检测并防止邮件欺骗

目录

简介

先决条件

- 要求
- 使用的组件

关于本文档

什么是邮件欺骗

邮件欺骗防御工作流程

- 第 1 层：对发件人域的有效性检查
- 第 2 层：使用DMARC验证From信头
- 第 3 层：防止垃圾邮件发送者发送伪造的电子邮件
- 第 4 层：通过邮件域确定恶意发件人
- 第 5 层:使用SPF或DKIM验证结果减少误报
- 第 6 层:检测可能具有伪造发件人名称的邮件
- 第 7 层：确认的欺骗电子邮件
- 第 8 层：防范网络钓鱼URL
- 第 9 层：通过思科安全邮件威胁防御(ETD)增强欺骗检测功能

利用欺骗防御还可以做什么

简介

本文档介绍在使用Cisco Secure Email时如何检测和防止邮件欺骗。

先决条件

要求

思科建议您先了解下列主题的相关知识：

- 思科安全电子邮件

使用的组件

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。

关于本文档

本文档适用于部署思科安全电邮的思科客户、思科渠道合作伙伴和思科工程师。本文档包括以下内容：

- 什么是邮件欺骗？
- 邮件欺骗防御工作流程
- 您还能如何防止欺骗？

什么是邮件欺骗

邮件欺骗是邮件信头伪造，邮件似乎来自某人或实际来源以外的其他地方。电子邮件欺骗用于网络钓鱼和垃圾邮件活动，因为当人们认为合法、可信的来源发送了电子邮件时，他们更可能打开该电子邮件。有关欺骗的详细信息，请参阅什么是邮件欺骗以及如何检测。

邮件欺骗可分为以下几类：

分类	描述	主要目标
直接域欺骗	在信封发件人中模拟类似域作为收件人的域。	员工
显示名称欺骗	“发件人”(From)信头显示具有组织执行名称的合法发件人。它们也称为业务邮件危害(BEC)。	员工
品牌名称模拟	“发件人”(From)信头显示具有知名组织品牌名的合法发件人。	客户/合作伙伴
基于网络钓鱼网址的攻击	包含URL的电子邮件，试图窃取敏感数据或登录受害者的信息。来自银行的虚假电子邮件，要求您点击链接并验证您的帐户详细信息，是基于URL的网络钓鱼攻击的一个示例。	员工/合作伙伴
表兄弟或外观相似的域攻击	“信封发件人”(Envelope from)或“发件人”(From)信头值显示了一个类似的发件人地址，该地址模拟真实地址以绕过发件人策略框架(SPF)、DomainKeys识别邮件(DKIM)和基于域的邮件身份验证、报	员工/合作伙伴

	告和一致性(DMARC)检查。	
帐户接管/受侵害的帐户	未经授权访问属于某人的真实电子邮件帐户，然后以合法电子邮件帐户所有者的身份向其他受害者发送电子邮件。	所有人

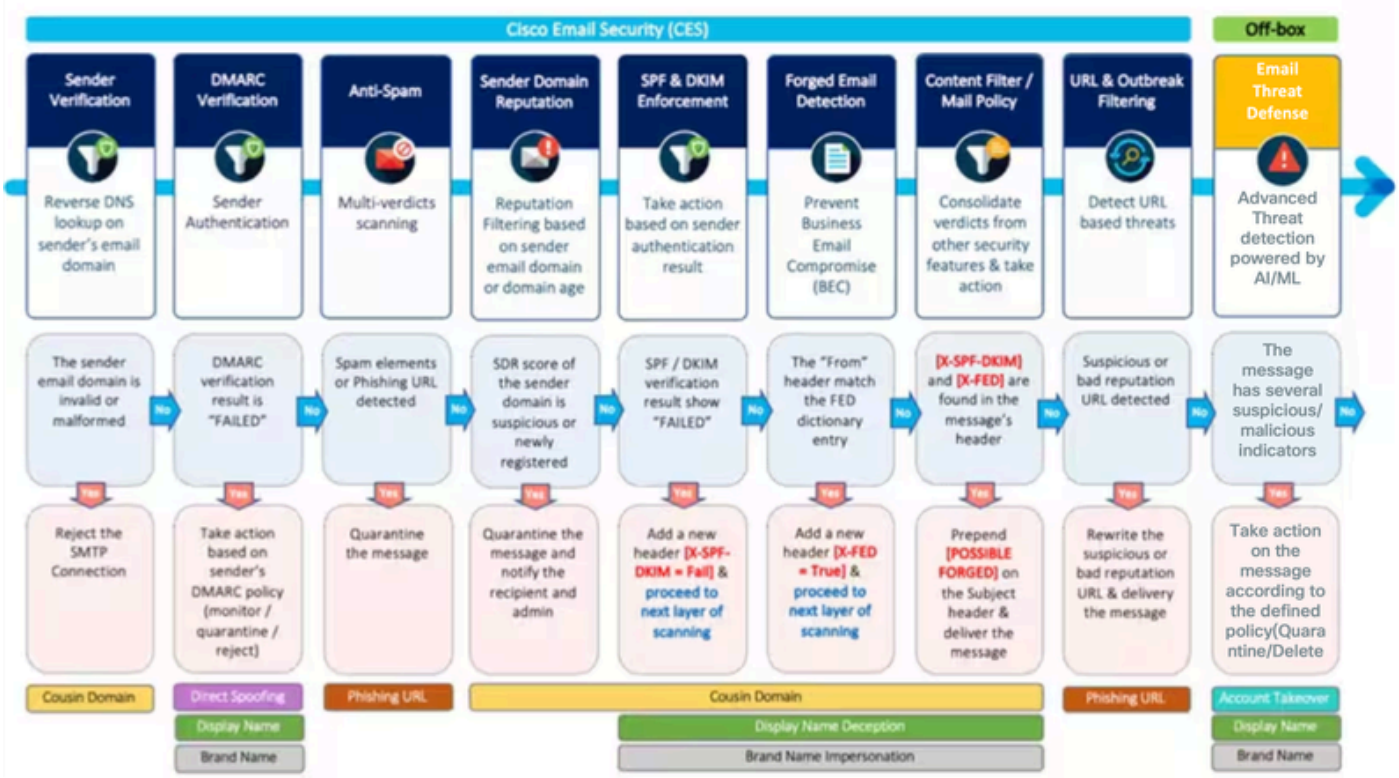
第一个类别涉及滥用电邮互联网信头中的Envelope From（信封发件人）值的所有者的域名。思科安全邮件可使用发件人域名服务器(DNS)验证来补救此攻击，以仅允许合法发件人。使用DMARC、DKIM和SPF验证可以在全球范围内获得相同的结果。

