Quick RSPAMD Mail Gateway Intro

Kevin Chege

SS-E 2019

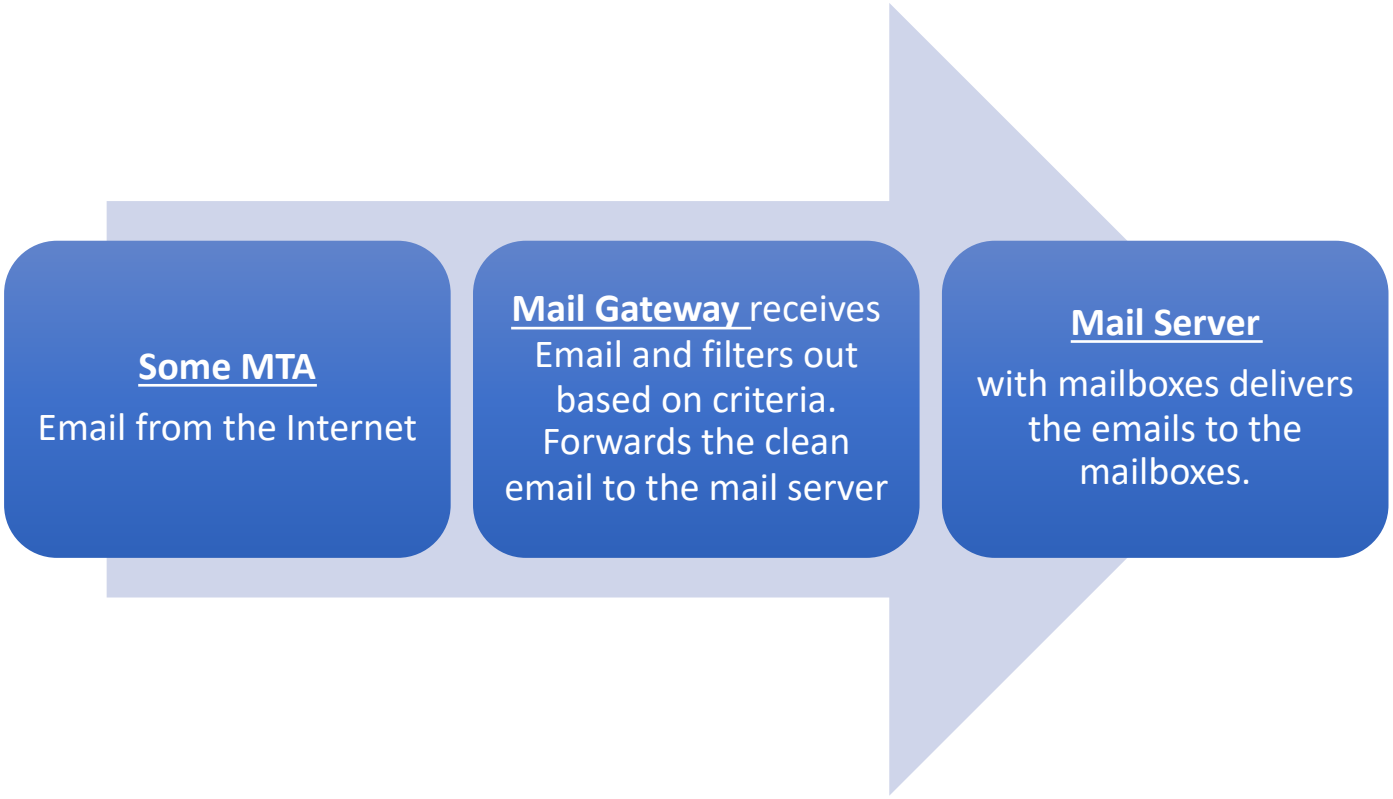
First a recap

- Postfix is our MDA/MTA and SMTP Server –
  - It works on port 25 (SMTP
  - it will send and receive emails but users wont be able to read them
- Dovecot is our IMAP and POP3 server
  - It allows users to check their emails
  - Dovecot allows users to read but not send emails
- Rainloop is a IMAP web client
  - It will not work without an IMAP server (Dovecot)
  - It will not send emails without Postfix

What is a Mail Gateway?

- A software/service/appliance that is able to receive and filter emails before they reach the email boxes
- Typically, a mail gateway will not contain mail box accounts and will only receive emails, filter them based on configured parameters, and then forward them to the mail server that contains the mailboxes
- The purpose is to remove dangerous or harmful content (like spam and viruses) on email before they reach user boxes
- A mail filter can process incoming emails and or outgoing emails

How it flows


Some MTA
Email from the Internet
Mail Gateway receives Email and filters out based on criteria. Forwards the clean email to the mail server
Mail Server
with mailboxes delivers the emails to the mailboxes.

Advantages

- Remove harmful email before it reaches mail boxes
  - Phishing emails, malware, viruses etc
- Remove the work of filtering email from the server that is handling email boxes
- Highly configurable and can block emails based on a number of criteria including content that is in the body of the email
- If hosted outside the network, can reduce load on the network connection/link (also known as far side scrubbing)

Disadvantages

- Mistakes in configuration may mean mail is not delivered. They are highly customisable with hundreds of options and parameters which you must be careful with
- Increase the number of email servers to be managed

Common tools used in Mail Gateways

- *Spamassassin* – No. 1 Open Source anti-spam platform giving system administrators a filter to classify email and block spam (unsolicited bulk email)
- *ClamAV* – Virus scanning software. Can be used for email scanning and web scanning
- *Amavisd* – interface between the MTA and the above tools. A common mail filtering installation with *Amavis* consists of an MTA, ClamAV and Spamassassin
- *MailScanner* - open source email security system design for Linux-based email gateways
- *Rspamd* – Powerful anti-spam software

Mail Gateway Appliances

These are solutions that can be installed on servers and provide Mail Gateway services

- Software:
  - Anti Spam SMTP Proxy - http://en.wikipedia.org/wiki/Anti-Spam_SMTP_Proxy
  - Mail Border - http://www.mailborder.com/
  - ScrolloutF1 - http://www.scrolloutf1.com/
  - Xeams - http://www.xeams.com/
- Hardware (Blackbox):
  - Barracuda - https://www.barracuda.com/products/emailsecuritygateway

What is Rspamd?

- Its an advanced spam filtering system that allows evaluation of messages by a number of rules including regular expressions, statistical analysis and custom services such as URL black lists. Each message is analysed by Rspamd and given a spam score.
- According to this spam score and the user's settings Rspamd recommends an action for the MTA to apply to the message: for example, to pass, to reject or to add a header.
- Rspamd is designed to process hundreds of messages per second simultaneously and has a number of features available.

What Can RSPAMD do?

- https://rspamd.com/features.html
- Check emails for DKIM, DMARC, SPF, IP Address reputation, Greylisting, Rate limiting and much more
- Has a web interface for easy reports gathering
- It works pretty well with default configuration but needs a lot of reading and testing to unlock its full potential

What we shall do in the lab