思科電子郵件安全裝置(ESA)反垃圾郵件效能檢查表

目錄

簡介

以下步驟和建議是用於減少通過ESA的垃圾郵件數量的「最佳實踐」。請注意，每個客戶都不同，其中一些建議可能會增加分類為垃圾郵件（誤報）的合法電子郵件數量。

基本設定

1. 確保開啟反垃圾郵件：

   檢查以確保所有MX記錄（包括低優先順序）MX記錄都通過ESA中繼郵件。確保裝置具有有效的反垃圾郵件功能金鑰。確保為所有適當的傳入郵件策略啟用反垃圾郵件。

2. 驗證是否正在接收反垃圾郵件規則更新。檢查以確認Security Services **>** **Anti**-Spam下的更新的最近時間戳是否來自最近2小時內。

3. 確保郵件正被反垃圾郵件掃描：

   檢查以下標題的未命中垃圾郵件示例：X-IronPort-Anti-Spam-Result:如果該報頭丟失：

   檢查以確保沒有任何允許清單條目或過濾器導致垃圾郵件繞過垃圾郵件掃描（請參閱下文）。檢查以確保郵件不會繞過掃描，因為它們超過了郵件掃描大小上限(預設為262144位元組)。減少此設定不會顯著提高效能，並且可能會導致丟失垃圾郵件。在評估過程中，還必須確保IPAS設定與測試的任何其他產品相同。檢查每個HAT條目並確認所有入站郵件流策略的「spam_check=on」。只要預設設定有「spam_check= on」，並且沒有任何郵件流策略明確將其關閉，就會正確配置。請特別注意TRUSTED/allowLIST設定。客戶經常會無意中將發件人新增到其轉發垃圾郵件的許可清單中 — 例如，通過將同時轉發垃圾郵件和合法電子郵件的ISP或合作夥伴的域新增到allowLIST發件人組中。

   快速檢查郵件過濾器，確保沒有任何「skip-spamcheck」過濾器。 如果有，請確保他們正在做他們應該做的事情（請記住，匹配單個rcpt-to可以匹配具有30個以上收件人的郵件）。

   查詢最近的SPAM示例（時間、日期、rcpt等），並參考mail_logs以檢視所發生的情況。確認Anti-Spam返回否定裁決。

4. 確保您正在對垃圾郵件肯定郵件執行所需的操作。檢查入站郵件策略，瞭解如何處理反垃圾郵件裁決。確保在預設策略中丟棄或隔離垃圾郵件正資訊和可疑郵件，並確保所有其他策略使用預設行為或故意覆蓋預設行為。

5. 如果誤報比漏報的垃圾郵件更少，則應用更積極的垃圾郵件閾值：

   如果誤報與「特定」閾值無關，請將垃圾郵件正閾值降低到80（預設為90）。

   如果誤報與「可疑」閾值無關，則將可疑垃圾郵件閾值降低到40（預設值為50）。

   如果大部分垃圾郵件投訴來自某個收件人子集，則您可以為這些具有較低垃圾郵件閾值的使用者建立單獨的郵件策略，以便更主動地僅為這些收件人進行篩選。

   對這些價值觀的改變不應掉以輕心，也不應在沒有確鑿資料來確認何為消除效果的情況下就予以頒佈。

   此外，不必為了避免誤報而在另一個方向上調整值。請確保將誤報和漏報提交給TAC。

6. 最佳化SBRS設定和HAT策略：

   大多陣列織都樂於將SBRS -10至–3.0新增到其阻止清單中，將SBRS -3.0至–1.0新增到其可疑清單中。更積極的客戶可以阻止將SBRS -10到–2.0，並將–2.0到–0.6新增到SUSPECTLIST。

   在某些情況下，發件人尚未獲得SenderBase信譽得分這一事實證明此發件人可能是垃圾郵件傳送者。您可以將SBRS「none」直接新增到獲得「限制」策略的發件人組，例如，新增到SUSPECT發件人組。

