Enhanced Connectors vs. Mail Flow Rules for Spam Filtering

https://campus.barracuda.com/doc/96010962/

Barracuda currently uses mail flow rules to manage mail flow with Office 365, meaning all email from the internet must first be filtered by Barracuda Networks before being routed to Office 365. Microsoft recommends using enhanced connectors on the Partner inbound connector that receives messages from the third-party application. If you are unsure of which method to use, see the following FAQs.

For more information from Microsoft, see:

- https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/manage-mail-flow-using-third-party-cloud#scenario-1---mx-record-points-to-third-party-spam-filtering
- https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/enhanced-filtering-for-connectors.

What is the difference between using the enhanced connector vs. the mail flow rule?

Using the enhanced connector allows Microsoft to bypass the Barracuda IP and identify the true source IP and apply SPF, DKIM, and DMARC authentication checks against it. Microsoft spam filtering is still enabled using the enhanced connector method.

Using the mail flow rule method will bypass ALL spam checks for messages sent from Barracuda IP ranges.

What can I expect using the enhanced connector method?

The enhanced connector method is only used to apply proper sender authentication policies. Emails that are marked safe by Barracuda can be identified as spam by Microsoft and placed in the user's junk folder or possibly even the hosted quarantine. This is dependent on the spam policies configured on the tenant.

Users that configure allowed senders and blocked senders locally in Outlook will still have those policies applied. Blocked senders allowed by Barracuda are placed in the user's junk folder. Allowed senders would not apply unless Microsoft determined the email as spam. Allowed senders in Outlook can still be blocked by Barracuda and never reach Office 365.

This method continually checks emails for spam. Administrators will need to investigate both Barracuda and Microsoft for email delivery issues, thus potentially increasing management overhead.

What can I expect using the mail flow rule method?

When using the mail flow rule method, all emails are given a spam confidence level (SCL) of -1 which

will ensure that emails from Barracuda are delivered to the user's inbox and not the junk folder or hosted quarantine. Any blocked senders that a user has configured will continue to be placed into their junk folder even though we set the SCL to -1 using the mail flow rule. Customers using the mail flow rule method might receive alerts from Microsoft for an ETR override alert. This alert means that Microsoft identified an email as potential phishing and would have put the email into the junk folder, but because of the mail flow rule, that action was not taken.

Which method should I use?

While both methods will work, customers should choose the method that works best with their configuration.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.