第4章 GWS邮件管理

练习1

略

DNS介绍

CNAME记录、TXT记录、MX记录、SPF、DKIM和DMARC 还有NS记录、A记录等。

Name/Host/Alias	Record Type	Priority	Value/Answer/Destination
Blank or @	A	NA	216.239.32.21
Blank or @	MX	1	ASPMX.L.GOOGLE.COM
Blank or @	MX	5	ALTI.ASPMX.L.GOOGLE.COM
Blank or @	MX	10	ASPMX3.GOOGLEMAIL.COM
mail	CNAME	NA	ghs.googlehosted.com.
Blank or @	TXT	NA	google-site-verification=6tTalLzrBX_Ks69jle8
www	CNAME	NA	ghs.googlehosted.com.

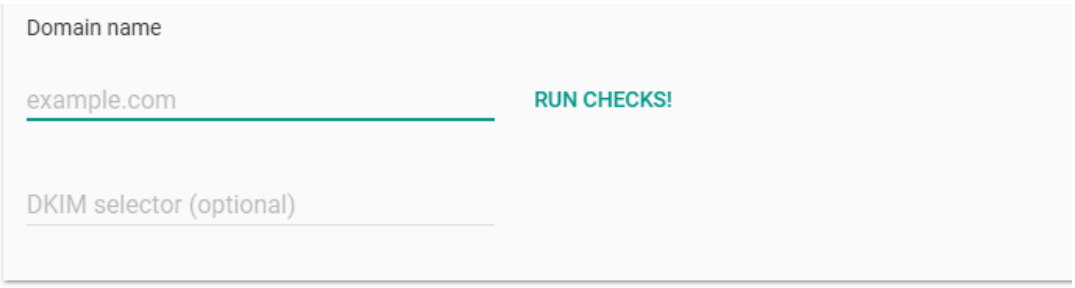
练习2

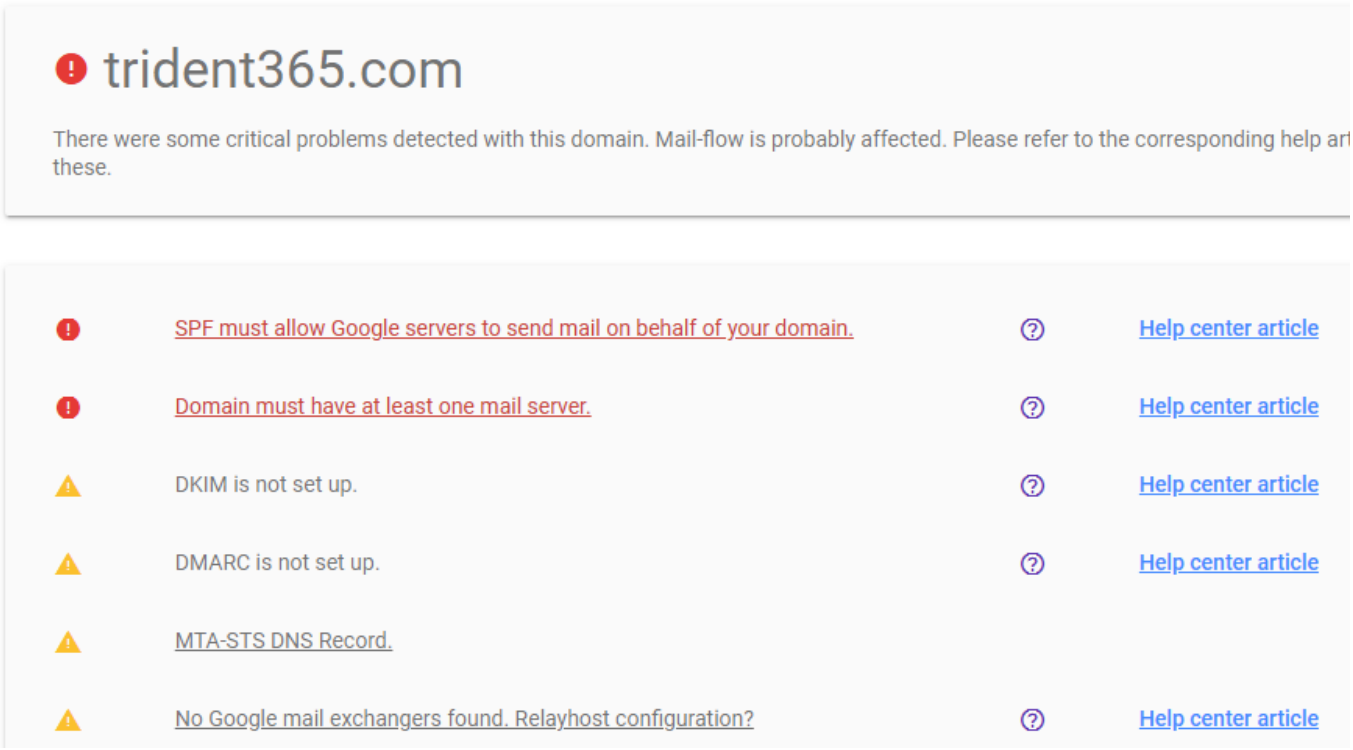
参考链接https://support.google.com/a/answer/140034

1.先要创建用户账号（应该是指邮箱）然后再将MX记录转到GWS上 2.TTL默认是3600，但正常使用Gmail后可以改为86400，这样更新频率会改为每天1次 3.如果是要把现行的邮箱系统转移到GWS上，可以保留现在的MX记录，但调低优先级（比如将优先级改为10+），当所有邮箱都经由Google后，再删除原MX记录，这样保证不会有邮件丢失

练习3

检查MX 工具URL为https://toolbox.googleapps.com/apps/checkmx/





点击报警会给出解决方法

测试1

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?

1. 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
2. **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**
3. Change your MX records in the admin console and reduce the Time to Live (TTL) value to one hour
4. Make the change in your DNS console and reduce the Time to Live (TTL) value to 1 hour

Which type of DNS record determines where mail destined for your domain is routed?

1. **MX Record**
2. TXT Record
3. NS Record
4. CNAME Record

In general, from where would you manage your domain's DNS records?