但是，其他类别仅部分违反发件人电子邮件地址的域部分。因此，仅使用DNS文本记录或发件人验证时，并不容易被阻止。理想情况下，最好将某些思科安全电邮功能与思科安全电邮威胁防御(ETD)相结合，以抵御此类高级威胁。如您所知，Cisco Secure Email的管理和功能配置因组织而异，不正确的应用会导致误报率很高。因此，了解组织的业务需求和定制功能至关重要。

邮件欺骗防御工作流程

图中显示了安全功能，这些功能可解决监控、警告和实施欺骗攻击的最佳实践（图1）。 本文档中提供了每个功能的详细信息。最佳做法是采用深度防御方法来检测邮件欺骗。攻击者可以随着时间的推移针对组织更改其方法，因此管理员必须监控所有更改并检查相应的警告和实施。

图1.思科安全邮件欺骗防御管道

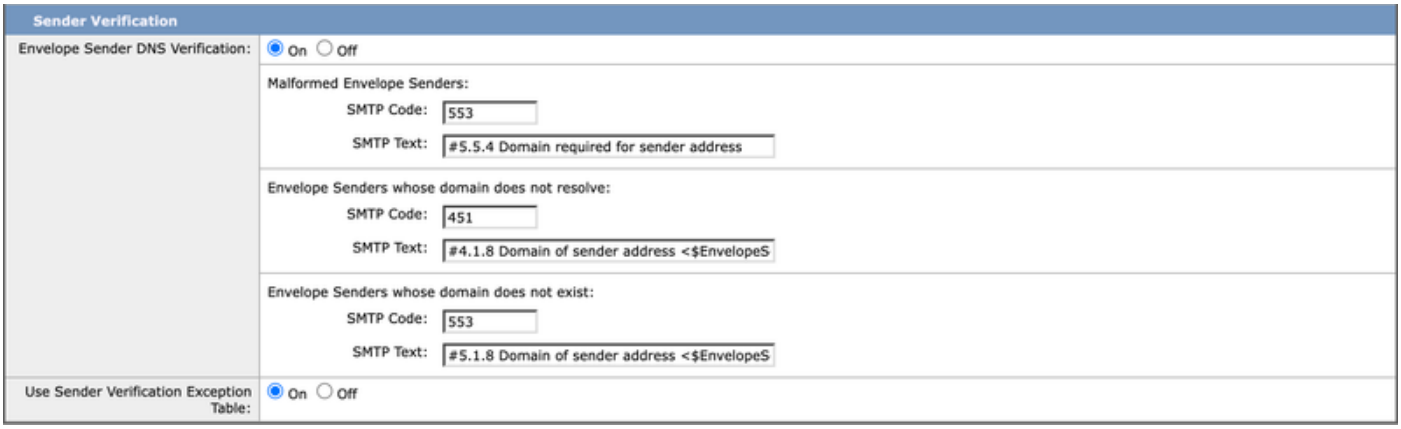


第 1 层：对发件人域的有效性检查

发件人验证是一种更直接的方法，可防止从假邮件域发送电子邮件，例如表兄弟域欺骗(例如，c1sc0.com是cisco.com的冒名者)。 思科安全电子邮件对发件人电子邮件地址的域执行MX记录查询，并在SMTP会话期间对MX记录执行A记录查找。如果DNS查询返回NXDOMAIN，它可以将该域视为不存在。攻击者伪造信封发件人的信息是一种常见技术，这样可以接受来自未经验证的发件人的邮件并进一步处理这些邮件。除非发件人的域或IP地址已预先添加到例外表中，否则思科安全邮件可以拒绝未通过使用此功能的验证检查的所有传入邮件。

