MS-203 Q&As

Microsoft 365 Messaging

Pass Microsoft MS-203 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have a Microsoft Exchange Online tenant that uses an email domain named contoso.corn.

An in-caning email messages route through an third-party filtering service named Filter1 to connector named Connector

You discover that incoming messages contain headers that specify the source IP address as Filter1.

You to ensure that incoming email messages contain headers that specify source IP address of the original sender. The solution must prevent any charges to the service.

What should you do?

A. From Microsoft 365 Defender portal configure enhanced filtering for Connector1.

B. Configure Connector to authenticate messages by using the IP address of Filter service.

C. Configure the MX Of contoso.com to point to contoso-can.mailgotection.outbok.com.

D. From the Exchange admin center. create a transport rule to rewrite header for incoming messages.

Correct Answer: C

QUESTION 2

You have a hybrid deployment between a Microsoft Exchange Online tenant and an on- premises Exchange Server 2019 organization.

Users report that emails sent from Exchange Online mailboxes to the on-premises Exchange Server mailboxes are undelivered.

You need to review the non-delivery report (NDR) for each undelivered email.

What should you use?

A. message trace in the Exchange admin center

B. auditing in the Exchange admin center

C. the SMTP protocol logs in Exchange Server

D. the transport logs in Exchange Server

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/exchange/monitoring/trace-an-email-message/message-trace-faq

QUESTION 3

You need to resolve the issue for the transport department users.

What is the best way to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Move the public folder mailbox that contains TransportPF to a server in the main office.

B. Move TransportPF to a public folder mailbox hosted in the main office.

C. Modify the default public folder mailbox for all the transport department users.

D. Instruct the transport department users to add TransportPF to their Favorites list in Outlook.

Correct Answer: B

References: https://docs.microsoft.com/en-us/exchange/recipients/mailbox-moves?view=exchserver-2019

