将思科电邮威胁防御(ETD)与思科安全访问集成的步骤：

目录

简介

本文档说明在ETD SMTP内联模式下将思科邮件威胁防御(ETD)与思科邮件DLP安全访问(SA)集成的步骤。这可确保在思科安全访问(SA)的帮助下扫描通过ETD的所有出站邮件以获取DLP。

概述

在当今的分布式工作环境中，电子邮件仍是企业的主要通信工具，因此也是网络攻击和数据泄露的最常见目标。为了应对这些不断演变的挑战，思科通过电邮威胁防御(ETD)和安全访问电邮数据丢失防御(DLP)提供全面的电邮安全方法。

通过将思科电邮威胁防御的威胁检测功能与安全访问电邮DLP的强大数据保护功能相结合，组织可以制定多层防御策略。这种方法不仅能保护来自外部参与者的收件箱，还能确保敏感的企业数据受到严格控制，无论用户位于何处，也不管用户以何种方式访问其电子邮件。

先决条件

访问下面的控制台。

1. 内联模式下的思科邮件威胁防御控制台(ETD)。

   ETD控制台用作您的邮件安全状态的集中管理平面。访问此控制台是配置环境防御高级威胁的第一步。

   - 为什么“内联模式”很重要：在内联模式下配置ETD时，它充当邮件传输代理(MTA)或位于邮件流路径中的直接集成。这样，系统可以在邮件发送到收件人的收件箱之前检查、阻止或修改邮件。
2. 思科安全访问控制台(SA)

思科安全访问是统一云交付的安全平台，将各种安全服务(包括防数据丢失(DLP))集成到单个聚合架构中。

- 为什么需要SA控制台：安全访问控制台是组织安全策略的协调中心。当ETD处理威胁特定邮件流时，您可以在安全访问控制台中定义更宽泛的DLP策略，以管理在整个企业中识别和处理敏感数据的方式。
- 控制台角色：此控制台允许管理员创建和应用数据分类规则（例如，识别PII、信用卡号或内部项目代码）。 通过访问SA控制台，您可以确保邮件DLP策略与整体安全策略同步，从而在两个邮件流量之间实现一致的实施。

