为Microsoft 365隔离&；配置安全邮件网关通知

目录

简介

背景信息

先决条件

- 要求
- 使用的组件

配置Microsoft 365(O 365)

- 在Microsoft Exchange Online中启用隔离通知
- 创建邮件流规则

配置思科安全邮件

验证

故障排除

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。

背景信息

在现代邮件基础设施中，通常部署多个安全层，这可能导致邮件被不同的系统隔离。为了增强用户体验并维护一致的通知工作流程，建议将隔离区管理集中到单个平台中。
本指南概述了将Cisco CES检测到的垃圾邮件（如垃圾邮件和灰色邮件）重定向到Microsoft 365用户隔离区的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- CES网关中的活动租户
- Microsoft Exchange Online中的活动租户
- 访问Microsoft 365(O365)服务
- Microsoft 365 Defender许可证（配置隔离策略和通知时需要）

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

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

有多个配置选项用于控制如何将邮件定向到Microsoft 365隔离区。
如果目标是防止最终用户访问隔离邮件或接收隔离通知，可以通过实施将邮件直接重定向到隔离的邮件流（传输）规则来实现此目的。

相反，如果要求最终用户接收隔离通知并能够放行邮件，则必须相应地调整规则配置。在这种情况下，垃圾邮件可信度(SCL)值必须设置为9，该值将邮件指定为高可信度垃圾邮件，并启用用户通知和释放功能。

这些配置在Microsoft的官方文档中有详细说明；Microsoft隔离通知配置。

本示例说明了允许最终用户接收隔离通知和放行邮件的配置。

创建邮件流规则

通知处于活动状态后，请配置一条规则，将由CES网关标记的邮件重定向到Microsoft托管的隔离区。

1. 打开Microsoft Exchange管理中心。
2. 从左侧菜单中，导航到邮件流>规则。
3. 单击Add a rule，然后选择Create a new rule。
4. 将规则名称设置为CSE Quarantine Rule。
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true。
7. 在Do the following下，选择Modify the message properties,Set the spam confidence Level，然后选择9。
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: Enabled

Enable or disable rule

Enabled

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

Set the spam confidence level (SCL) to '9'

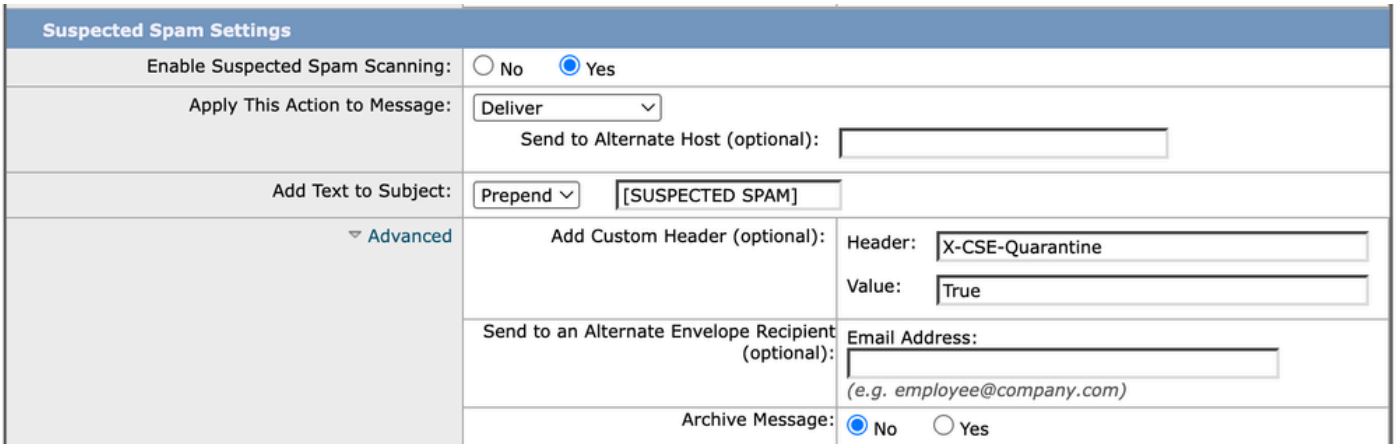
Rule comments

配置思科安全邮件

在思科CES中，自定义信头(X-CSE-Quarantine:true)可以添加到必须重定向到Microsoft隔离区的任何邮件中。CES中的任何内容过滤器或引擎都可以标记这些邮件。在本示例中，它配置为可疑垃圾邮件。

1. 打开Cisco Secure Email Management Console。
2. 导航到邮件策略>传入邮件策略。
3. 编辑要修改的策略(例如，选择Default Policy)。
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：
    - 信头名称：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。

