#### **Domain Name System (DNS) Records**

1. Which type of DNS record determines where mail destined for your domain is routed?
2. TXT Record
3. CNAME Record
4. MX Record
5. NS Record
6. What are common uses for a DNS TXT record when using G Suite? (Choose 2)
7. Domain verification
8. Customise a Google service address
9. Email security records
10. Control inbound mail to your domain
11. In general, from where would you manage your domain's DNS records?
12. In the G Suite admin console
13. In your domain registrar console
14. In your local DNS files
15. All of the above
16. You need to make a change to your MX records and you want the change to be implemented as soon as possible. What approach can you take?
17. Make the change in your DNS console and reduce the Time to Live (TTL) value to 1 hour. Once the change has been implemented revert the TTL value to 24 hours
18. Change your MX records in the admin console and reduce the Time to Live (TTL) value to one hour
19. Make the change in your DNS console and reduce the Time to Live (TTL) value to 1 hour
20. Change your MX records in the admin console and reduce the Time to Live (TTL) value to one hour. Once the change has been implemented revert the TTL value to 24 hours

#### **Enhancing Email Security**

1. What is the main purpose of a Sender Policy Framework (SPF) record?
2. It can be used to verify that message content is authentic and has not changed
3. It specifies which servers/domains can send messages on your behalf
4. It defines the action to take on suspicious incoming messages
5. You have been asked to implement DomainKeys Identified Mail (DKIM) for your organization. How would you do this?
6. Enable DKIM from Apps > G Suite > Gmail > Authenticate email
7. Generate a DKIM record from Apps > G Suite > Gmail > Authenticate email. Add the record to your DNS records and then start authentication from the admin console
8. Enable DKIM directly in your DNS records
9. Generate a key from your DNS records and add it to the G Suite admin console. Then Enable DKIM from Apps > G Suite > Gmail > Authenticate email
10. What policy defines what to do if an incoming message is not authenticated?
11. DKIM
12. SPF
13. DMARC
14. All of the above
15. DKIM adds an encrypted signature to the header of all outgoing messages. What happens if you don't turn on email signing with your own domain DKIM key?
16. Messages are sent as normal with no additional headers
17. Gmail signs all outgoing messages with this default DKIM domain key d=\*.gappssmtp.com
18. Gmail signs all outgoing messages with a key generated using the From address in the message
19. Gmail signs all outgoing messages with a temporary key generated for your domain

#### **Email Safety and End User Access**

1. The attachment section in the Gmail Safety settings page allows you to protect against malicious attachments. What actions can you perform on a suspicious attachment? (Choose 2)
2. Send to a designated user
3. Keep email in inbox and show warning
4. Move email to spam
5. Keep email in inbox without warning
6. What are valid reasons for allowing per-user outbound gateways in your organization? (Choose 2)
7. Mail delivery times are improved because messages bypass the Gmail servers
8. An outbound gateway can prevent the appearance of "on behalf of" addresses in the From field
9. Allows your users to send mail from their business and personal Gmail account from one inbox
10. An outbound gateway ensures that the same mail server delivers all messages from otherdomain and that server has a record that the mail has been sent
11. Google recommends against the use of the Image URL proxy whitelist?
12. True
13. False
14. You have enabled protection against anomalous attachment types in emails from the Gmail > Safety page but you are finding some emails with valid attachment types are not being delivered. How can you resolve this?
15. Ask each user to create a whitelist of allowable file types
16. Add a whitelist of allowable file types to the entry in the Attachments section on the Safety page
17. You cannot control what file types are considered anomalous so you must disable this protection to allow messages to be delivered
18. Have all messages that trigger this setting delivered to a quarantine and then release the messages manually

#### **Prevention of Spam, Phishing and Malware**

1. Messages from a single person that you trust are being marked as spam by Gmail. What approach is best to ensure that these messages reach the intended recipients inboxes?
2. Add the user's email address to your email whitelist
3. Ask each of your users to add the contact to their personal contacts
4. Add a spam setting which bypasses spam filters for messages received from addresses within an approved senders list. Add the user's email address to the list
5. Setup a security sandbox rule for the user to have all mail verified by the sandbox prior to delivery
6. Which of the following are reasons to use an inbound gateway? (Choose 2)
7. Can be used for batch delivery of email to Gmail
8. Spam filtering
9. Message archiving
10. Improves mail delivery performance
11. When malware is detected by the security sandbox, what action is taken?
12. The message is quarantined for further investigation
13. The message is deleted
14. The message is delivered to the recipient's spam folder
15. The message is delivered to the recipient's inbox with a warning
16. Your organization has been receiving unwanted emails from another organization and attempts by you to get the organization to stop sending the emails have failed. How can you stop messages from this organization from reaching your users?
17. Ask each of your user's to block the domain
18. Configure a blocked senders list and add the domain's IP address to the list
19. Configure a blocked senders list and add the domain name to the list
20. Contact Google Support and ask them to block the organization for you

#### **Compliance**

1. In which type of compliance control can you apply a Data Loss Prevention (DLP) rule for Gmail?
2. Attachment compliance
3. Objectionable content
4. Content compliance
5. Optical Character Recognition (OCR)
6. What actions can an administrator perform on a quarantined message? (Choose 2)
7. Deliver to another recipient
8. Allow
9. Return to sender
10. Deny
11. Which statements are true for an objectionable content rule? (Choose 2)
12. In an objectionable content setting you use a predefined list of objectionable words for filtering for objectionable content
13. In an objectionable content setting you create word lists for filtering for objectionable content
14. An objectionable content setting works on inbound messages only
15. An objectionable content setting works on inbound and outbound messages
16. You want to prevent your users from receiving mail from baddomain.com. What is the best way to achieve this?
17. Add baddomain.com to a blocked senders list
18. Configure the 'Restrict delivery' setting to prevent message exchange between your users and baddomain.com
19. Add baddomain.com's IP address to the blocked senders list
20. Create a security sandbox rule to filter and delete messages to/from baddomain.com

#### **Mail Routing**

1. Which mail delivery scheme allows messages to be delivered to multiple mailboxes?
2. Direct delivery
3. Split delivery
4. Dual delivery
5. Indirect delivery
6. Which features in G Suite can be used to leverage Google's spam protection for users who are on a non-Gmail mail platform? (Choose 2)
7. Outbound gateway
8. Alternate secure route
9. Non-Gmail mailbox
10. SMTP Relay service
11. What advantages does a routing setting have over an outbound gateway when you need to route mail through an external mail server?
12. A routing setting can be applied at an OU level
13. A routing setting can be applied to specific senders and recipients
14. Address lists can be used to control or bypass a routing setting
15. All of the above
16. What must you define before you can change the route in a routing setting?
17. A mail host
18. An outbound gateway
19. An SMTP relay
20. Alternate secure route