SPF配置和最佳實踐

目錄

簡介

本檔案介紹思科電子郵件安全裝置(ESA)上使用傳送者原則框架(SPF)的不同案例。

必要條件

思科建議您瞭解以下主題：

- Cisco ESA
- AsyncOS的所有版本

什麼是SPF?

Sender Policy Framework(SPF)是一個簡單的電子郵件驗證系統，旨在通過提供一種機制來檢測電子郵件欺騙，該機制允許接收郵件交換器檢查來自域的傳入郵件是否正由該域管理員授權的主機傳送。域的授權傳送主機清單以特殊格式的TXT記錄的形式發佈在該域的域名系統(DNS)記錄中。電子郵件垃圾郵件和網路釣魚經常使用偽造的發件人地址，因此發佈和檢查SPF記錄可以視為反垃圾郵件技術。

ESA是否會受到很大影響？

從CPU前景看，效能不會受到巨大影響。但是，啟用SPF驗證將增加DNS查詢和DNS流量的數量。對於每條消息，ESA可能必須啟動1-3個SPF DNS查詢，這將導致DNS快取早於以前過期。因此，ESA也將為其他進程生成更多查詢。

除了上述資訊外，SPF記錄將是TXT記錄，它可能大於常規DNS記錄，並可能導致一些額外的DNS流量。

如何啟用SPF?

以下說明來自《高級使用手冊》關於設定SPF驗證的說明：

要在預設郵件流策略上啟用SPF/系統獨立資料格式(SIDF):

1. 按一下**Mail Policies > Mail Flow Policy**。
2. 按一下**Default Policy Parameters**。
3. 在預設策略引數中，檢視**安全功能**部分。
4. 在SPF/SIDF Verification部分中，按一下**Yes**。
5. 設定一致性級別（預設值為SIDF相容）。 此選項可讓您確定要使用的SPF或SIDF驗證標準。除了SIDF一致性之外，您還可以選擇與SIDF相容，該功能將SPF和SIDF相結合。*《最終使用手冊》中提供了合規級別詳細資訊。*
6. 如果選擇與SIDF相容的一致性級別，請配置驗證是否將PRA身份的**通過**結果降級為**無**(如果有Resent-Sender:或Resent-From:郵件中存在標頭。出於安全考慮，您可以選擇此選項。
7. 如果選擇了SPF的一致性級別，請配置是否根據HELO身份執行測試。可以使用此選項通過禁用HELO檢查來提高效能。這非常有用，因為spf-passed過濾器規則首先檢查PRA或MAIL FROM身份。裝置僅對SPF一致性級別執行HELO檢查。

若要對SPF驗證結果執行操作，請新增內容篩選器：

1. 為每種SPF/SIDF驗證型別建立spf-status內容過濾器。使用命名約定來指示驗證型別。例如，對通過SPF/SIDF驗證的郵件使用**SPF-Passed**，對由於在驗證過程中出現暫時性錯誤而未通過的郵件使用**SPF-TempErr**。有關建立spf-status內容過濾器的資訊，請參閱GUI中的spf-status內容過濾器規則。
2. 處理一些SPF/SIDF驗證的郵件後，按一下**Monitor > Content Filters**以檢視觸發每個經過SPF/SIDF驗證的內容過濾器的郵件數。

「Helo測試」的開關是什麼意思？如果某個域的Helo測試失敗，將會發生什麼情況？

如果選擇了SPF的一致性級別，請配置是否根據HELO身份執行測試。可以使用此選項通過禁用HELO檢查來提高效能。這非常有用，因為spf-passed過濾器規則首先檢查PRA或MAIL FROM身份。裝置僅對SPF一致性級別執行HELO檢查。

有效的SPF記錄

要通過SPF HELO檢查，請確保為每個傳送MTA包含SPF記錄（與域分開）。 如果不包括此記錄，HELO檢查可能會導致HELO身份的**None**判定。如果您注意到您域的SPF發件人返回了大量的**None**裁決，則這些發件人可能未為每個傳送MTA包含SPF記錄。

如果未配置郵件/內容過濾器，則郵件將被傳送。同樣地，您可以對每個SPF/SIDF判定使用消息/內容過濾器執行某些操作。

下列哪種最佳方法僅針對一個外部域啟用它？

要啟用某個域的SPF，可能需要使用啟用SPF的郵件流策略定義新的發件人組；然後建立前面提到的過濾器。

是否可以對可疑垃圾郵件啟用SPF檢查？

思科反垃圾郵件會在計算垃圾郵件分數時考慮許多因素。具有可驗證的SPF記錄可能會降低垃圾郵件分數，但仍有可能將這些郵件捕獲為可疑垃圾郵件。

最佳可能的解決方案是允許將發件人IP地址列出，或建立郵件過濾器來跳過具有多種條件（遠端IP、郵件發件人、X-skipspamcheck標頭等）的垃圾郵件檢查。 傳送伺服器可以新增報頭，以標識來自其他消息的一種型別。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 電子郵件驗證最佳實踐 — 部署SPF/DKIM/DMARC
- 技術支援與文件 - Cisco Systems