最佳实践:如果信封发件人字段的邮件域无效，则配置思科安全邮件以拒绝SMTP会话。通过配置邮件流策略、发件人验证和例外表（可选），仅允许合法发件人。 有关详细信息，请访问使用发件人验证的欺骗保护。

图像2.默认邮件流策略中的“发件人验证”部分



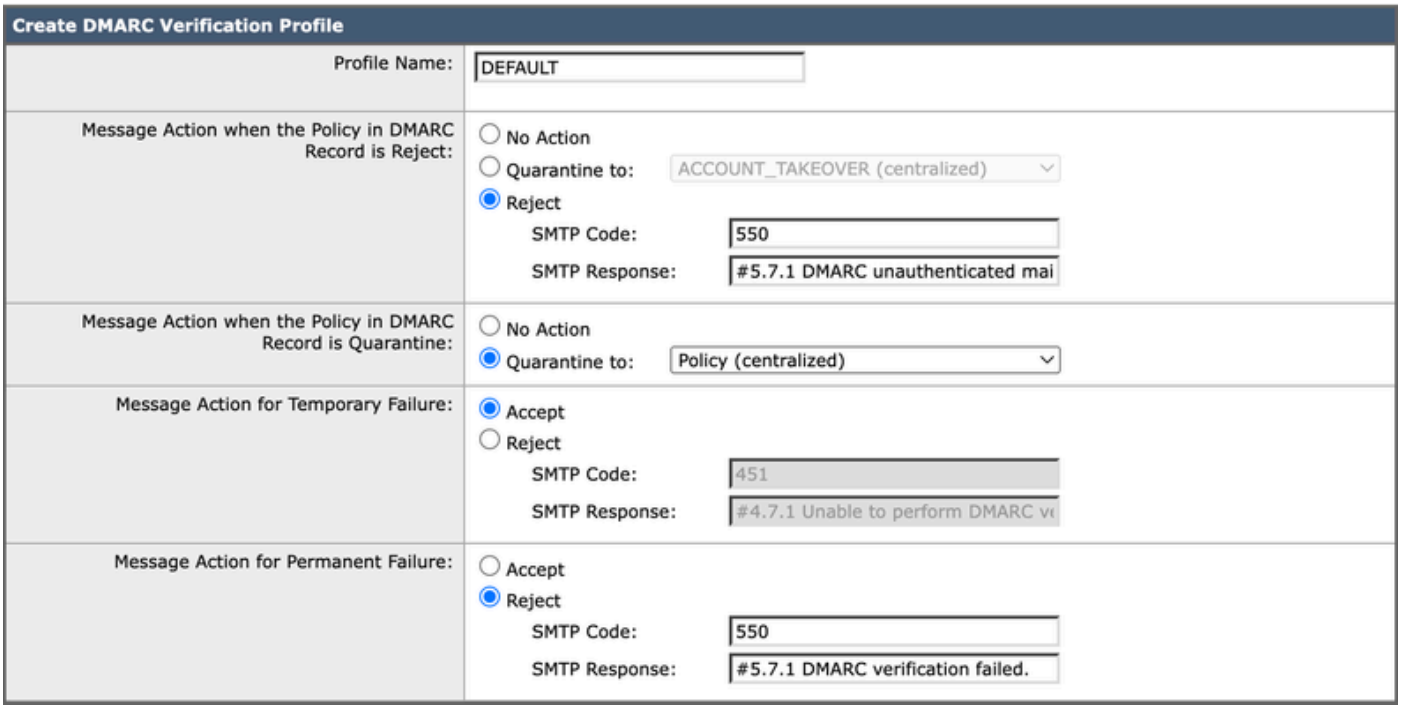
第 2 层：使用DMARC验证From信头

DMARC验证是抵御直接域名欺骗(Direct Domain Spoofing)的强大得多的功能，还包括显示名称和品牌假冒攻击。DMARC将使用SPF或DKIM（发送域源或签名）进行身份验证的信息与From报头中呈现给最终接收者的信息相关联，并确定SPF和DKIM标识符与FROM报头标识符一致。

要通过DMARC验证，传入邮件必须至少通过其中一种身份验证机制。此外，Cisco Secure Email还允许管理员定义DMARC验证配置文件，以覆盖域所有者的DMARC策略，并向域所有者发送聚合(RUA)和故障/调查(RUF)报告。这有助于加强他们的身份验证部署。

最佳实践:编辑使用发件人建议的DMARC策略操作的默认DMARC配置文件。此外，必须编辑DMARC验证的全局设置才能生成正确的报告。正确配置配置文件后，必须在邮件流策略默认策略中启用DMARC验证服务。

