Barracuda®

BARRACUDA EMAIL SECURITY GATEWAY

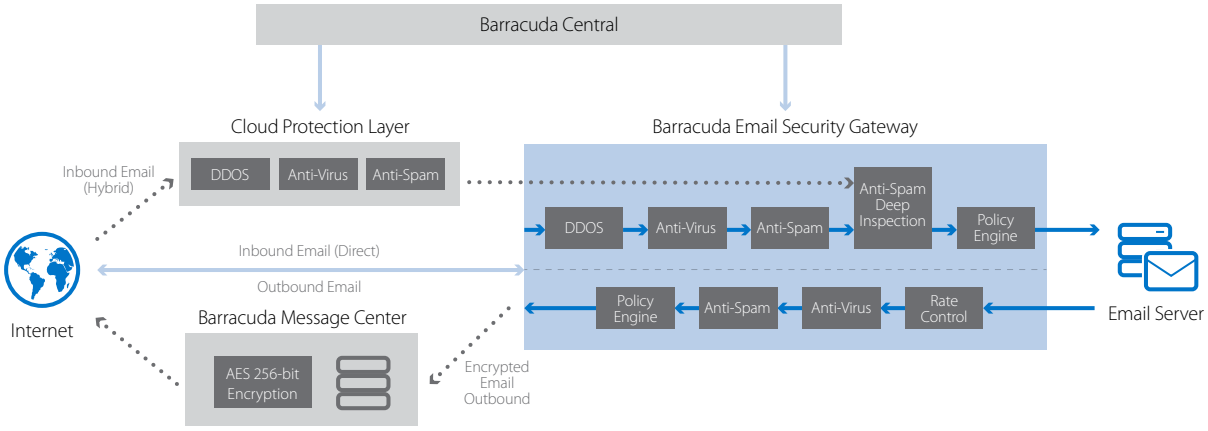
Barracuda Networks Email Security Technology

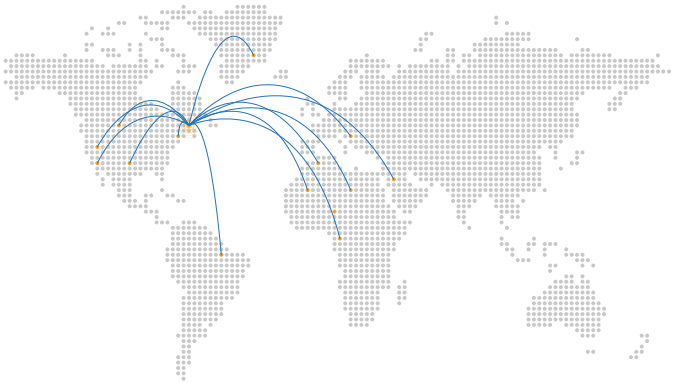
The Barracuda Email Security Gateway is a comprehensive email security solution that manages all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. Flexible deployment options include hardware and virtual appliances, cloud services and hybrid configurations — making this solution ideal for safeguarding any size organization. In addition to protecting traffic to and from the Internet, the solution also includes a Microsoft Exchange Anti-virus Agent to protect internal emails. Widely used by over 75,000 organizations, the award-winning Barracuda Email Security Gateway has no per-user, per-agent or per-server fees.

Barracuda Email Security Gateway's comprehensive features and functionality yield a phenomenal 95 percent spam catch rate out of the box with one of the lowest false positive rates in the industry. Although affordable and easy to use, the Barracuda Email Security Gateway provides the most effective and complete email security in the industry.

Comprehensive Approach to Email Security

The Barracuda Email Security Gateway's multilayered approach to email security provides the most comprehensive protection available. It also optimizes email performance several ways to affordably process millions of messages per day. Its internal filtering technology employs time-tested defense layers while the Cloud Protection Layer adds advanced cloud-based technologies: the Barracuda Anti-Fraud Intelligence Engine detects and blocks fraudulent emails and the Barracuda Anti-Virus Supercomputing Grid detects and blocks polymorphic viruses that try to evade detection by changing their signatures.





Barracuda Central monitors data 24x7 from tens of thousands of collection points located in over 80 countries and more than 40,000 Barracuda Spam & Virus Firewalls in use by customers. As new threats emerge, Barracuda Central is quick to respond to early outbreaks and delivers the latest definitions automatically through Barracuda Energize Updates.

