Module 8 – Lab 7 - Exercise 4 – Final Assessment

If you were unable to solve the final assessment problem on your own, perform the following steps to help guide you to a resolution.

Task 1 – Troubleshoot your Hybrid Deployment

The reason emails are being delivered to Adatum users' Junk Email folders rather than to their Inboxes is due to the configuration of the Sender Policy Framework (SPF) record. The SPF record enables receiving mail exchangers to verify whether incoming mail from a domain comes from a host authorized by that domain's administrators.

For Adatum, the SPF record is currently only valid for users who are using the default **onmicrosoft.com** domain as their primary email. This is because the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain has not been fully validated to Adatum's domain controller (LON-DC1). **xxxUPNxxx.xxxCustomDomainxxx.xxx** has only been added to **Adatum.com** for routing messages, and the Outbound Connector that you earlier configured is using the external IP address (provided by your lab hosting provider) to route all messages instead of the smart host proxy.

What this means is that from a routing perspective, it appears to the **Adatum.com** domain that these emails are spoofing the **xxxUPNxxx.xxxCustomDomainxxx.xxx** domain. This is causing email traffic to fail the SPF check, which causes the messages to land in recipient's Junk Email folder.

The following steps will guide you on how to validate the cause of this problem, and then instruct you on how to resolve it.

1. You should still be logged into LON-EX1 from the prior exercise; if necessary, log in as the **Administrator** with a password of **Pa55w.rd**.
2. In your **Edge** browser, if the Exchange admin center for Exchange Online tab is still open, then skip to step 4.

   If the Exchange admin center for Exchange Online tab is no longer open but the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab are still open, then proceed to step 3.

   However, if you had to close your browser to refresh it in the prior lab exercise and the **Microsoft Office Home** tab and the **Microsoft 365 admin center** tab are no longer open, then select a new tab, navigate to **https://portal.office.com** and log in as **admin@xxxxxZZZZZZ.onmicrosoft.com** (where xxxxxZZZZZZ is the tenant prefix provided by your lab hosting provider) with your tenant email password provided by your lab hosting provider, and then in the **Microsoft Office Home** tab, select **Admin** to open the Microsoft 365 admin center.
3. You will now navigate to the **Exchange admin center** for Exchange Online. In the **Microsoft 365 admin center**, in the left-hand navigation page, select **Show all** (if necessary), and then under the **Admin centers** group select **Exchange**.

4. In the **Exchange admin center** for Exchange Online, select **mail flow** in the left-hand navigation pane, and then in the expanded **mail flow** group, select **Message trace.**
5. In the **Message trace** window, the **Default queries** tab is displayed across the top of the page. Select the **Custom queries** tab instead.
6. On the **Custom queries** tab, select **+Start a trace** on the menu bar.
7. In the **New message trace** window that appears, enter the following information to create a 24-hour search window (anything longer will not display the search results, but rather write them to a csv file):
   - Senders: leave default (All)
   - Recipients**:** enter **Alex** and then select **Alex Wilber**
   - Time range: Last 2 days (do not change)
   - Report type: **Summary report**
8. Select the **Search** button.
9. Once the message trace has completed, select one of the messages whose status is displayed as **FilteredAsSpam.**
10. The **Message trace** for the email will open in a new pane. Under **Message Events,** verify the last event was that the message was delivered to the Junk Email folder.

    Note: You should verify at the top of the window that the sender was Allan Yoo, which indicates this email was a valid email that should not have been classified as spam.
11. In the **Message trace** window, select the **X** to **Close** the window.
12. You will now troubleshoot the issue to determine why email from Allan's on-premises mailbox is being delivered to Alex's Microsoft 365 mailbox but placed in his Junk Email folder; in other words, why Allan's email is considered as spam.

    When you own an email domain (as Adatum does with it xxxCustomDomainxxx.xxx domain), you can use DNS to help ensure that messages from senders in that domain are legitimate by using SPF authentication. SPF verifies the source IP address of the message against the owner of the sending domain.

    You will begin the troubleshooting process by checking the **message properties** to verify the **SPF threshold**. To do this, you must start an **InPrivate Browsing** session so that you can sign into Alex Wilber's email without having to sign out of the already established admin session that you have with the normal Edge browser.

