配置安全邮件网关以使用Microsoft隔离和Microsoft隔离通知

目录

简介

本文档介绍将思科安全邮件(CES)与Microsoft 365隔离集成所需的配置步骤。

概述

在现代邮件基础设施中，通常实施多个安全层，导致邮件被不同系统隔离。为了简化用户体验并提高通知一致性，将隔离管理集中到单一平台中是很有益的。本指南说明如何将Cisco CES识别的不需要的邮件（如垃圾邮件和灰色邮件）重定向到Microsoft 365用户隔离区。

先决条件

要完成此配置，请确保您具有以下配置：

1. 思科安全邮件网关中的活动租户
2. Microsoft Exchange online中的活动租户。
3. 访问Microsoft 365(O365)服务
4. Microsoft 365 Defender许可证（配置隔离策略和通知时需要）

配置Microsoft 365(O 365)

首先设置Microsoft 365以接收和管理隔离的邮件。

在Microsoft Exchange Online中启用隔离通知

您可以参阅官方Microsoft文档来配置隔离邮件的用户通知：
[Microsoft隔离通知配置]

创建邮件流规则

通知处于活动状态后，请配置一条规则，将思科安全邮件网关标记的邮件重定向到Microsoft的托管隔离区。

1. 打开Microsoft Exchange管理中心。
2. 从左侧菜单中，转到Mail Flow → Rules。
3. 单击Add a rule，然后选择Create a new rule。
4. 将规则名称设置为：CSE隔离规则。
5. 在Apply this rule if下，选择The message header，然后选择matches text patterns。
6. 在报头名称中，输入：X-CSE-Quarantine，并将值设置为匹配：对。
7. 在Do the following下，选择Redirect the message to，然后选择Hosted Quarantine。
8. 保存配置。
9. 保存后，确保规则已启用。

在图片中，您可以看到规则的外观。

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Enabled

Updating the rule status, please wait...

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Microsoft规则

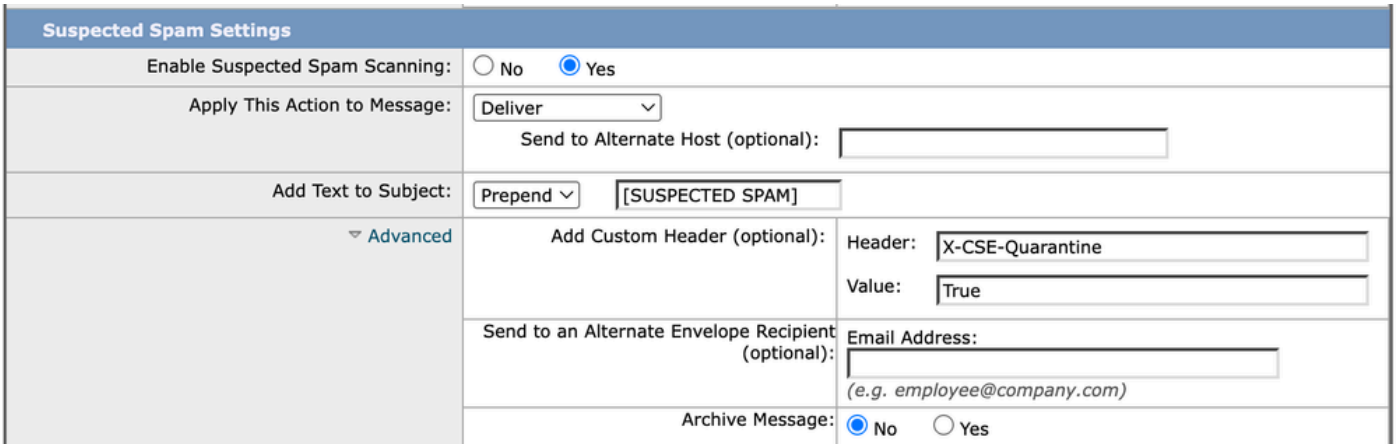
配置思科安全邮件

在Cisco CES中，您可以添加自定义信头(X-CSE-Quarantine:true)指向要重定向到Microsoft隔离区的任何邮件。

CES中的任何内容过滤器或引擎都可以标记这些邮件。在本例中，我们将其配置为可疑垃圾邮件。

1. 打开Cisco Secure Email Management Console。
2. 转到Mail Policies → Incoming Mail Policies。
3. 编辑要修改的策略(例如，选择默认策略)。
4. 点击所选策略的垃圾邮件设置。
5. 在Suspect Spam下，将操作从Quarantine更改为Deliver。
6. 单击Advanced并添加自定义信头：
    - 报头名称:X-CSE-Quarantine
    - 值：true（与Microsoft规则中使用的值相同）
7. 单击Submit，然后单击Commit Changes以应用配置。

