Barracuda®

Comprehensive Email Filtering

White Paper

Email has undoubtedly become a valued communications tool among organizations worldwide. With frequent virus attacks and the alarming influx of spam, email loses the efficiency to communicate. Spam messages represent the vast majority of email traffic on the Internet. Spam is no longer a simple annoyance; it is a significant security issue and a massive drain on financial resources.

This is simply astounding and unacceptable. It's time to take control of spam and virus attacks.

Filtering Email in Two Advanced Processes

Today, there are a number of solutions designed to help alleviate the spam problem. Barracuda Networks designed the affordable Barracuda Email Security Gateway as an easy-to-use, enterprise-class hardware and software solution for businesses of all sizes that comprehensively evaluates each email, using two main classes of sophisticated algorithms and techniques: Connection Management and Mail Scanning.

During the connection management process, emails are filtered through five defense layers to verify authenticity of envelope information, and any inappropriate incoming mail connections are dropped even before receiving the message. Any emails that survive the connection verification process must then undergo a thorough mail scanning process that involves an additional seven defense layers of message analysis. The algorithms and techniques used by the Barracuda Email Security Gateway are continuously updated via the hourly Barracuda Energize Updates service to stay ahead of spam trends as they emerge.

Connection Management

The Connection Management process generally requires less processing time. For the average small or medium business, more than half of the total email volume can be blocked through Connection Management techniques. Extremely large Internet Service Providers (ISPs) or even small Web hosts, while under attack, may observe block rates at the Connection Management layers exceeding 99 percent of total email volume.

Network Denial of Service Protection

Built on a hardened and secure operating system, the Barracuda Email Security Gateway receives email on behalf of the organization, insulating the organization's email server from receiving direct Internet connections and the associated threats.

Rate Controls

Automated spam software can be used to send large amounts of email to a single email server. To protect the email infrastructure from these flood-based attacks, the Barracuda Email Security Gateway counts the number of incoming connections from a particular IP address and throttles the connections once a particular threshold is exceeded.

Organizations that relay email through known servers or communicate frequently with known partners can and should add the IP addresses of those trusted relays and good email servers to the Rate Control exemption list.

Spam History

Spam is one form of abuse of the Simple Mail Transfer Protocol (SMTP), which is implemented in email systems on the basis of RFC 524. First proposed in 1973, RFC 524 was developed during a time when computer security was not a significant concern. As such, RFC 524 is no longer a secure command set, making it and SMTP susceptible to abuse.

Most spam-making tools exploit the security holes in SMTP. They do this by forging email headers, disguising sender addresses, and hiding the sending system, such that it becomes difficult or even impossible to identify the true sender.

To address some of SMTP's security holes, enhancement protocols to the venerable SMTP have been proposed. Most of these enhancement protocols involve features to accurately identify the sender before accepting the email. However, it would be difficult for these new protocols to be widely adopted because anyone who implements the new protocol would only be able to accept email from others who have also implemented the new protocol. So, without a more secure SMTP in the near future, spam will continue to be a problem, driving organizations to seek out effective spam-blocking solutions.
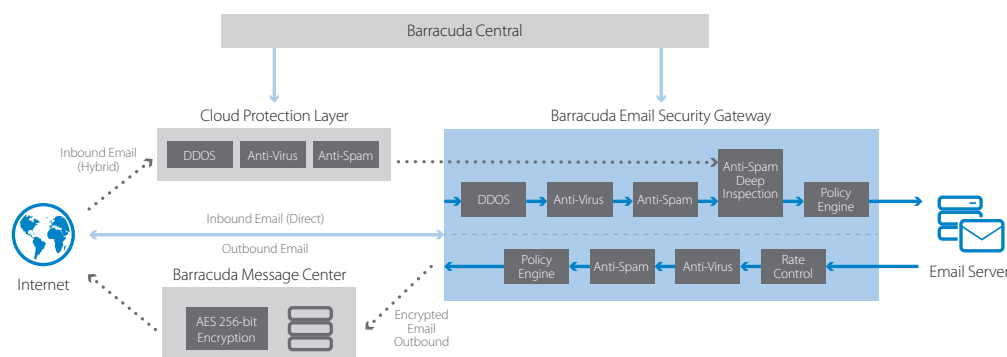
IP Analysis

After applying rate controls based on IP address, the Barracuda Email Security Gateway then performs analysis on the IP address.

- **Barracuda Reputation**. Barracuda Reputation is maintained by Barracuda Labs and includes a list of IP addresses of known, good senders as well as known spammers. Updates to the Barracuda IP Reputation database are delivered to the Barracuda Email Security Gateway via Barracuda Energize Updates.

- **External block lists**. The Barracuda Email Security Gateway enables administrators to take advantage of external block lists which are also known as real-time block lists (RBLs) or DNS block lists (DNSBLs). Several organizations maintain external block lists, such as spamhaus.org.