    Right-click on the **Edge** icon on your taskbar and select **Start InPrivate Browsing**. Maximize the EDGE window that appears.

    Important: The next steps are not typical troubleshooting steps when dealing with messaging issues. Typically, you would request the message as an attachment to be sent to your account to check the message properties. These next steps are for the purposes of expediency and are for the purposes of the VM lab environment.

13. Maximize the InPrivate browser window and enter the following URL: **https://portal.office.com**

14. In the **Sign in** window, enter **alexw@xxxxxZZZZZZ.onmicrosoft.com** (where **xxxxxZZZZZZ** is the tenant prefix provided by your lab hosting provider) and then select **Next.**
15. In the **Enter password** window, enter your tenant email password provided by your lab hosting provider and then select **Sign in**.
16. In Alex's **Office 365 Home** page, note all the Microsoft 365 application icons that appear in the column on the left. These are the apps that are enabled for Alex given his Office 365 E5 product license. Select **Outlook**.
17. Alex's Microsoft 365 mailbox will open in **Outlook**. If a **Welcome** window appears, select **X** in the upper-right corner to close it.
18. In **Alex Wilber's** mailbox, select the **Junk Email** folder.
19. In the **Junk email** folder, right-click on the message from **Allan Yoo**, and in the menu that appears, select **View,** and then **View message details**.
20. In the **Message details** window that appears, the information is difficult to comprehend. To solve this, you will copy this information and paste it into the Azure Message Header Analyzer utility, which will make it easier to troubleshoot the cause of the issue.

    Select all the Message details information by dragging your cursor from the top left corner all the way to the last line, then right-click and select **Copy**.
21. Open a new tab in the **InPrivate Browser** and then enter the following URL in the address bar: **https://mha.azurewebsites.net/pages/mha.html**
22. In the **Message Header Analyzer** window, there is an **Insert the message header you would like to analyze** banner at the top of the page. Below this banner is a text box. Paste the Message Details you copied from the earlier step into the text box (right-click in the box and select **Paste**).
23. After pasting the Message details into the **Message Header Analyzer** text box, select the **Analyze headers** button that appears below the text box.
24. A table of information will appear below the **Analyze headers** button. Scroll down until you reach the **Other headers** section.
25. The information that you are looking for should be in the second row with a header of **Received-SPF** and a Value of: **Received-SPF: Fail (protection.outlook.com: domain of xxxUPNxxx.xxxCustomDomainxxx.xxx does not designate External IP address as permitted sender**)

    IMPORTANT: This message indicates that the referenced domain is not a validated sender according to the Sender Policy Framework (SPF), which is designed to prevent email spoofing. The system works by verifying that each email message is sent from an authorized IP address; however, when the domain is not considered a valid sender, then the message is treated as spam.

    You can resolve this issue by updating the SPF record located on LON-DC1 in the DNS Manager.

26. Switch to **LON-DC1**, and if necessary, log in as the **Administrator** account with the password **Pa55w.rd**.

27. If the **Server Manager** appears on the taskbar, then select it now; otherwise, select the **magnifying glass (Search)** icon, enter **Server** in the **Search** box, and then select **Server Manager** in the search results menu.
28. In **Server Manager**, select the **Tools** tab at the top right corner of the page, and then in the menu that appears, select **DNS**. This will open DNS Manager,
29. In the **DNS Manager** window, in the **File Explorer** section in the left-hand column, under **LON-DC1** expand the **Forward Lookup Zones** folder and then select the **xxxUPNxxx.xxxCustomDomainxxx.xxx** zone.
30. In the DNS record pane on the right, double-click the **Text record (TXT)** whose **Data** value is **v=spf1 include: spf.protection.outlook.com -all**.
31. A **xxxUPNxxx.xxxCustomDomainxxx.xxx Properties** window will open. In this window under the **Text field,** you must modify the data to show your **External IP address**. You should modify the value so that it appears as follows:

    v=spf1 ip4: nnn.nnn.nnn.nnn include:spf.protection.outlook.com -all

    NOTE: Replace **nnn.nnn.nnn.nnn** with the IP address provided by your lab hosting provider. For example, if your IP address was 64.64.221.224, the value would appear as:

