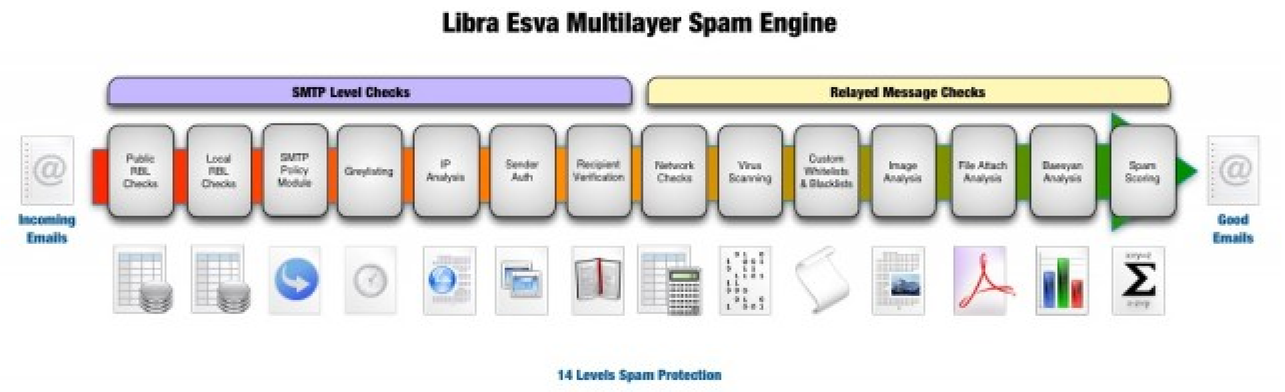
Multilayer Antispam Engine Explained

Introduction

Libraesva ESG Antispam Engine is based on a multi layered analysis; each incoming message is checked against 14 levels before Libraesva ESG takes the decision to deliver it as clean and safe or to block it.

Understanding the message flow and each layer response is very important to diagnose any message delivery problem.

The multi layered anti-spam engine can be graphically explained as follows:



As is clearly visible in the above image there are two main groups of checks:

- The first seven, identified as "**SMTP Level Checks**"
- The next seven that are performed only on accepted messages (i.e. if the message passes the SMTP Level ones), identified as "**Relayed Message Checks**"

Understanding this difference in very important as all Libraesva ESG logic relies on this assumption:

- The **SMTP Level Checks** are something related to Message Relay: if a message is blocked by one of these first seven checks, the email will be rejected, in short we will not accept the message, we will not allow relay!

    - The **Relayed Message Checks** are performed only on messages that are accepted, in other words messages are relayed.

A single failure in the first seven checks will cause a message reject; all accepted messages will be analyzed against all next seven checks by default.

Let’s see in detail every single check.

SMTP Level Checks

1) Public RBL

The sender mail server address is checked against public RBLs. If the IP address is listed in one of configured RBLs will be rejected. The list of public RBL to check is defined under System->Relay->RBL Checks.

Exceptions allowed? : Yes
How? : System->Relay->SMTP Override

2) Local RBL
The sender mail server address is checked against Local RBL service, when active. If the IP address is listed in the Local RBL will be rejected. Local RBL can be configured under menù System->Local RBL Configuration

Exceptions allowed? : Yes
How? : System->Local RBL Configuration->Whitelist/Blacklist

3) Greylisting
If the service is active, the sender triplet (ip, mail from, rcpt to) is checked against already known ones. If the triplet is present the message will pass, otherwise will be rejected with a temporary smtp error.

Exceptions allowed? : Yes
How? : System->Greylisting->Custom Entries

4) IP Analisys
This layer is checking for SPF authorized senders against active policies as defined under menù System->Relay->SPF Checks. If the sender defined an SPF record and if the sender IP is in the range of it the check will pass.

Exceptions allowed? : Yes
How? : System->Relay->SMTP Override

5) Sender Auth
This module verifies the sender conformity to the followings: non FQDN senders, unknown hostnames, invalid sender domains, unauthorized destinations, antispoofing

Exceptions allowed? : Yes
How? : System->Relay->SMTP Override

6) Recipient Verification
If enabled on local domains under menù System->Relay->Relay Domains, this check will verify that the recipient email address is existing on your domain and if not will reject the message.

Exceptions allowed? : No, you can only enable/disable on a domain base

7) SMTP Policy
This check is in charge of verifying sender quotas against policies defined under menù System->SMTP Policy Quotas. If the quota limiti s reached will reject (or defer) the message.

Exceptions allowed? : No, refine your policies to match what needed

All the SMTP Rejects above are logged into Libraesva ESG database and can be viewed via Message Tracking Feature or SMTP Rejected Report.

×**WARNING:** The SMTP Checks Override workaround will exclude listed IPs from all the following checks at once: Public RBL, Local RBL, Greylisting, IP Analysis and Sender Auth.

×**NOTE:** Trusted Hosts/Networks, as defined under menù System->Relay->Trusted Networks, and SMTP Auth Clients, as defined under menù System->Relay->SMTP Auth, are excluded from SMTP Checks 1 to 5 above.

Relayed Message Checks

1) Network Checks

This check verifies the message hash against public databases of spammers; Razor, Pyzor and DCC are the online networks checks that are performed. You can disable those checks under menù System->Spam & Quarantine Settings->Antispam General Settings.

2) Virus Scanning

Each message is virus scanned. This check is mandatory and can not be disabled in any case. All messages (in/out) will be always virus checked!

3) WhiteLists & Blacklist

This module will check the message envelope sender against local blacklists or whitelists. Entries can be populated from menù Lists.

4) Image Analysis

This layer is in charge of checking embedded images for spam.

5) File Attachement

All message attachments are checked against policy compliance as defined under menù System->Spam & Quarantine Settings->Attachment Checks.

6) Bayesian Analysis

Libraesva ESG can take advantage of bayesian analysis and give confidence about a new message looking back to previously learned ones. This check can be disabled under menù System->Spam & Quarantine Settings->Antispam General Settings.

7) Spam Scoring

This final module is in charge of summarizing all checks, giving a spam score to each analyzed message. This score is compared against defined spam score thresholds and identified consequently as good/spam.

×**NOTE:** Whitelist at point 3 above will exclude at once the followings checks if sender matches: Network Checks, Image Analysis, Bayesian Analysis, Spam Scoring. File checks policies will be evaluated in any case. AV Scanning is always performed and cannot be disabled.