檢測並阻止郵件欺騙

目錄

簡介

本文檔介紹如何在使用思科安全郵件時檢測並防止郵件欺騙。

必要條件

需求

思科建議您瞭解以下主題。

- 思科安全電子郵件

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

關於此檔案

本文檔適用於部署思科安全電子郵件的思科客戶、思科管道合作夥伴和思科工程師。本檔案涵蓋：

- 什麼是電子郵件欺騙？
- 電子郵件欺騙防禦工作流程
- 您還能採取哪些措施來防止欺騙？

什麼是電子郵件欺騙

電子郵件欺騙是郵件頭偽造，郵件似乎來自某人或實際來源以外的其他地方。電子郵件欺騙用於網路釣魚和垃圾郵件活動，因為當人們認為合法、可信的源已傳送電子郵件時，他們更可能打開電子郵件。有關欺騙的詳細資訊，請參閱什麼是電子郵件欺騙以及如何檢測它。

電子郵件欺騙屬於以下類別：

類別	說明	主要目標
直接域欺騙	在「信封發件人」中模擬與收件人域類似的域。	員工
顯示名稱欺騙	「寄件者」標頭顯示合法寄件者，其執行名稱為組織。它們也稱為商業電子郵件危害(BEC)。	員工
品牌名稱模擬	「寄件者」標頭會顯示具有知名組織品牌名稱的合法寄件者。	客戶/合作夥伴
基於Phish URL的攻擊	URL的電子郵件，嘗試從受害者處竊取敏感資料或登入資訊。來自銀行的偽造電子郵件，要求您點選連結並驗證帳戶詳細資訊，是基於URL的網路釣魚攻擊的一個示例。	員工/合作夥伴
表兄弟或相似域攻擊	信封發件人或發件人信頭值顯示類似的發件人地址，該地址模擬實際發件人地址以繞過發件人策略架構(SPF)、域金鑰辨識郵件(DKIM)和基於域的郵件身份驗證、報告和一致性(DMARC)檢查。	員工/合作夥伴
帳戶接管/受侵害的帳戶	未經授權即可存取某人的真實電子郵件帳戶，然後以合法電子郵件帳戶擁有者的身份將電子郵件傳送給其他受害者。	所有人

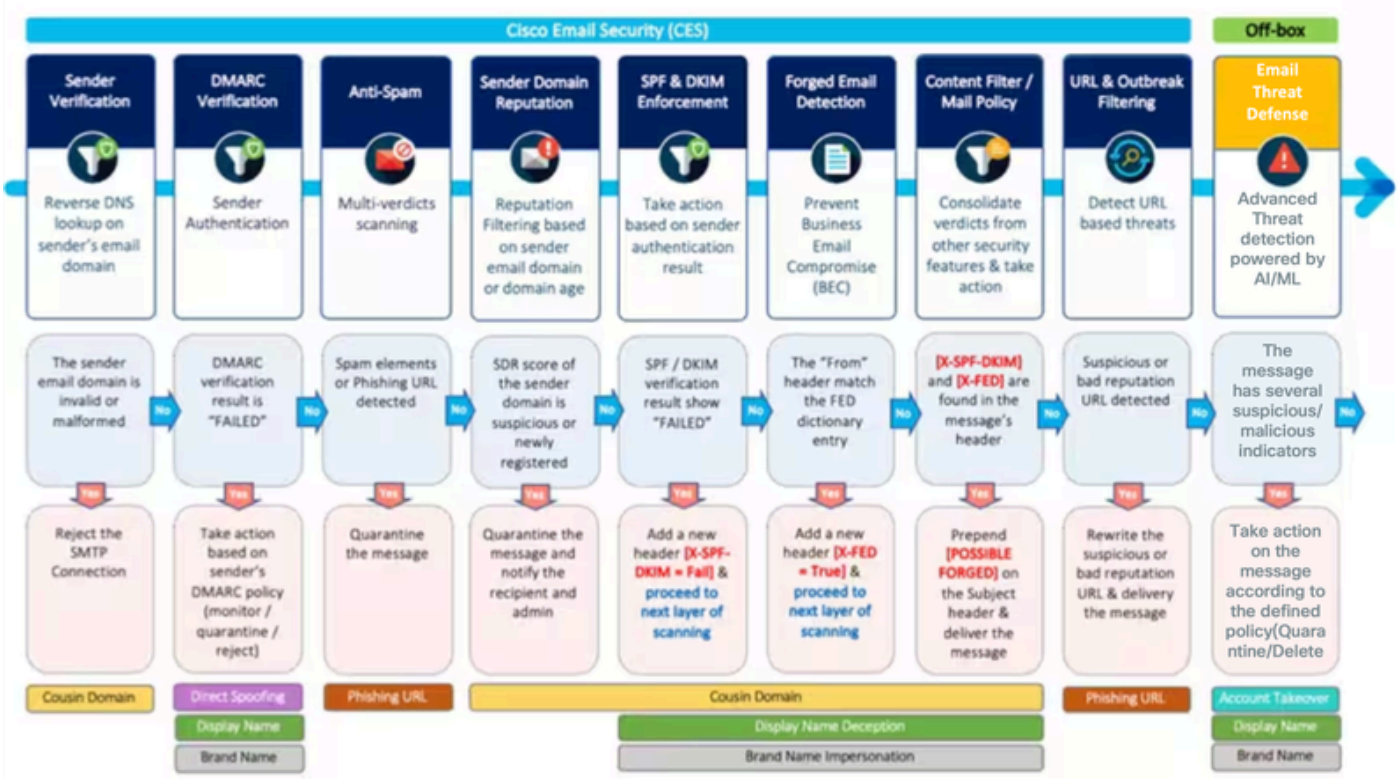
第一類涉及濫用電子郵件的Internet報頭中的「信封發件人」(Envelope From)值。Cisco Secure Email可以透過使用發件人域名伺服器(DNS)驗證來僅允許合法發件人來補救此攻擊。使用DMARC、DKIM和SPF驗證可在全球範圍內獲得相同的結果。

但是，其他類別僅部分違反發件人電子郵件地址的域部分。因此，僅使用DNS文本記錄或發件人驗證並不容易被阻止。理想情況下，最好將某些思科安全電郵功能與思科安全電郵威脅防禦(ETD)相結合，以抵禦此類高級威脅。如您所知，Cisco Secure Email的管理和功能配置可能因組織而異，不當的應用可能會導致誤報率很高。因此，瞭解組織的業務需求和定製功能至關重要。

電子郵件欺騙防禦工作流程

圖中顯示了安全功能，這些功能涉及監控、警告和強制執行欺騙攻擊的最佳做法（圖1）。本檔案提供每個功能的詳細資訊。最佳做法是採用深度防禦方法來檢測郵件欺騙。攻擊者可以隨時間推移針對組織更改其方法，因此管理員必須監控所有更改並檢查相應的警告和實施。

