W-3, D-1

1. What is EOP? Explain the purpose of EOP.

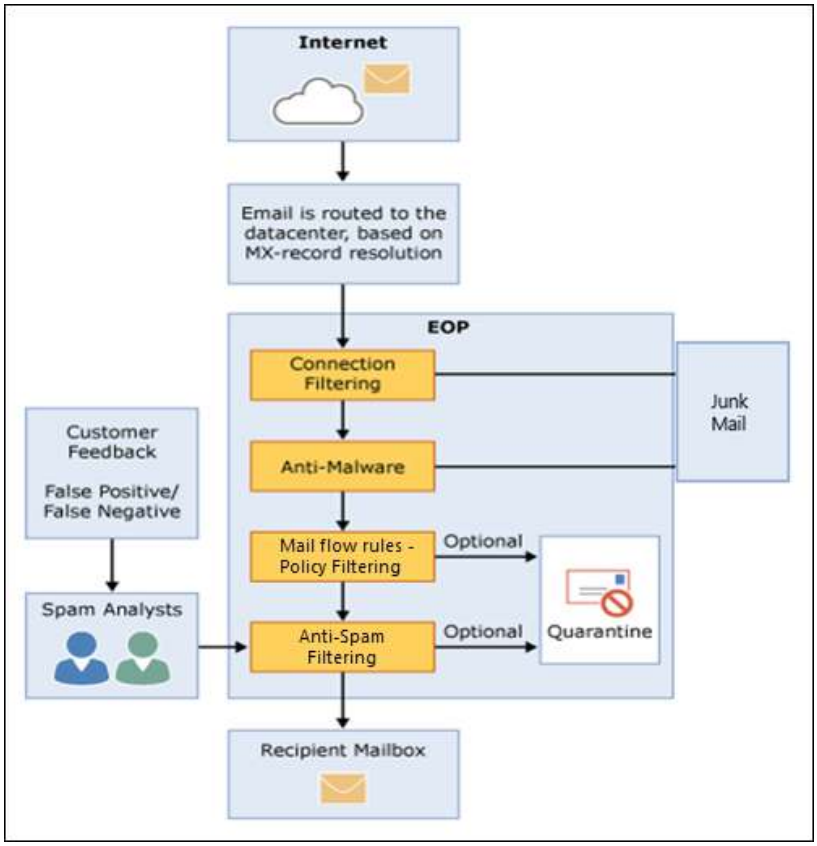
EOP	✓ EOP stands for Exchange Online Protection ✓ Exchange Online Protection (EOP) is the cloud-based filtering service that helps protect your organization against spam and malware. ✓ EOP is included in all Microsoft 365 organizations with Exchange Online mailboxes.
Purpose of EOP	✓ Inbound spam detection ✓ Outbound spam detection ✓ Backscatter protection ✓ Bulk mail filtering ✓ Malicious URL block-lists ✓ Anti-phishing protection ✓ Anti-spoofing protection