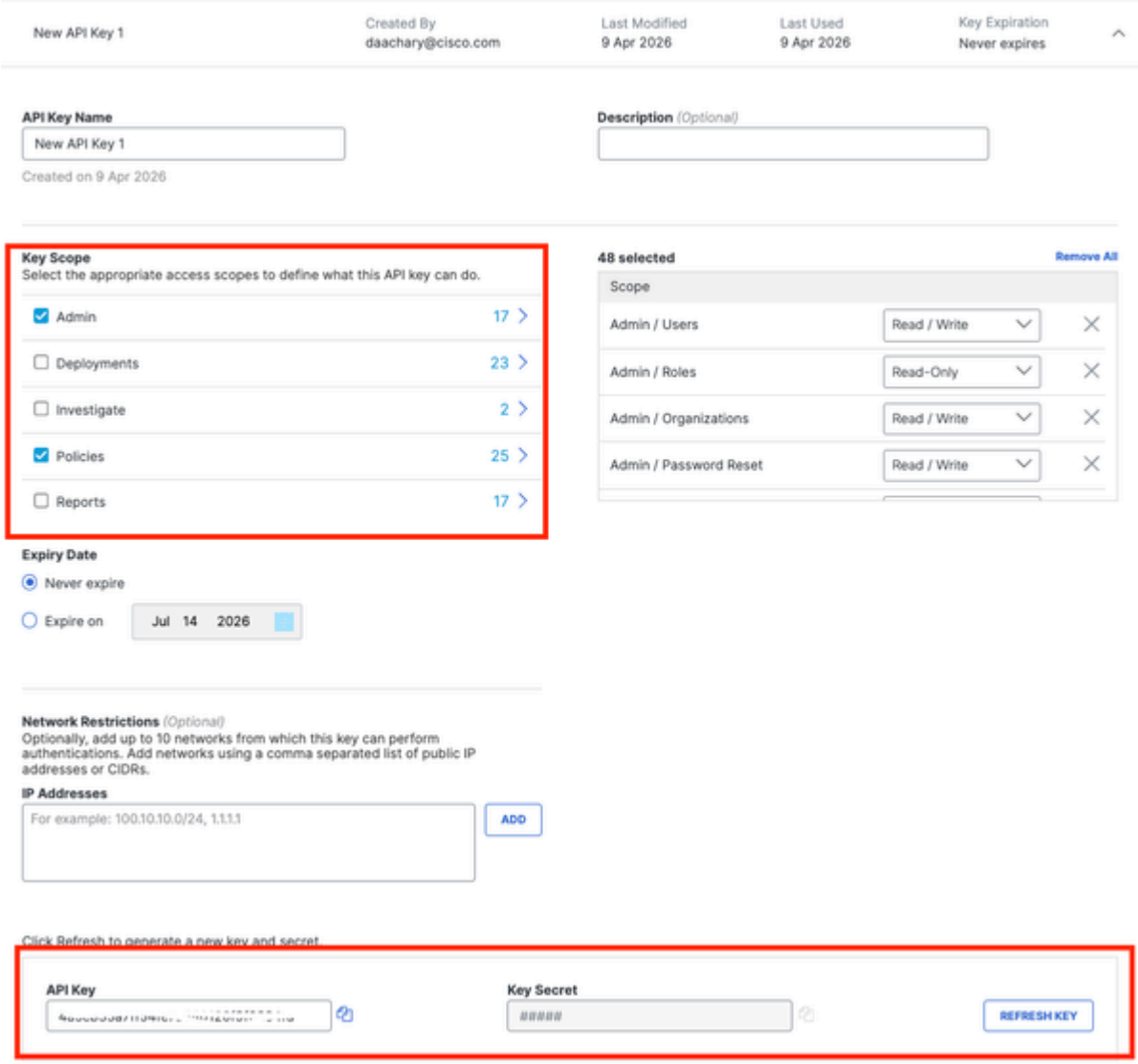
配置

集成步骤

步骤 1：在思科安全访问中生成API凭证

首先，您必须在Secure Access控制台内生成必要的API凭证以授权连接。

1. 登录到Cisco Secure Access控制面板。
2. 导航到Admin> API Keys。
3. 选择选项以创建新的API密钥。
4. 将以下范围分配给密钥:AdminandPolicy。
   - [屏幕截图:安全访问API密钥配置]



步骤 2：配置密钥过期

根据组织的安全策略定义API密钥的生命周期。

- 选项 1：永不过期 — 提供不间断服务，无需手动轮换。
- 选项 2：特定日期 — 设置定义的到期时间表。
  - 重要说明：如果选择设置到期日期，请确保计划轮换流程。必须在到期日期之前重新配置ETD控制台中的API密钥，以防止DLP服务中断。