   對於「限制」策略，將每小時最大收件人數更改為5。

   考慮建立多個「限制」策略以實施每小時不同的收件人限制 — 例如，對SBRS介於–2和–1到5個收件人之間的發件人和對SBRS介於–1和0到20個收件人之間的發件人進行速率限制。

7. 為「已限制」郵件流策略啟用發件人驗證：

   客戶可能會選擇將不存在或未正確配置DNS的發件人新增到SUSPECTLIST發件人組。

   DNS中不存在連線主機PTR記錄。由於臨時DNS故障，連線主機PTR記錄查詢失敗。

   連線主機反向DNS查詢(PTR)與正向DNS查詢(A)不匹配。

   由於DNS配置不當的發件人可能會產生誤報，因此客戶可能需要設定單獨的郵件流策略，該策略返回一個自定義4xx響應，指示拒絕原因郵件。

   有關發件人驗證的詳細資訊，請檢視「聯機幫助」或《AsyncOS使用手冊》

8. 啟用LDAP接受和目錄收集攻擊保護：

   許多垃圾郵件傳送者向大量無效地址傳送電子郵件，因此阻止傳送到無效收件人的發件人也可

以減少垃圾郵件。

如果LDAP接受已開啟，請確保也為每個入站監聽程式配置了目錄蒐集保護(DHAP)，每個IP的最大無效嘗試次數為5到10次。

9. 啟用內容詞典：

   您的ESA附帶兩個內容詞典：profanity.txt和sexual_content.txt。雖然使用這些詞典可能會產生誤報，但一些客戶發現，過濾郵件流中的不當詞語可能會降低「錯誤的人」收到「錯誤電子郵件」的風險。 這些過濾器只能通過為特定郵件策略中的一組使用者啟用它們來應用於「噪音輪子」。

10. 向思科TAC報告錯誤分類消息。

11. 要防止大量誤報，應禁用出站掃描的SBRS。這是因為SBRS會檢視傳入IP的信譽，而在內部網路中，大多數IP是動態的。請按照下一節中的步驟操作。

啟用SBNP

1. 確保入站和出站郵件位於不同的偵聽程式上。

2. 對下面的出站郵件禁用SenderBase查詢。要從GUI執行此操作，請轉至Network > Listeners，選擇任何出站偵聽器，選擇「Advanced」，然後取消選中「Use SenderBase IP profiling」旁邊的框。

   SenderBase網路參與(SBNP)可以顯著提高信譽過濾器、反垃圾郵件和病毒爆發過濾器的效力。如果使用反垃圾郵件功能，SBNP對效能沒有明顯影響，並且高度安全。

   附註：您的組織收到的垃圾郵件數量將隨時間變化。可能更多垃圾郵件通過ESA，只是因為您收到的垃圾郵件比過去更多。您可以通過檢視Incoming Mail Overview頁面並新增「stopped by reputation filtering」和「spam messages detected」行專案來跟蹤此行為。

SBRS原理

誤報的最大擔憂是重要電子郵件可能會丟失。在這種情況下，隔離或丟棄垃圾郵件正電郵的做法存在問題。如果將合法電子郵件傳送到隔離區或垃圾郵件資料夾，則需要主動搜尋才能進入，並「注意」該郵件被誤分類為垃圾郵件。

與之相反，阻止清單和限費率電子郵件被阻止的方式是立即通知發件人。如果此發件人不是垃圾郵件傳送者，他們可能會找到其他與您聯絡的方法。事實上，作為一項整體政策，預設阻止然後根據請求接受可信的合作夥伴，對於某些企業而言是更好的選擇。

如果設定得當，頻寬限制很少會影響合作夥伴，但會提供保護，防止域感染病毒。扼殺也讓垃圾郵件傳送者望而卻步。我們瞭解一種垃圾郵件製造者技術，可購買大量IP、生成足夠「好」的電子郵件以獲得SBRS得分，然後開始傳送垃圾郵件。較大的可疑清單範圍應該會捕獲這些郵件，限制它們造成的損害，並且最終可能導致它們停止向您的域傳送垃圾郵件。