在图片中，您可以看到配置的外观。

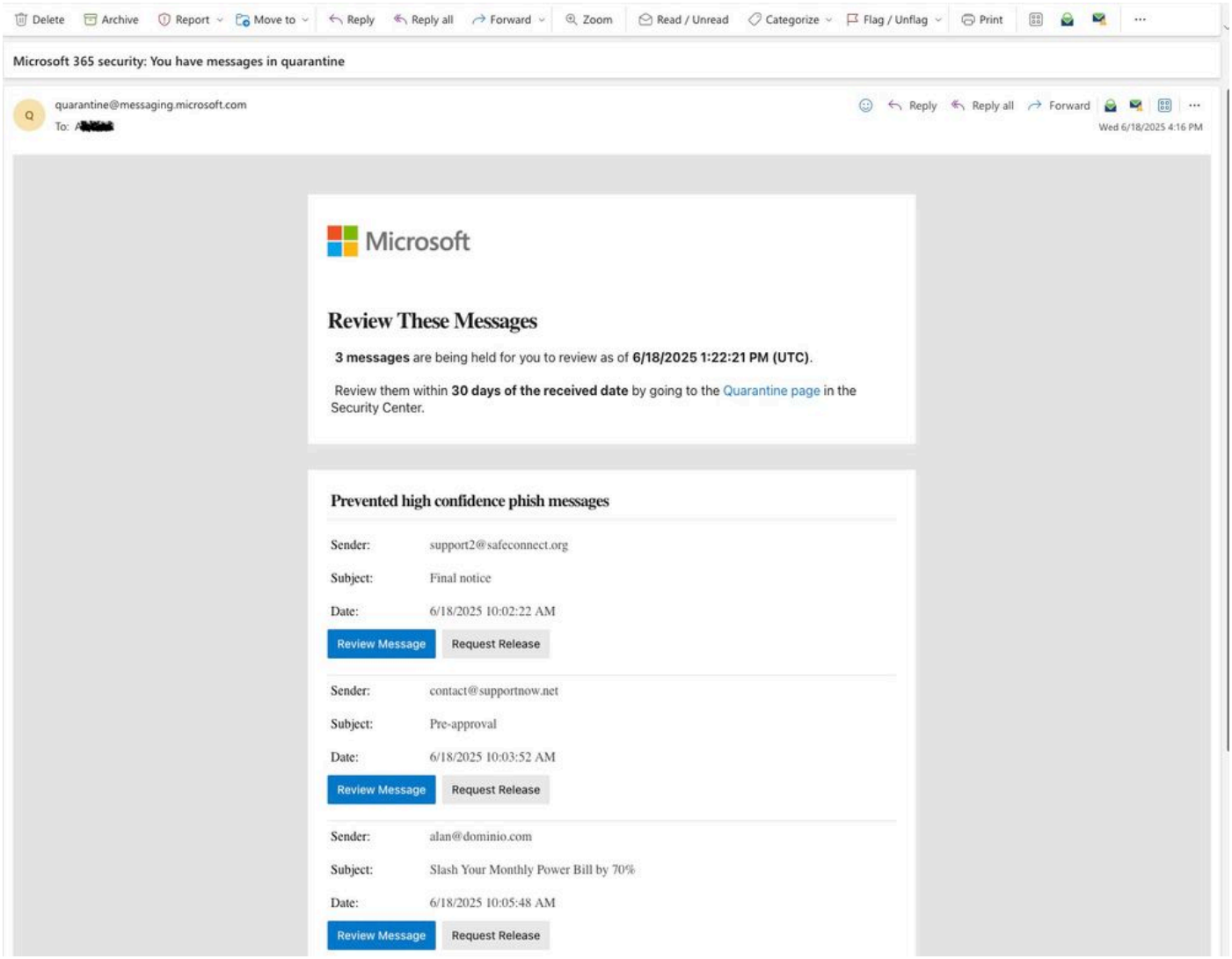


CES配置

验证

从此以后，思科CES识别为潜在垃圾邮件的电子邮件将使用自定义信头进行标记。Microsoft 365检测到此标记并将邮件重定向到用户隔离区。

用户将¡根据Microsoft 365配置接收隔离通知。


Delete
Archive
Report
Move to
Reply
Reply all
Forward
Zoom
Read / Unread
Categorize
Flag / Unflag
Print
Microsoft 365 security: You have messages in quarantine
quarantine@messaging.microsoft.com
To: A[redacted]
Reply
Reply all
Forward
Wed 6/18/2025 4:16 PM
Microsoft
Review These Messages
3 messages are being held for you to review as of 6/18/2025 1:22:21 PM (UTC).
Review them within 30 days of the received date by going to the Quarantine page in the Security Center.
Prevented high confidence phish messages
Sender: support2@safeconnect.org
Subject: Final notice
Date: 6/18/2025 10:02:22 AM
Review Message
Request Release
Sender: contact@supportnow.net
Subject: Pre-approval
Date: 6/18/2025 10:03:52 AM
Review Message
Request Release
Sender: alan@dominio.com
Subject: Slash Your Monthly Power Bill by 70%
Date: 6/18/2025 10:05:48 AM
Review Message
Request Release

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。