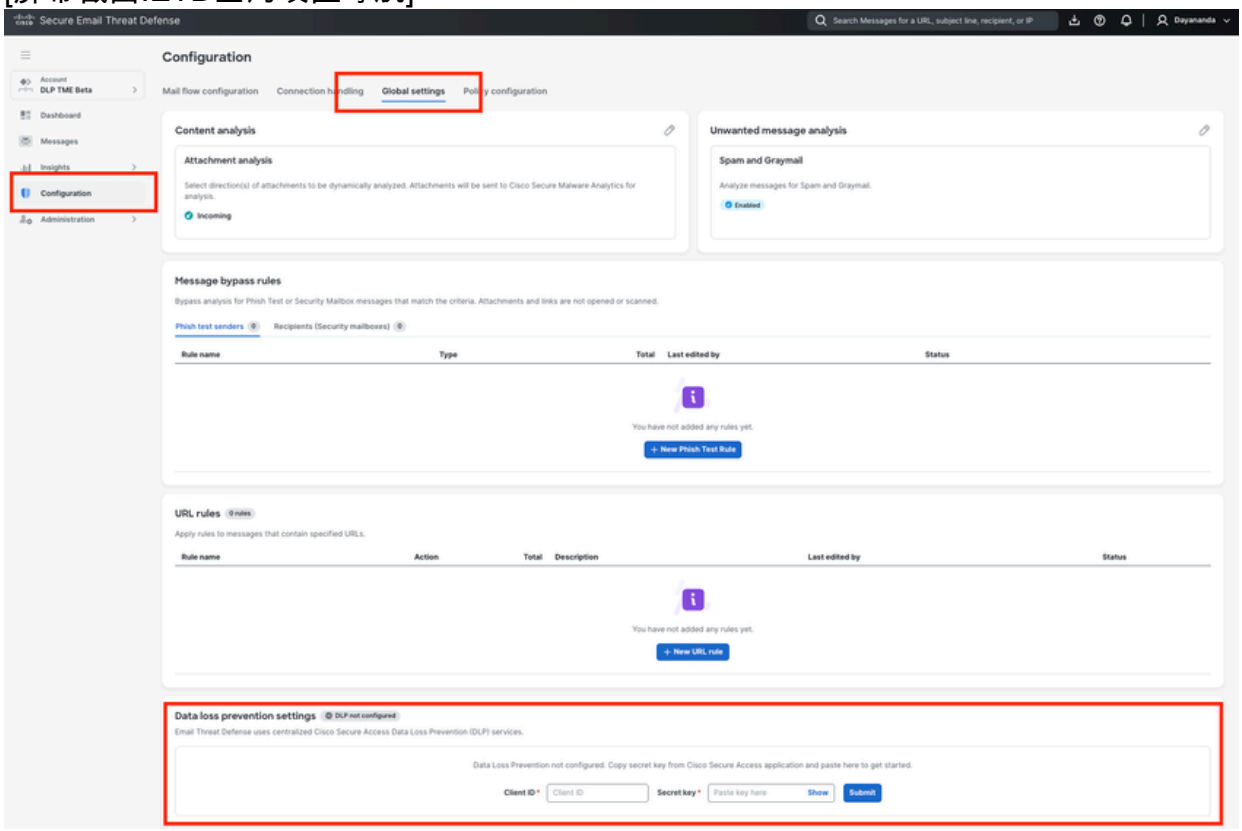
步骤 3：保护您的凭据

生成密钥后，系统将显示API密钥和密钥密钥。

- 操作：将这些凭证复制并存储在安全位置（例如密码管理器）中。
- 警告：导出此屏幕后，Key Secret将不可见。如果丢失，您需要生成新的密钥对。

步骤 4：访问ETD配置

在凭证安全的情况下，进入ETD控制台完成链接。

1. 登录到Cisco ETDconsole。
2. 导航到配置>全局设置。
   - [屏幕截图:ETD全局设置导航]
   - 

步骤 5：最终确定集成

通过输入从安全访问获得的凭证完成握手。

1. 在Global Settings菜单中，找到Data Loss Prevention(DLP)部分。
2. 输入步骤3中保存的Client ID(API Key)和Secret Key(Key Secret)。
3. 保存更改。

成功验证后，思科ETD与思科安全访问之间的集成已完成，您的DLP策略将准备就绪，可在您的电子邮件流量中实施。

现在，ETD和安全访问的集成已完成。
NOTE:请参阅如何在Cisco安全访问(SA)和Cisco邮件威胁防御(ETD)中配置邮件DLP策略，以在Cisco邮件DLP安全访问中创建DLP策略。

故障排除 注释

如果在集成过程中或之后遇到问题，请查看以下常见场景和补救步骤：

1. ETD中未接受API凭证

- 症状：在ETD中输入客户端ID和密钥时，系统返回身份验证错误。
- 分辨率：
  - 验证API密钥是否使用完全所需的作用域：“Admin”和“Policy”。如果选择了其他作用域或者这些作用域丢失，连接将失败。
  - 将客户端ID或密钥粘贴到ETD控制台时，确保不会意外复制前导空格或尾随空格。

2.丢失或遗忘的密钥密钥

- 症状：您导航离开Secure Access API创建屏幕，无法再查看密钥密钥。
- 解决方案：出于安全原因，密钥密钥在创建时只显示一次。如果未安全地保存它，则必须删除安全访问中未完成的API密钥并生成一个新密钥。

3. DLP策略未在电子邮件流量上实施

- 症状：集成显示为成功，但配置的DLP策略无法捕获或阻止敏感邮件。
- 分辨率：
  - 检查API到期：如果您为API密钥到期选择“Select a specific date”（选择特定日期）（第2步），请验证密钥是否未过期。如果存在，则必须生成并应用新的密钥对。
  - 验证ETD部署模式：确保以内联模式部署思科ETD。ETD必须处于直接邮件流路径中，才能根据安全访问DLP裁决主动阻止或修改邮件。
  - 同步时间：在初始集成后，允许后端系统在几分钟内同步策略，然后再测试DLP规则。

4.一段时间稳定后的服务中断

- 症状：DLP实施在正常运行数月后突然停止工作。
- 解决方案：这通常是由过期API密钥引起的。导航至Admin -> API Keyin Cisco Secure Access以检查用于ETD的密钥的状态。实施密钥轮换流程，以在到达到期日期之前更新

ETD中的凭证。

摘要

将思科电邮威胁防御(ETD)与思科安全访问(SA)集成是建立统一数据丢失防护(DLP)战略的关键步骤。通过在Secure Access控制台中生成带有“Admin”和“Policy”范围的安全API密钥，并在ETD的全局设置中配置这些凭证，管理员可以在两个平台之间创建无缝的通信网桥。

完成此握手后，ETD可以主动将邮件元数据传递给安全访问DLP引擎。这使您的组织能够从单个集中控制面板（安全访问）管理所有数据保护策略，同时保持对邮件流量(ETD)的深入可视性和实施。

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）。