



Barracuda Email Security Service

Cloud-based email security and Data Loss Prevention

The Barracuda Email Security Service is a comprehensive and affordable cloud-based email security service that protects both inbound and outbound email against the latest spam, viruses, worms, phishing and denial of service attacks. The Barracuda Email Security Service leverages advanced security technologies from the industry-leading Barracuda Spam & Virus Firewall and features rich cloud-based protection, including:

- Rate control and Denial of Service (DoS) protection
- Reputation-based blocking from known spam and malware sources
- Patent-pending Barracuda Anti-Virus Supercomputing Grid
- Anti-phishing, using the Barracuda Anti-Fraud Intelligence
- Protection against spam, phishing, fraud and other emails with malicious intent
- Custom sender/recipient policy
- Data Loss Prevention
- Email encryption

Comprehensive Protection

Spam and viruses are blocked in the cloud prior to delivery to the customer, providing additional Denial of Service protection. In addition, cloud-based filtering offloads any processing required for spam and virus filtering from the email server. By leveraging the computing power of the cloud, the Barracuda Anti-Virus Supercomputing Grid is optimized to block new polymorphic virus threats and new virus outbreaks. Additionally, Barracuda Anti-Fraud Intelligence provides targeted protection against phishing and fraudulent emails.

Data Loss Prevention

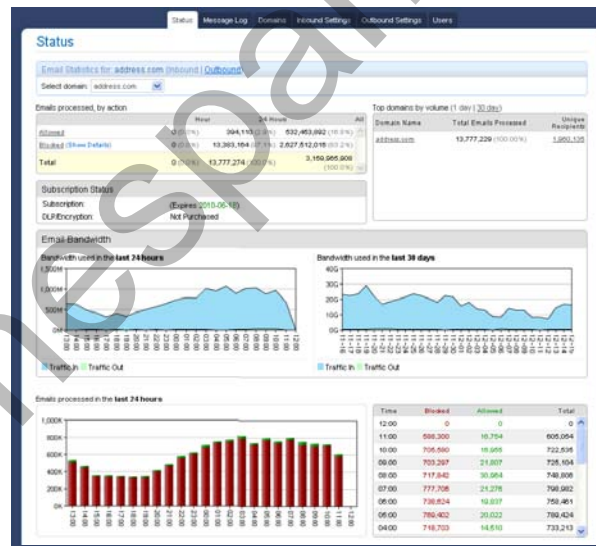
Advance features like email encryption and attachment content scanning prevent data theft via email. Email encryption ensures that only authorized recipients can access email and its attachments in outbound email.

Email Continuity Services

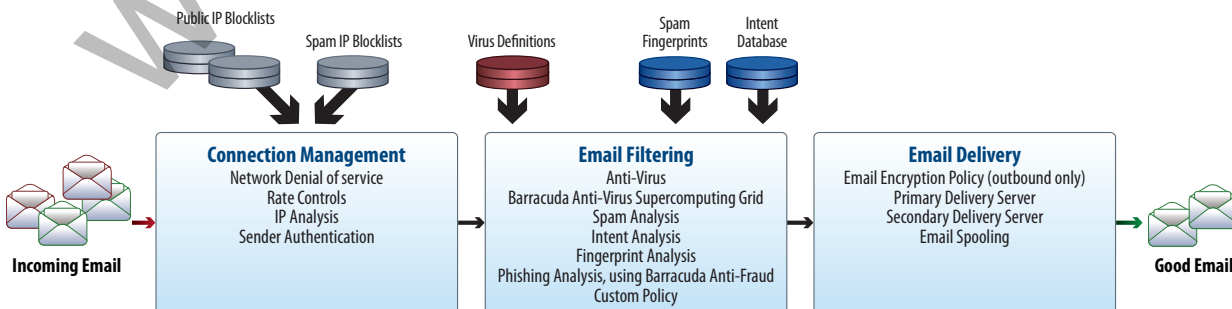
The Barracuda Email Security Service provides delivery to an alternate server if the primary server is unavailable, and will store email for up to 96 hours if both destinations are unavailable. During this time, users can log into the service to check email. Once service is reestablished, the Barracuda Email Security Service begins email spooling for fast restoration of email.