2. What does EOP protect and filter Microsoft 365 inbound mail?

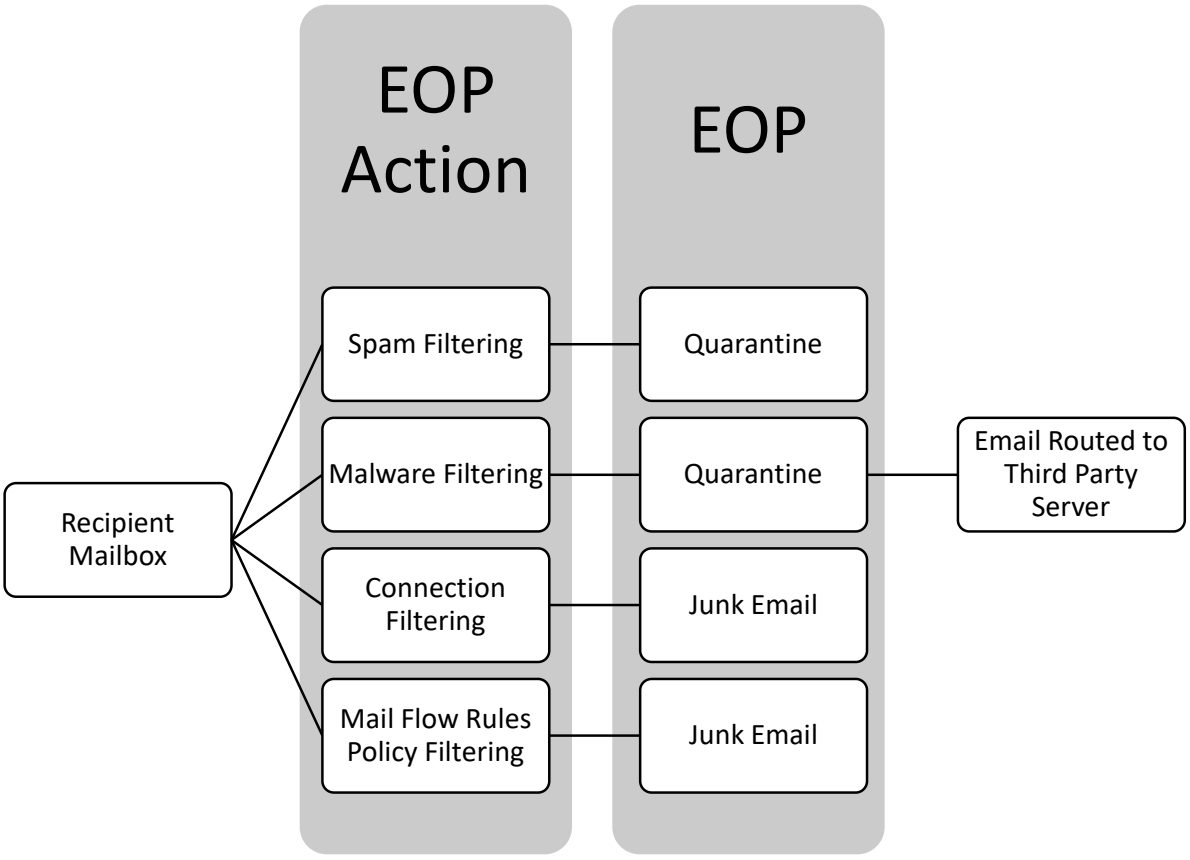
EOP for Inbound Email
I. Initially, email messages are routed to the data center based on MX-record resolution. II. Incoming message initially passes through **Connection Filtering** & **Malware Filtering** which checks the sender's reputation and inspects the message for malware. The majority of spam is stopped at this point and deleted by EOP and send the email to Junk Email. III. Messages continue through **Mail flow rules policy filtering**, where messages are evaluated against custom mail flow rules/transport rules that have been created or enforced from a template. For example, you can have a rule that sends a notification to a manager when mail arrives from a specific sender. Data loss prevention (DLP) checks also occur at this point. IV. Next, messages pass through **Spam Filtering**. A message that's determined to be spam can be sent to a user's Junk Email folder or the quarantine, among other options. V. After a message passes all of these protection layers successfully, it's delivered to the recipient. VI. Customers can give feedback whether the messages are False Positive or False Negative.

W-3, D-1

Overall Scenario for EOP of Inbound Email



EOP for Outbound Email



W-3, D-1

3. How does Malware filtering work? How to block any attachment in inbound mail?

Malware Filtering	✓ Built-in Function - o EOP provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect the network from spam transferred through email. o Admins do not need to set up or maintain the filtering technologies, which are enabled by default. However, admins can make company-specific filtering customizations. ✓ Custom Function – o EOP offers multilayered protection that's designed to catch all known malware. o Messages transported through the service are scanned for malware (viruses and spyware). If malware is detected, the message is deleted. o Notifications may also be sent to senders or admins when an infected message is deleted and not delivered. o You can also choose to replace infected attachments with either default or custom messages that notify the recipients of the malware detection.
Custom Settings	I. Malware Detection Response II. Common Attachment Types Filter III. Malware Zero-hour Auto Purge IV. Notifications V. Administrator Notifications VI. Customize Notifications

Block Attachment in Inbound Email for All users

Please go to – https://outlook.office365.com/ecp

Please navigate to –

① **protection** > ② **malware filter** > ③ double click on the **Default** > ④ **settings** > ⑤ Under **Common Attachment Types Filter**, choose **on** & select any file type that you want to block > ⑥ press **Save**

W-3, D-1

4. How to block or allow any IP?

Allow or Block IP for All users	
Please go to – https://outlook.office365.com/ecp Please navigate to – ① **protection** > ② **connection filter** > ③ double click on the **Default** > ④ **connection filtering** > ⑤ By clicking "**+**" sign you can allow or block IP/IP ranges > ⑥ press **Save**	
Enable Safe list	This is the list of trusted partners. By checking you are allowing all IP's from trusted partners of Microsoft. It will never be detected as spam.

5. How to block or allow any sender or domain? How long messages are retained in quarantine by default? Is the duration changeable?

