



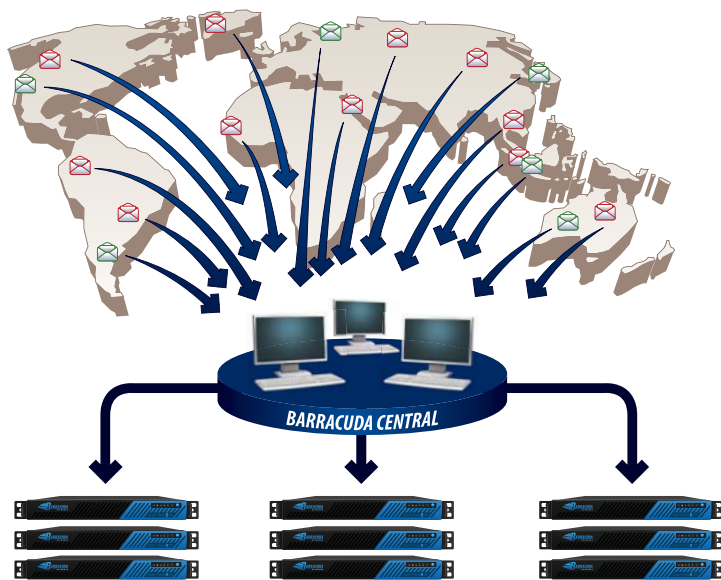
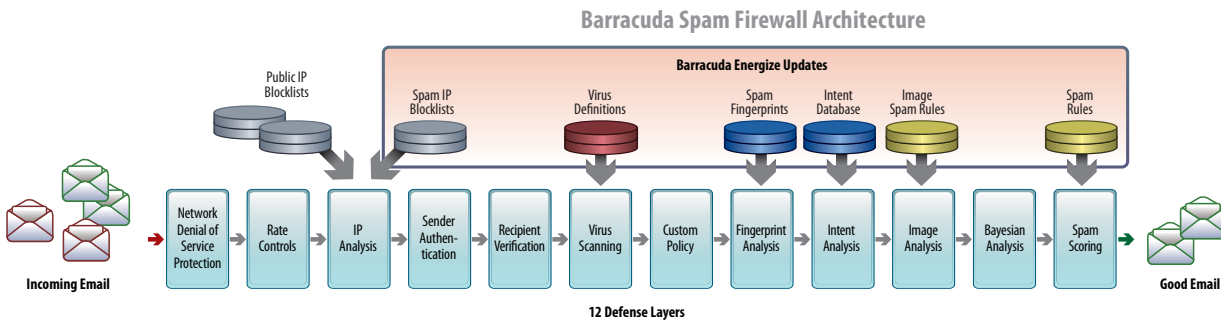
# Barracuda Networks Email Security Technology

The Barracuda Spam Firewall is an integrated hardware and software solution, which utilizes advanced technology to protect your email server from spam, virus, spoofing, phishing and spyware attacks. Barracuda Networks has continually introduced pioneering technology to provide you with the best email security protection at the best value. These industry-leading innovations include powerful triple-layer virus protection featuring Barracuda Real-Time Protection, a third generation multi-pass Optical Character Recognition (OCR) engine for complete image spam protection, and unique Predictive Sender Profiling technologies that catch spammers who try to evade traditional reputation filters.

Barracuda Networks 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 Spam Firewall provides the most effective defense capabilities in the industry for complete email security protection.

## Comprehensive Approach to Complete Email Security

**12 Defense Layers:** Barracuda Networks multilayered approach to email security provides the most comprehensive protection available, and optimizes the processing of each email to maximize performance and process millions of messages per day. Behind the industry-leading initiatives of Predictive Sender Profiling and Barracuda Real-Time Protection are 12 explicit defense layers including: Denial of Service and Security Protection, Rate Controls, IP Reputation Analysis, Sender Authentication, Recipient Verification, Virus Protection, Policy (user-specified rules), Fingerprint Analysis, Intent Analysis, Image Analysis, Bayesian Analysis, and a Spam Rules Scoring engine.