1. All of the options here
2. In your local DNS files
3. **In your domain registrar console**
4. In the Google Workspace admin console

What are common uses for a DNS TXT record when using Google Workspace? (Choose 2)

1. Customise a Google service address
2. Control inbound mail to your domain
3. **Domain verification**
4. **Email security records**

邮件安全

3招SPFDKIM和DMARC SPF: verify the domain you own DKIM: prevent email spoofing on outbound message by adding an encrypted header DMARC: tell email servers how to handle messages that fail SPF/DKIM checks

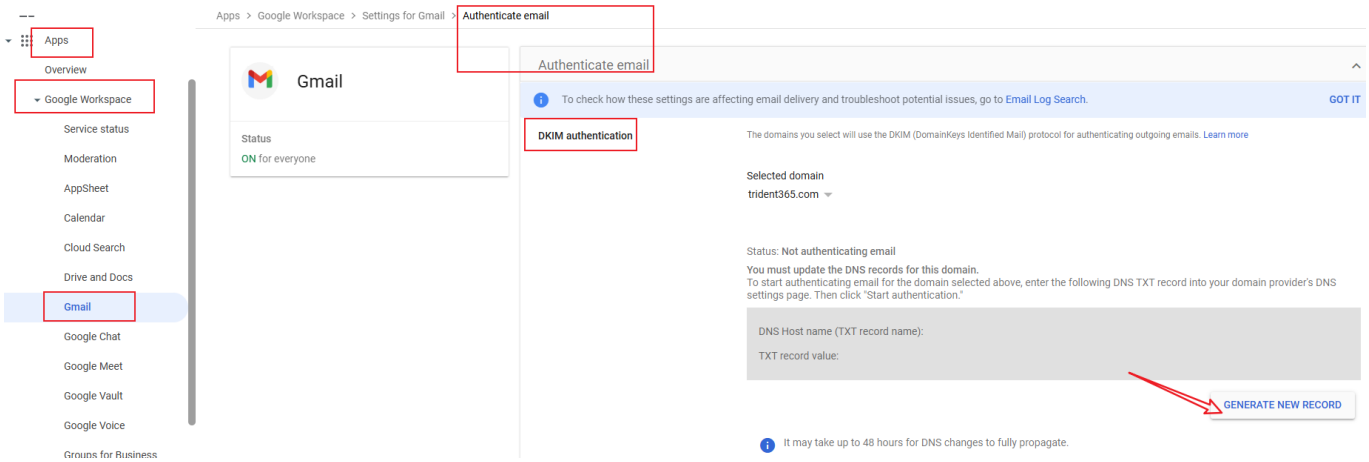
练习1

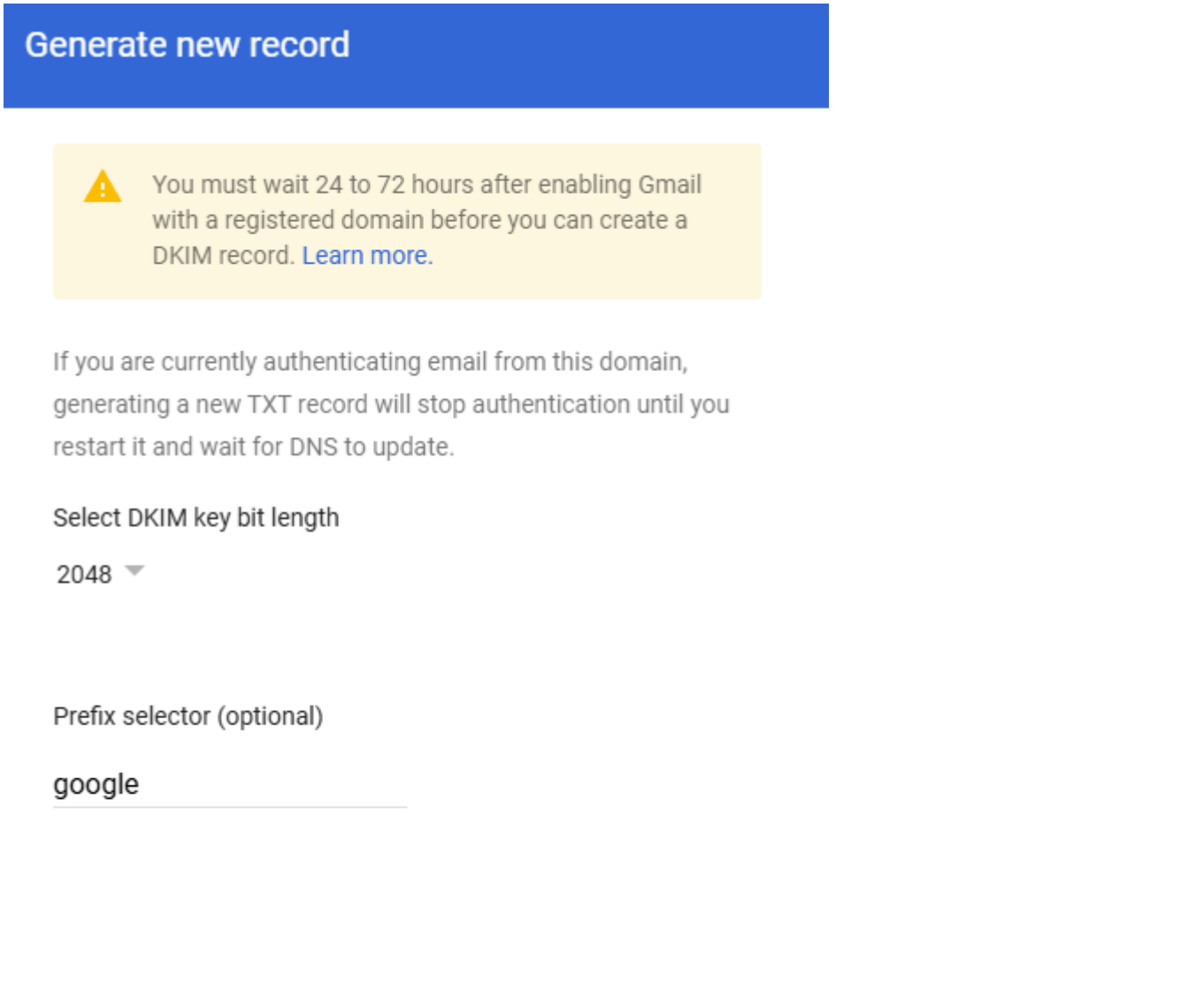
SPF通过添加TXT记录到DNS中 Xserver中已经有一条记录了，现在在后面追加

```
include:_spf.google.com ~all
```

