ESA上的常見配置錯誤

目錄

簡介

本文檔介紹郵件安全裝置(ESA)上的常見配置錯誤。

ESA上的常見配置錯誤是什麼？

無論您是正在設定新的評估還是正在檢視現有配置，都可以參考常見配置錯誤的清單。

帽子

- 請勿將正的SBRS評分（如+5或+7）放入允許清單。9.0到10.0的範圍是可以接受的，但分數越低，垃圾郵件通過的可能性就越高。
- 除非您確實需要並瞭解這些資訊，否則請禁用UNKNOWNLIST、信封發件人DNS驗證和連線主機DNS驗證。
- 不要在每個郵件流策略中更改郵件大小和其他策略設定，請轉到「郵件流策略」選單並選擇最後一個選項「預設策略引數」。
- 將大多數發件人的最大連線數限製為三個，並將此設定為新郵件流策略的預設值。
- 檢查BLOCKLIST中是否包含從–10.0到–2.0的SenderBase評分。文檔和設定嚮導過於保守；當前在此範圍內沒有誤報。

政策

- 在誰獲得策略後命名策略，而不是指定策略執行的操作。將任何內容過濾器命名為它們的用途，並使用縮寫，如Q_basic_attachments、D_spoofers、Strip_Multi-Media，其中Q表示隔離，D表示丟棄。
- 非預設策略應對反垃圾郵件、防病毒、內容過濾器和爆發過濾器使用「使用預設設定」，但您真正需要特殊設定的情況除外。如果不需要，請不要在每個策略中重新建立這些設定。
- 取消勾選「Drop infected attachments」（丟棄感染病毒的附件），否則您將會在病毒已被清除的地方傳遞許多空白的電子郵件。
- 出站防病毒設定應通知發件人，而不是收件人

- 應在出站時禁用爆發過濾器和反垃圾郵件

傳入中繼

如果「Monitor > Overview」顯示來自您自己的伺服器和域的連線，您需要將它們新增到傳入中繼設定。在使用GUI時，一個非常常見的錯誤是認為您已經啟用了傳入中繼功能，而您所做的只是將條目新增到表中。此外：

- 為它們新增一個特殊的HAT發件人組（在ALLOWLIST上）以用於報告目的。 選擇無速率限制或DHAP，但垃圾郵件和病毒檢測正常。
- 新增郵件過濾器以匹配您的BLOCKLIST策略操作。例如：

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

在極少數情況下重新注入電子郵件（例如，通過入站郵件策略重新處理使用者間郵件），過濾器還需要免除重新注入介面。通常情況下，這不是必需的。

DNS

許多客戶迫使ESA查詢其內部DNS伺服器而失去了習慣。在大多數安裝中，我們需要的100%的DNS記錄都在Internet上，而不是在內部DNS中。查詢Internet根伺服器更有意義，可以減少內部DNS上的轉發負載。

郵件和內容過濾器

最常見的錯誤是將匹配條件放在內容過濾器不需要的地方。 大多數過濾器應列出某些操作，但條件應留空。過濾器將始終為*true*，並且始終運行。通過根據需要建立新的傳入或傳出郵件策略，並將此過濾器應用到策略，可以控制哪些使用者/策略接收這些操作。以下是錯誤和正確的示例：

- 在郵件過濾器中使用rcpt-to條件幾乎總是錯誤。正確的過程是編寫傳入內容過濾器，並通過新增基於收件人的傳入郵件策略使其特定於特定的使用者。
- 對是否存在附件進行內容過濾器測試，然後丟棄該附件幾乎總是錯誤。正確的方法是始終丟棄該附件，而不測試其是否存在。
- 使用deliver()幾乎總是錯誤。 「傳送」表示跳過任何剩餘的過濾器，然後傳送。如果只想傳遞而不跳過其餘過濾器，則不需要任何顯式操作（隱式傳遞）。

開放中繼預防

某些服務將檢查您的消息傳輸代理(MTA)是否接受可能導致開放中繼條件的地址。由於將MTA保留為正常工作的開放中繼是不好的，這些站點可能會將您新增到阻止清單中，除非您在SMTP會話中拒絕這些危險地址。

為它們新增一個特殊的HAT發件人組（在ALLOWLIST上）以用於報告目的。選擇無速率限制或DHAP，但允許垃圾郵件和病毒檢測。

- 更改為嚴格地址解析（預設設定為「鬆動」）。 這是防止地址中出現雙@符號所必需的。

- 拒絕（非刪除）無效字元。這對於防止地址中出現雙@符號也是必要的。
- 拒絕（不接受）文字，並輸入以下字元：*%!\\/?

相關資訊

- 技術支援與文件 - Cisco Systems