图3. DMARC验证配置文件



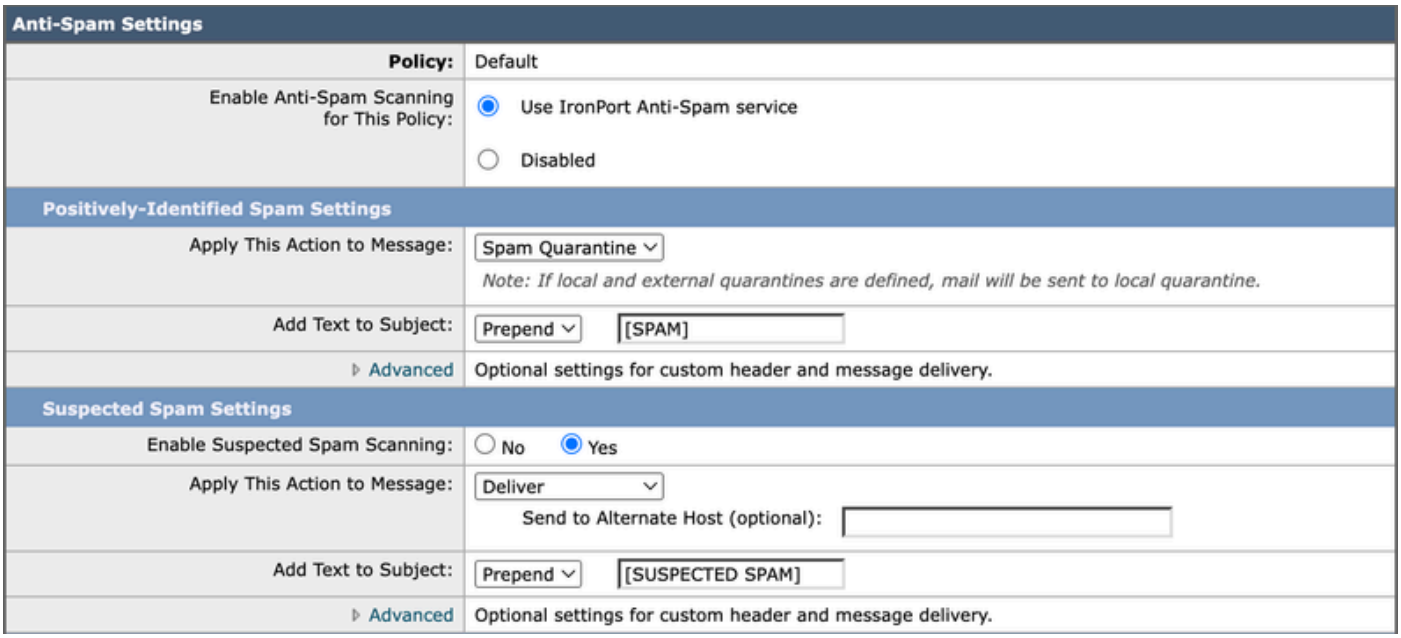
注意：DMARC必须通过发送域的所有者以及域监控工具（例如Cisco Domain Protection）来实施。如果实施得当，思科安全邮件中的DMARC实施有助于防止未经授权的发件人或域向员工发送网络钓鱼邮件。有关思科域保护的更多信息，请访问以下链接：Cisco Secure Email Domain Protection概览。

第 3 层：防止垃圾邮件发送者发送伪造的电子邮件

欺骗攻击可能是垃圾邮件活动的另一种常见形式。因此，启用反垃圾邮件保护对于有效识别包含垃圾邮件/网络钓鱼元素的欺诈邮件并积极阻止这些邮件至关重要。反垃圾邮件与本文档中详细描述的其他最佳实践操作相结合，可在不丢失合法电邮的情况下提供最佳结果。

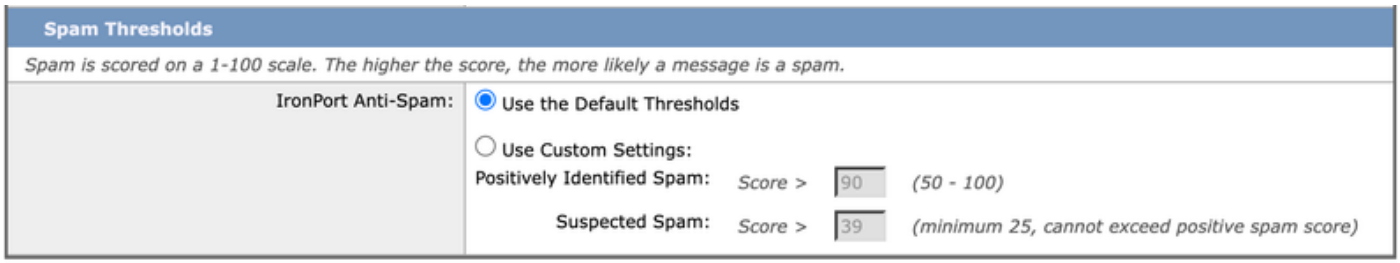
最佳实践:在默认邮件策略中启用反垃圾邮件扫描，并设置隔离操作，以正确定义垃圾邮件设置。将全球垃圾邮件的最小扫描大小至少增加到200万。

图4.默认邮件策略中的反垃圾邮件设置



垃圾邮件阈值可以针对正垃圾邮件和可疑垃圾邮件进行调整，以提高或降低敏感度（图5）；但是，思科不鼓励管理员执行此操作，并且只使用默认阈值作为基线，除非思科另有说明。