圖1.思科安全電子郵件欺騙防禦管線

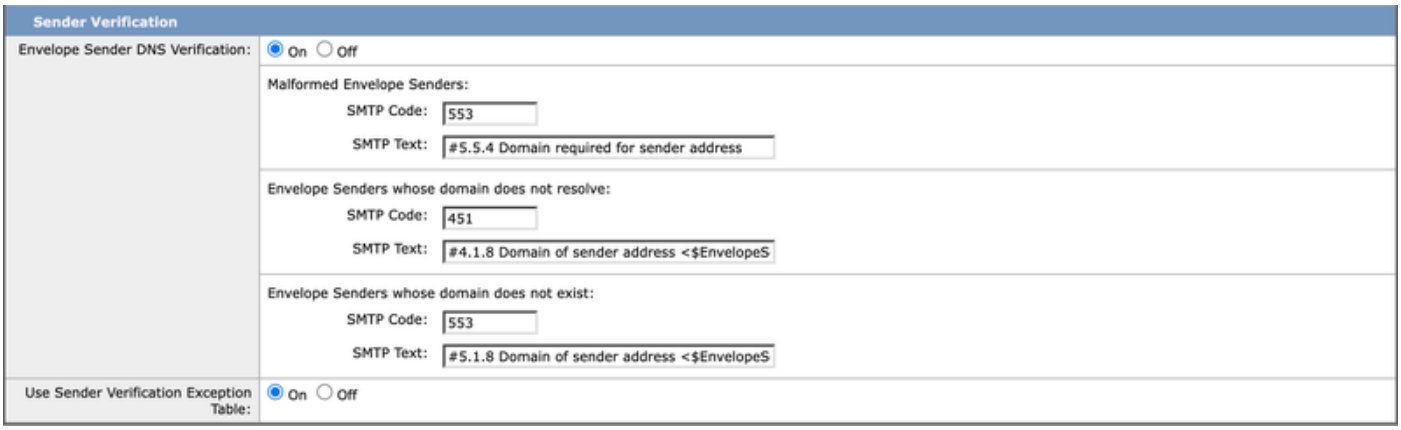


第1層：對發件人域的有效性檢查

發件人驗證是防止從假郵件域傳送電子郵件的更直接的方法，例如表兄弟域欺騙(例如，c1sc0.com是cisco.com的冒充者)。Cisco Secure Email對發件人電子郵件地址的域執行MX記錄查詢，並在SMTP會話期間對MX記錄執行A記錄查詢。如果DNS查詢返回NXDOMAIN，它可以將域視為不存在。攻擊者通常使用偽造信封發件人資訊的方法，以便接收來自未經驗證的發件人的郵件並進行進一步處理。除非發件人的域或IP地址已預增加到例外表中，否則思科安全郵件可以拒絕所有未通過使用此功能的驗證檢查的傳入郵件。

最佳實踐：如果信封發件人欄位的電子郵件域無效，則配置Cisco Secure Email以拒絕SMTP通話。透過配置郵件流策略、發件人驗證和例外表（可選），只允許合法發件人。有關詳細資訊，請訪問使用發件人驗證的Spoof Protection。

圖2.預設郵件流策略中的發件人驗證部分



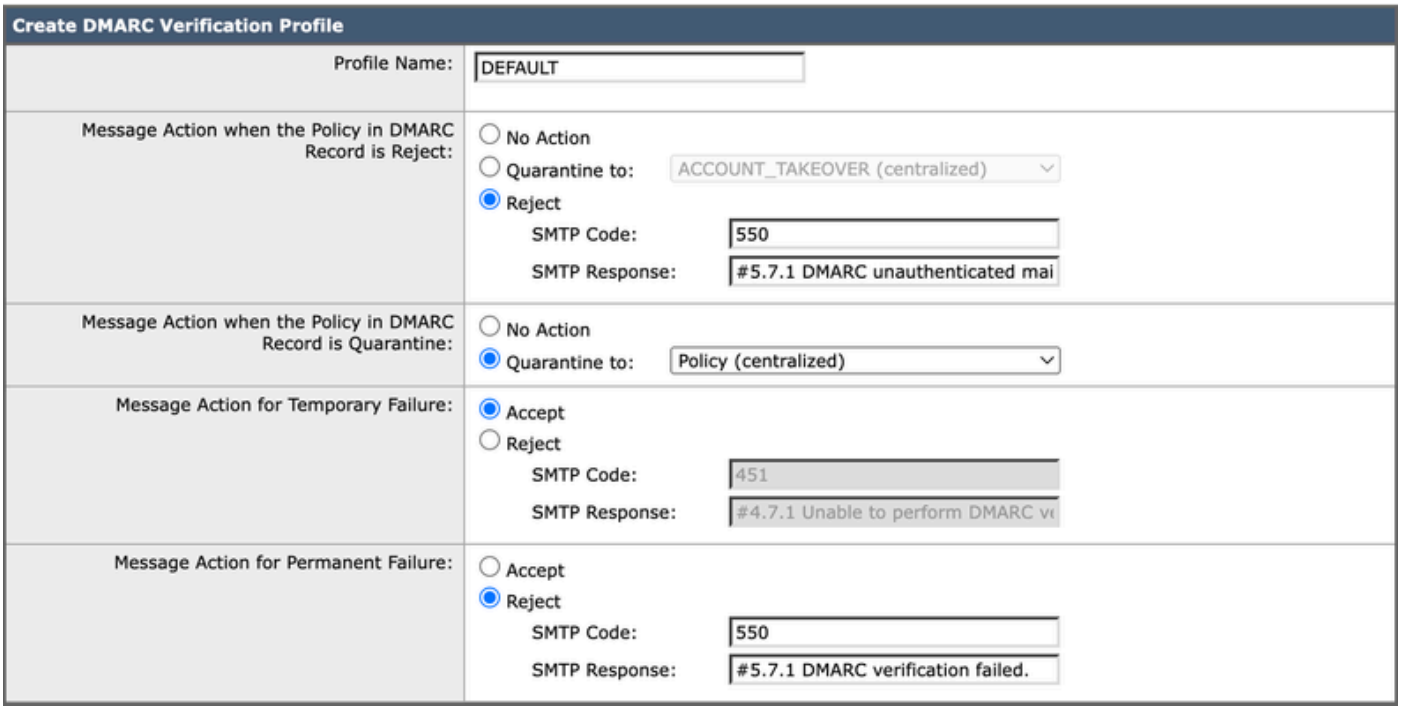
第2層：使用DMARC驗證From報頭

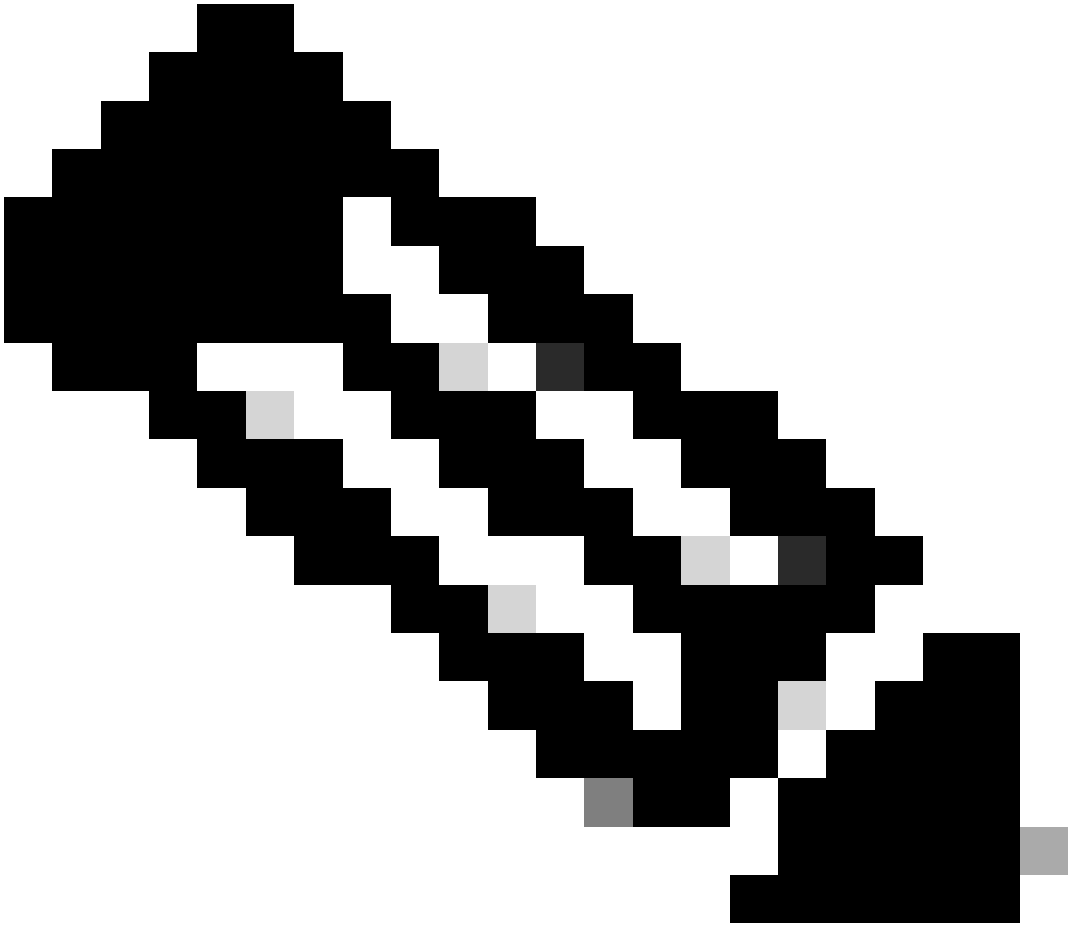
DMARC驗證是抵禦直接域欺騙的強大功能，還包括顯示名稱和品牌模擬攻擊。DMARC將使用SPF或DKIM（傳送域源或簽名）進行身份驗證的資訊與From報頭中呈現給最終接收方的資訊進行關聯，並確定SPF和DKIM識別符號與FROM報頭識別符號對齊。