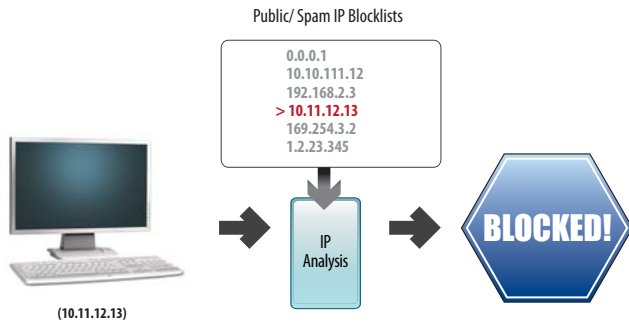
**Barracuda Central:** All Barracuda Networks products are backed by Barracuda Central, a 24x7 advanced technology center consisting of highly trained engineers who continuously monitor and block the latest Internet threats. Barracuda Central collects emails, URLs and other data from tens of thousands of collection points located in more than 80 countries. In addition, Barracuda Central collects data contributions from more than 40,000 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 Firewalls provide comprehensive and accurate protection against the latest threats.

*Barracuda Central monitors data 24x7 from tens of thousands of collection points located in over 80 countries and more than 40,000 Barracuda Spam 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*

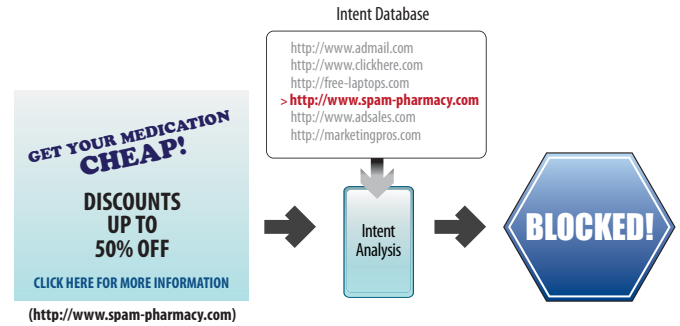
**BARRACUDA SPAM FIREWALL**

## Barracuda Networks Email Security Technology: A Look Inside

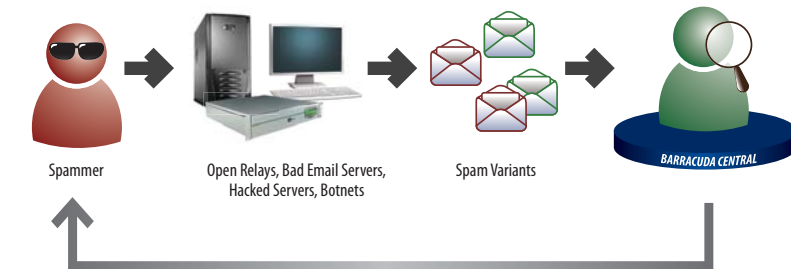


With Barracuda Reputation analysis, the Barracuda Spam Firewall can quickly and efficiently make decisions to block or accept email messages based on the sender's IP address

**Intent Analysis:** Barracuda Central maintains reputation on spam domains, phishing domains, or Web sites known to host malware. When these domain names are embedded in email message bodies, the Intent Analysis layer of the Barracuda Spam Firewall can quickly block email messages based on a simple database lookup. Typically, about 25 percent to 35 percent of all email that passes through previous protection layers can be blocked by the Intent Analysis defense layer. The combination of the IP and reputation data provides the most complete reputation analysis in the industry. Updates to the Barracuda Reputation and Intent Analysis databases are delivered automatically to the Barracuda Spam Firewall via Barracuda Energize Updates.



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



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

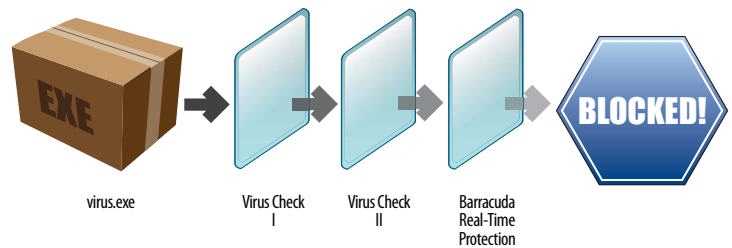
**Barracuda Real-Time Protection:** Barracuda Real-Time Protection is a set of advanced technologies that enables Barracuda Spam Firewalls to immediately block the latest virus, spyware, and other malware attacks as they emerge. These capabilities provide industry-leading response times to email-borne threats by adding a third layer of antivirus protection to the Barracuda Spam Firewall. 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 Spam Firewalls submitting the corresponding fingerprints with an instruction to immediately block the message, stopping the attack in real time and providing the fastest response to email-borne virus threats in the industry. Barracuda Central blocks thousands of threat variants in real-time every day as they attempt to proliferate over the Internet.