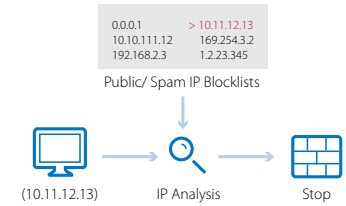
Barracuda Central

All Barracuda Networks products are backed by Barracuda Central, a 24x7 advanced technology center consisting of highly trained engineers who continuously monitor and block the latest Internet threats. Barracuda Central collects emails, URLs and other data from tens of thousands of collection points located in more than 80 countries. In addition, Barracuda Central collects data contributions from more than 50,000 Barracuda products in use by customers. Barracuda Central analyzes the data collected and develops defenses, rules and signatures to defend your network.

As new threats emerge, Barracuda Central is quick to respond to early outbreaks and delivers the latest definitions through Barracuda Energize Updates. These updates require zero administration and ensure that the Barracuda Spam & Virus Firewalls provide comprehensive and accurate protection against the latest threats.

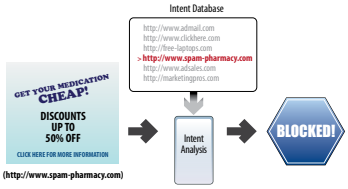
Anti-Spam Protection

Barracuda Reputation: Barracuda Central collects IP addresses used in spam attacks and legitimate email campaigns for reputation analysis. Reputation analysis lets the Barracuda Email Security Gateway filter look up senders' IP addresses on Barracuda Networks' block or allow lists. "Grey area" addresses are analyzed through nine other defense layers. Reputation and other upfront checks let the Barracuda Email Security Gateway block over half of emails in the connection-management layers before emails are received.



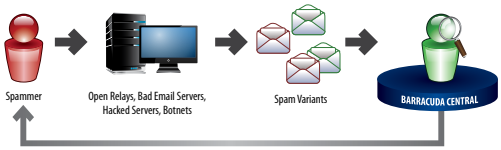
With Barracuda Reputation analysis, the Barracuda Email Security Gateway can quickly and efficiently make decisions to block or accept email messages based on the sender's IP address.

Intent Analysis: Barracuda Central maintains reputation data on spam domains, phishing domains, and malware sites. The Intent Analysis layer does a database lookup of domain names embedded in email text. It blocks emails carrying known spam domain names. The Intent Analysis layer blocks 25 to 35 percent of emails that pass previous protection layers. Barracuda Networks' IP and reputation data provide the most complete reputation analysis in the industry.



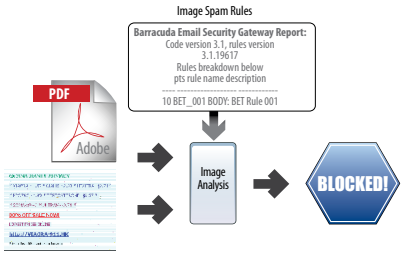
Based on Barracuda Networks extensive and continually updated intent database, the Barracuda Spam & Virus Firewall can rapidly block emails that contain spam domains embedded in the message.

Predictive Sender Profiling: Predictive Sender Profiling uses behavioral analysis to identify and block spammers from bypassing reputation analysis by obfuscating their web identities. Using a network of over 75,000 customer systems worldwide, Barracuda Networks collects the most diverse email data for profiling spammers' behavior.



Predictive Sender Profiling looks beyond the apparent reputation of the sender and digs deeper into the campaign itself to identify anomalous activity.

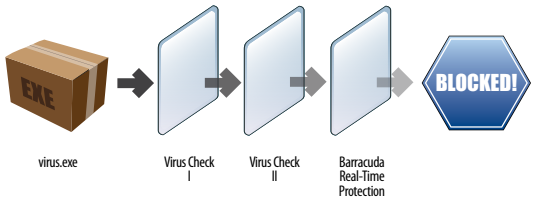
Deep Content Scanning: Image spam, which embeds text in images to hide from traditional spam filters, represents 1/3 of all traffic on the Internet. The Barracuda Email Security Gateway uses industry-leading techniques such as multi-pass optical character recognition (OCR), image processing and animated GIF analysis. These technologies block image spam with 95 percent accuracy. Spammers also use PDF files to try to bypass text and image scanning. Barracuda Central has captured over 100,000 variants of PDF spam. Through sophisticated PDF filtering in the rules scoring engine, the Barracuda Email Security Gateway defends against all types of PDF files used in spam attacks.



The Barracuda Email Security Gateway provides third-generation image spam defense technology for complete protection against spammers attempts to embed text inside images with the intent of hiding content from traditional spam filters.