图5.默认邮件策略中的反垃圾邮件阈值设置



注意：思科安全邮件提供附加智能多扫描(IMS)引擎，该引擎提供与反垃圾邮件引擎不同的组合以提高垃圾邮件捕获率（最积极的捕获率）。

第 4 层：通过邮件域确定恶意发件人

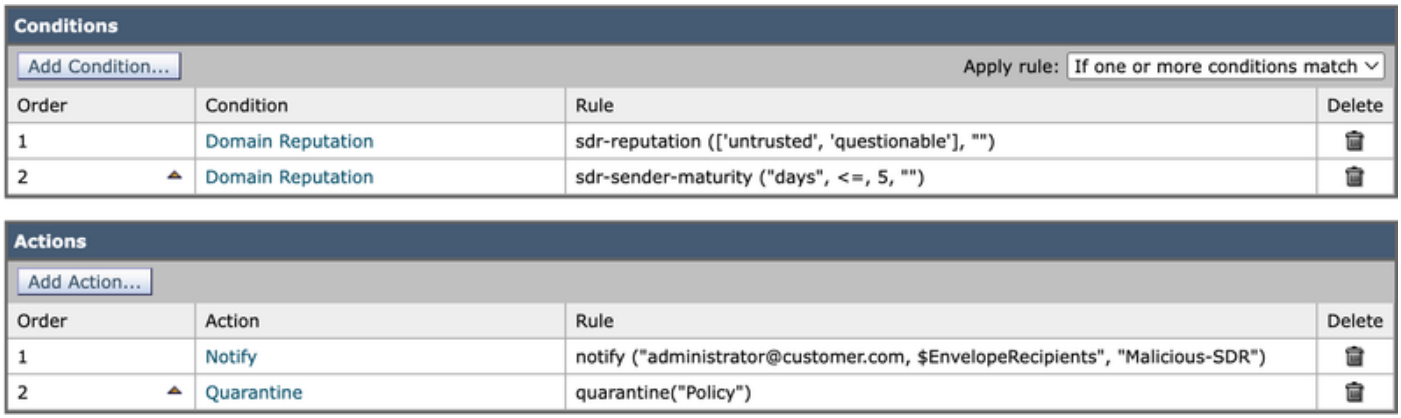
思科Talos发件人域信誉(SDR)是一项云服务，根据邮件信封和信头中的域为邮件提供信誉判定。基于域的信誉分析通过超越共享IP地址、托管或基础设施提供商的信誉，实现更高的垃圾邮件捕获率。相反，它基于与完全限定域名(FQDN)关联的功能以及简单邮件传输协议(SMTP)会话和邮件报头中的其他发件人信息来导出判定。

发件人成熟度是建立发件人信誉的基本功能。发件人成熟度根据多个信息源自动生成垃圾邮件分类，可能与基于Whois的域年龄不同。发件人成熟度设置为30天的限制，超过此限制后，域被视为邮

件发件人成熟，且未提供进一步详细信息。

最佳实践:创建传入内容过滤器，捕获SDR信誉判定处于“不可信/可疑”或“发件人成熟度小于或等于5天”的发送域。建议的操作是隔离邮件并通知邮件安全管理员和原始收件人。有关如何配置SDR的更多信息，请观看思科视频Cisco Email Security Update(Version 12.0):发件人域信誉(SDR)

图像6.包含通知和隔离操作的SDR信誉和域年龄的内容过滤器。

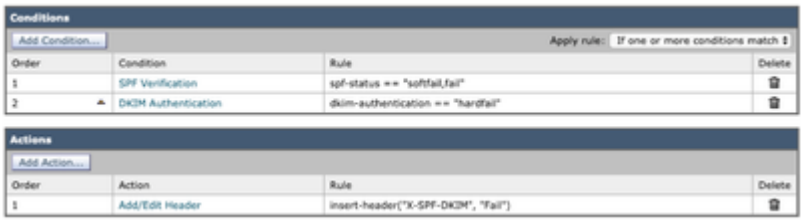


第 5 层:使用SPF或DKIM验证结果减少误报

必须执行SPF或DKIM验证（两者或其中之一），以便为大多数攻击类型建立多层欺骗邮件检测。思科建议对未通过SPF或DKIM验证的邮件添加新的报头（例如[X-SPF-DKIM]），并使用伪造邮件检测(FED)功能对结果进行操作（稍后将介绍该功能），以提高欺骗邮件的捕获率，而不是采取最终操作（例如丢弃或隔离）。

最佳实践:创建内容过滤器，检查通过以前检查的每个传入邮件的SPF或DKIM验证结果。对未通过SPF或DKIM验证并传送到下一层扫描的邮件添加新的X报头（例如X-SPF-DKIM=Fail）— 伪造邮件检测(FED)。