- **Customer-defined policy for allowed IP addresses**. The Barracuda Email Security Gateway enables administrators to define a list of trusted email servers by IP address. By adding IP addresses to this list, administrators can avoid spam scanning of good email, both reducing processing requirements and eliminating the chances of false positives.

- **Customer-defined policy for blocked IP addresses**. The Barracuda Email Security Gateway also enables administrators to define a list of bad email senders. In some cases, administrators may choose to utilize the IP block lists to restrict specific email servers as a matter of policy rather than as a matter of spam protection.

In general, external blacklists take precedence over subsequent allow lists ("whitelists") on the sender email address or domain, recipient, headers or message body. The Barracuda Email Security Gateway does have an option to delay RBL checks so that subsequent allow lists can take precedence over external block lists.

Sender Authentication

Declaring an invalid "from" address is a common practice by spammers. The Barracuda Email Security Gateway utilizes a number of techniques to both validate the sender as well as apply policy.

- **Protocol compliance**. First and foremost, the sender is validated for being specified properly. Examples of enforcement policies include, forcing RFC 821 compliance or requiring fully-qualified domain names.

- **DNS lookup**. To prevent senders from faking a "from" domain, a DNS lookup is performed on the sender domain to ensure that the domain exists.

- **Sender spoof protection**. The Barracuda Email Security Gateway has the option to prevent "spoofing" of an organization's own domain by disallowing emails using that domain name to be sent from outside the organization. Note that sender spoof protection should not be enabled if the organization sends messages from outside their internal email infrastructure (e.g., in the case of marketing bulk-mail services).

- **Custom policies**. Organizations can define their own allowed sender domains or email addresses. They can also define their own block lists based on sender domains or email addresses. Note that allow lists override block lists.

- **Sender policy framework (SPF)**. SPF is a proposed standard with growing momentum, designed to prevent spoofing of email domains. SPF provides a means for organizations to declare their known email servers in their DNS records so that email recipients can validate the identity of the sender domain based on the IP address of the sending email server. The Barracuda Email Security Gateway enables email administrators to block or tag messages on failed SPF checks.

- **Domain Keys**. The Barracuda Email Security Gateway enables administrators to inspect email messages for DomainKeys (DKIM) and take action when messages fail signature verifcation.

Recipient Verification

Many spammers attack email infrastructures by harvesting email addresses. The Barracuda Email Security Gateway verifies the validity of recipient email addresses through multiple techniques.

- **Protocol compliance**. Similar to Sender Authentication, a recipient is first validated for being specified properly. An example of an enforcement policy includes, forcing RFC 821 compliance.

IP Address
A unique identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.

False Positive
A legitimate email that is accidentally identified as spam

Barracuda Labs
An advanced technology center at Barracuda Networks, consisting of highly trained engineers that monitor the latest Internet threats and develop mitigation strategies. As new forms of spam emerge, Barracuda Labs is quick to respond to early outbreaks and delivers the latest spam definitions through Barracuda Energize Updates.

Barracuda Energize Updates
A subscription service that automatically provides the latest spam-blocking techniques, lists of known spammers, and spam and virus definitions for the Barracuda Email Security Gateway from the engineers at Barracuda Labs. Updates are delivered on an hourly basis to ensure all Barracuda Email Security Gateways are equipped with the latest definitions and the most comprehensive protection.

Domain Name System (DNS)
A DNS stores and associates many types of information with domain names (computer hostnames), and most importantly, translates domain names to IP addresses.

Vanity Domain Names
Domain names that are typically registered to individuals or families for the use of email. They typically do not have their own email server, but share an email server with a hosting company.

- **Custom policies**. Organizations can define their policies based on allowed recipient email addresses for which spam scanning should be disabled. They can also define their own block lists based on email addresses. Note that allow lists override block lists.
- **LDAP recipient verification**. Customers of Barracuda Email Security Gateway models 300 and higher can choose to reject messages if the recipient email addresses do not appear in the LDAP directory.
- **SMTP recipient verification**. By default, the Barracuda Email Security Gateway rejects messages if the downstream mail server does not accept mail for that recipient.

Mail Scanning

As spammers become more sophisticated, Mail Scanning techniques equally grow in their importance.

Virus Scanning

The most basic level of Mail Scanning is virus scanning. The Barracuda Email Security Gateway utilizes three layers of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing well-respected and effective open source virus definition lists along with Barracuda Networks' own proprietary virus definitions, Barracuda Email Security Gateway customers receive the best and most comprehensive virus and malware protection available. The three layers of virus scanning, includes:

- **Powerful open source virus definitions**. Barracuda Networks leverages the open source community to help monitor and block the latest virus threats.
- **Proprietary virus definitions**. Barracuda Networks proprietary virus definitions are gathered and maintained by Barracuda Labs, an advanced 24/7 security operations center that works to continuously monitor and block the latest Internet threats.
- **Barracuda Real-Time Protection**. Barracuda Real-Time Protection is a set of advanced technologies that enable Barracuda Email Security Gateways to immediately block the latest virus, spyware and other malware attacks as they emerge. Barracuda Real-Time Protection allows customers the ability to report virus and spam propagation activity at an early stage to Barracuda Labs. With this feature enabled any new virus or spam outbreak can be stopped in real-time for industry-leading response times to email-borne threats.

