How to block or quarantine email from specific countries (Geo-Blocking)

×This HOWTO applies both to ESG 4.X and ESG 5.X

Indroduction

Cyber-war is a reality and ever evolving geo-political tensions shape and modify the cyber risk for organizations and states.

The quick escalation of the current war in Europe led the national CSIRTs (Computer Security Incident Response Teams) to issue guidelines for mitigating risks related to potential cyber-attacks to companies, institutions, infrastructure and communication systems.

This document is about mitigating risks by blocking email based on the geographical location of the host it has been originated or relayed through.

Email as an attack vector and Geo-Blocking

The most common use of email as an attack vector is through phishing and malware campaigns. Email is the most used communication channel between organizations, most of the breaches start with an email and targeted campaigns are a quite common attack tool used by state actors and politically motivated cybercriminals.

Geo-Blocking is one of the tools that can be used to minimize the attack surface in regards to attacks being originated from specific countries. Attackers can, of course, route the attacks through different countries but this involves additional steps and increases the chances of the attacks being detected. Even if Geo-Blocking is not a silver bullet, it may be one of the rational mitigation measures to be implemented when the geo-political situation increases the chances of attacks from certain geographical areas.

Every organization has its own needs. Some organizations are exposed to frequent communications to some countries, some other organization aren’t. For some organizations plainly blocking traffic from some countries is feasible, for some other organizations it isn’t

and a more elaborated approach is needed.

This document helps Libraesva ESG customers in defining and implementing an email geo-blocking strategy that fits their needs.

Choosing the strategy: rejecting vs quarantining

There are two possible strategies: rejecting all email from a specific origin or accepting it and quarantining it.

Rejecting strategy

Rejecting email at the SMTP level can be done by dropping connections from IP addresses belonging to a specific country. It is simple and effective in terms of resource usage but it leaks information to the potential attacker: they will immediately know that you are adopting this kind of mitigation measure.

Rejecting has also another disadvantage: you have no visibility on what email traffic has been rejected, you don’t know whether there was some legit traffic among it and you are not aware of targeted attack attempts.

Finally: rejecting email relies on the geo-location of the connecting IP address and this is sub-optimal. The email might have been relayed through a country you are not blocking even though it has been originated in a country you would like to block.

Quarantining strategy

Quarantining, on the other hand, involves accepting and analyzing all email but silently quarantining (not delivering) email from specific origins.

One advantage of quarantining versus rejecting is that by accepting such email traffic you not leaking any information to the potential attacker.

By quarantining you also have full visibility on the blocked traffic and you can analyze the email samples in order to detect attempted attacks and investigate the technical tools and strategies the attackers are using (our analysts are always here to help you in this task).

Also, the quarantining strategy can be defined not only on the last-hop (the final relay that is attempting to deliver the email) but also on any of the intermediate hops. You can also decide

to block email that has been originated (first-hop) or relayed through (intermediate-hop) a specific country.

Finally, with a quarantining strategy you are free to define exceptions and, for example, block email from an entire country except the one originated from a few specific organizations you entertain relationships with.

All this said, we do generally suggest a quarantining strategy. Only under very particular circumstances a reject strategy can be evaluated. Our technical support team is available in helping you with this decision.

Implementing the quarantining strategy on Libraesva ESG

Libraesva ESG geo-locates all the relays involved in the delivery of each email. They are listed in the “Received:” headers.

Some of these headers can be spoofed by the attackers but others can’t. For example the last hop cannot ever be spoofed and also the headers in email relayed through third party services (major email providers or email delivery platforms) cannot be spoofed.

