PROGIST

Incoming DMARC configuration for Microsoft 365 Exchange Online platform

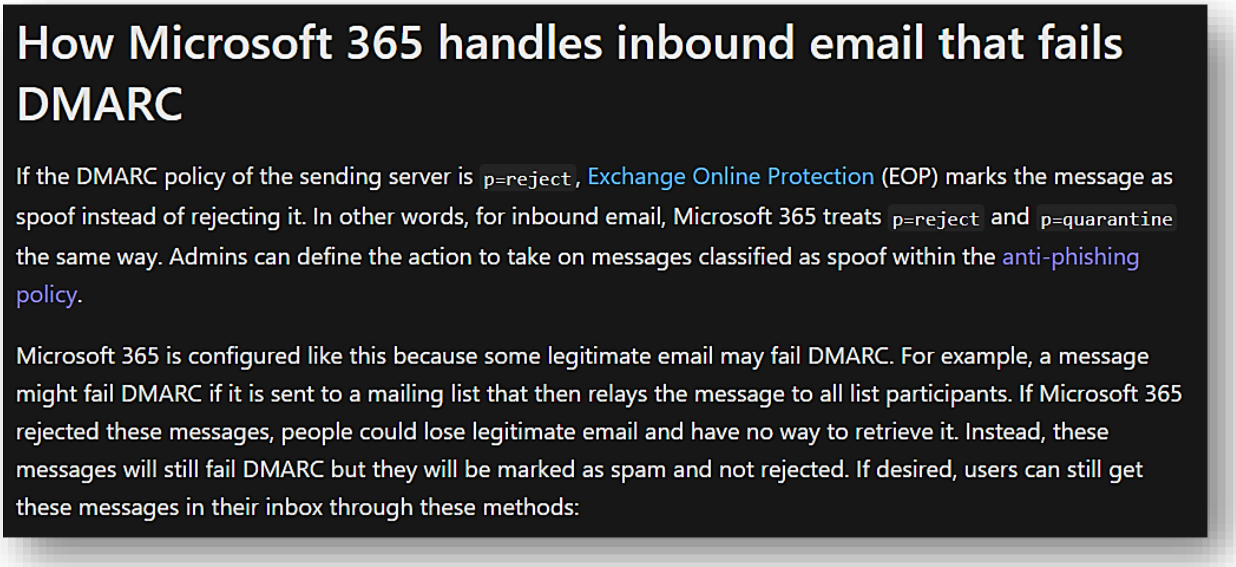
Problem Statement:

Microsoft 365 email platform does not reject the emails failing DMARC policy despite the policy being set to "p=reject".

This is an approach which Microsoft has taken to avoid legitimate emails being blocked. However, this approach from Microsoft also introduces a gap in the DMARC deployment, resulting in spoofed mails to bypass DMARC control.

Please refer to below link for DMARC policy of Microsoft.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dmarc-to-validate-email?view=o365-worldwide#how-microsoft-365-handles-inbound-email-that-fails-dmarc



How Microsoft 365 handles inbound email that fails DMARC

If the DMARC policy of the sending server is `p=reject`, Exchange Online Protection (EOP) marks the message as spoof instead of rejecting it. In other words, for inbound email, Microsoft 365 treats `p=reject` and `p=quarantine` the same way. Admins can define the action to take on messages classified as spoof within the anti-phishing policy.

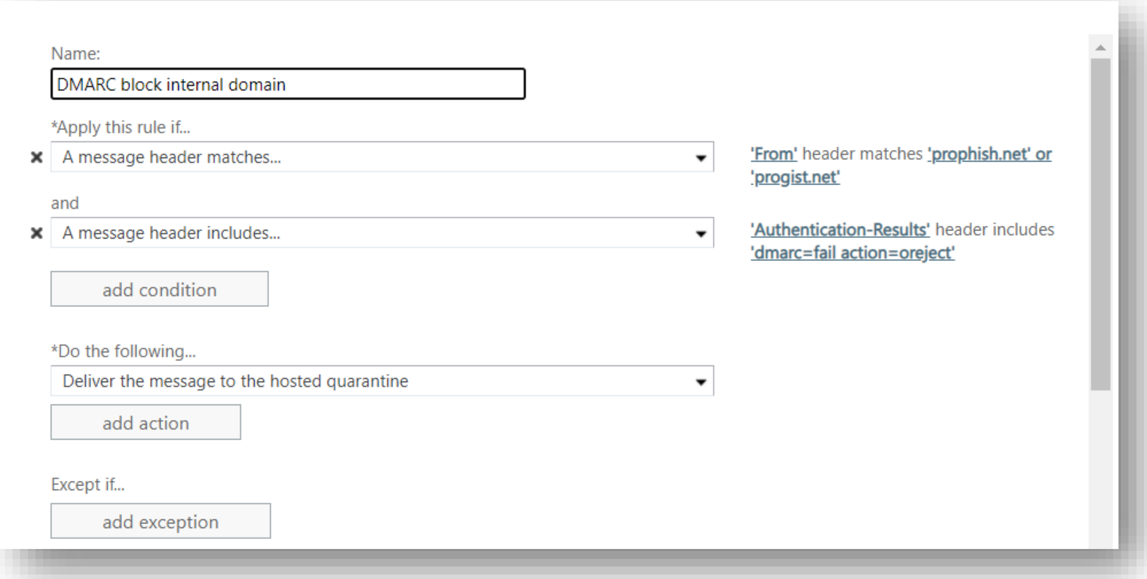
Microsoft 365 is configured like this because some legitimate email may fail DMARC. For example, a message might fail DMARC if it is sent to a mailing list that then relays the message to all list participants. If Microsoft 365 rejected these messages, people could lose legitimate email and have no way to retrieve it. Instead, these messages will still fail DMARC but they will be marked as spam and not rejected. If desired, users can still get these messages in their inbox through these methods:

