Using a Signature Service with Impersonation Protection

https://campus.barracuda.com/doc/101713562/

Customers that are using a signature service with M365 may notice that their internal emails are being flagged/remediated by Impersonation Protection.

Normally, internal emails are not analyzed by our classifiers for inbound mail and only analyzed by our ATO (Account Takeover) classifier, which is looking for very specific type of threat (i.e., phishing). Since internal communications may use language that is not common in external communications, the emails are more likely to be seen as frauds/scams.

Because the internal email is being routed out of M365 first, and then back in, the message properties now indicate that this is an “External” email, and therefore our external email classifiers will be applied.

There are a few ways to solve for this:

1. Update your mail flow rule for the signature service to not route internal emails and have a signature applied. This will keep message properties as “Internal” and would no longer be analyzed as external messages.
2. Create a mail flow rule to modify a specific message header, which is used to identify whether an email is internal or external
3. Create an exemption policy within Impersonation Protection.

Update the Signature Service Rule

This should be as simple as modifying the existing rule for the signature service and putting an exception in place *or* making it only apply if the sender is internal and the recipient is external.

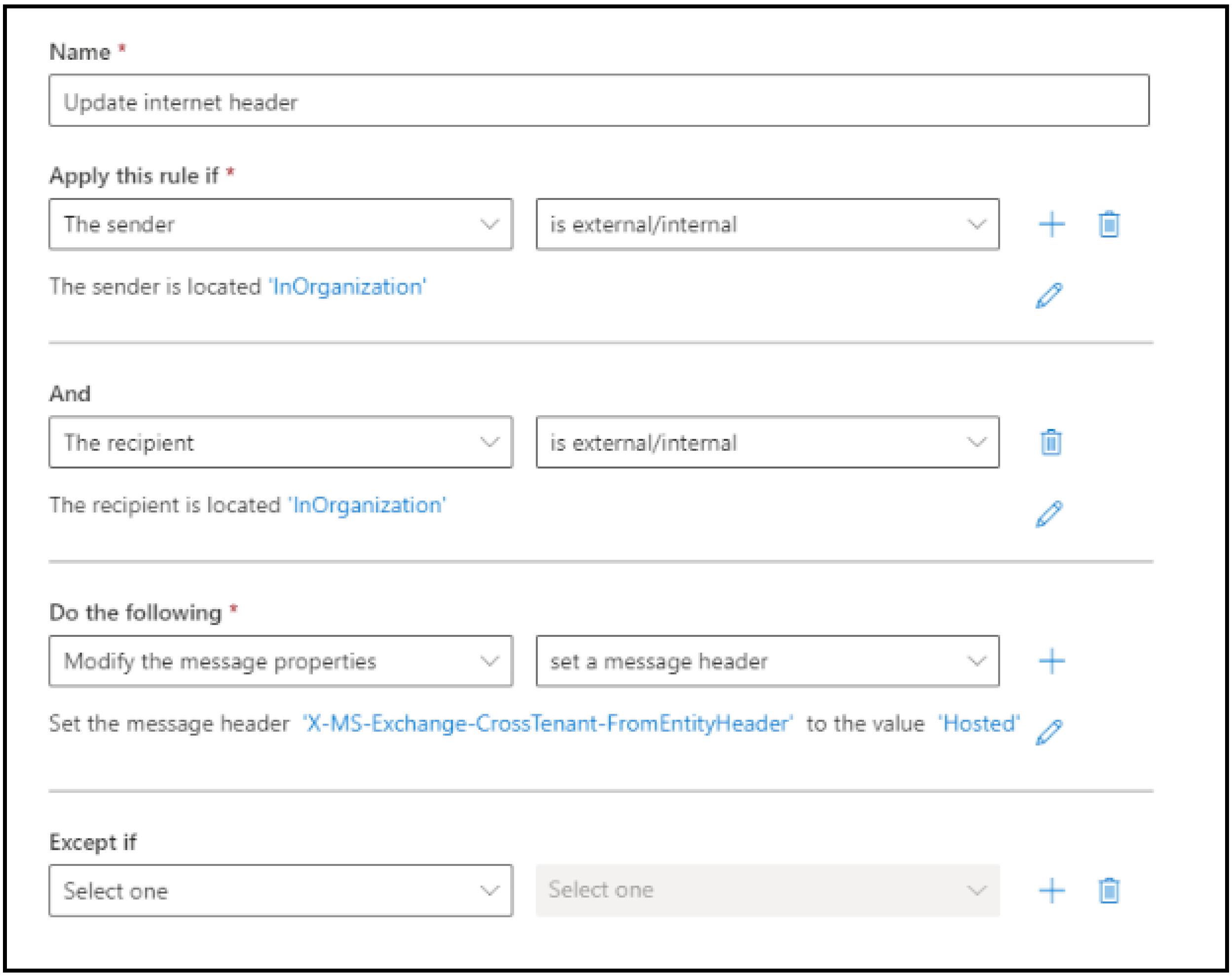
Create a Mail Flow Rule to Modify Message Properties

The message header that we use to determine if an email is internal or external is `X-MS-Exchange-CrossTenant-FromEntityHeader`. This header can have different settings: *Hosted, Internet, or HybridOnPrem*. Emails that originate externally will have values of Internet or HybridOnPrem. Internal emails will be identified as Hosted.

Configure as follows:

Apply this rule if

`the sender` > `is internal`
and
`the recipient` > `is internal`
Do the following
`Modify the message properties` > `set a message header: X-MS-Exchange-CrossTenant-FromEntityHeader`
To the value
`Hosted`



Name *

Update internet header

Apply this rule if *

The sender — is external/internal

The sender is located 'InOrganization'

And

The recipient — is external/internal

The recipient is located 'InOrganization'

Do the following *

Modify the message properties — set a message header

Set the message header 'X-MS-Exchange-CrossTenant-FromEntityHeader' to the value 'Hosted'

Except if

Select one — Select one

Make exemption within Impersonation Protection

Within Impersonation Protection, you can create an exemption for domains, which will skip any sort of classifier analysis.

Creating an exemption for your own domain here is a relatively low risk solution as long as the following two criteria are met:

1. Your domain has a DMARC policy in `p=reject` mode *and*
2. DMARC checking is enabled and enforced at the gateway.

With the above two conditions being true, the only emails that would be reaching a users inbox from your own domain would be those that are either a) internal mails or b) a legitimate third party that is spoofing your domain. If either of these conditions are false, it is not advisable to make an exemption for your own domain.

Figures