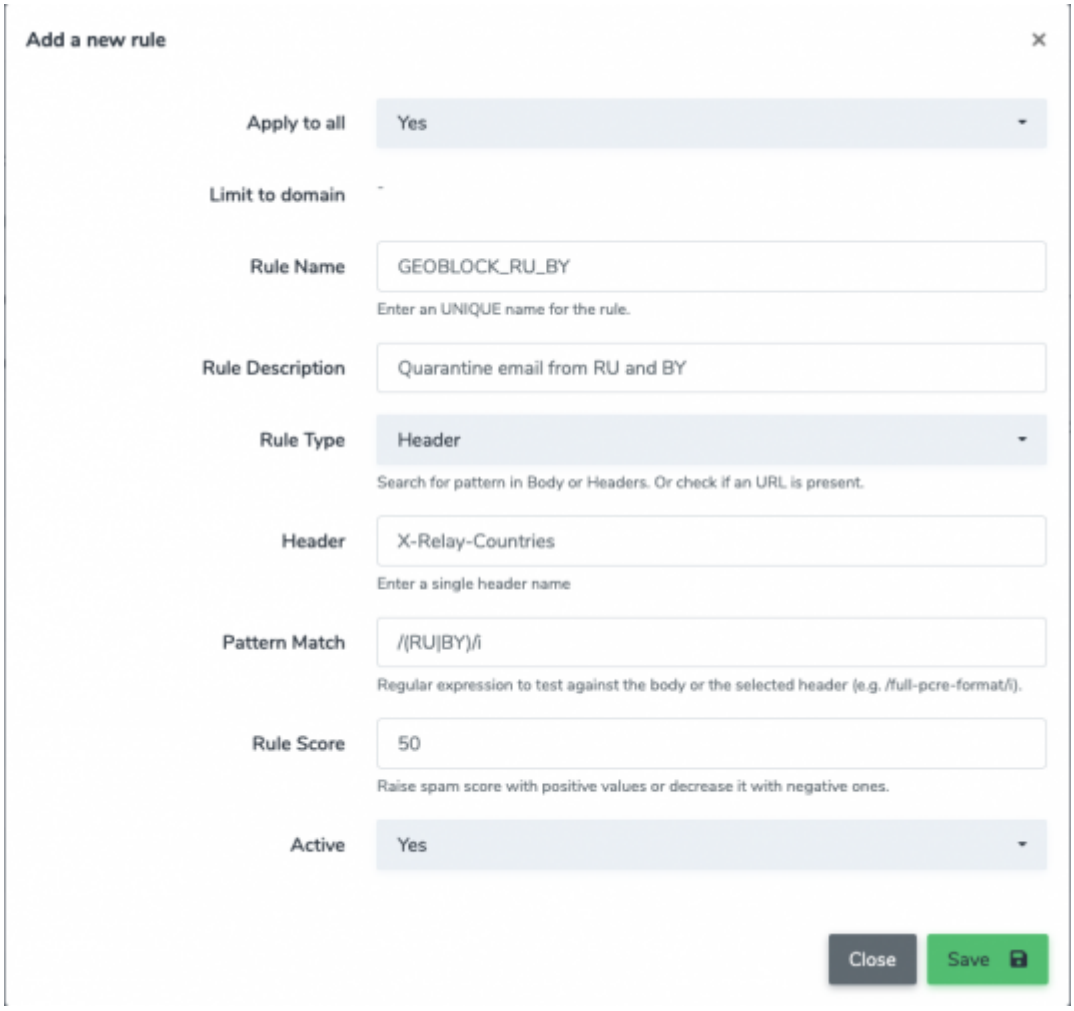
Through a “Custom Spam Policy” you can define the list of countries you want to block.

Let’s start with one example: blocking all email originated or routed through Russia or Bielorussia.

On ESG 5.x go to: Admin area -> Antispam settings -> Custom spam policies

On ESG 4.x go to: System -> Content analysis > Anti-spam settings > Custom spam policies

Click on “new” and enter a rule like this:



In the *"Apply to all"* field you can choose a recipient domain if you wan to apply the rule only to email delivered to one domain.

The *"Pattern match"* field contains a regular expression that contains the two-letter country codes of the counties you want to block. You can find a list of all the country codes here. If you don't know what a regular expression is just copy the pattern and modify it by entering, inside the brackets, the list of country codes separated by **"|"**;

The pattern **/(RU|BY)/i** performs the check on all the hops, first, intermediate and final. Any hop that is in Russia or Bielorussia will trigger this rule.