Virus Scanning takes precedence over all other Mail Scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from "whitelisted" IP addresses, sender domains, sender email addresses or recipients are still scanned for viruses and blocked if a virus is detected.

Custom Policy

Administrators can choose to define their own policies, perhaps for compliance or governance reasons, which take precedence over spam blocking rules delivered to the system automatically through Barracuda Energize Updates. The Barracuda Email Security Gateway enables administrators to set custom content filters based on the subject, message headers, message bodies and attachment file type. In general, administrators do not need to set their own filters for the purposes of blocking spam, as these forms of rules are delivered to Barracuda Email Security Gateways automatically through Barracuda Energize Updates.

Fingerprint Analysis

A message "fingerprint" is based on commonly used message components (e.g., an image) across many instances of spam. Fingerprint analysis is often as a useful mechanism to block future instances of spam once an early outbreak is identified.
Engineers at Barracuda Labs work around the clock to identify new spam fingerprints which are then updated on all Barracuda Email Security Gateways through hourly Barracuda Energize Updates.

Intent Analysis

All spam messages have an "intent" – to get a user to reply to an email, visit a Web site or call a phone number. Intent analysis involves researching email addresses, Web links and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Frequently, Intent Analysis is the defense layer that catches phishing attacks. The Barracuda Email Security Gateway features multiple forms of Intent Analysis.

Spoofing or Spoofing Attack
A spoofing attack is a situation where one person or program, successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage. Spoofing is often used in spam attacks to forge sender email addresses.

Sender Policy Framework (SPF)
SPF is an extension to SMTP that helps prevent sender forgery. It is also a free, open standard.

Lightweight Directory Access Protocol (LDAP)
LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.

- **Intent analysis**. Markers of intent, such as URLs, are extracted and compared against a database maintained by Barracuda Labs, and then delivered to the Barracuda Email Security Gateway via hourly Barracuda Energize Updates.
- **Real-time intent analysis**. For new domain names that may come into use, Real-Time Intent Analysis involves performing DNS lookups against known URL block lists.
- **Multilevel intent analysis**. Use of free Web sites to redirect to known spammer Web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. Multilevel Intent Analysis involves inspecting the results of Web queries to URLs of well-known free Web sites for redirections to known spammer sites.

Image Analysis

Today, image spam represents about one third of all traffic on the Internet. While Fingerprint Analysis captures a significant percentage of images after they have been seen, the Barracuda Email Security Gateway also uses Image Analysis techniques which protect against new image variants. These techniques include:

- **Optical character recognition (OCR)**. Embedding text in images is a popular spamming practice to avoid text processing in anti-spam engines. OCR enables the Barracuda Email Security Gateway to analyze the text rendered inside the images.

- **Image processing**. To mitigate attempts by spammers to foil OCR through speckling, shading or color manipulation, the Barracuda Email Security Gateway also utilizes a number of lightweight image processing technologies to normalize the images prior to the OCR phase. More heavyweight image processing algorithms are utilized at Barracuda Labs to quickly generate fingerprints that can be used by Barracuda Email Security Gateways to block messages.

- **Animated GIF analysis**. In addition, the Barracuda Email Security Gateway contains specialized algorithms for analyzing animated GIFs for suspect content.

Bayesian Analysis

Bayesian Analysis is a linguistic algorithm that profiles language used in both spam messages and legitimate email for any particular user or organization. To determine the likelihood that a new email is spam, Bayesian Analysis compares the words and phrases used in the new email against the corpus of previously identified email. The Barracuda Email Security Gateway only uses Bayesian Analysis, after administrators or users profile a corpus of at least 200 legitimate messages and 200 spam messages.

Spam Scoring

Beyond absolute blocks that a single filter can apply, the Barracuda Email Security Gateway also includes a sophisticated scoring engine that weighs multiple factors where a single filter may result into restrictive policy. By combining multiple rules with known weightings, the Barracuda Email Security Gateway can deliver a strong confidence interval for spam messages.

The Barracuda Email Security Gateway enables administrators to set global spam scores. Certain models of the Barracuda Email Security Gateway also support per domain and per user thresholds.

Mail Hash or Message Digest
A number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that a different set of text would produce the same hash value.

Phishing
Phishing is a criminal activity where phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.

Bayesian Analysis
A technique used for identifying spam. Named after Thomas Bayes, a mathematician who developed a theory of probability inference, this technique analyzes each message based on the statistical frequency of word occurrence of a user's previous email activity to determine if the message is spam or legitimate.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.