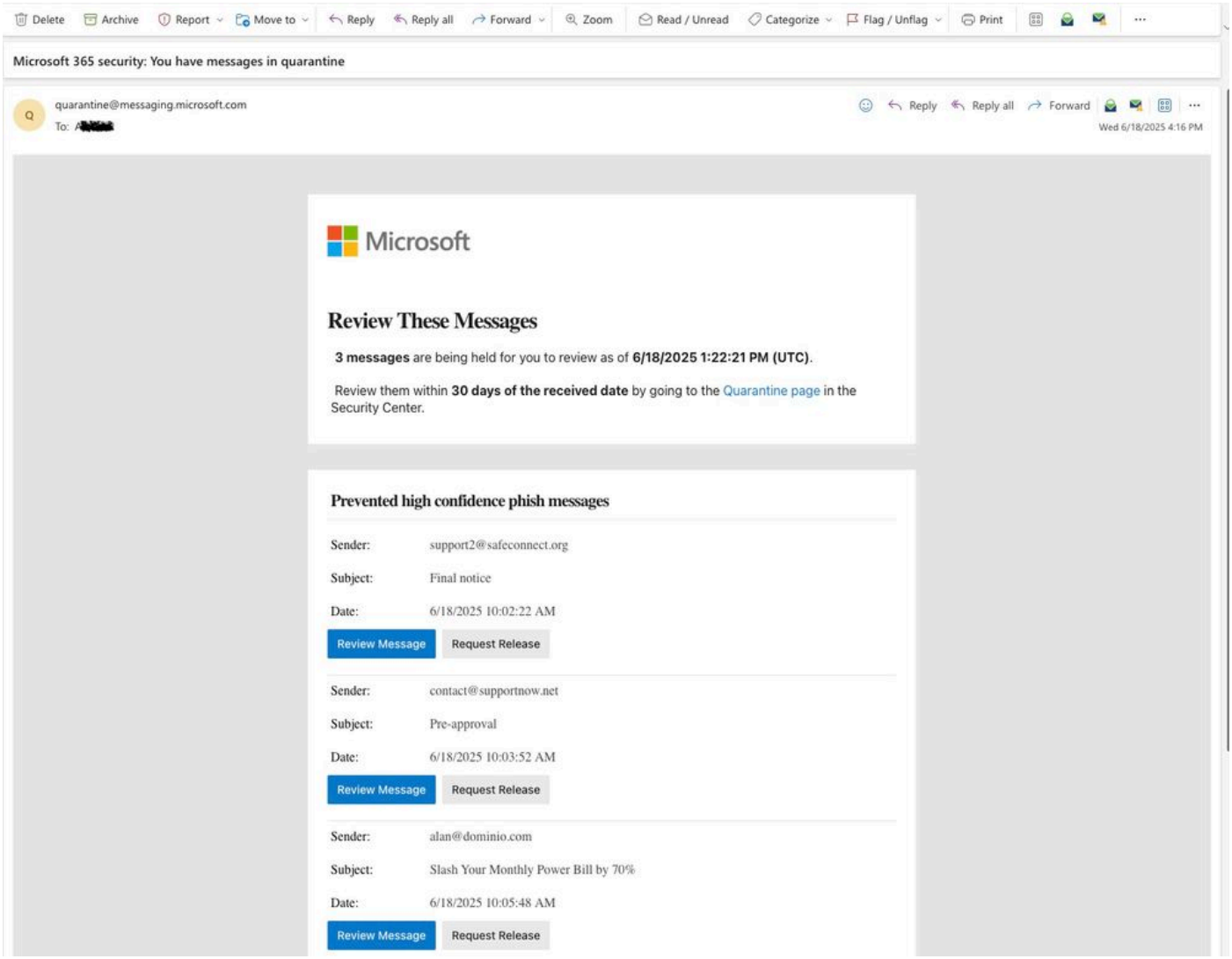


CES配置

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Microsoft隔离区。

用户将根据Microsoft 365配置接收隔离通知。

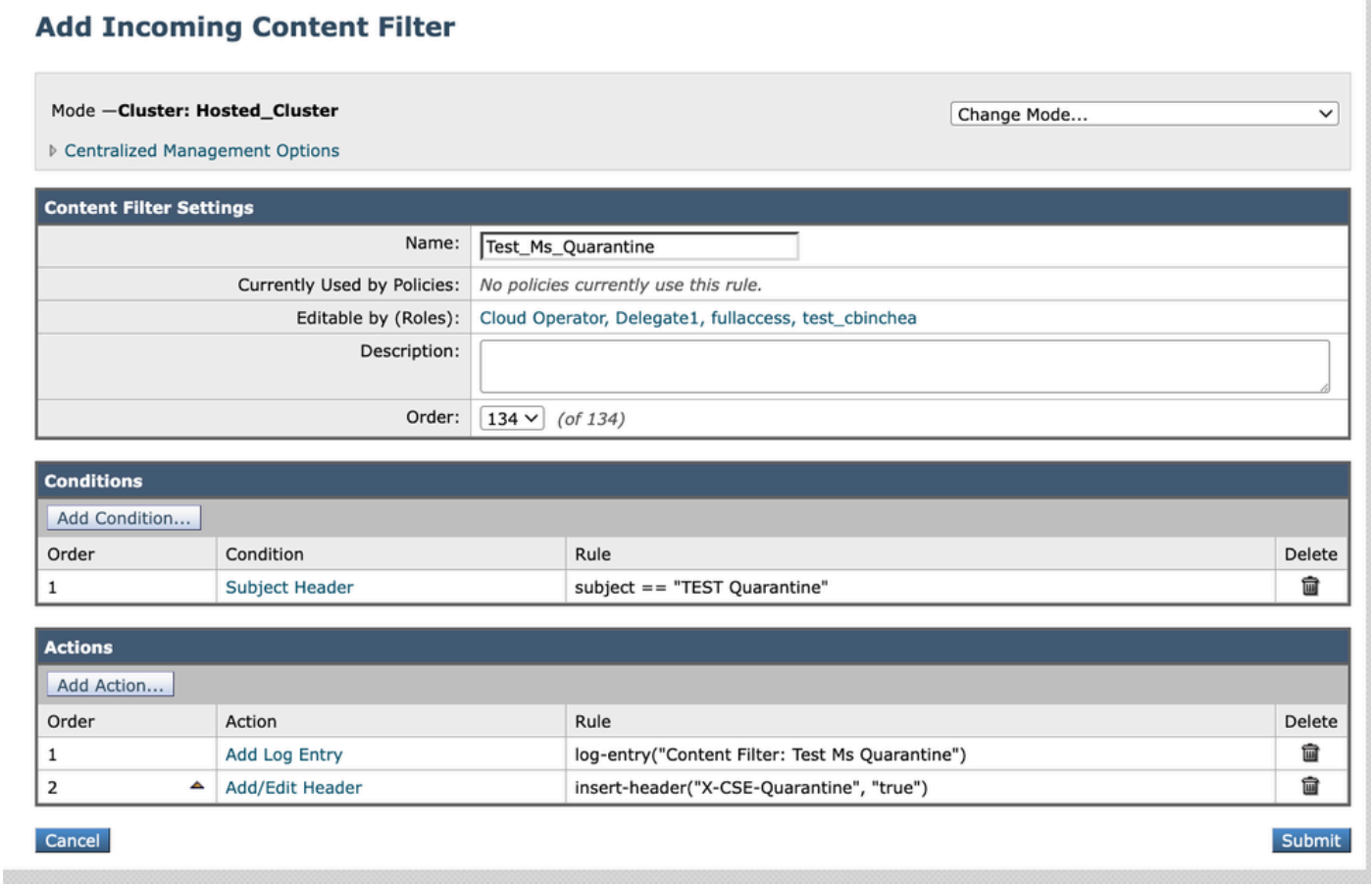


故障排除

为了验证配置的有效性并确认Microsoft将邮件路由到预期隔离区，可以创建传入内容过滤器，以便在邮件主题与特定关键字或模式匹配时插入相同的信头。

通过实施此过滤器，安全邮件网关(SEG)会附加指定的报头，从而允许Microsoft 365根据标准反垃圾邮件逻辑处理邮件 — 有效复制在报头由本地垃圾邮件过滤引擎注入时可能发生的行为。

以下是内容过滤器的示例：


Add Incoming Content Filter
Mode —Cluster: Hosted_Cluster
Change Mode...
Centralized Management Options
Content Filter Settings
Name:
Test_Ms_Quarantine
Currently Used by Policies:
No policies currently use this rule.
Editable by (Roles):
Cloud Operator, Delegate1, fullaccess, test_cbinchea
Description:
Order:
134
(of 134)
Conditions
Add Condition...
Order
Condition
Rule
Delete
1
Subject Header
subject == "TEST Quarantine"
Actions
Add Action...
Order
Action
Rule
Delete
1
Add Log Entry
log-entry("Content Filter: Test Ms Quarantine")
2
Add/Edit Header
insert-header("X-CSE-Quarantine", "true")
Cancel
Submit

内容过滤器测试

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）。