图7.检查具有SPF或DKIM失败结果的邮件的内容过滤器



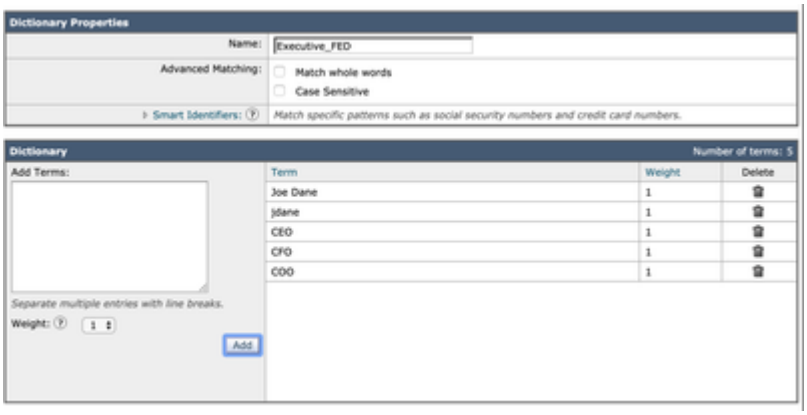
第 6 层:检测可能具有伪造发件人名称的邮件

作为SPF、DKIM和DMARC验证的补充，伪造邮件检测(FED)是防止邮件欺骗的另一个重要防线。FED是补救滥用消息正文中“发件人”值的欺骗攻击的理想选择。假设您已经知道组织中的执行名称，您可以创建这些名称的字典，然后使用内容过滤器中的FED条件引用该字典。此外，除执行名称外，您还可以使用DNSTWIST(DNSTWIT)根据域创建表兄弟域或外观相似的域词典，以匹配外观相似的域欺骗。

最佳实践:识别组织中可能伪造其邮件的用户。创建为高管提供帐户的自定义词典。对于每个执行名称，词典必须包含用户名和所有可能的用户名作为术语（图8）。 词典完成后，在内容过滤器中使用“伪造邮件检测”(Forged Email Detection)，将传入邮件的“发件人”(From)值与这些词典条目匹配。

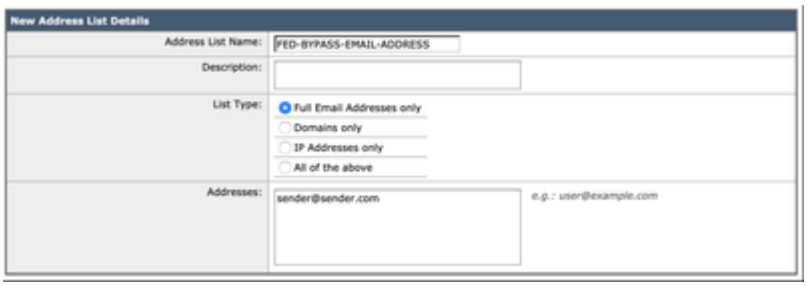
注意：考虑到大多数域不是注册的排列，DNS发件人验证可以防止这些域被注册。如果选择使用字典条目，请只注意注册的域，并确保每个字典不超过500-600个条目。

图8.用于伪造邮件检测的自定义目录



可以选择在信封发送中添加邮件域的例外条件，以绕过FED检测。或者，可以创建自定义地址列表，以绕过FED检查到Fromheader（图9）中显示的邮件地址列表。

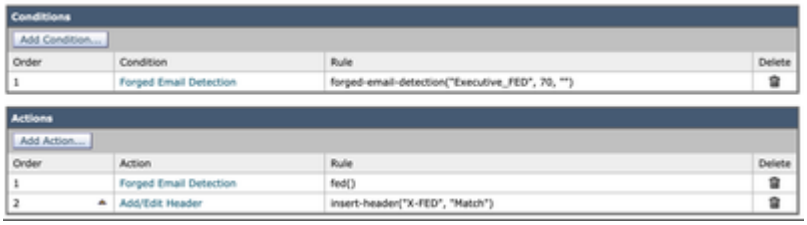
图9.创建地址列表以绕过FED检测



应用“伪造邮件检测”(Forged Email Detection)专有操作删除“发件人”(From)值并查看邮件收件箱中的实际信封发件人邮件地址。然后，在匹配条件的消息上添加新的X报头（例如，X-

FED=Match），并继续将消息传送到下一层检查（映像10），而不是应用最终操作。

图10.建议的FED内容过滤器设置

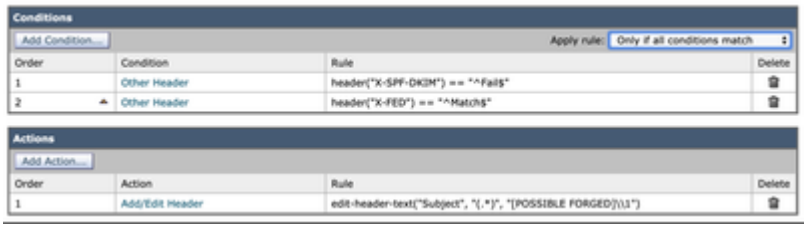


第 7 层：确认的欺骗电子邮件

通过引用管道中各种安全功能的其他判定（例如SPF/DKIM Enforcemen和FE生成的X报头信息），识别真正的欺骗活动会更加有效。例如，管理员可以创建内容过滤器来识别由于SPF/DKIM验证结果失败(X-SPF-DKIM=Fail)和哪个From报头与FED字典条目(X-FED=Match)而添加了两个新X报头的邮件。