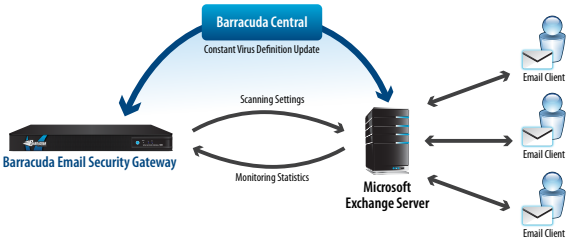
AntivirusProtection

Triple-Layer Virus Protection: The Barracuda Email Security Gateway scans emails and incoming files using three powerful layers of virus scanning technology. It also decompresses archives for complete protection. This triple-layer antivirus protection uses powerful open source and propriety virus definitions, which automatically update via Energize Updates and Real Time Protection. Virus scanning takes precedence over other email scans. Barracuda Spam & Virus Firewalls worldwide collectively block more than one million virus attempts on a typical day.



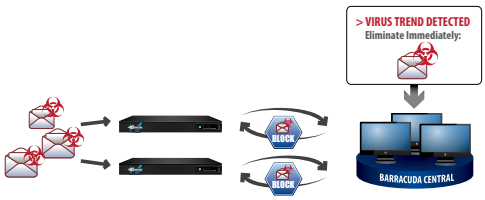
Barracuda Networks triple-layer virus protection includes powerful open source and proprietary virus definitions and Barracuda Real-Time Protection for the most comprehensive email-borne virus and malware protection in the industry.

Internal Email Protection: With its antivirus agent for Microsoft Exchange, the Barracuda Email Security Gateway protects internal emails. Viruses can easily enter an internal email system through the use of Outlook Web Access or POP/IMAP on systems not under the organization's control. The agent runs as a Windows service on the Exchange server letting the server scan internal emails for viruses. It uses the same virus definitions as the Barracuda Email Security Gateway. Configuring and monitoring the agent are also done via the Barracuda Email Security Gateway's intuitive web interface. The Barracuda Email Security Gateway provides a single place for managing inbound, outbound and internal email virus protection.



The antivirus agent for Microsoft Exchange protects internal emails.

Barracuda Real-Time Protection: Barracuda Real-Time Protection is a set of advanced technologies that lets the Barracuda Spam & Virus Firewalls instantly block the latest viruses and other malware as they emerge. It draws from the largest and most diverse installed base in the industry to detect early trends in email threats. Immediately upon virus or malware classification, Barracuda Real-Time Protection sends a response via Barracuda Central to any Barracuda Email Security Gateway that has submitted the malware fingerprints to block the message. This, plus a third layer of antivirus protection, enables the fastest response to email-borne virus threats in the industry.



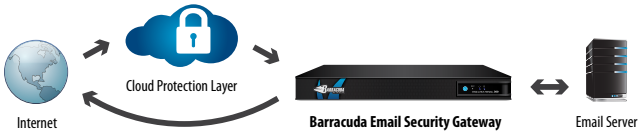
Barracuda Real-Time Protection draws from the largest and most diverse installed base in the industry to detect early trends in email-borne threats. Immediately upon virus or malware classification, Barracuda Central responds to any Barracuda Email Security Gateways submitting the corresponding fingerprints with an instruction to immediately block the message.

Cloud Protection Layer

Cloud Protection Layer: The Barracuda Email Security Gateway is integrated with a cloud-based service that prefilters emails before delivery to the on-site Barracuda Email Security Gateway, which performs further security checks and is needed for outbound filtering. The Cloud Protection Layer uses technologies that have been time tested with the Barracuda Email Security Gateway along with advanced cloud-based technologies including:

• Barracuda Anti-Fraud Intelligence Engine, which detects and blocks fraudulent emails

• Barracuda Anti-Virus Supercomputing Grid, which detects and blocks polymorphic viruses that try to evade detection by changing their signatures



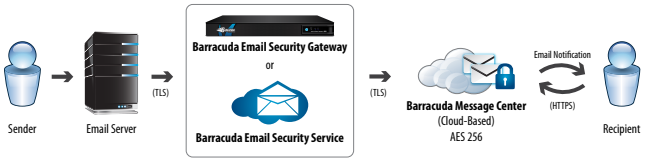
The Cloud Protection Layer stops spam and malware in the cloud. It also provides email continuity.

Policy and Compliance

Outbound Filtering: The Barracuda Email Security Gateway also filters outbound emails. Outbound filtering prevents organizations from being put on spam block lists and prevents sensitive data in emails from leaving the organization. Employees can inadvertently cause internal systems to become a source for botnet spam. Using a subset of its defense layers, the Barracuda Email Security Gateway's outbound filtering stops outbound spam and viruses. It also lets administrators enforce content polices for data loss prevention and to meet other content standards in outgoing emails. Predefined filters and custom policies can be used to detect sensitive data and block or encrypt emails.

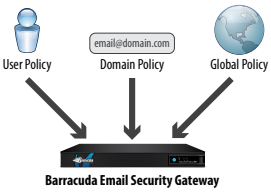
Outbound filtering protects organizations from being placed on spam block lists and leaking sensitive data in emails.