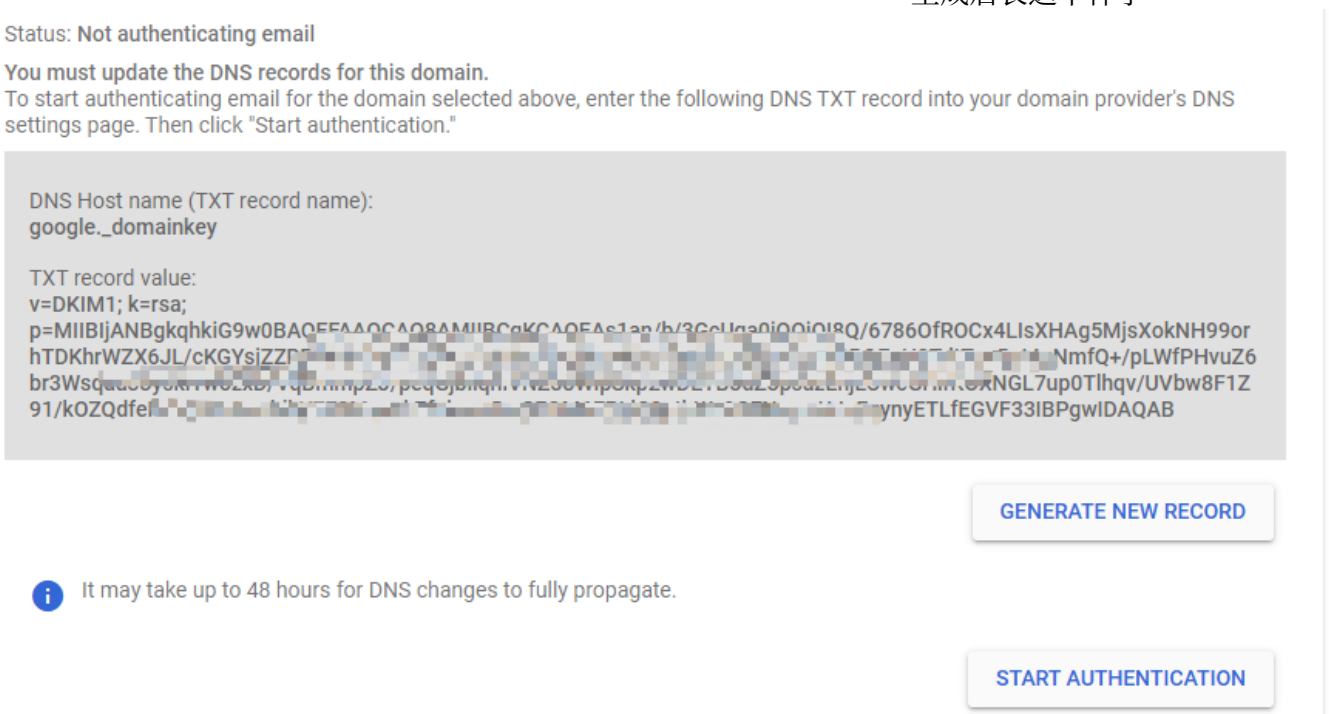
记录生效需要24小时左右 参考链接：https://support.google.com/a/answer/33786#zippy=%2Cspf-%E8%AE%B0%E5%BD%95%E7%A4%BA%E4%BE%8B

练习2



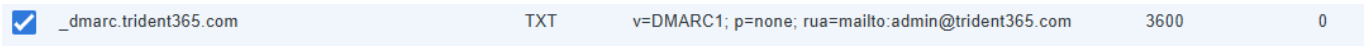


生成后长这个样子



生成的记录在Xserver的DNS DKIM记录中已经有了，一模一样。 参考链接：
https://support.google.com/a/answer/174124

练习3



这条TXT记录告诉收件邮箱服务器，如果判定Fail□如何操作，这里是通知管理员。

测试2

What is the main purpose of a Sender Policy Framework (SPF) record?

1. **It specifies which servers/domains can send messages on your behalf**
2. It can be used to verify that message content is authentic and has not changed
3. It defines the action to take on suspicious incoming messages

You have been asked to implement DomainKeys Identified Mail (DKIM) for your organization. How would you do this?

1. Enable DKIM from Apps > Google Workspace > Gmail > Authenticate email
2. Enable DKIM directly in your DNS records
3. Generate a key from your DNS records and add it to the Google Workspace admin console. Then Enable DKIM from Apps > Google Workspace > Gmail > Authenticate email
4. **Generate a DKIM record from Apps > Google Workspace > Gmail > Authenticate email. Add the record to your DNS records and then start authentication from the admin console**

What policy defines what to do if an incoming message is not authenticated?

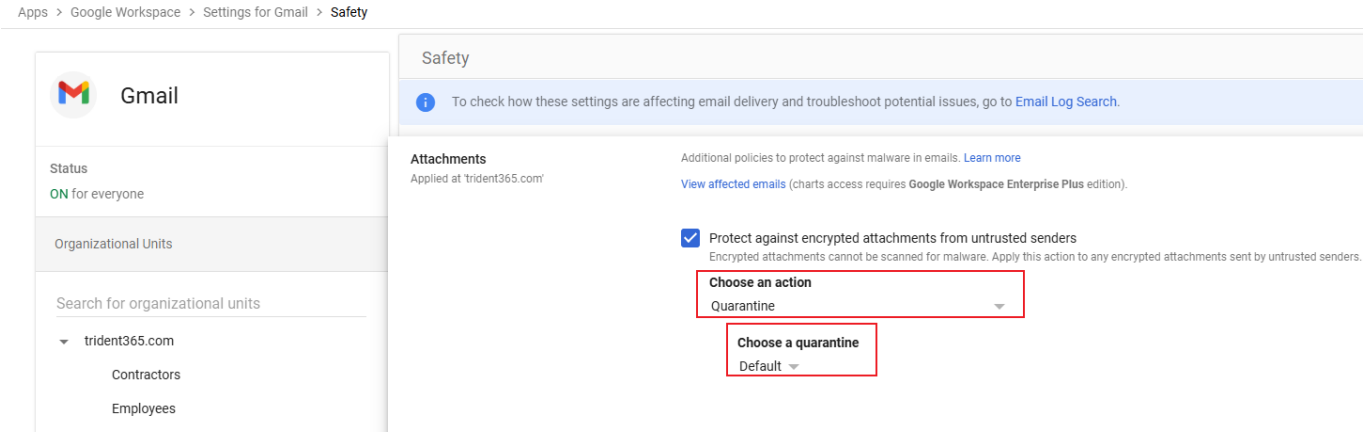
1. SPF
2. DKIM
3. All of the options here
4. **DMARC**

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?

