

D&S Helpdesk

Portal > Knowledgebase > SecurityGateway > Default Settings > ForgedFrom Filter

ForgedFrom Filter

Jason Pomery - 2020-05-22 - 0 Comments - in Default Settings

The purpose of this filter is to catch emails where someone is trying to use an internal name on an external email. In order to replicate the ForgedFrom filter in SecurityGateway there are a couple of minor changes required. I've posted a screenshot below of the test filter from Meducom. There are no TextFiles so the RegEx needs to be put directly in the filter. You also no longer require the REGEX: in front of the expression as there is a drop down where you select Match Regular Expression. The last part where it states sender address does not contain is where you will list all the personal email addresses for the employees. If they are not added here they could be prevented from sending messages from their external email addresses. The rest of the filter is pretty self explanatory from the image below.

The screenshot shows the configuration for a "Message Content Filter Rule". At the top, there are buttons for "Save and Close" and "Close". The "Properties" section includes a checked box for "This rule is enabled", a domain dropdown set to "-- Global --", and a "Rule name" field containing "ForgedFrom". Under "Apply this rule if:", the "All conditions are met (AND)" option is selected, with a checkbox for "... within a proximity of 300 characters" which is unchecked. The "Conditions" section contains a text box with the following text: "If the 'FROM' HEADER matches regular expression '(?=-.*Jason)(?=-.*Pomery)!' (Remove) and if the SENDER ADDRESS does not contain '@meducom.ca' (Remove) and if the SENDER ADDRESS does not contain 'jpomery@gmail.com' (Remove) ...then reject the message." Below this is a link: "Click here to add a condition for this rule". The "Action" dropdown is set to "Reject", and the "SMTP Response" field contains the text "Sorry, this message looks like spam".

Message Content Filter Rule Help | Close

Save and Close Close

Properties

This rule is enabled

For domain: -- Global --

Rule name: ForgedFrom

Apply this rule if:

All conditions are met (AND)

... within a proximity of 300 characters

Any conditions are met (OR)

Conditions:

If the "FROM" HEADER matches regular expression '(?=-.*Jason)(?=-.*Pomery)!' (Remove)
and if the SENDER ADDRESS does not contain '@meducom.ca' (Remove)
and if the SENDER ADDRESS does not contain 'jpomery@gmail.com' (Remove)
...then reject the message.

[Click here to add a condition for this rule](#)

Action: Reject

SMTP Response:
Sorry, this message looks like spam