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 Spam Firewalls submitting the corresponding fingerprints with an instruction to immediately block the message

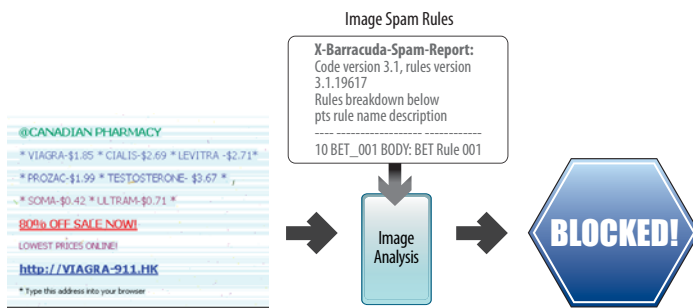
**Predictive Sender Profiling:** Relying solely on reputation analysis is no longer enough to efficiently prevent today's sophisticated spam attacks; therefore to be effective, reputation data must be augmented with behavioral profiling techniques. With elite spammers expiring their use of domain names in one to five minute intervals, Predictive Sender Profiling is the only practical technique to block spammers that obfuscate their Web identities. Barracuda Networks industry-leading Predictive Sender Profiling probes deeper into email campaigns to identify bad sender behavior and block attempts by spammers to bypass traditional reputation analysis by obfuscating their identities. Utilizing a network of more than 40,000 customer systems worldwide, Barracuda Networks has the most diverse compilation of email available for profiling the behavior of spammers. Using this data enables the Barracuda Spam Firewall to look beyond the apparent reputation of the sender and dig deeper into the campaign itself to identify anomalous activity, allowing Barracuda Networks to effectively block spam typically unstopable by traditional reputation analysis.

**Triple-Layer Virus Protection:** The Barracuda Spam Firewall scans all email messages and all incoming files for viruses using three powerful layers of virus scanning technology and automatically decompresses archives for complete virus protection. Barracuda Networks triple-layer virus blocking includes powerful open source and propriety virus definitions, which are automatically updated via Barracuda Energize Updates, and Barracuda Real-Protection. When new spam and virus outbreaks occur, Barracuda Real-Time Protection will automatically block these threats in real-time. Virus scanning takes precedence over all other mail scanning techniques, and it is applied even when mail passes through the connection management layers. Barracuda Spam Firewalls around the world collectively block more than one million virus attempts on a typical day.



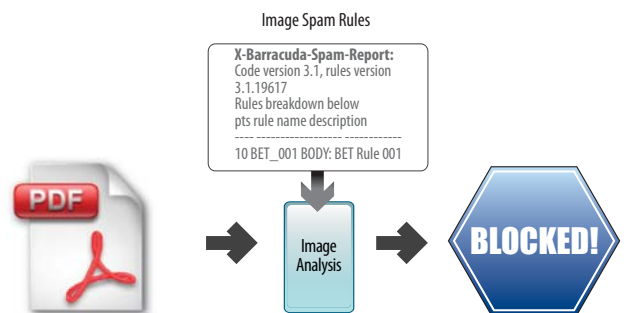
Barracuda Networks triple-layer virus protection includes powerful open source and proprietary virus definitions and Barracuda Real-Time Protection for the most comprehensive email-borne virus and malware protection in the industry

**Image Spam Protection:** Image spam, which generally embeds text inside images with the intent of hiding content from traditional spam filters, represents approximately one-third of all traffic on the Internet. The Barracuda Spam Firewall was the first major email security product to include image analysis techniques to protect against new image spam variants. These industry-leading techniques include optical character recognition (OCR), image processing and animated GIF analysis. Barracuda Networks image spam defense also calls upon third-generation technology including a multi-pass OCR engine that renders spammers' tricks to hide text behind color or blurred images ineffective. In addition, it offers automated fingerprint generation for the fastest detection of previously issued image spam possible. These technologies combined garner the Barracuda Spam Firewall an accuracy rating of 95 percent in identifying and blocking image spam. Image spam and fingerprint updates are delivered automatically to all Barracuda Spam Firewalls through Energize Updates.