要透過DMARC驗證，傳入的電子郵件必須至少透過其中一種驗證機制。此外，Cisco Secure Email還允許管理員定義DMARC驗證配置檔案，以覆蓋域所有者的DMARC策略，並向域所有者傳送聚合(RUA)和故障/鑑識(RUF)報告。這有助於加強他們的身份驗證部署。

最佳實踐：編輯使用發件人建議的DMARC策略操作的預設DMARC配置檔案。此外，必須編輯DMARC驗證的全局設定才能生成正確的報告。正確配置配置檔案後，必須在郵件流策略預設策略中啟用DMARC驗證服務。

圖3.DMARC驗證配置檔案





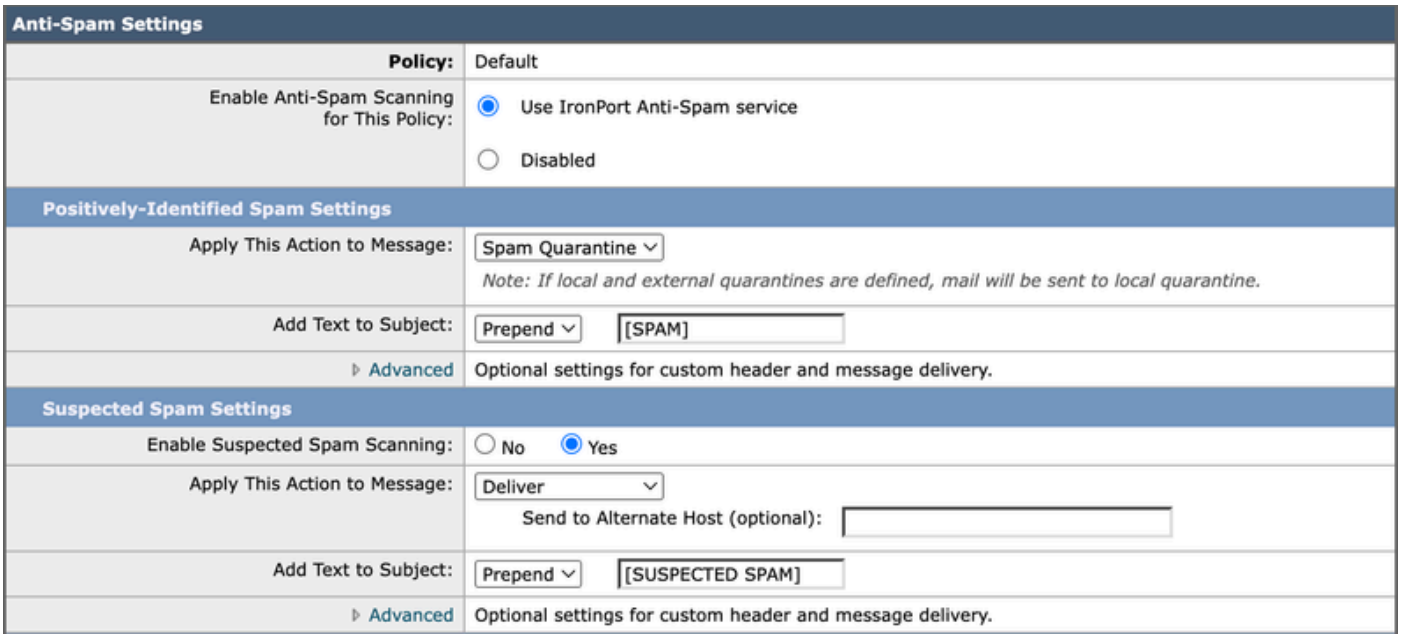
注意：實施DMARC必須同時傳送域的所有者和域監控工具，例如Cisco域保護。如果實施得當，思科安全郵件中的DMARC實施有助於防止未經授權的發件人或域向員工傳送網路釣魚郵件。有關思科域保護的詳細資訊，請訪問此連結：思科安全電子郵件域保護概覽。

第3層：防止垃圾郵件傳送者傳送偽造的電子郵件

欺騙攻擊可能是垃圾郵件活動的另一種常見形式。因此，啟用反垃圾郵件保護對於有效辨識包含垃圾郵件/網路釣魚元素的欺詐電子郵件並積極阻止它們至關重要。反垃圾郵件與本文檔中全面描述的其他最佳實踐操作相結合，可在不丟失合法電子郵件的情況下提供最佳結果。

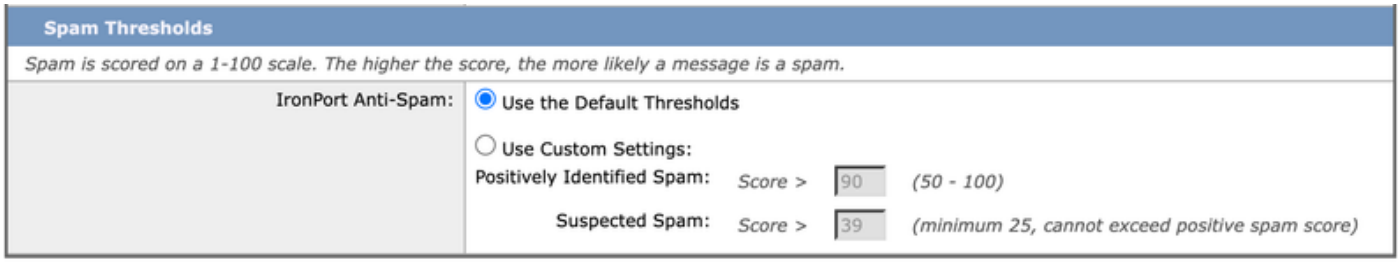
最佳實踐：在預設郵件策略中啟用反垃圾郵件掃描，並設定隔離區操作以明確辨識垃圾郵件設定。將全球垃圾郵件的最小掃描大小增加到至少200萬封。