建议的操作可以是隔离邮件并通知收件人，或者继续传送原始邮件，但将[可能伪造的]字词作为警告发送到主题行，如图所示（图11）。

图11.将所有X报头合并为一个（最终）规则



第 8 层：防范网络钓鱼URL

针对网络钓鱼链接的保护已集成到Cisco安全邮件的URL和爆发过滤中。混合威胁将欺骗和网络钓鱼邮件结合起来，使目标看起来更加合法。启用爆发过滤对于帮助实时检测、分析和阻止此类威胁至关重要。我们有必要了解，URL信誉是在反垃圾邮件引擎内部评估的，并且可用作垃圾邮件检测决策的一部分。如果反垃圾邮件引擎不停止将URL作为垃圾邮件的邮件，则会通过安全管道后部的URL和爆发过滤对其进行评估。

建议：创建内容过滤规则，阻止具有恶意信誉分数的URL，并将具有中性信誉分数的URL重定向至思科安全代理（映像12）。 通过启用邮件修改启用威胁爆发过滤器。URL重写允许思科安全代理

（图13）分析可疑URL。 有关更多的信息，访问：为安全邮件网关和云网关配置 URL 过滤

图12. URL信誉的内容过滤器

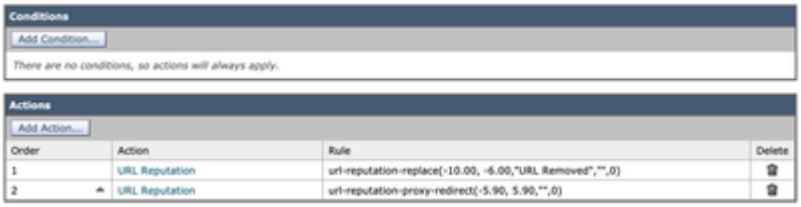
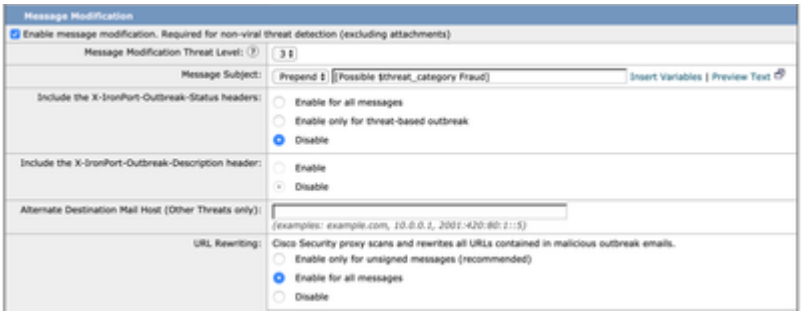


图13.在爆发过滤中启用URL重写



第 9 层：通过思科安全邮件威胁防御(ETD)增强欺骗检测功能

思科提供邮件威胁防御，这是一个云原生解决方案，利用思科Talos的卓越威胁情报。它具备支持API的架构，可加快响应速度、完整的电邮可视性（包括内部电邮）、提供更好的情景信息的对话视图，以及用于自动或手动补救Microsoft 365邮箱中潜在威胁的工具。有关详细信息，请访问思科安全邮件威胁防御产品手册。

思科安全邮件威胁防御使用发件人身份验证和BEC检测功能来打击网络钓鱼。它集成了机器学习和人工智能引擎，将本地身份和关系建模与实时行为分析相结合，以防御基于身份欺骗的威胁。它可模拟组织内部和个人之间的信任邮件行为。邮件威胁防御还具有其他主要功能，其中包括以下优势：

- 利用高级威胁检测功能发现已知、新兴和有针对性的威胁。
- 识别恶意技术并获得特定业务风险的情景。
- 快速搜索危险威胁并进行实时补救。
- 利用可搜索的威胁遥感勘测技术可对威胁进行分类，并了解您的组织哪些部分最容易遭受攻击。