    v=spf1 ip4: 64.64.221.224 include:spf.protection.outlook.com -all

    IMPORTANT: By adding your external IP address to the TXT record containing the SPF value, you are verifying that the IP address is a valid sender along with Microsoft 365. This corrects the issue with the Sender Policy Framework (SPF), since the SPF value specifically calls out Adatum's external IP address. The domain is now considered a valid sender, which allows emails that are sent from mailboxes on LON-EX1 to arrive in the recipients' Inboxes rather than their Junk Email folders.
32. After modifying the **Text** value, select **OK**.
33. This will resolve the junk email issue and all new emails being sent from on-premises mailboxes will now pass SPF validation**.** You can verify this by sending an email from **Beth Burke's** on-premises mailbox to **Alex Wilber's** Microsoft 365 mailbox, and the email should be delivered to Alex's Inbox since it should not be recognized as spam.

    Switch to **LON-EX1**, and if necessary, log in as the **Administrator** with a password of **Pa55w.rd.**
34. In LON-EX1, you need to open Outlook for Beth Burke's on-premises mailbox. The InPrivate Browsing session should still have Alex Wilber's mailbox open, so you cannot use that session. Instead, hover your mouse over the Edge icon on the taskbar and select the **Microsoft 365 admin center**. This will navigate you to the primary Edge browsing session.
35. In your Edge session, select a new tab and then open **Outlook Web App** by entering the following URL: **https://xxxUPNxxx.xxxCustomDomainxxx.xxx/owa** (where xxxUPNxxx is the unique UPN name assigned to your tenant by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's custom domain).

    Note: If you receive a page indicating **Your connection isn't private**, this is due to a certificate issue in the VM environment that you can ignore for the purpose of this lab. To bypass this error, select the **Advanced** button, and then select **Continue to localhost (unsafe)**.

36. In **Outlook**, enter **Adatum\Beth** in the **Domain\username** field, enter **Pa55w.rd** in the **Password** field, and then select **sign in**. If requested, select your **Language** and **Time zone** and then select **Save**.
37. In Beth's on-premises mailbox, you should now send an email to Alex Wilber's Microsoft 365 mailbox. Select **New** in the ribbon, and in the email's **To** address line, enter **alexw@xxxxxZZZZZZ.onmicrosoft.com** (where **xxxxxZZZZZZ** is the tenant ID provided by your lab hosting provider).
38. Enter **SPF test** in the **Subject** line, enter **Email from Beth's on-premises mailbox to Alex's M365 mailbox** in the body of the email, and then select **Send**.
39. At this point, hover your mouse over the Edge icon on the task bar and select **Alex Wilber's mailbox** that appears in the **InPrivate Browsing** session.
40. Close the **Message details** window that was left open from earlier in this task.
41. You should now see Beth's email in Alex's Inbox.

    Note: If the message email sent by Beth still is delivered to the Junk Email folder, on LON-EX1, open the server manager. In the server manager, select Tools and then DNS to open up the DNS Manager. In the DNS Manager, expand Forward Lookup Zones then right click on **xxxUPNxxx.xxxCustomDomainxxx.xxx owa** (where xxxUPNxxx is the unique UPN name assigned to your tenant by your lab hosting provider and xxxCustomDomainxxx.xxx is your lab hosting provider's custom domain) and select **Transfer from Master**. Close and re-open the DNS Manager and verify the SPF record has been updated to reflect what was set in step #31 above. Repeat steps 37-41.

    Congratulations! You have completed the Final Assessment lab by solving the email delivery issue in which email sent from on-premises users to Microsoft 365 users were treated as spam. By correcting the SPF value for the accepted domain, emails from on-premises users to Microsoft 365 users in Adatum's hybrid deployment will now be delivered to their recipients' Inboxes rather than their Junk Email folders.
42. Leave both Edge sessions open and do NOT close any browser tabs.
43. Prior to starting this Final Assessment lab, you initiated a mailbox migration that migrated Allan Yoo's on-pre mises mailbox to Microsoft 365. That process normally takes about an hour to complete. You then proceeded to this Final Assessment lab, which you completed while the mailbox migration was in progress.

    You should now return to the final task in the prior lab exercise to test whether Allan's on-premises mailbox migrated successfully to Microsoft 365.

End of Exercise.