1. Gmail signs all outgoing messages with a temporary key generated for your domain
2. **Gmail signs all outgoing messages with this default DKIM domain key d=*.gappssmtp.com**
3. Gmail signs all outgoing messages with a key generated using the From address in the message
4. Messages are sent as normal with no additional headers

邮件安全配置

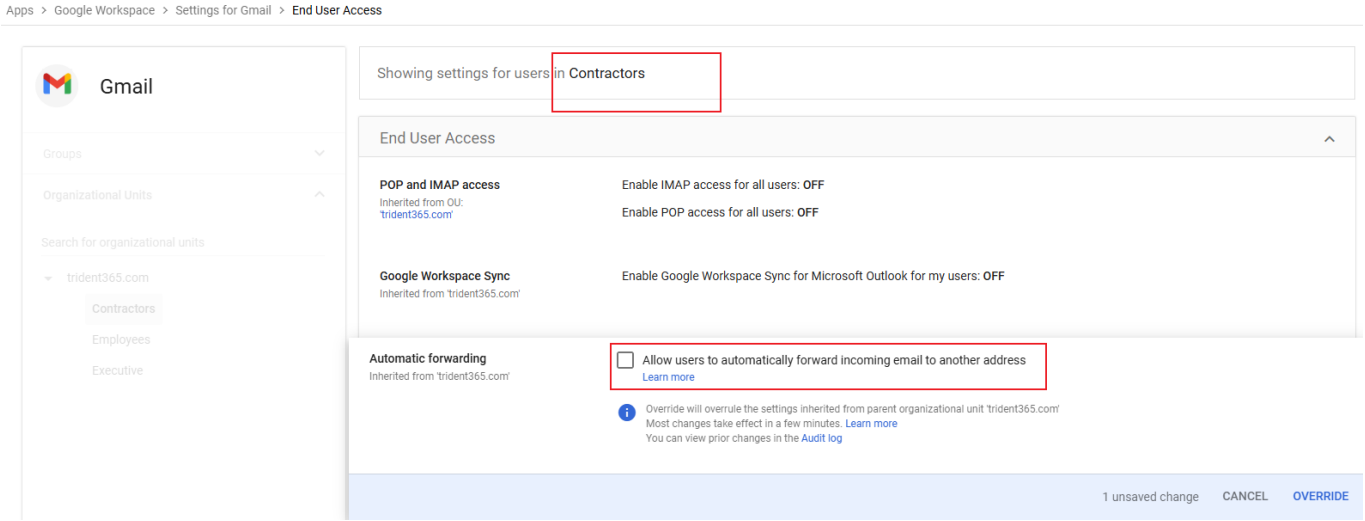
对于未受信任的发件人的加密附件，处理方式是隔离。



既便你把某一个域加为安全，但这里的设定仍然会生效。各自相互独立

练习2

对于外包人员，禁止他们的自动转发邮件到个人邮箱，并且禁止POP和IMAP但那些开户GWS Sync的人例外。



现在Rules也会终止工作

测试3

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)

1. Keep email in inbox without warning
2. **Move email to spam**
3. Send to a designated user
4. **Keep email in inbox and show warning**

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?

1. Ask each user to create an allowlist of allowable file types
2. **Add an allowlist of allowable file types to the entry in the Attachments section on the Safety page**
3. Have all messages that trigger this setting delivered to a quarantine and then release the messages manually
4. You cannot control what file types are considered anomalous so you must disable this protection to allow messages to be delivered

What are valid reasons for allowing per-user outbound gateways in your organization? (Choose 2)

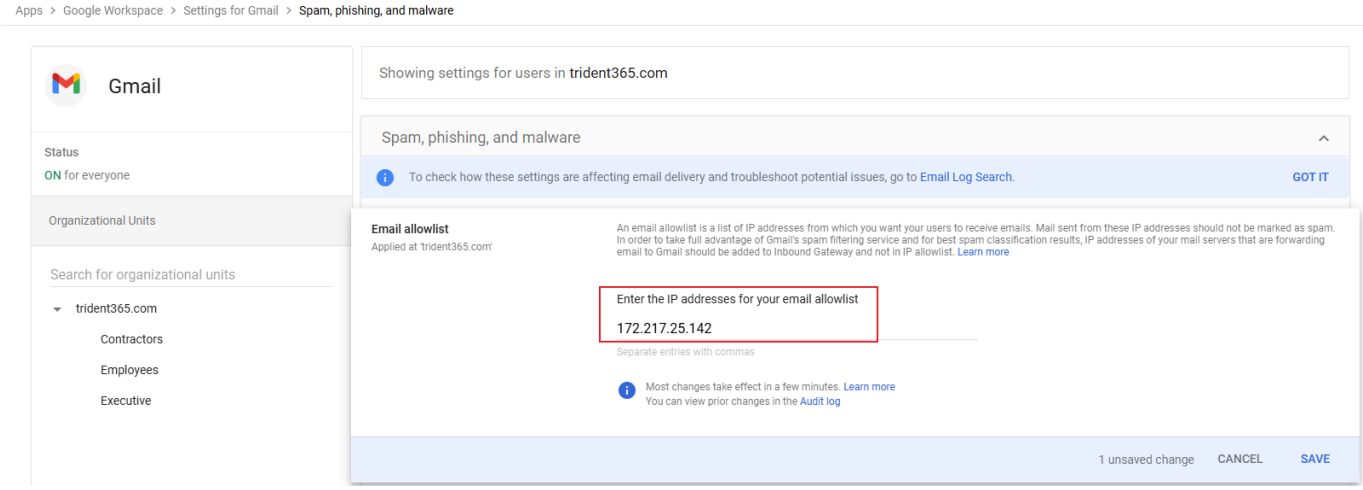
1. **An outbound gateway ensures that the same mail server delivers all messages from otherdomain and that server has a record that the mail has been sent**
2. Mail delivery times are improved because messages bypass the Gmail servers
3. **An outbound gateway can prevent the appearance of “on behalf of” addresses in the From field**
4. Allows your users to send mail from their business and personal Gmail account from one inbox

Google recommends against the use of the Image URL proxy allowlist?