If you want to limit the check to the first hop (the host that first originated the email) you can change the pattern to: **/(RU|BY)$/i**

If you want to limit the check to the last hop (the host delivered the email to ESG) you can change the pattern to: **/^(RU|BY)/i**

×For the techies: this regexp is applied to a string containing a list of two-letter country-codes ordered in the inverse order of the email hops. For example en email that has been originated in Italy and has a second hop in the United States will result in: **"US IT"**

The field *“Rule score”* is the score that will be added to the message when the rule triggers. The default score for quarantining an email is 4. With a very high score like the one in the example you are guaranteed that the email will not be delivered and it will also be hidden from the quarantine report (by default messages with scores above 25 are hidden from the quarantine reports). This means that the recipients will not even see these messages in their quarantine report.

Feel free to use a lower score or to change the quarantine report visibility threshold if you want these messages to be listed in the quarantine report.

Exceptions

Configuring exceptions is easy.

The simplest exception is a whitelist. Assuming you want to allow email to come in from some domains located in a country you are blocking, you can enter a whitelist with the domain in the From field. We suggest to make sure that the originating domain is adequately protected with SPF or (even better) DMARC.

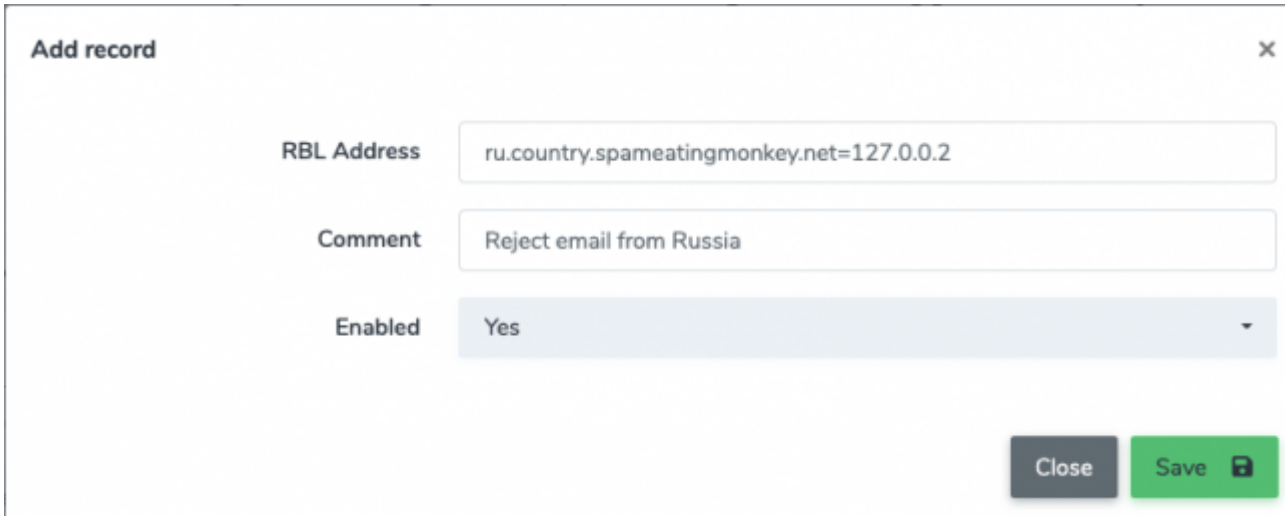
Implementing the reject strategy in Libraesva ESG

This can be done by using a geographical RBL. Here are the instructions:

On ESG 5.x go to Admin area -> Mail transport -> Relay configuration -> RBL filtering

On ESG 4.x go to System -> Mail transport -> Relay configuration -> RBL filtering

Click on “New” and enter an entry like the following one:



The example above rejects email originated from Russia.

In order to block another country just enter a new entry and replace the two-letter country code at the beginning of the “RBL Address” with the country-code of your choice.

For example, to block Bielorussia enter in the “RBL Address” field the following:

`by.country.spameatingmonkey.net=127.0.0.2`

You can find a list of all the country codes here.

×This configuration will reject email. The rejection is definitive (SMTP code 5XX) and the sender will receive a bounce notification.