图14.思科安全邮件威胁防御提供有关您的组织如何成为目标的信息。

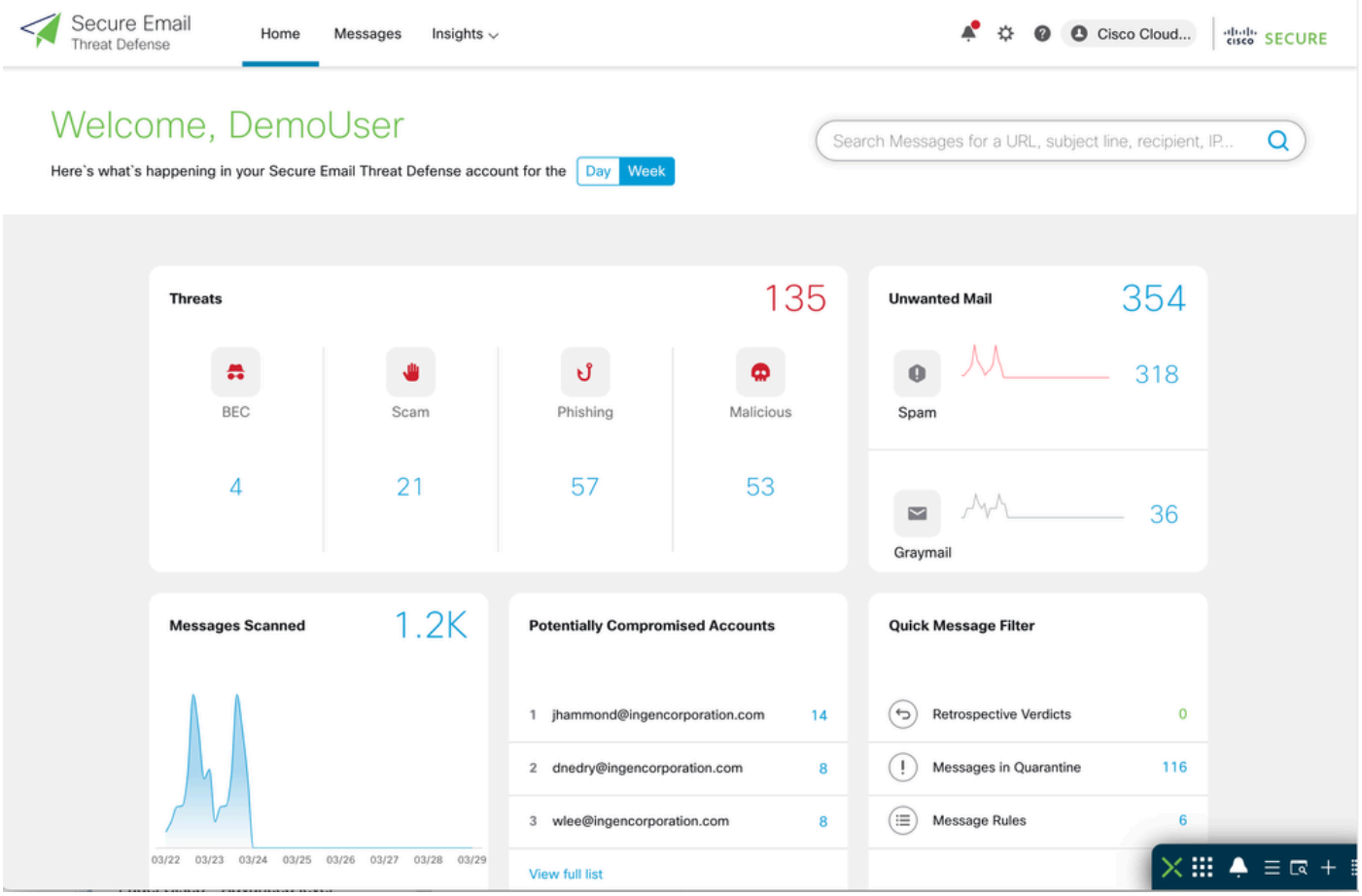
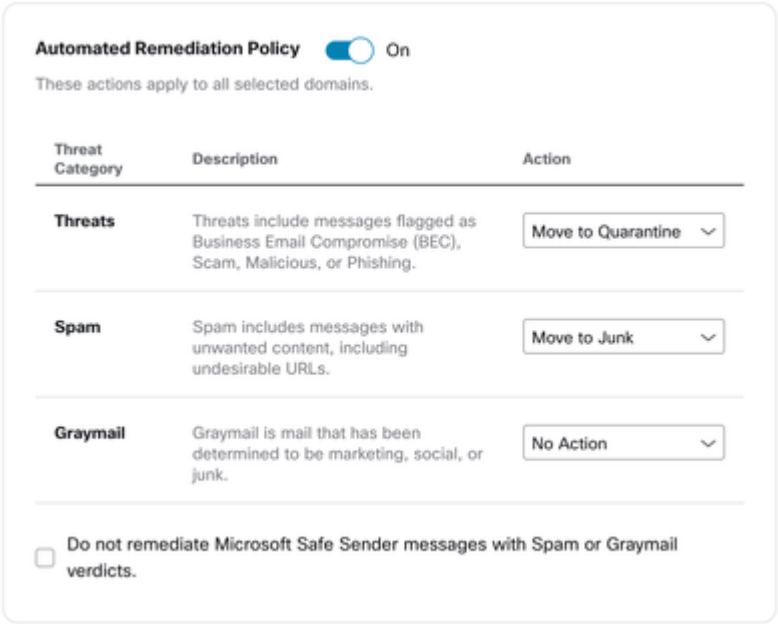


图15.思科邮件威胁防御策略设置会自动确定邮件是否与选定的威胁类别匹配



利用欺骗防御还可以做什么

许多欺骗可以通过一些简单的预防措施进行补救，这些预防措施包括（但不限于）：

- 将允许主机访问表(HAT)中列出的域限制在极少数核心业务合作伙伴。
- 持续跟踪和更新SPOOF_ALLOW发件人组中的成员（如果已创建）并使用最佳实践链接中提供的说明。
- 启用灰色邮件检测，并将它们放在垃圾邮件隔离区中。

但最重要的是，启用SPF、DKIM和DMARC并相应地实施它们。但是，有关发布SPF、DKIM和DMARC记录的指导不属于本文档的范围。为此，请参阅本白皮书：电子邮件身份验证最佳实践：部署SPF、DKIM和DMARC的最佳方法。

了解补救电子邮件攻击（如此处讨论的欺骗活动）所面临的挑战。如果您对实施这些最佳实践有任何疑问，请与Cisco技术支持联系并创建案例。或者，请与您的思科客户团队联系，获取解决方案和设计指南。有关思科安全邮件的详细信息，请参阅思科安全邮件网站。

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）。