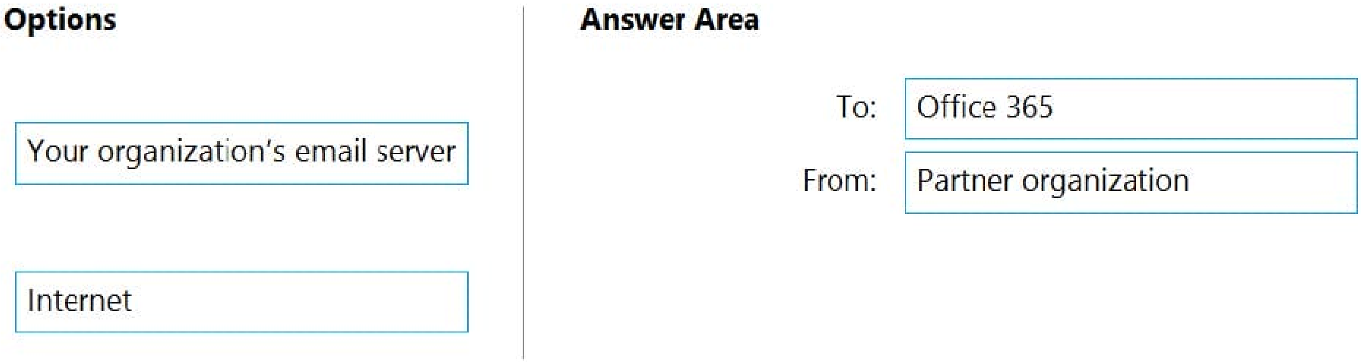
QUESTION 4

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Options

Your organization's email server

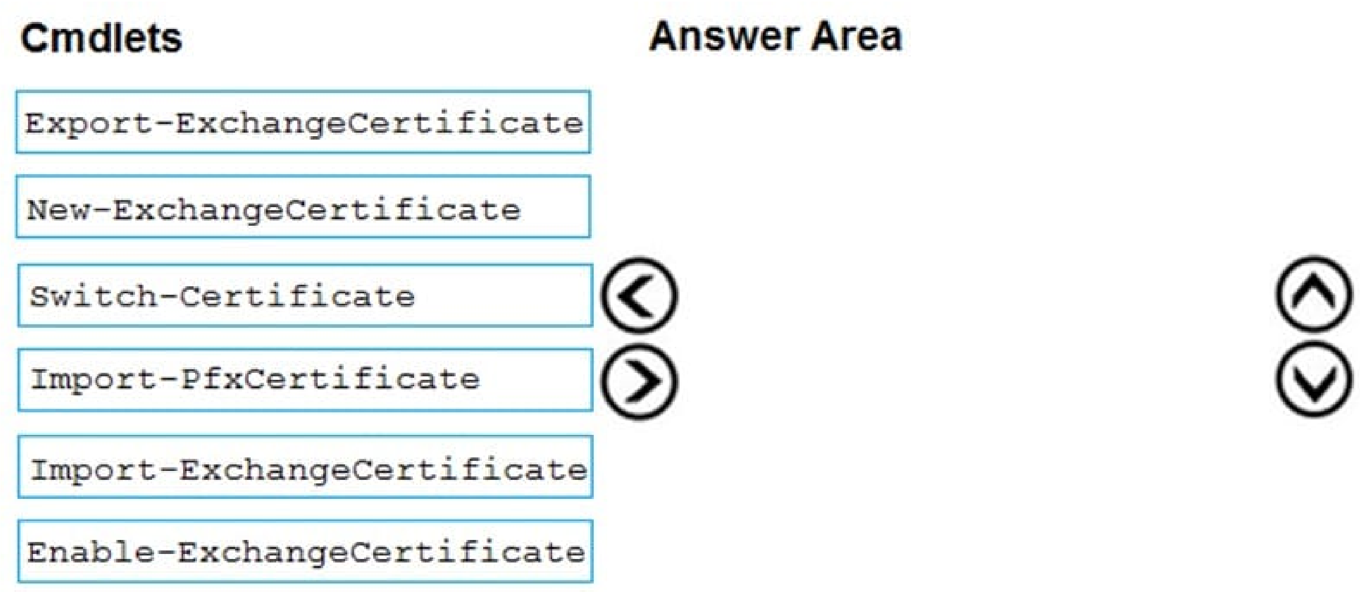
Internet

Answer Area

To: Office 365

From: Partner organization

Correct Answer:



Cmdlets

Answer Area

```
Export-ExchangeCertificate
New-ExchangeCertificate
Switch-Certificate
Import-PfxCertificate
Import-ExchangeCertificate
Enable-ExchangeCertificate
```

Box 1: Yes

The Safe Attachments 1 policy applies to Group1. Alex Wilber is in Group1.

Box 2: No

Megan Bowen is in Group2. The Safe Attachments 2 policy applies to Group2. The Safe Attachments 2 policy will block the email rather then remove the attachment and deliver the email.

Box 3: No

Lynne Robbins is in the Sales department which means she is a member of Group3. She is also a member of Group2 and Group4.

The Safe Attachments 2 policy blocks emails and applies to Group2. There are no other Safe Attachments policies that apply to Group3 or Group4. Therefore, Safe Attachments 2 is the only policy that applies to Lynne Robbins so you do not

need to increase the priority of the policy to block the emails.

QUESTION 5

You need to prevent email messages from a domain named fabrikam.com from being delivered to the mailboxes of your organization.

To complete this task, sign in to the Microsoft 365 admin center.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

1.

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email and Collaboration > Policies and Rules > Threat policies > Anti-spam in the Policies section. To go directly to the Anti-spam policies page, use https://security.microsoft.com/antispam.

2.

On the Anti-spam policies page, click Create policy and then select Inbound from the drop down list.

3.

The policy wizard opens. On the Name your policy page, configure these settings:

-Name: Enter a unique, descriptive name for the policy.

-Description: Enter an optional description for the policy.

When you\\'re finished, click Next.

4.

On the Users, groups, and domains page that appears, identify the internal recipients that the policy applies to (recipient conditions):

-Users: The specified mailboxes, mail users, or mail contacts in your organization.

-Groups: The specified distribution groups, mail-enabled security groups, or Microsoft 365 Groups in your organization.

-Domains: All recipients in the specified accepted domains in your organization.

Click in the appropriate box, start typing a value, and select the value that you want from the results. Repeat this process as many times as necessary. To remove an existing value, click remove × next to the value.

For users or groups, you can use most identifiers (name, display name, alias, email address, account name, etc.), but the corresponding display name is shown in the results. For users, enter an asterisk (*) by itself to see all available

values. Multiple values in the same condition use OR logic (for example, or). Different conditions use AND logic (for example, and).

- Exclude these users, groups, and domains: To add exceptions for the internal recipients that the policy applies to (recipient exceptions), select this option and configure the exceptions. The settings and behavior are exactly like the

conditions. When you\\'re finished, click Next.