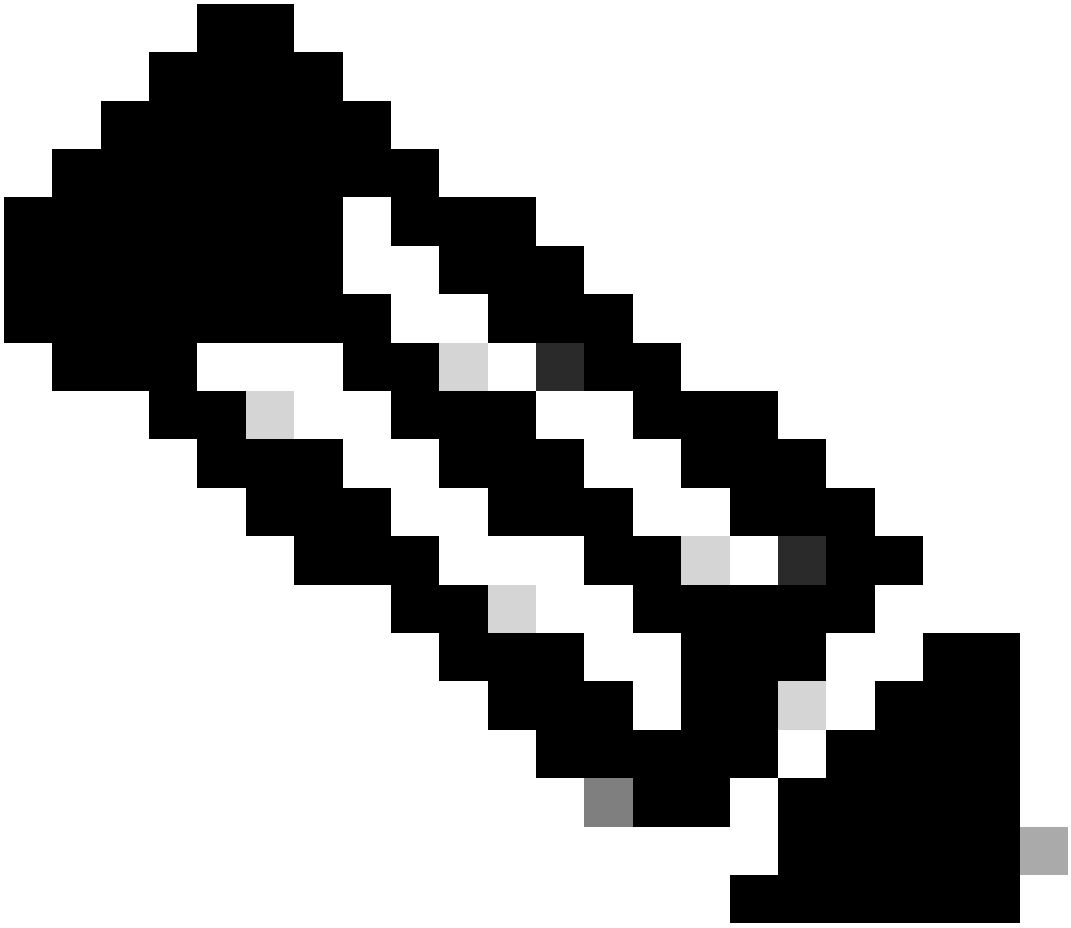
圖4.預設郵件策略中的反垃圾郵件設定



垃圾郵件閾值可以針對正垃圾郵件和疑似垃圾郵件進行調整，以提高或降低敏感度（圖5）；但是，思科不鼓勵管理員執行此操作，除非思科另有說明，否則僅使用預設閾值作為基線。

圖5.預設郵件策略中的反垃圾郵件閾值設定





注意：思科安全郵件提供一個附加的智慧多掃描(IMS)引擎，該引擎與反垃圾郵件引擎提供不同的組合，以提高垃圾郵件捕獲率（最主動的捕獲率）。

第4層：透過郵件域確定惡意發件人

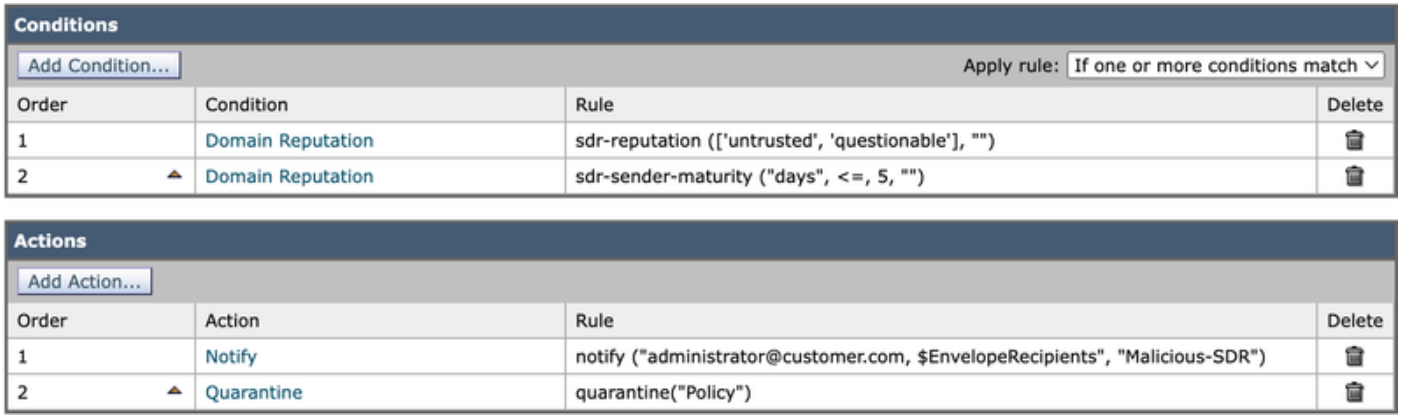
Cisco Talos發件人域信譽(SDR)是一項雲服務，根據郵件信封和信頭中的域為電子郵件提供信譽判定。基於域的信譽分析透過超越共用IP地址、託管或基礎設施提供商的聲譽來實現更高的垃圾郵件捕獲率。相反，它基於與完全限定域名(FQDN)相關的功能以及簡單郵件傳輸協定(SMTP)會話和郵件報頭中的其他發件人資訊來派生裁決。

Sender Maturity是建立發件人信譽的基本功能。發件人成熟度根據多個資訊源自動為垃圾郵件分類生成，可能與基於Whois的域年齡不同。發件人成熟度設定為30天的限制，超過此限制後，域將視為電子郵件發件人成熟，且不提供其他詳細資訊。

最佳實踐：建立傳入內容過濾器，捕獲SDR信譽判定處於「不可信/有問題」或「發件人成熟度」小於或等於5天的傳送域。建議的操作是隔離郵件並通知郵件安全管理員和原始收件人。有關如何配置SDR的詳細資訊，請觀看Cisco影片，網址為Cisco Email Security Update (Version 12.0)： Sender

[Domain Reputation (SDR)]

圖6.SDR信譽和域年齡的內容過濾器，包含通知和隔離操作。



Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-reputation (['untrusted', 'questionable'], "")	
2	Domain Reputation	sdr-sender-maturity ("days", <=, 5, "")	

Actions

Add Action...

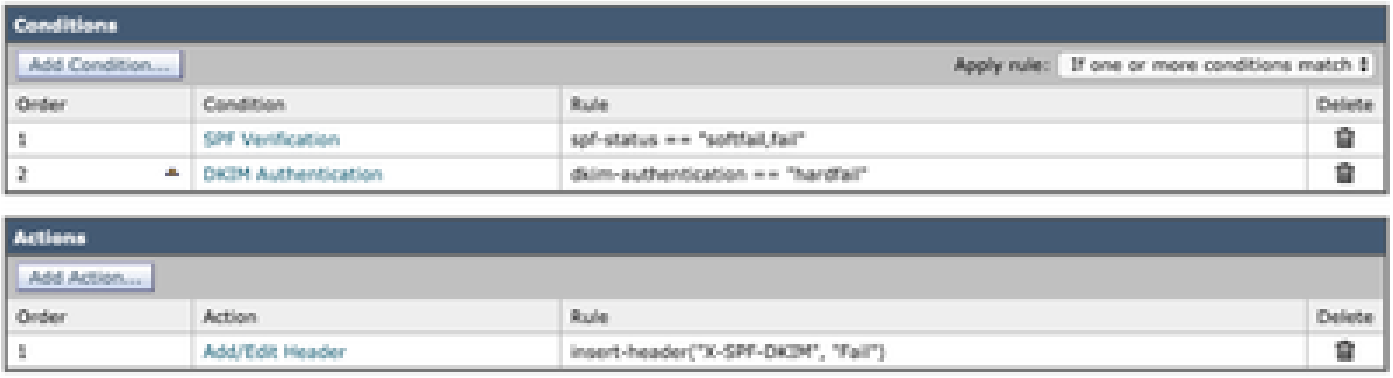
Order	Action	Rule	Delete
1	Notify	notify ("administrator@customer.com, $EnvelopeRecipients", "Malicious-SDR")	
2	Quarantine	quarantine("Policy")	

