Reverse DNS Blocking

https://campus.barracuda.com/doc/39819732/

The Barracuda Email Security Gateway does 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 or create Custom Reverse DNS Rules to quarantine or block outbound messages from those domains.

Blocking by Top Level Domain (TLD)

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 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.

Whitelist Override for TLDs

Use the Custom Reverse DNS Rules to quarantine or block outbound 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. You can use the Custom Reverse DNS Rules to whitelist all or part of a hostname from which you want to always allow mail, both inbound and outbound. With the whitelist option you can thereby override the Common Reverse DNS Rules settings for TLDs. If you have blocked any TLDs in Common Reverse DNS Rules, for example, you can use the Custom Reverse DNS Rules whitelist option to allow mail from one or more hostnames within that TLD.

Messages With a Missing PTR record

Use the Block Missing PTR Records setting to enable blocking mail from IP addresses with no PTR (reverse DNS) record defined.

Many mail servers do not have their reverse DNS configured properly, which may cause legitimate mail to be blocked when Block Missing PTR Records is set to Yes.