

通過思科郵件安全裝置(ESA)進入組織的垃圾郵件

目錄

[簡介](#)

[方法](#)

[1.合法郵件/行銷郵件](#)

[2.未正確更新反垃圾郵件](#)

[3.郵件策略或郵件過濾器](#)

[4.郵件流策略](#)

[5.郵件為垃圾郵件](#)

簡介

本文檔介紹垃圾郵件進入組織的五種方法。

方法

1.合法郵件/行銷郵件

合法郵件已被使用者選擇，或者其名稱已出售給其他組織。在第一種情況下，使用者需要採取措施取消訂閱清單。如果是後者，請將郵件再次提交到spam@access.ironport.com，以便全域性更新反垃圾郵件定義，從而提高ESA的總體垃圾郵件捕獲率。在傳入郵件策略中啟用行銷郵件可能有助於改變此郵件被視為「行銷」而不是「垃圾郵件」的感覺。

2.未正確更新反垃圾郵件

反垃圾郵件已禁用或功能金鑰已過期。若要檢查並檢視是否正在更新Anti-Spam，請轉到**GUI >安全服務> IronPort Anti-Spam**。在此面板中，您應該會看到過去6小時內規則集或引擎的更新。此外，您還可以從頂部此頁籤中確保啟用反垃圾郵件服務。要檢視「功能金鑰」狀態，可以轉至「系統管理」頁籤>「功能金鑰」以檢查「反垃圾郵件」金鑰的狀態。

3.郵件策略或郵件過濾器

如果按客戶郵件策略為特定發件人或收件人禁用反垃圾郵件安全引擎，則垃圾郵件會進入您的組織。另一種跳過垃圾郵件過濾的方法是通過郵件過濾器(CLI:filters命令)。

4.郵件流策略

使用消息的ICID對消息進行分類。在這種情況下，反垃圾郵件安全功能可能關閉，這將覆蓋郵件策略。您可以通過檢視郵件日誌來確定這一點，在日誌中，您首先需要複查ICID才能瞭解郵件被分類到哪個SenderGroup。從這裡檢視關聯的郵件流策略。如果您的AllowList中有大量條目，您可能需要檢查某些進入的郵件，看看它們是否已被反垃圾郵件引擎掃描。開啟郵件的信頭並查詢信頭X-IronPort-Spam，如果存在此信頭，則表示郵件確實通過引擎。

5.郵件為垃圾郵件

該郵件是實際的垃圾郵件。您已確認反垃圾郵件引擎已使用郵件跟蹤功能掃描郵件（在郵件跟蹤中查詢「CASE」）。如果案件判決為否定且您認為郵件為垃圾郵件，請將原始郵件提交到 spam@access.ironport.com。這可能是因為剛剛發佈了一個新的垃圾郵件威脅，或者是一個經過重新設計的舊威脅。

垃圾郵件的提交處理既是一個自動過程，也是一個手動過程，不會針對您的特定提交提供任何反饋。您可以隨時聯絡Cisco TAC並請求評估和響應。