第5層：使用SPF或DKIM驗證結果減少誤報

必須執行SPF或DKIM驗證（兩者或其中之一），以便為大多數攻擊型別建立多層欺騙性郵件檢測。思科建議對未通過SPF或DKIM驗證的郵件增加如[X-SPF-DKIM]的新報頭，而不是採取最終操作（例如丟棄或隔離），而是使用偽造郵件檢測(FED)功能配合結果（稍後將介紹該功能），以提高欺騙電子郵件的捕獲率。

最佳實踐：建立一個內容過濾器，檢查透過以前檢查的每個傳入郵件的SPF或DKIM驗證結果。在SPF或DKIM驗證失敗並傳送到下一層掃描的郵件上增加新的X-header（例如X-SPF-DKIM=Fail）- 偽造郵件檢測(FED)。

圖7.檢查包含失敗SPF或DKIM結果的郵件的內容過濾器



Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	SPF Verification	spf-status == "softfail,fail"	
2	DKIM Authentication	dkim-authentication == "hardfail"	

Actions

Add Action...

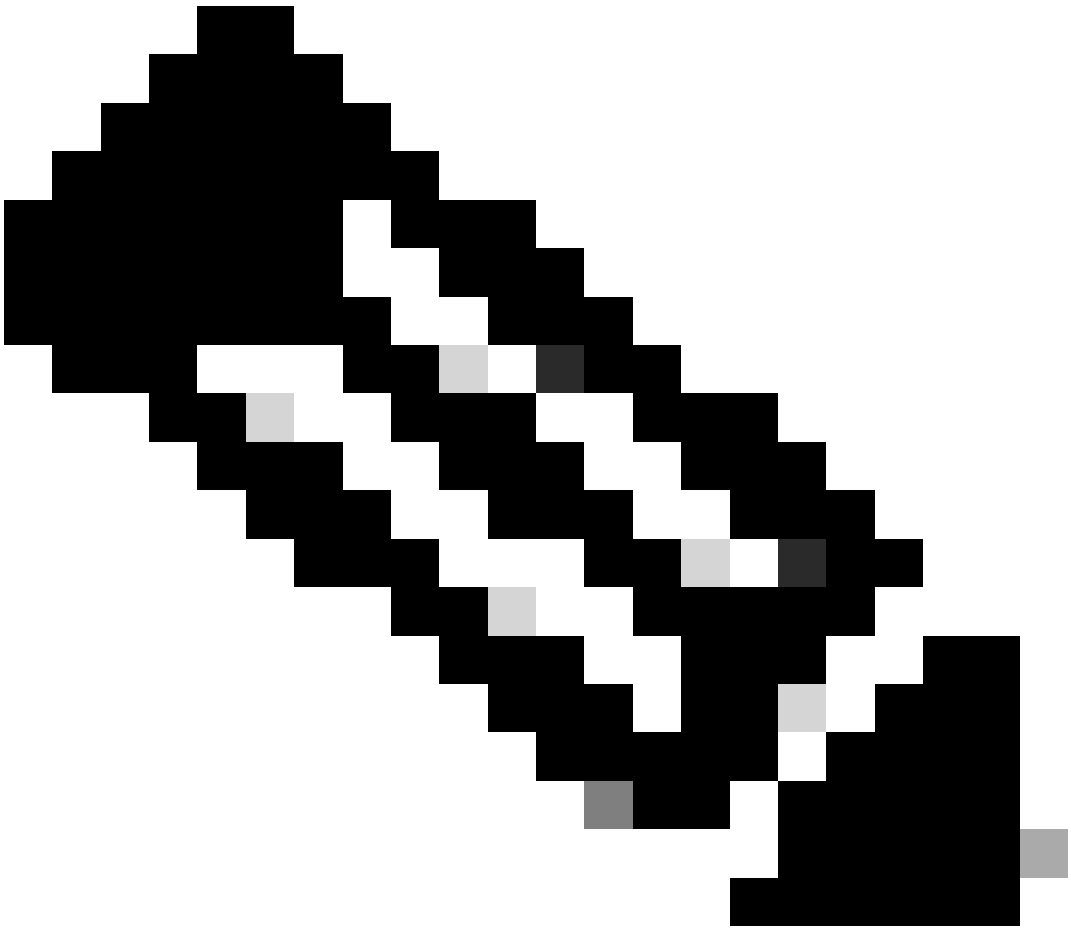
Order	Action	Rule	Delete
1	Add/Edit Header	insert-header("X-SPF-DKIM", "Fail")	

第6層：檢測可能帶有偽造發件人名稱的郵件

除了SPF、DKIM和DMARC驗證之外，偽造的電子郵件檢測(FED)是防止郵件欺騙的另一個關鍵防線。FED是補救濫用消息正文中的「發件人」值的欺騙性攻擊的理想之選。假設您已經知道組織內的執行名稱，您可以建立這些名稱的詞典，然後在內容篩選器中以FED條件參照該詞典。此外，除了管理名稱之外，您還可以使用DNSTWIST (DNSTWIT)基於您的域建立表項域或外觀相似的域的詞典，以與外觀相似的域欺騙進行匹配。

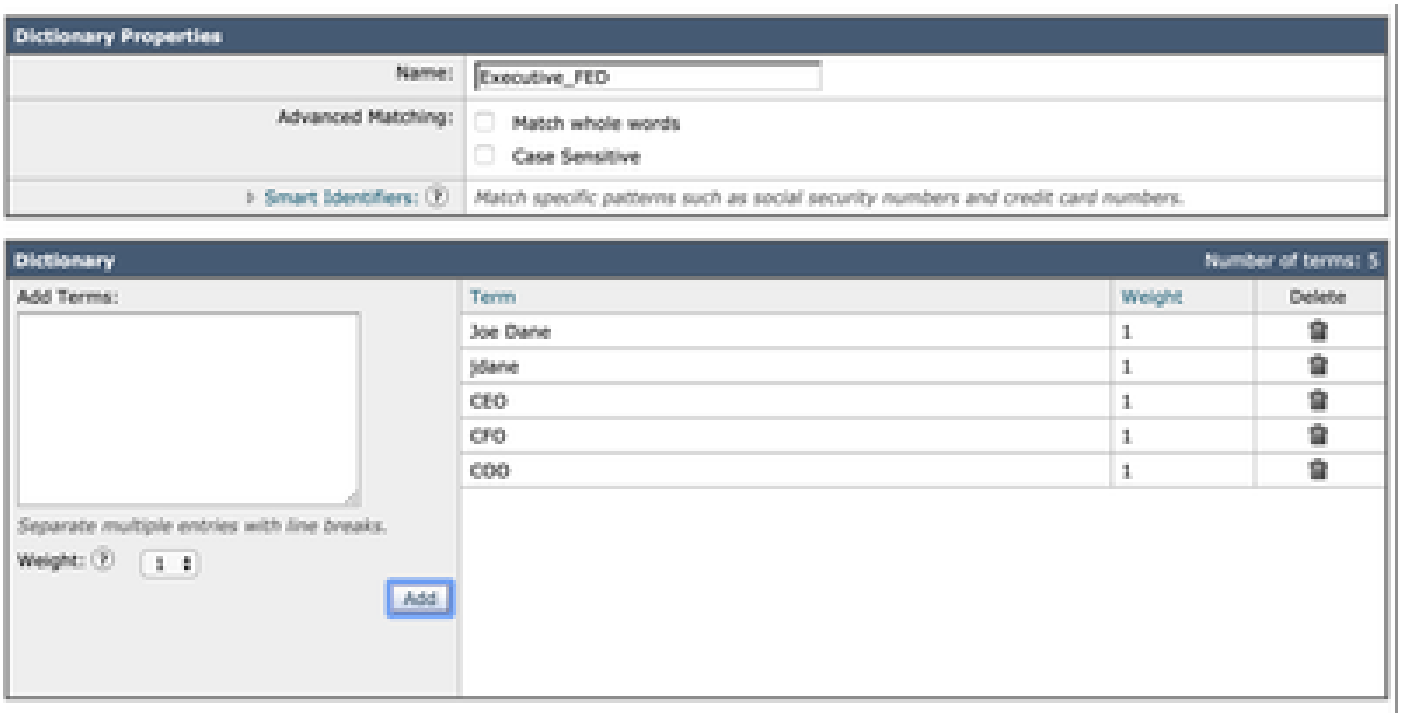
最佳實務：辨識貴組織內可能偽造訊息的使用者。建立為主管記錄的自定義詞典。對於每個執行名稱，詞典必須包括使用者名稱和所有可能的使用者名稱作為辭彙（圖8）。詞典完成時，請在內容過