Block or Allow Sender or Domain for all users
Please go to – https://outlook.office365.com/ecp Please navigate to – ① **protection** > ② **spam filter** > ③ double click on the **Default** > ④ **block lists** > ⑤ By clicking "**+**" sign you can block sender or domain > ⑥ press **Save**
In the very next option **allow lists** – by clicking "**+**" sign you can also allow sender or domain
How long messages are retained in quarantine by default - **15 Days (max 30 days)**
Change the Duration
Please go to – https://outlook.office365.com/ecp Please navigate to – ① **protection** > ② **spam filter** > ③ double click on the **Default** > ④ **spam and bulk actions** > ⑤ Under **Quarantine**, please type the desired dasys in **Retain Spam for (days)** > ⑥ press **Save**

W-3, D-1

6. How to filter messages based on language or country or regions?

Filter Messages Based on Language or Country for all Users
Please go to – https://outlook.office365.com/ecp Please navigate to – ① **protection** > ② **spam filter** > ③ double click on the **Default** > ④ **international spam** > ⑤ Check the box for enabling filter for languages &countries and select the languages and countries that you would like to block > ⑥ press **Save**

7. Explain the different ways of mail auto-forwarding.

Mail Auto Forwarding from EAC
Please go to – https://outlook.office365.com/ecp Please navigate to – ① **recipients** > ② mailboxes > ③ double click on the user mailbox that you want to enable the Mail Auto Forwarding > ④ **mailbox features** > ⑤ Under the **Mail Flow category, Delivery Options** click **View details**
⑥ **Enable forwarding** > ⑦ if you want to keep a copy of that email to the mailbox please check this, otherwise leave it > ⑧ **Browse** > ⑨ select the forwarding email > press **OK**
From now on, if anyone sends an email to that user, that email message will be forwarded to forwarding email.

Mail Auto Forwarding from OWA
Please go to – https://outlook.office365.com Please navigate to – ① **settings** (gear sign) > ② **View all Outlook settings**
③ **Mail** > ④ **Forwarding** > ⑤ **Enable forwarding** & write down the email where you want to forward > ⑥ if you want to keep a copy of that email to the mailbox please check this, otherwise leave it > ⑦ press **Save**

W-3, D-1

Mail Auto Forwarding from Outlook Client
Please open Outlook Client. Please navigate to – ① **Rules** > ② **Create Rule**
Please press – ③ Advanced Options
④ please select any condition > ⑤ change the parameter accordingly by clicking this > ⑥ press **Next**
⑦ select **forward it to people or public group** > change the forwarding email accordingly by clicking this > ⑨ press **Next**
Please press **Next** again
Press **Finish** to save the rule. This rule will work as Auto Forwarding.

8. How to Analyze Message Header.

Message Header from OWA	✓ https://outlook.office365.com > select the message > right click on the message > **view message details**
Message Header from Outlook Client	✓ Open outlook client > double click on the message > **File** > **Properties** > **Internet Headers**

9. What is spam confidence level (SCL)?

SCL	Definition	Default action
-1	✓ The message skipped spam filtering. ✓ For example, the message is from a safe sender, was sent to a safe recipient, or is from an email source server on the IP Allow List	Deliver the message to the recipients' inbox.
0, 1	✓ Spam filtering determined the message was not spam.	Deliver the message to the recipients' inbox.
5, 6	✓ Spam filtering marked the message as Spam	Deliver the message to the recipients' Junk Email folder.
9	✓ Spam filtering marked the message as High confidence spam	Deliver the message to the recipients' Junk Email folder.

W-3, D-1

10.Explain the features of EAC Protection.

Protection (MaCoS)	malware filter	✓ Default ✓ Custom (+)	Settings	✓ Malware Detection Response (Inform the Recipient) ✓ Common attachment Types Filter ✓ Malware Zero Hour Auto Purge ✓ Notification (Sender/Administrator)
			Applied to (only for Custom)	✓ Recipient ✓ Domain
	connection filter	Default	Connection filtering	IP Allow List
				IP Block List
				Enable Safe List (trusted senders IP list)
	spam filter	✓ Default ✓ Custom (+)	Spam and Bulk Actions	✓ Spam (what to do – move junk email) ✓ High Confidence Spam (what to do – move junk email) ✓ Bulk Email (7 Default) ✓ Quarantine (15 Default/30 Max)
			Block lists	✓ Sender ✓ Domain
			Allow Lists	✓ Sender ✓ Domain
			International spam	✓ Language ✓ Country or Region
			Advanced options	✓ SPF ✓ NDR ✓ …… ✓ Test Mode Option
			Applied to (only for Custom)	✓ Recipient ✓ Domain
	outbound filter			
	quarantine	(All Quarantine Messages)		
	action center			
	dkim	(Accepted Domain list)	✓ Enable ✓ Disable	