Solution:

To address this gap in Office 365 DMARC deployment, we can create a transport rule using the "Authentication-results" header. Based on the requirement we can split this deployment into 2 rules (one for the domain we have control over and other for the domain we do not have control over).

1. If mail is received using our domains in "from email address", we can configure the rule to quarantine the emails. This will prevent the email from being delivered to the users.
   The rule will check if the mail is using our mail domain and also, if the DMARC is failing. Based on this action would be defined.

   Note: Before implementing this rule, we must ensure all our authorised mail senders are passing DMARC requirement, else legitimate mails might get rejected. Also, it is recommended to test the rule for few users before deploying for all users (as the mail flow/routing might differ for different organisation)



Name:
DMARC block internal domain

*Apply this rule if...
A message header matches...
'From' header matches 'prophish.net' or 'progist.net'

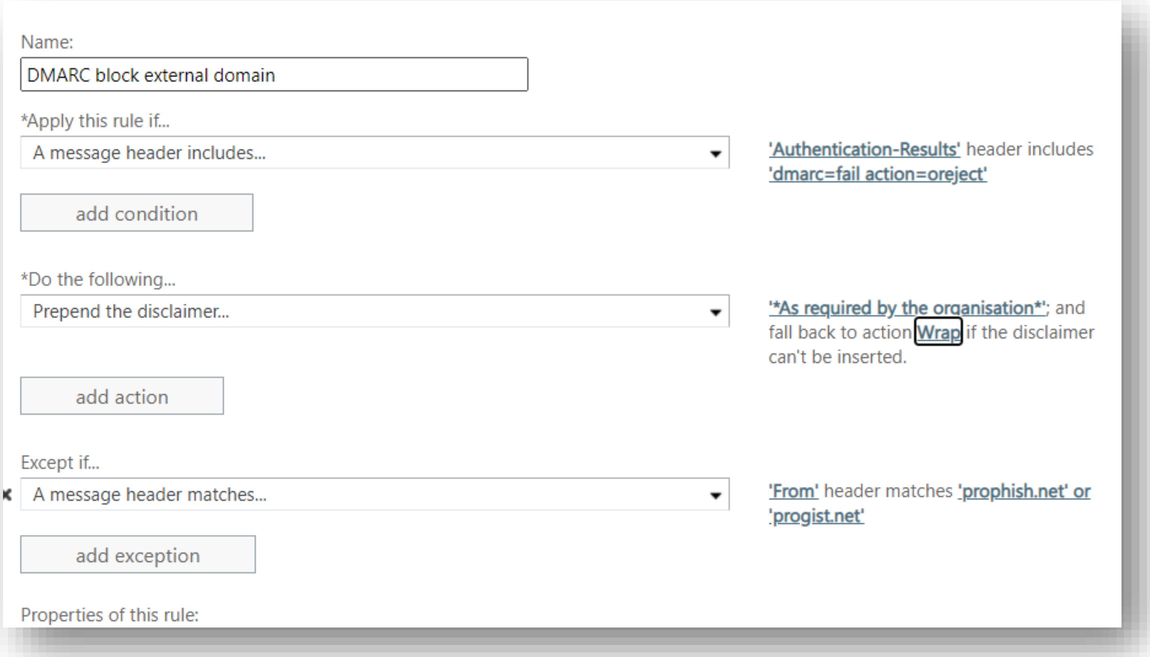
and
A message header includes...
'Authentication-Results' header includes 'dmarc=fail action=oreject'

*Do the following...
Deliver the message to the hosted quarantine

Except if...

2. If the mail is received from any other external domain and the DMARC result is "fail" then we can add disclaimer to alert the user that the mail could be malicious.

   Note: We are configuring disclaimer instead of blocking these emails to avoid email block due to sending domain issues. However, if required the rule can be configured to block the email automatically.



Name:

DMARC block external domain

*Apply this rule if...

A message header includes...

'Authentication-Results' header includes 'dmarc=fail action=oreject'

*Do the following...

Prepend the disclaimer...

'*As required by the organisation*'; and fall back to action Wrap if the disclaimer can't be inserted.

Except if...

A message header matches...

'From' header matches 'prophish.net' or 'progist.net'

Properties of this rule:

Considerations:

1. DMARC should always be validated on the outermost gateway. This rule shall not behave as expected if there is another layer of filter above O365.
2. These will only work for domain spoofed phishing emails and will not work for other types of fraudulent email like display name spoofing and so on.
3. The rule will block spoofed emails only if the DMARC policy is set to reject.
4. The rule shall be configured only after ensuring all the legitimate mails are passing DMARC check to avoid legitimate emails getting blocked.