濾器中使用「偽造郵件檢測」，將傳入郵件的「發件人」值與這些詞典條目相匹配。



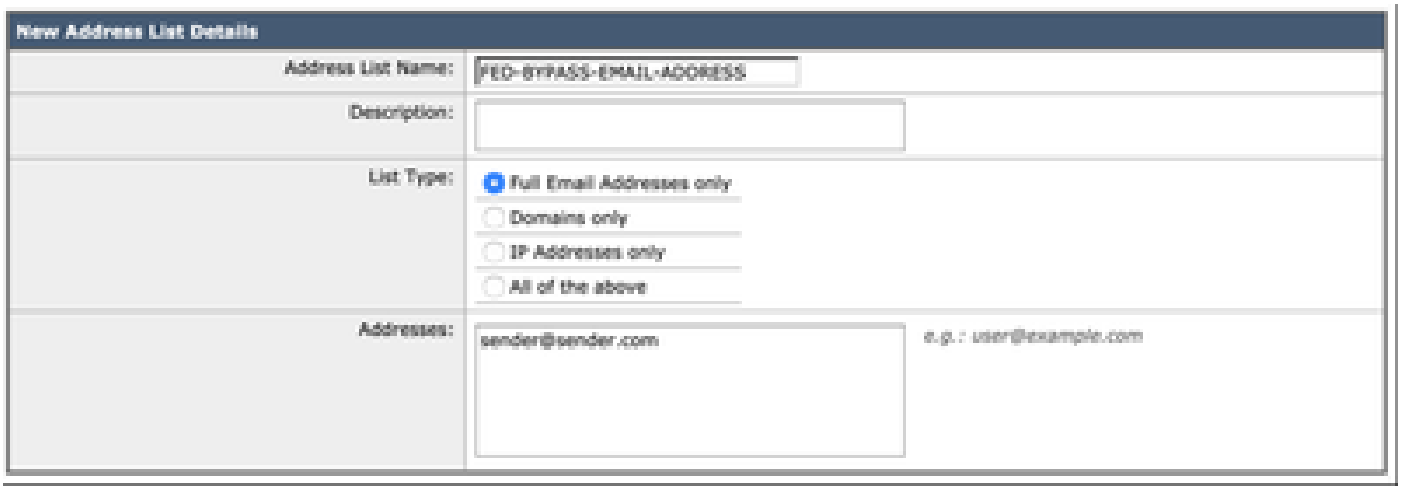
注意：由於大多數域不是已註冊的置換，因此DNS發件人驗證可針對這些域提供保護。如果您選擇使用詞典專案，請只注意註冊的網域，並確定每個詞典不超過500-600個專案。

圖8.用於偽造郵件檢測的自定義目錄



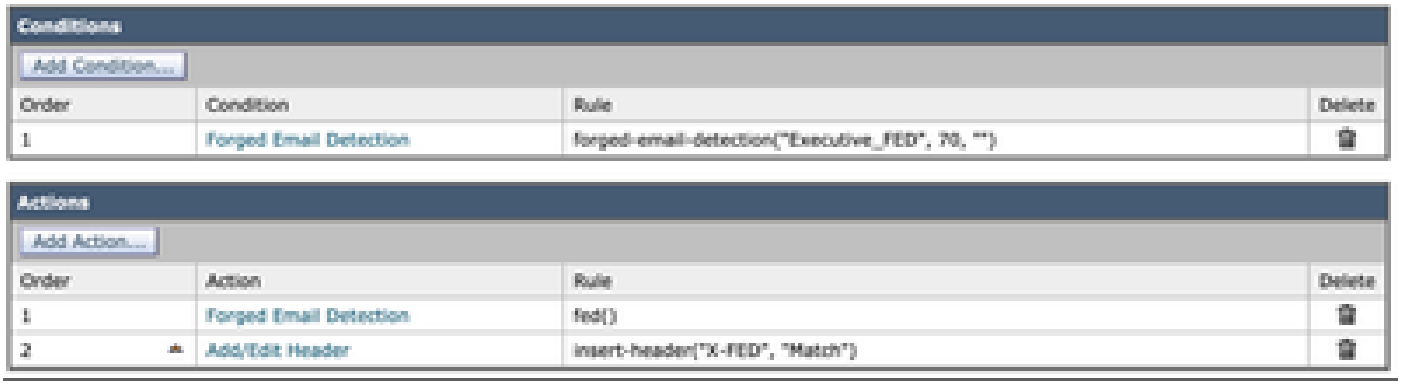
可以選擇在信封傳送中增加電子郵件域的例外條件，以繞過FED檢測。或者，可以建立自定義地址清單，以繞過FED檢查對FromHeader中顯示的電子郵件地址清單的檢查（圖9）。

圖9.建立地址清單以繞過FED檢查



應用「偽造郵件檢測」專有操作刪除「發件人」值，並檢視郵件收件箱中的實際信封發件人郵件地址。然後，在符合條件的郵件上增加新的X-header（例如，X-FED=Match），並繼續將郵件傳遞到下一層檢查（圖10），而不是應用最終操作。

圖10.FED的建議內容篩選器設定

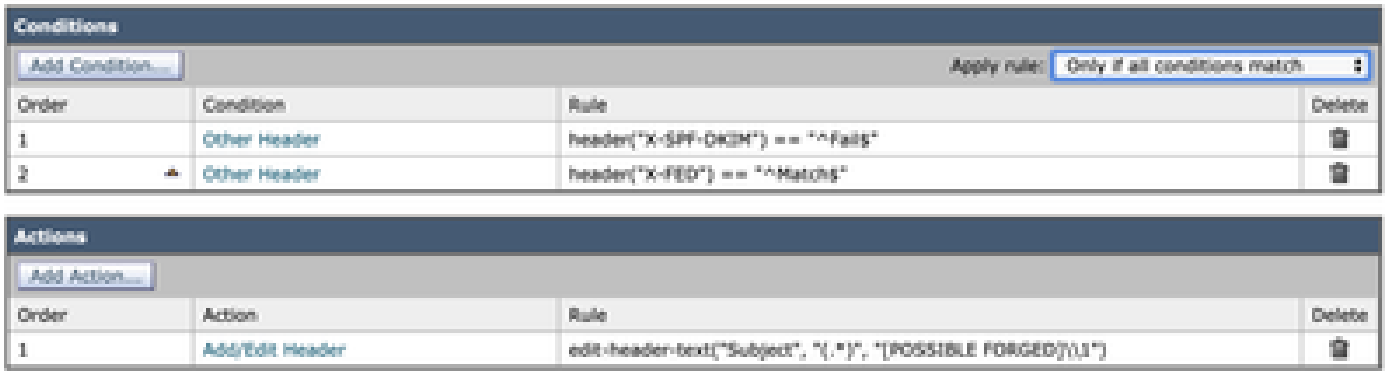


第7層：確定身份的欺騙電子郵件

透過引用管道中各種安全功能（如SPF/ DKIM Enforcemen和FE生成的X報頭資訊）的其他判決，辨識真正的欺騙活動會更加有效。例如，管理員可以建立一個內容過濾器來辨識由於SPF / DKIM驗證結果失敗(X-SPF-DKIM=Fail)而增加有新X報頭的郵件以及哪些From報頭與FED詞典條目匹配(X-FED=Match)。