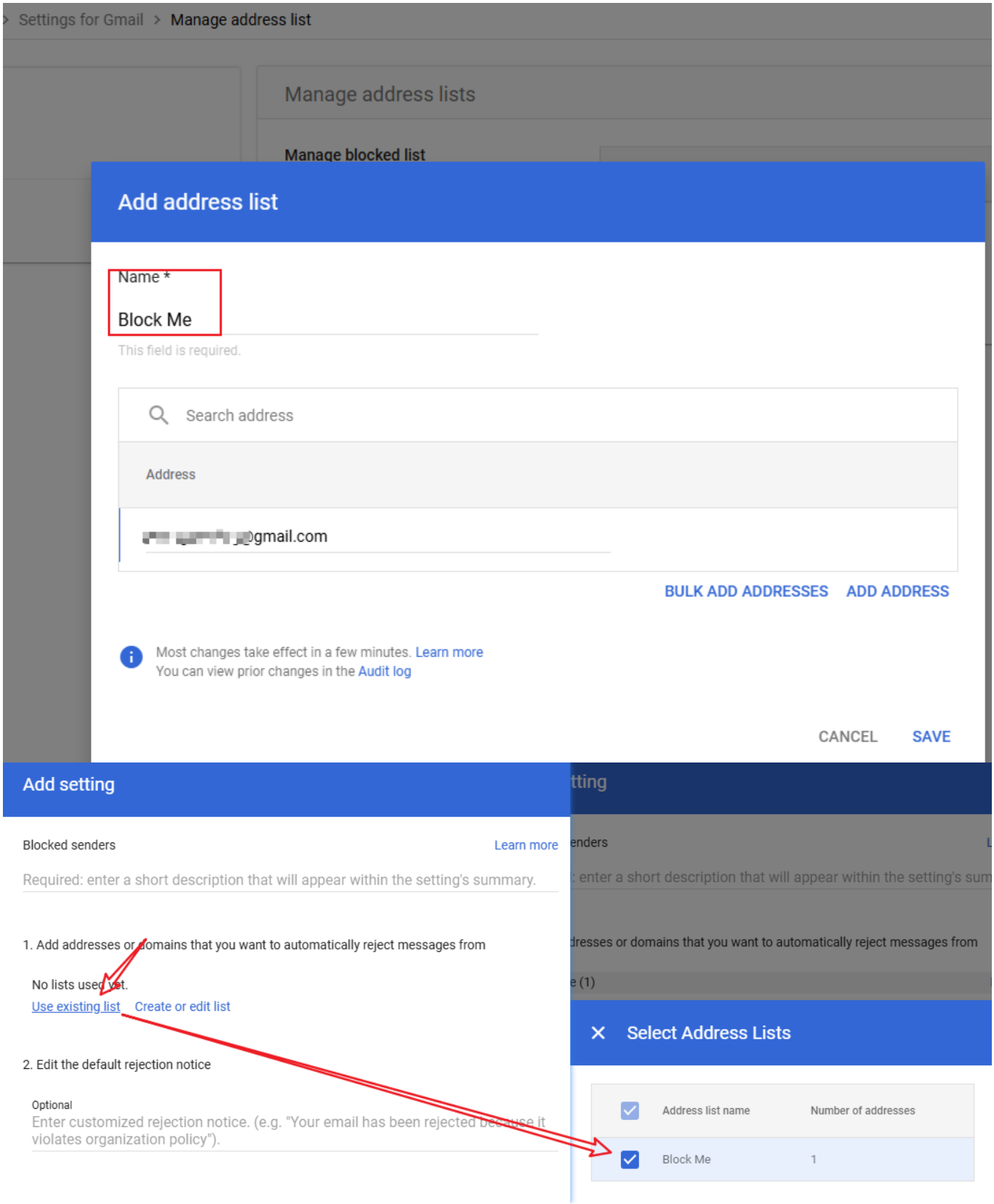
1. **True**
2. False

练习1

添加一个信任IP地址，虽然是信任，但如果从它发出来可疑邮件，仍然会被放入垃圾邮箱



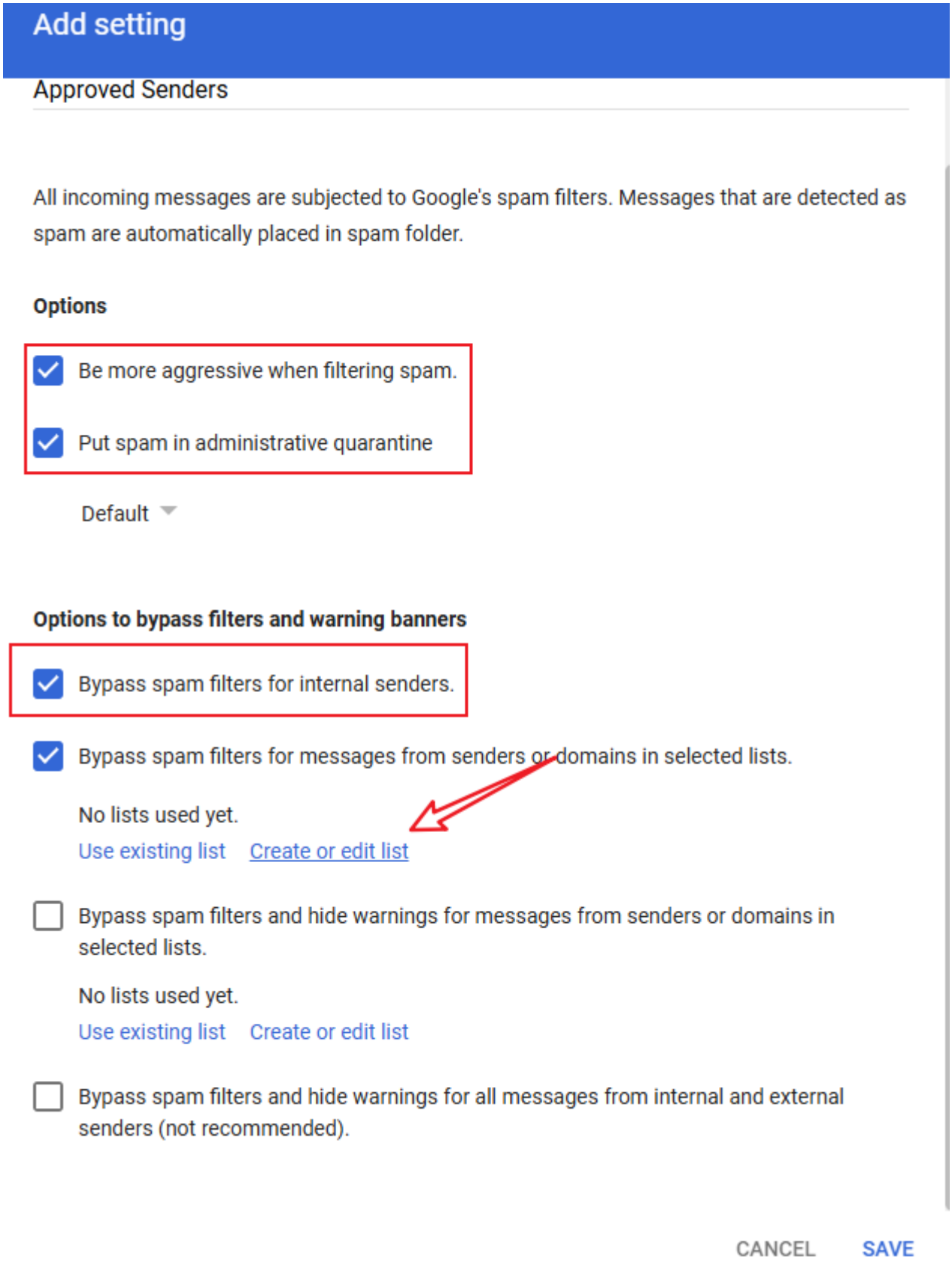
从自己的邮箱发一封邮件给GWS管理员邮箱。 在Console中添加黑名单

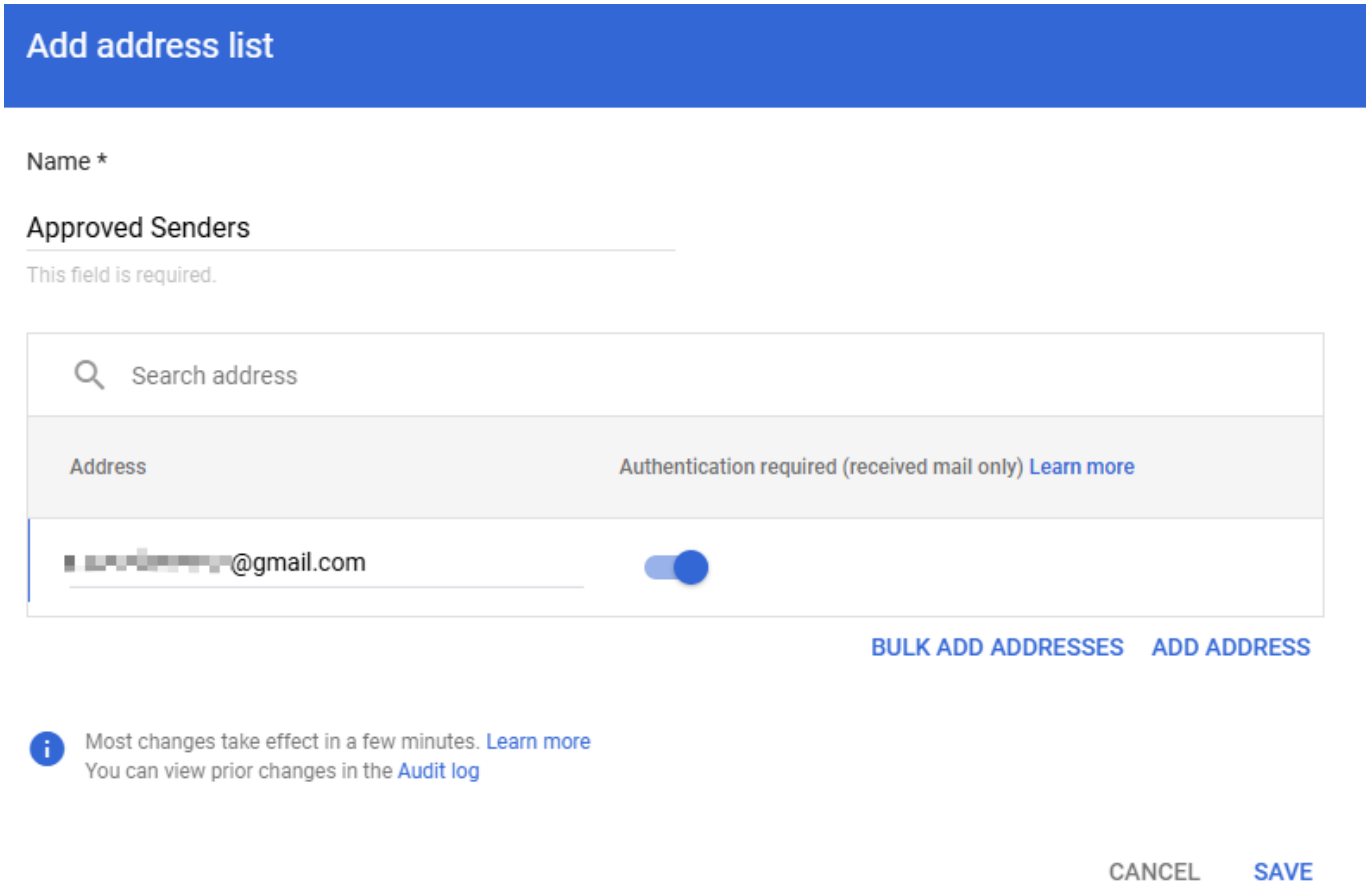


参考链接：https://support.google.com/a/answer/2364632?hl=zh-Hans&sjid=16549908282098203174-AP

练习2

创建白名单 Gmail>Spam,Phishing and Malware>Spam


Add setting
Approved Senders
All incoming messages are subjected to Google's spam filters. Messages that are detected as spam are automatically placed in spam folder.
Options
Be more aggressive when filtering spam.
Put spam in administrative quarantine
Default
Options to bypass filters and warning banners
Bypass spam filters for internal senders.
Bypass spam filters for messages from senders or domains in selected lists.
No lists used yet.
Use existing list
Create or edit list
Bypass spam filters and hide warnings for messages from senders or domains in selected lists.
No lists used yet.
Use existing list
Create or edit list
Bypass spam filters and hide warnings for all messages from internal and external senders (not recommended).
CANCEL
SAVE



虽然添加了白名单，但仍然要做验证，即Sender authentication保护，所以不要关闭它

除了增加SpamFilter另一个措施是使用预Scan

参考链接：https://support.google.com/a/answer/7380368

测试4

Which of the following are reasons to use an inbound gateway? (Choose 2)

1. Can be used for batch delivery of email to Gmail
2. Improves mail delivery performance
3. **Spam filtering**
4. **Message archiving**

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. What approach is best to stop messages from this organization from reaching your users?

