsolicited email allowed into your users' inboxes.

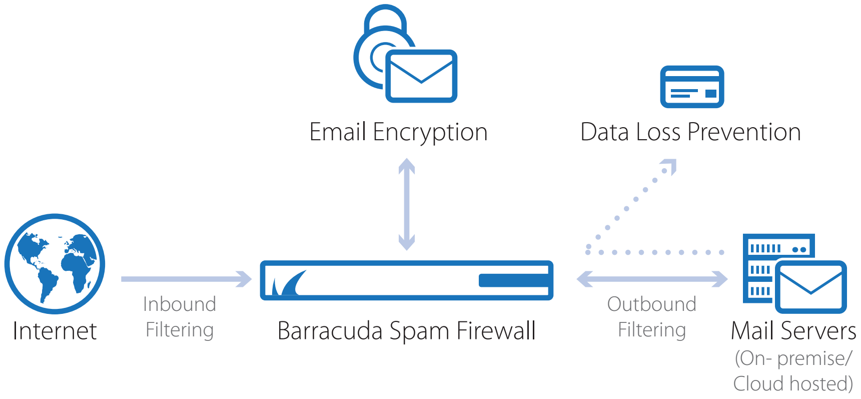
Additionally, should your email server be unreachable for any reason, email continuity is offered by the Cloud Protection Layer (CPL) of the Barracuda Spam Firewall. Emails can be spooled in CPL and re-delivered once the mail service is available. The separate CPL interface also allows for viewing and downloading of all incoming emails.

This easy-to-use solution provides you with flexibility in deployment as well since installation time is minimal, and can be done before, during, or after your transition from an on-premises to a cloud-based email service..

Complete Email Protection in Amazon Web Services

Barracuda Advantage

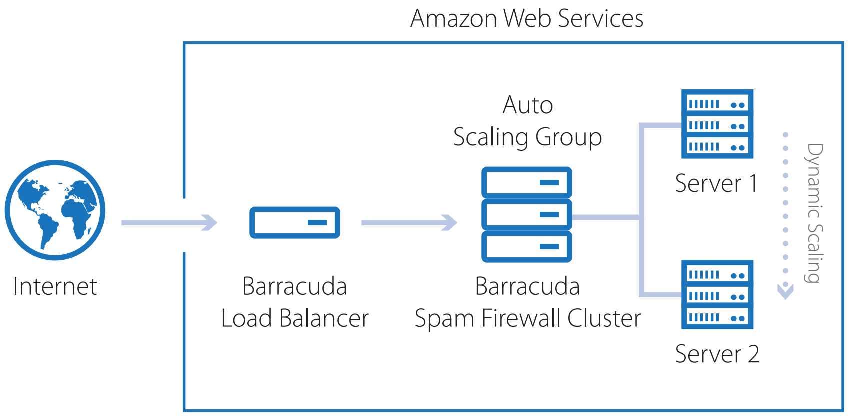
- Granular Inbound Filtering
- Granular Outbound Filtering
- Email Encryption
- Data Loss Prevention
- Email Continuity



Scalable Security

Barracuda Advantage

- Centralized Management & Administration
- Configuration Sync across BSF cluster



Get a Free 30-Day Trial.

For more information, visit barracuda.com/aws