建議的操作可以是隔離郵件並通知收件人，或者繼續傳遞原始郵件，但將[可能偽造]的字詞作為警告傳送給收件人，如圖所示（圖11）。

圖11.將所有X頁首組合成單一（最終）規則



第8層：防止網路釣魚URL

針對網路釣魚連結的保護已整合到Cisco Secure Email中的URL和爆發過濾中。混合威脅將欺騙和網路釣魚郵件結合在一起，使目標看起來更加合法。啟用爆發過濾對於幫助即時檢測、分析和阻止此類威脅至關重要。我們有必要知道，URL信譽是在反垃圾郵件引擎中進行評估的，可用於垃圾郵件檢測決策的一部分。如果反垃圾郵件引擎不停止包含URL為垃圾郵件的郵件，則會透過安全管道後部的URL和爆發過濾對其進行評估。

建議：建立內容過濾器規則，阻止具有惡意信譽分數的URL，並將具有中性信譽分數的URL重定向到思科安全代理（圖12）。透過啟用郵件修改啟用威脅爆發過濾器。URL重寫允許思科安全代理分析可疑URL（圖13）。有關詳細資訊，請訪問：為安全電子郵件網關和雲網關配置URL過濾

圖12.URL信譽的內容過濾器

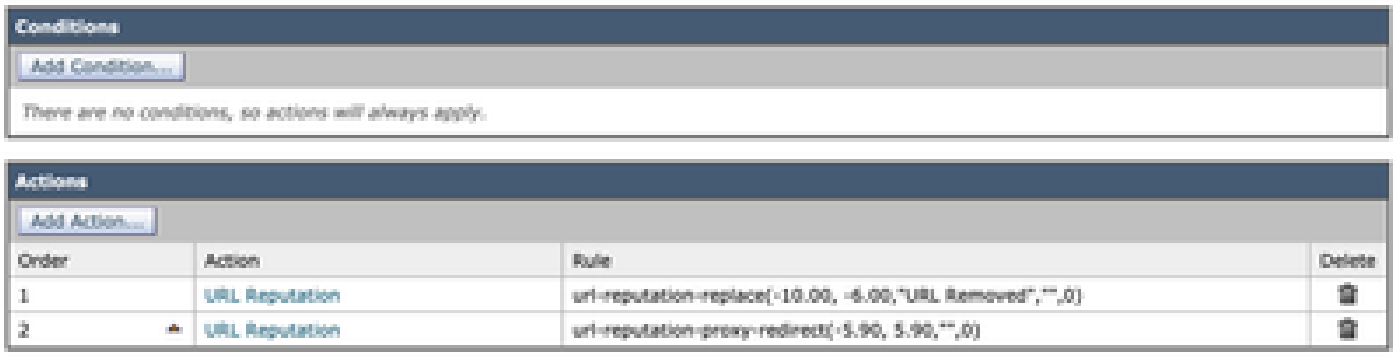
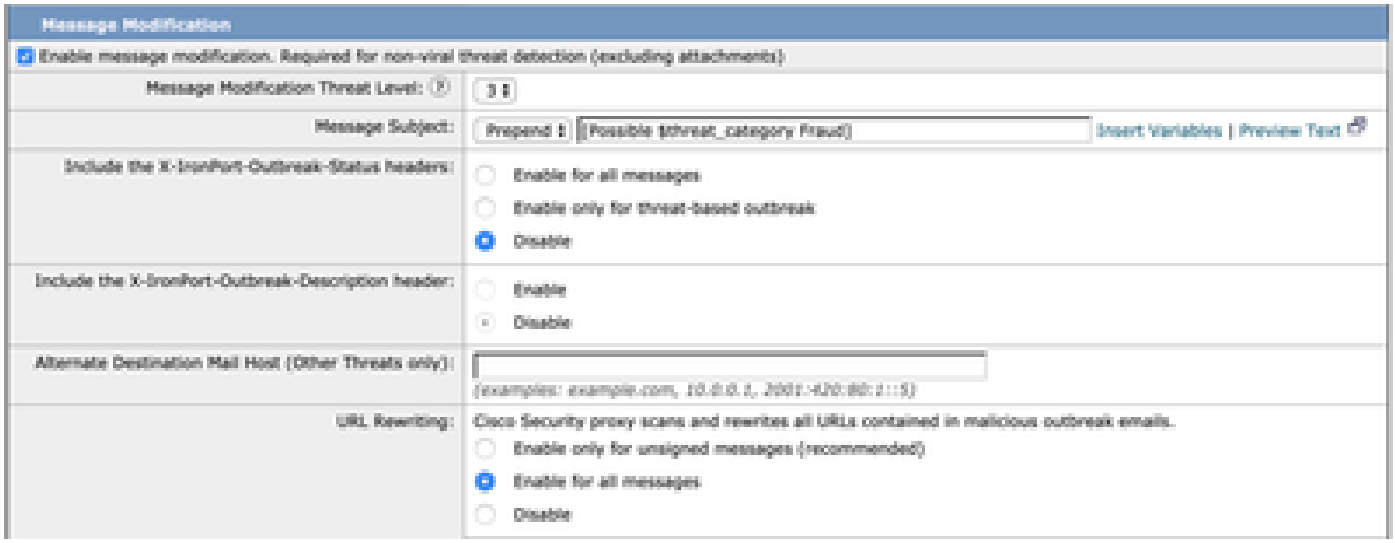


圖13.在爆發過濾中啟用URL重寫



第9層：透過思科安全郵件威脅防禦(ETD)增強欺騙檢測功能

思科提供電郵威脅防禦，這是利用思科Talos的卓越威脅情報的雲本地解決方案。它具備支援API的架構，可加快響應速度、完整的電郵可視性（包括內部電郵）、提供更好情景資訊的通話檢視，以及用於自動或手動補救Microsoft 365郵箱中潛在威脅的工具。有關詳細資訊，請訪問思科安全電子郵件威脅防禦產品手冊。

思科安全郵件威脅防禦使用發件人身份驗證和BEC檢測功能打擊網路釣魚。它整合了機器學習和人工智慧引擎，將本地身份和關係模型與即時行為分析相結合，以防禦基於身份欺騙的威脅。它在組織內部和個人之間構建值得信賴的電子郵件行為模型。電子郵件威脅防禦除了其他重要功能外，還具有以下優勢：

- 利用高級威脅檢測功能發現已知、新興和有針對性的威脅。
- 辨識惡意技術並獲得特定業務風險的情景。
- 快速搜尋危險威脅並進行即時補救。
- 利用可搜尋的威脅遙測技術將威脅分類，並瞭解組織的哪些部分最容易受到攻擊。