Encryption: The Barracuda Email Security Gateway offers a number of encryption features. It is fully integrated with a cloud-based email encryption service for outbound emails. Emails that match policy or are marked for encryption via the Barracuda Outlook Add-in are securely sent via TLS to the Barracuda Message Center. The Barracuda Message Center uses AES with 256 bit keys to encrypt emails. To encrypt email traffic between sites over the Internet, the Barracuda Email Security Gateway Message Transport Agent supports SMTP over TLS. This can be used between Barracuda Spam & Virus Firewalls or other email servers that support SMTP over TLS.



Outbound email encryption protects sensitive data in emails. It provides secure transit and storage for emails.

Policy Management: Built for the diverse needs of small and medium businesses, enterprises, educational institutions, government institutions and ISPs, the Barracuda Email Security Gateway offers global, domain-level, and individual user policy control. Depending on the model, policies can be combined and customized for maximum flexibility. Several spam-scanning features can be customized for each email user including block lists, allow lists, quarantining, scoring thresholds and Bayesian analysis. Domain-level features for policy management include: inbound and outbound quarantines, outbound encryption, block and allow lists based on IP address or sender/recipient email address or domain, reporting, and recipient validation via LDAP.



Barracuda Email Security Gateway offers per-user, domain and global policy management.

BARRACUDA EMAIL SECURITY GATEWAY

Barracuda Email Security Gateway Core Technologies

Hardened OS: Based on the Linux open source kernel long popular with security researchers, the Barracuda Email Security Gateway's OS is hardened for maximum security and stability. In addition to thorough internal testing, Barracuda Networks collaborates with the community of "white hat" security researchers who work with security vendors to uncover and resolve potential vulnerabilities in both the Linux operating system and its associated utilities. While the vast majority of technology in the Barracuda Email Security Gateway is proprietary, Barracuda Networks seeks to leverage secure and functional open source alternatives whenever possible.

Barracuda Central: Barracuda Central is the 24/7 security center operated by Barracuda Networks to monitor and block the latest Internet threats. Data collected at Barracuda Central is analyzed and used to create definitions for automatic Energize Updates that fuel the Barracuda Email Security Gateway. Barracuda Central is backed by Barracuda Labs, a global multidisciplinary research and threat analysis team that develops innovative technologies across Barracuda Networks' business areas. Barracuda Lab evaluates the threat ecosystem and creates security intelligence for distribution via Barracuda Central to defend customers.

Mail Transport and Relay: The Barracuda Email Security Gateway features a robust Message Transport Agent (MTA) capable of handling high SMTP connection and mail delivery volumes. For inbound protection, the MTA includes rate controls, IP reputation analysis, sender authentication, and recipient verification, which allow it to reject SMTP connections before it actually receives any messages. For relaying outbound mail, the Barracuda Email Security Gateway supports access controls and SMTP Authentication to ensure that the Barracuda Email Security Gateway safely relays email without risk of acting as an open relay. The outbound mail relay also performs rate control checks based on sender IP address or sender email address. The Barracuda Email Security Gateway MTA also supports a built-in journaling function for use with message archivers.

Email Continuity: : The Barracuda Email Security Gateway provides email continuity in case of disasters through its Cloud Protection Layer. In the event of on-premises disruptions, emails can be spooled in this cloud layer for up to 96 hours with attempts to resend the spooled messages at preset intervals. An alternative destination can also be specified for email delivery if delivery to the primary destination fails.

Role-based Administration: The Barracuda Email Security Gateway offers role-based administration which features a number of built-in account roles. Management tasks can be delegated based on account roles such as Admin, Domain Admin, and Helpdesk. Domain administration can be delegated to the Domain Admin or to Helpdesk roles, which can be assigned to specific users.

Clustering: The Barracuda Email Security Gateway can cluster multiple nodes for redundancy and to increase capacity. For central management, Barracuda Spam & Virus Firewalls share configurations and policy across the cluster. Administrators can change policy and access any message received across the cluster from any node. For redundant quarantine mail storage, all quarantined messages are stored in at least two nodes in the cluster – ensuring message availability if one node fails. Barracuda Email Security Gateway clusters can create redundancy across sites as well.

Barracuda Networks Commitment to Innovation

Barracuda Networks is committed to providing you with the most advanced and comprehensive email security. Through Barracuda Networks' proven multilayered approach backed by the constant vigilance of the highly-trained engineers at Barracuda Central, the Barracuda Email Security Gateway offers the most sophisticated and effective email security technology in the industry. For more information on the technologies outlined here, along with Barracuda Networks latest innovations, visit www.barracuda.com/technology.

US 11.0