1. Configure a blocked senders list and add the domain's IP address to the list
2. Ask each of your user's to block the domain
3. **Configure a blocked senders list and add the domain name to the list**
4. Contact Google Support and ask them to block the organization for you

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?

1. Setup a security sandbox rule for the user to have all mail verified by the sandbox prior to delivery
2. **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**
3. Ask each of your users to add the contact to their personal contacts
4. Add the user's email address to your email allowlist

邮件合规检查

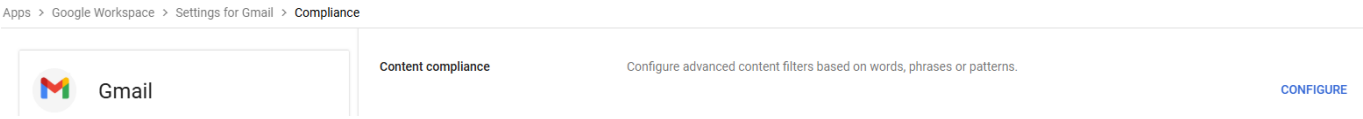
1. Attachment compliance
2. Content compliance
3. objectionable content compliance

触发后的动作

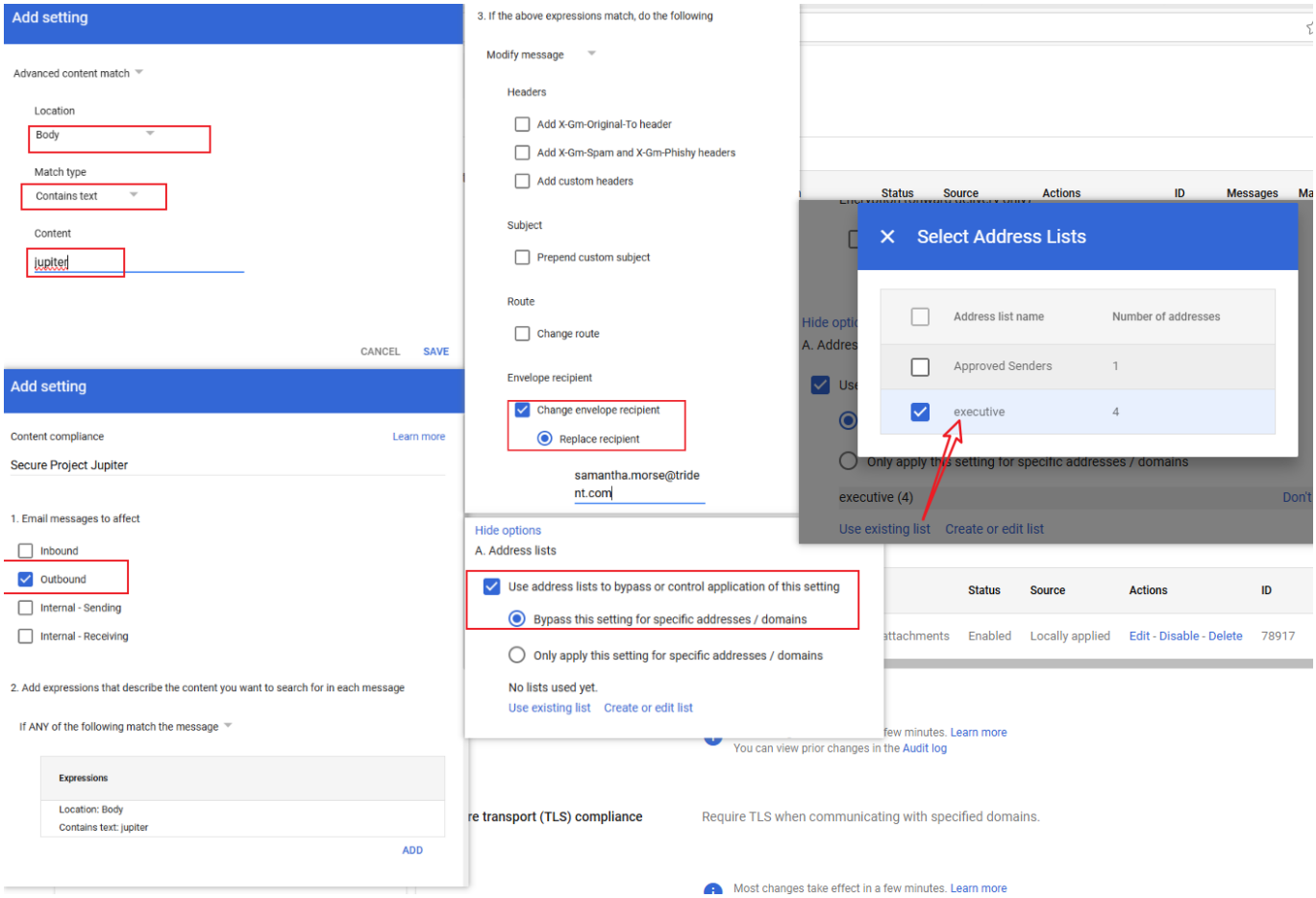
1. rejected before reaches the recipient
2. be sent to admin
3. be modified before delivery