圖14.思科安全郵件威脅防禦提供有關您的組織如何成為攻擊目標的資訊。

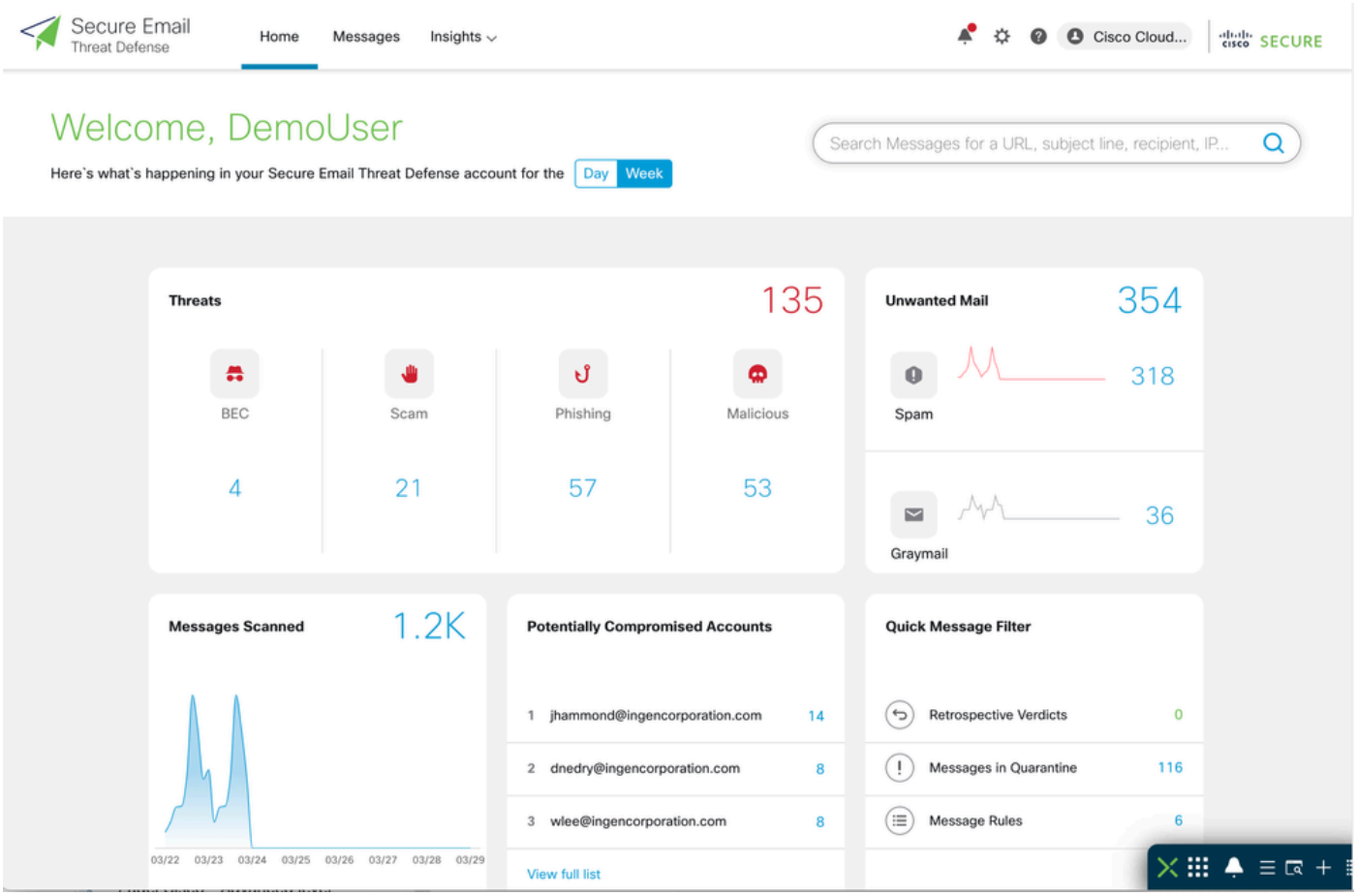
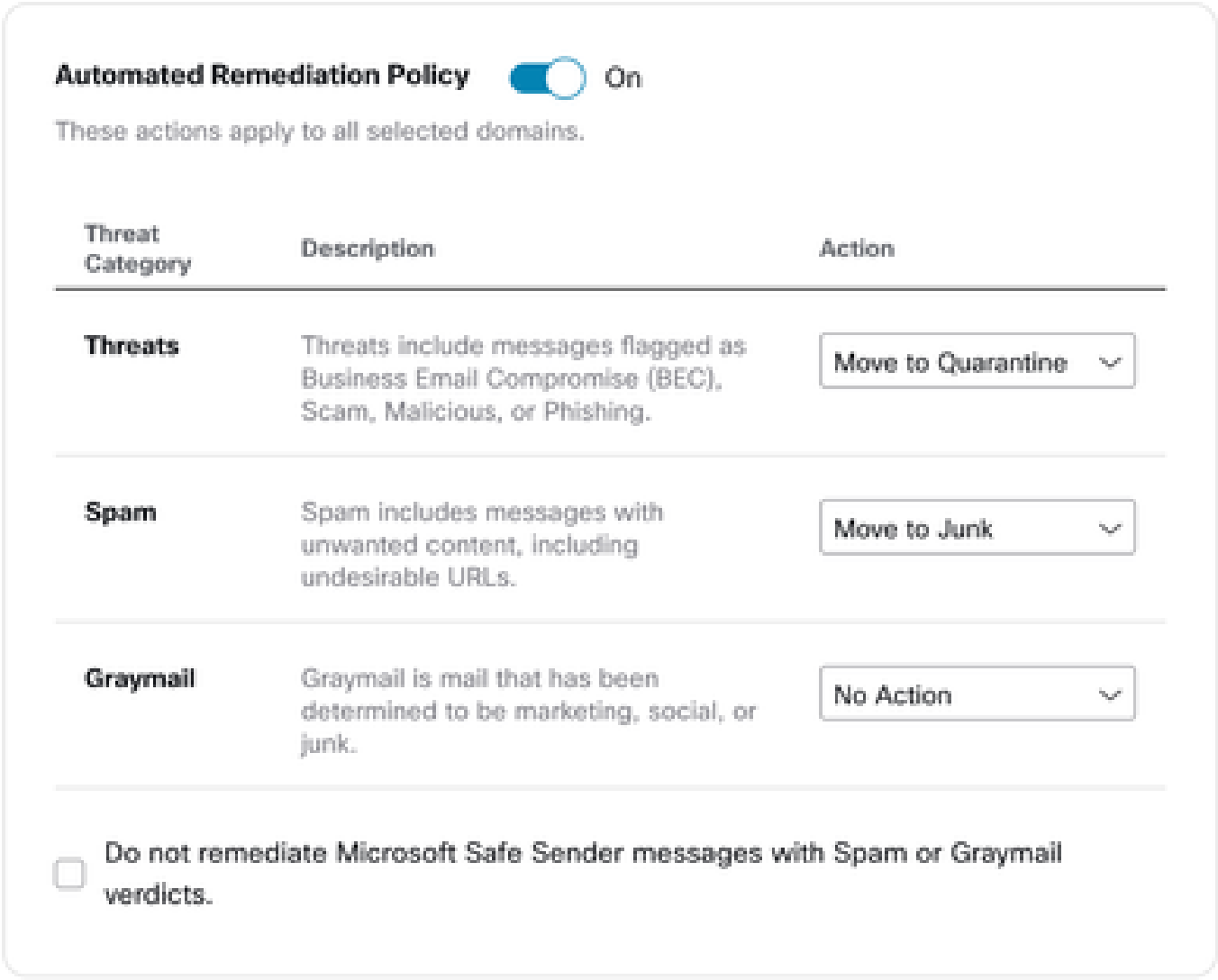


圖15.思科郵件威脅防禦策略設定自動確定郵件是否與所選威脅類別匹配



您還能如何防止欺騙

許多欺騙可以透過一些簡單的預防措施進行補救，這些預防措施包括但不限於以下幾項：

- 將允許主機訪問表(HAT)中列出的域限制在極少數核心業務合作夥伴。
- 如果您已經建立了SPOOF_ALLOW發件人組中的成員，請繼續跟蹤和更新該組中的成員，並使用最佳做法連結中提供的說明。
- 啟用灰色郵件檢測，並將它們放在垃圾郵件隔離區中。

但最重要的是，啟用SPF、DKIM和DMARC並適在地實施它們。但是，有關發佈SPF、DKIM和DMARC記錄的指南不在本文檔的討論範圍之內。有關這方面的資訊，請參閱以下白皮書：[電子郵件身份驗證最佳實踐：部署SPF、DKIM和DMARC的最佳方法](#)。

瞭解補救電子郵件攻擊所面臨的挑戰，例如此處討論的欺騙活動。如果您對實施這些最佳實踐有任何疑問，請與Cisco技術支援聯絡並建立一個案例。或者，請與您的思科客戶團隊聯絡，獲取解決方案和設計手冊。有關Cisco Secure Email的詳細資訊，請參閱Cisco Secure Email 網站。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。