5. On the Bulk email threshold and spam properties page that appears, configure the following settings:

- Bulk email threshold: Specifies the bulk complaint level (BCL) of a message that triggers the specified action for the Bulk spam filtering verdict that you configure on the next page (greater than the specified value, not greater than or equal

to). A higher value indicates the message is less desirable (more likely to resemble spam). The default value is 7. For more information, see Bulk complaint level (BCL) in EOP and What\\'s the difference between junk email and bulk email?. By default, the PowerShell only setting MarkAsSpamBulkMail is On in anti-spam policies. This setting dramatically affects the results of a Bulk filtering verdict: MarkAsSpamBulkMail is On: A BCL that\\'s greater than the threshold is converted to an SCL 6 that corresponds to a filtering verdict of Spam, and the action for the Bulk filtering verdict is taken on the message. MarkAsSpamBulkMail is Off: The message is stamped with the BCL, but no action is taken for a Bulk filtering verdict. In effect, the BCL threshold and Bulk filtering verdict action are irrelevant.

-Increase spam score, Mark as spam* and Test mode: Advanced Spam Filter (ASF) settings that are turned off by default.

The Contains specific languages and from these countries settings are not part of ASF.

- Contains specific languages: Click the box and select On or Off from the drop down list. If you turn it on, a box appears. Start typing the name of a language in the box. A filtered list of supported languages will appear. When you find the language that you\\'re looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click remove × next to the value.

- From these countries*: Click the box and select On or Off from the drop down list. If you turn it on, a box appears. Start typing the name of a country in the box. A filtered list of supported countries will appear. When you find the country

that you\\'re looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click remove × next to the value. When you\\'re finished, click Next.

6. On the Actions page that appears, configure the following settings:

-Message actions: Select or review the action to take on messages based on the following spam filtering verdicts: Spam High confidence spam Phishing High confidence phishing Bulk

-

Retain spam in quarantine for this many days: Specifies how long to keep the message in quarantine if you selected Quarantine message as the action for a spam filtering verdict. After the time period expires, the message is deleted, and is not recoverable. A valid value is from 1 to 30 days.

-

Add this X-header text: This box is required and available only if you selected Add X-header as the action for a spam filtering verdict. The value you specify is the header field name that\\'s added to the message header. The header field value is always This message appears to be spam.

- Prepend subject line with this text: This box is required and available only if you selected Prepend subject line with text as the action for a spam filtering verdict. Enter the text to add to the beginning of the message\\'s subject line.

-

Redirect to this email address: This box is required and available only if you selected the Redirect message to email address as the action for a spam filtering verdict. Enter the email address where you want to deliver the message. You can enter multiple values separated by semicolons (;).

-Enable safety Tips: By default, Safety Tips are enabled, but you can disable them by clearing the checkbox.

- Enable zero-hour auto purge (ZAP): ZAP detects and takes action on messages that have already been delivered to Exchange Online mailboxes.

ZAP is turned on by default. When ZAP is turned on, the following settings are available: Enable ZAP for phishing messages: By default, ZAP is enabled for phishing detections, but you can disable it by clearing the checkbox. Enable ZAP for spam messages: By default, ZAP is enabled for spam detections, but you can disable it by clearing the checkbox.

When you\\'re finished, click Next.

7. On the Allow and block list flyout that appears, you are able to configure message senders by email address or email domain that are allowed to skip spam filtering. In the Allowed section, you can configure allowed senders and allowed domains. In the Blocked section, you can add blocked senders and blocked domains. The steps to add entries to any of the lists are the same:

-Click the link for the list that you want to configure: Allowed > Senders: Click Manage (nn) sender(s). Allowed > Domains: Click Allow domains. Blocked > Senders: Click Manage (nn) sender(s). Blocked > Domains: Click Block domains.

-In the flyout that appears, do the following steps: Click + Add senders or Add domains. In the Add senders or Add domains flyout that appears, enter the sender\\'s email address in the Sender box or the domain in the Domain box. As you\\'re typing, the value appears below the box. When you\\'re finished typing the email address or domain, select the value below the box. Repeat the previous step as many times as necessary. To remove an existing value, click remove × next to the value.

When you\\'re finished, click Add senders or Add domains.

- Back on the main flyout, the senders or domains that you added are listed on the page. To remove an entry from this page, do the following steps: Select one or more entries from the list. You can also use the Search box to find values in the list. After you select at least one entry, the delete icon appears Click the delete icon to remove the selected entries

When you\\'re finished, click Done.

Back on the Allow and block list page, click Next when you\\'re read to continue.

8.

On the Review page that appears, review your settings. You can select Edit in each section to modify the settings within the section. Or you can click Back or select the specific page in the wizard. When you\\'re finished, click Create.

9.

On the confirmation page that appears, click Done.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide