IP Analysis Inbound

https://campus.barracuda.com/doc/3866684/

About IP Analysis

After applying rate controls, the Barracuda Email Security Gateway then performs analysis on the IP address, applying tag, quarantine or block policies that you configure in the **BLOCK/ACCEPT** pages.

Once the true sender of an email message is identified, the reputation and intent of that sender should be determined before accepting the message as valid, or "not spam". The best way to address both issues is to know the IP addresses of good senders and forwarders of email and define those on the Barracuda Email Security Gateway as *Allowed* by adding them to a *whitelist* of known good senders. Various methods for discerning "good" senders of email versus spammers are described in this section to help you to quickly configure your Barracuda Email Security Gateway per the needs of your organization.

> Barracuda Networks does NOT recommend whitelisting domains because spammers will spoof domain names. When possible, it is recommended to whitelist (Allow) by IP address only.

Known Forwarders

On the **BASIC > IP Configuration** page you can specify the IP addresses of any machines that are set up specifically to forward mail to the Barracuda Email Security Gateway from outside sources. These are called **Known Forwarders** and will bypass SPF, Rate Control and IP Reputation checks. In the IP Analysis layer, the Barracuda Email Security Gateway examines the Received headers and evaluates the first non-known IP address when applying the above filters and other block and accept policies.

IP Reputation

The Barracuda Email Security Gateway enables administrators to define a list of trusted (known) mail servers by IP address. By adding IP addresses to this list, administrators can avoid spam scanning of good email, thereby both reducing processing load and eliminating the chances of false positives. Note that virus scanning and blocked attachment checks are still enforced.

Likewise you can define a list of bad email senders. In some cases, you may choose to utilize IP blocklists on the **BLOCK/ACCEPT > IP Filters** page to restrict specific mail servers as a matter of policy rather than as a matter of spam.

Barracuda Reputation (BRBL)

Barracuda Reputation is a database maintained by Barracuda Central and includes a list of IP addresses of known good senders as well as known spammers, or IP addresses with a "poor" reputation. This data is collected from spam traps and other systems throughout the Internet. The sending history associated with the IP addresses of all sending mail servers is analyzed to determine the likelihood of legitimate messages arriving from those addresses. Barracuda Central continuously updates Barracuda Reputation.

On the **BLOCK/ACCEPT > IP Reputation** page, it is strongly recommended that the Barracuda Reputation Blocklist (BRBL) option be set to "Block".

Email Categorization

(Available in version 6.1 and higher) This feature replaces the Barracuda Reputation Whitelist feature in version 6.1 and higher. Email Categorization gives administrators more control over what they believe to be spam, even though those messages may not meet the technical definition of spam. Most users do not realize that newsletters and other subscription-based emails, while they are considered to be bulk email, are not technically unsolicited - which means that they can not be blocked by default as spam.

The senders of these emails may have a good reputation, but the user may no longer want to receive, for example, a mass mailing from a club or vendor membership. The Email Categorization feature assigns these kinds of emails to categories that display on the **BLOCK/ACCEPT > IP Reputation** page, and the administrator can then create **Block**, **Quarantine, Tag** or **Whitelist** (allow) policies by category. Or the action can be **Off**, in which messages are not scanned for Email Categorization. If the message action is **Tag**, the message subject will indicate the category name.

Categories supported are:

- **Transactional Emails** - Emails related to order confirmation, bills, bank statements, invoices, monthly bills, UPS shipping notices, surveys relating to services rendered and or where transactions took place. The default action is **Whitelist** (allow).

Barracuda recommends setting **Whitelist** for the **Transactional Emails** category to prevent overlooking potentially important billing, bank statements and other time sensitive information.

- **Corporate Emails** - Email sent from MS Exchange Server that involves general corporate communications. Does not include marketing newsletters. The default action is **Whitelist** (allow).
- **Marketing Materials and Newsletters** - Promotional emails from companies such as Constant Contact. The default action is **Off** (no action taken).
- **Mailing Lists** - Emails from mailing lists, newsgroups, and other subscription-based services such as Google and Yahoo! Groups. The default action is **Off**.
- **Social Media** - Social media notifications from sites such as Facebook, LinkedIn and Twitter. The default action is **Off**.
- **Other** - On the Message Log page, the administrator has the opportunity to assign selected messages in the log to a custom category that is 'written in' when clicking the **Categorize** button in the log. See the **BASIC > Message Log** page for details.

Exempting IP Addresses from the BRBL and Other Blocklists

The BRBL and other blocklists that you specify on the **BLOCK/ACCEPT > IP Reputation** page can be overridden by listing the IP addresses or email addresses:

- In the **Barracuda Reputation, External RBL IP Exemption Range** section of the **BLOCK/ACCEPT > IP Reputation** page. Here, you can exempt particular IP addresses from RBL checks, including from the **Barracuda Reputation Blocklist**. Messages from these IP addresses will be subject to all other spam and virus checks.
- In the **Allowed IP/Range** section or **Blocked IP/Range** section of the **BLOCK/ACCEPT > IP Filters** page.
- In the **Allowed Email Addresses and Domains** section or **Blocked Email Addresses and Domains** section of the **BLOCK/ACCEPT > Sender Filters** or **BLOCK/ACCEPT > Recipients** pages.

Subscribing to External Blocklist Services

The **BLOCK/ACCEPT > IP Reputation** page allows you to use various blocklist services. Several organizations maintain external blocklists; if you are using a paid or free external blocklist, you can leverage the blocklist if you are within the terms of service. External blocklists, sometimes called DNSBLs or RBLs, are lists of IP addresses from which potential spam originates. In conjunction with Barracuda Reputation, the Barracuda Email Security Gateway uses these lists to verify the authenticity of the messages you receive.

Be aware that blocklists can generate false-positives (legitimate messages that are blocked). However, because the Barracuda Email Security Gateway sends notifications when it rejects such messages, the sender will be notified and legitimate senders will therefore know to try re-sending their message or otherwise notify the recipient that their messages are being blocked.

Subscribing to blocklist services does not hinder the performance of the Barracuda Email Security Gateway. Query response time is typically in milliseconds, so delays are negligible. Once the Barracuda Email Security Gateway queries a blocklist service, that query is cached on your own local DNS for a period of time, making further queries very fast.

Sender Whitelisting - Precedence

The users' sender whitelists (if the whitelist/blocklist setting is enabled for user accounts) can be overridden by global settings. For example, if the administrator turns on Spoof Protection, which is a global setting, it will supersede any user's whitelist entry. If a user needs to supercede an global IP address block, that user should communicate to the administrator and request that the email or IP address be added to a global whitelist on the Barracuda Email Security Gateway.

Sender filters check:

- The **Envelope From**, **Header From** and **Reply To** fields for per-user settings
- The **Envelope From** for global settings and for per-domain settings

Reverse DNS Blocking

The Barracuda Email Security Gateway can do a reverse DNS lookup on inbound and outbound IP connections and finds the hostname associated with the IP address of the sender. By configuring rules on the **BLOCK/ACCEPT > Reverse DNS** page, you can choose to apply **Common Reverse DNS Rules** by country, **Custom Reverse DNS Rules** that you define, or both to block, quarantine, tag (inbound only) or whitelist (Custom Reverse DNS Rules only).

The last part of a hostname is known as the top level domain, or TLD. Most TLDs include a country identifier, such as .ca for Canada, .ru for Russia, etc. If most or all of the mail that you receive from a particular country is spam, you can use the **Common Reverse DNS Rules** to tag (inbound only), block or quarantine any any message that has an associated hostname that includes that country's TLD. Email which is not blocked is subject to all of the usual spam and virus checks. Use the **Custom Reverse DNS Rules** to tag, quarantine or block messages from hostnames ending with values that you specify. List the sending domains or subdomains you want to whitelist on the **BLOCK/ACCEPT > Sender Filters** page.