How does incoming filtering work

Question

What is incoming email filtering and how does it works?

Answer

Email filtering separates legitimate email from unsolicited bulk email with the help of advanced algorithms and spam pattern detection methods.

It works by Re-routing the email through filters.

Spamexperts incoming spam filter is a gateway solution.

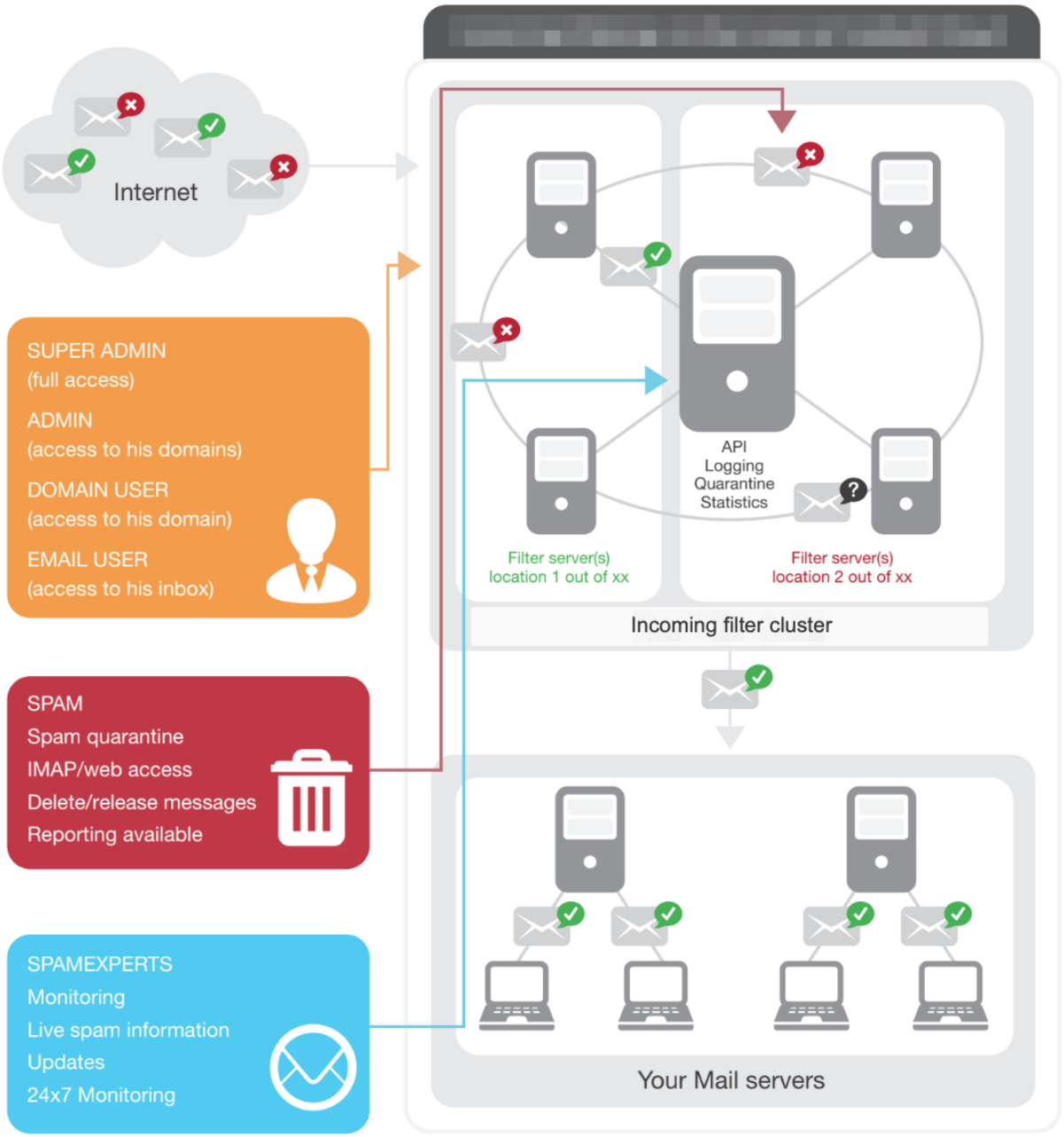
Activation is done via a simple DNS adjustment. Once the MX-records are changed, all inbound email goes to the Spamexperts system first, where it is filtered and then relayed to the unchanged destination mail servers of your clients.

Deployment

The actual message filtering is done in the highly redundant Spamexperts Hosted Cloud.

This solution is fully managed, maintained, and 24/7/365 monitored by Spamexperts.

Filtering work flow:



The filtering of e-mails is done on two levels.

- ◦ At the **SMTP level**, the validity of the sending mail server is checked. The e-mail data stream is collected until the *RCPT TO* command. This way, the e-mail can be logged, but the usage of resources is minimized.
  - ◦ If there is no reason to mark the sender as 'suspected', the e-mail is sent to the next validation step immediately.
  - ◦ If the sender is known as a malicious source, the e-mail is blocked immediately; the sender receives a 5xx code with explanation. This is a *permanent reject*.
  - ◦ If there is no reason to entitle the sender as malicious, but the sender is trusted neither, a grey-listing algorithm will temporarily block the e-mail (*temporarily rejected*).
  - ◦ An RFC-compliant mail server will retry; at the first retry after 10 minutes the e-mail will be accepted by the Spamexperts filters, and the e-mail will be

forwarded to the next validation step.

- ○ At the **DATA level**, the complete e-mail is loaded and verified. Advanced statistical algorithms are used to qualify the e-mail. Because multiple of those algorithms are used, the risk of an incorrect reject (*false positive*) is almost zero - the logs of Spamexperts show that this only happens in 0,001% of all cases.

E-mail that is blocked on the DATA level is put into the quarantine mailbox and can be released from there. E-mail that is blocked on the SMTP level cannot be recovered: the e-mail was simply not received completely.

Revision #2
Created 2026-08-07 14:32:05 UTC by Sarath
Updated 2026-08-07 15:48:57 UTC by Sarath