The Barracuda Spam Firewall 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

**PDF Spam Protection:** By using PDF files that require the use of document viewing applications, such as Adobe Reader, spammers attempt to bypass text and image scanning engines. Barracuda Central has captured samples from PDF spam campaigns that have employed more than 100,000 variants, highlighting the need to employ sophisticated content analysis filters when spammers evade traditional reputation filters. Because these PDF attacks utilize existing botnets to generate similar traffic patterns on the Internet as more traditional spam attacks, both Barracuda Reputation and Fingerprint Analysis techniques enable the Barracuda Spam Firewall to block a significant portion of PDF spam early in the message scanning process. In addition, by utilizing the Image Analysis layer, the Barracuda Spam Firewall blocks image-only PDF files containing spam content while delivering legitimate PDF files. Through sophisticated PDF filtering technologies in the rules scoring engine, the Barracuda Spam Firewall can target the full document PDF files used in spam attacks. Utilizing these highly effective defense layers, the Barracuda Spam Firewall leverages new and existing definitions, which are developed by Barracuda Central, to block new spam variants even if the content is carried in PDF files.



Utilizing a number of its highly effective defense layers the Barracuda Spam Firewall blocks new spam variants, including spam campaigns in which spammers embed messages within PDF documents



# BARRACUDA SPAM FIREWALL

## Barracuda Spam Firewall Core Technologies



**Hardened Operating System:** Based on the popular Linux open source kernel that has stood up to scrutiny among security researchers, the Barracuda Spam Firewall operating system is hardened for maximum security and stability. In addition to thorough internal testing, Barracuda Networks credits the community of “white hat” security researchers that continually 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 Spam Firewall is proprietary, Barracuda Networks seeks to leverage secure and functional open source alternatives whenever possible.



**Per-User Policy Control:** Built for the diverse needs of small and medium businesses, enterprises, educational institutions, government institutions, and ISPs, the spam scanning engine of the Barracuda Spam Firewall supports granular policy at the individual user level. Depending on the model of Barracuda Spam Firewall, several spam scanning features, including block lists (“blacklists”), allow lists (“whitelists”), quarantine capabilities, scoring thresholds, and Bayesian analysis can be customized for each email user. This per-user policy control offers another level of granularity above competing systems which may only offer policy controls at a domain level.



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



**Encryption:** To encrypt email traffic between sites across the Internet, the Barracuda Spam Firewall Message Transport Agent supports TLS (Transport Layer Security). SMTP/TLS email traffic is encrypted over the Internet using SSL (Secure Sockets Layer) and can be used between Barracuda Spam Firewalls or in conjunction with other popular email servers, such as Microsoft Exchange, that support SMTP/TLS. Unlike end-to-end encryption techniques that typically require special client software, SMTP/TLS is gateway-based encryption that is transparent to users. Moreover, because internal email traffic remains in the clear, content-based policies can still be enforced at the gateway prior to encryption.



**Clustering:** The Barracuda Spam Firewall supports clustering of multiple nodes for both redundancy and to increase total system capacity. For centralized management, Barracuda Spam Firewalls share configuration and policy across the cluster, and administrators can change policy or access any message received across the cluster from any individual node. For redundancy of quarantine mail storage, all quarantined messages are stored in at least two nodes in the cluster – ensuring that messages are always available in the event that one node becomes unavailable. Barracuda Spam Firewall clusters can span geographies to facilitate redundancy across sites.

## Barracuda Networks Commitment to Innovation

Barracuda Networks is committed to providing you with the most advanced and comprehensive email security protection. Through Barracuda Networks proven multilayered approach backed by the dedication and constant vigilance of the highly-trained engineers at Barracuda Central, the Barracuda Spam Firewall offers the most sophisticated and effective email security technology in the industry. For additional information on the technologies outlined here, along with Barracuda Networks latest innovations, visit [www.barracuda.com/technology](http://www.barracuda.com/technology).