DLP对策

练习1

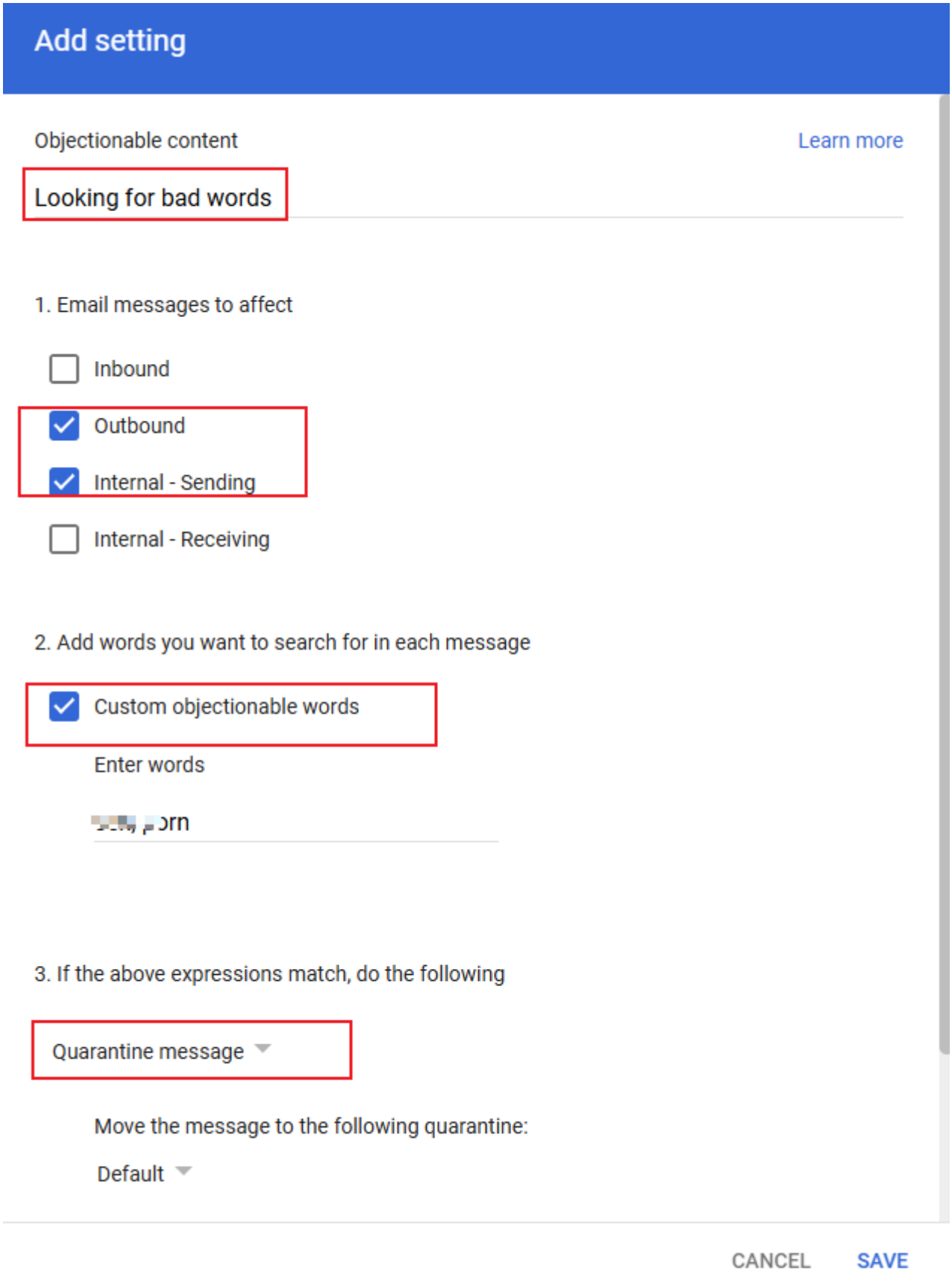


练习2

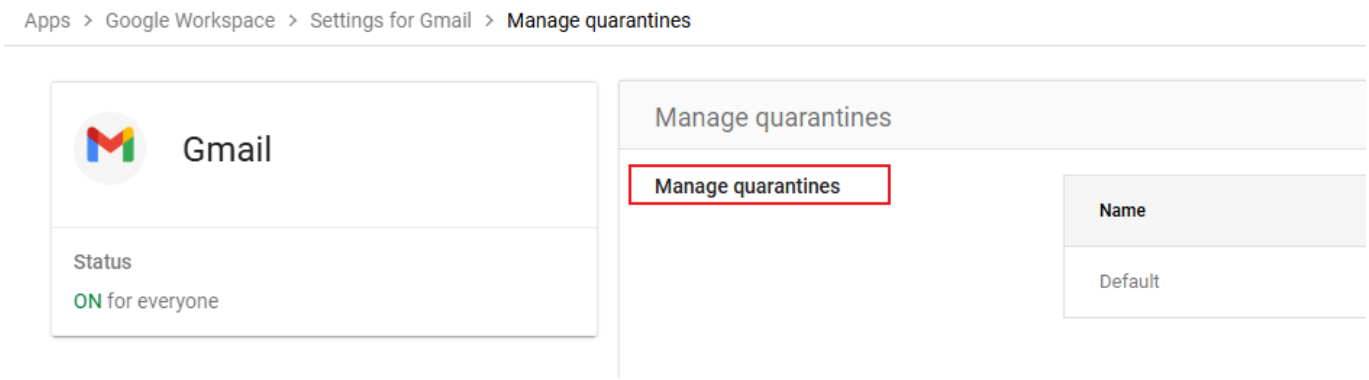


然后发一封包含Jupiter□在标题或是正文）的邮件到自己个人邮箱，发现是收不到的。

练习3



发送违规邮件，然后查看隔离邮件（使用管理员账号）



也可以访问下列URL https://email-quarantine.google.com/adminreview

管理员需要定期处理隔离邮件，如果30天内不处理，会被自动删除

其他合规对策

1. email and chat auto-deletion 删除超过某一时间的信息
2. OCR for email attachment (并不是所有GWS版本都支持)
3. restrict delivery (一般用于教育账号)
4. Security sandbox (微软家的EDR也有这个功能)

测试5

You want to prevent your users from receiving mail from baddomain.com. What is the best way to achieve this?

1. **Add baddomain.com to a blocked senders list**
2. Add baddomain.com's IP address to the blocked senders list
3. 1Create a security sandbox rule to filter and delete messages to/from baddomain.com
4. Configure the 'Restrict delivery' setting to prevent message exchange between your users and baddomain.com

What actions can an administrator perform on a quarantined message? (Choose 2)

1. **Deny**
2. **Allow**
3. Return to sender
4. Deliver to another recipient

In which type of compliance control can you apply a Data Loss Prevention (DLP) rule for Gmail?

1. Objectionable content
2. **Content compliance**
3. Optical Character Recognition (OCR)
4. Attachment compliance

Which statements are true for an objectionable content rule? (Choose 2)

1. **An objectionable content setting works on inbound and outbound messages**
2. In an objectionable content setting you use a predefined list of objectionable words for filtering for objectionable content
3. An objectionable content setting works on inbound messages only
4. **In an objectionable content setting you create word lists for filtering for objectionable content**