Easy-to-Use

The Barracuda Email Security Service can start filtering inbound and outbound email in a matter of minutes without any additional software or hardware. Users can access their own message log to deliver quarantined emails or whitelist senders to ease the burden of administration.



The Barracuda Email Security Service provides cloud-based filtering for inbound and outbound email and displays the number of messages with statistics on how they were processed.





Typical Deployment



Technology Overview

Barracuda Email Security Service includes the following technologies to provide the most comprehensive email security.

- **Backed by Barracuda Central** – Barracuda Central is a powerful operations center providing maximum protection against spam, spyware, viruses and other threats. Security analysts at Barracuda Central monitor the Internet for new trends and develop new ways to counteract evolving threats.
- **Barracuda Reputation and Intent Analysis:** Reputation data remains an important baseline for sender profiling. For reputation analysis, the Barracuda Email Security Service leverages data on both the network addresses used to send email, as well as the domain names embedded in the Web links of emails gathered by Barracuda Central.
- **Predictive Sender Profiling:** Industry-leading Predictive Sender Profiling probes deeper into sent email to identify bad sender behavior and block identity obfuscation techniques, despite a sender’s lack of prior spamming history.
- **Barracuda Real-Time Protection:** Barracuda Real-Time Protection is a set of advanced technologies that enables Barracuda Email Security Service to immediately block the latest virus, spyware, and other malware attacks as they emerge. These capabilities provide industry-leading response times to email-borne threats by adding a third layer of anti-virus protection to the Barracuda Email Security Service.
- **Virus Protection using Barracuda Anti-Virus Supercomputing Grid:** The Barracuda Email Security Service scans all email messages and all incoming files for viruses using three powerful layers of virus scanning technology, in addition to Barracuda Anti-Virus Supercomputing Grid. Archives are automatically decompressed for complete virus protection. Barracuda Anti-Virus Supercomputing Grid utilizes patent-pending technology to leverage the power of an extensible cloud. Outbreaks are analyzed to predict how virus variants might proliferate to protect against polymorphic viruses.
- **Barracuda Anti-Fraud Intelligence** – In addition to checking for spam, Barracuda Email Security Service analyzes all messages for scams and frauds, by leveraging the Barracuda Anti-Fraud Intelligence engine.
- **Data Loss Prevention and Email Encryption** – Barracuda Email Security Service includes advanced content scanning technologies to detect specified keywords inside attachments. Custom policies based on attachment content scanning enable organizations to encrypt email to prevent loss of sensitive and confidential information.

TECHNICAL SPECIFICATIONS

Security Features

Comprehensive Protection

- Spam and virus filtering
- Prevents spoofing, phishing and malware
- Denial of Service protection
- Directory harvest protection
- Outbound email filtering

Spam Filter

- Rate control
- IP Reputation Analysis
- Fingerprint analysis
- Barracuda Anti-Fraud Intelligence

Sender Authentication

- Sender Policy Framework
- Emailreg.org

Advanced Policy Controls

- IP and content-based filtering
- Content encryption

Advanced Policy Controls (Continued)

- Sender/recipient filtering
- RBL and DNSBL support
- Keyword blocking
- TLS encryption policy

Virus Filter

- Triple-layer virus blocking
- Barracuda Real-Time Protection
- Decompression of archives
- File type blocking
- Barracuda Anti-Virus Supercomputing Grid

Data Loss Prevention

- Attachment content-based filtering
- Email encryption

Email Continuity

Administrators

- Failover to alternate destination
- Email spooling for up to 96 hours
- Priority-based spooling after outage
- Policy-based

End Users

- Access to spooled email through Web interface during outage
- Single Sign-on

System Features

Administrators

- Web-based interface
- User account administration
- LDAP interface

End Users

- User-based filtering
- End user quarantine and digest emails