設定安全電子郵件閘道的寄件者網域例外清單

目錄

簡介

本檔案說明「新變更」，即思科安全電子郵件閘道(SEG)的寄件者網域信譽(SDR)設定選項「網域例外清單」。

作者：Chris Arellano Cisco TAC工程師。

必要條件

需要有關SEG設定和配置的一般知識。

適用於思科安全郵件網關(SEG)的AsyncOS 15.0和更高版本。

對SDR功能的一般瞭解。

需求

啟用發件人域信譽服務並使用「僅域」選項建立地址清單。

採用元件

- 本文中的資訊係根據以下軟體和硬體版本：
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1及更高版本。
- SEG發件人域信譽。
- 地址清單。

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。

概觀

發件人域信譽是一項雲服務，可收集多個發件人值、導出裁決並提供選項以對這些裁決採取行動。SDR允許設定透過使用應用於域例外清單的地址清單繞過受信任的域。

在SEG 15.0之前的AsynOS版本中，SDR域例外清單有2個選項：

- 已啟用=匹配信封來源，域繞過SDR操作。
- 停用=僅當全部存在時匹配：信封發件人+友好發件人+答覆收件人+ SPF + DKIM + DMARC。

SEG 15.0和更新版本的域例外清單：

- 已啟用=匹配信封來源，域繞過SDR操作。
- Disabled =如果域存在於以下任何值中，則匹配：
  - HELO
  - RDNS
  - 起始信封
  - 從
  - 回覆

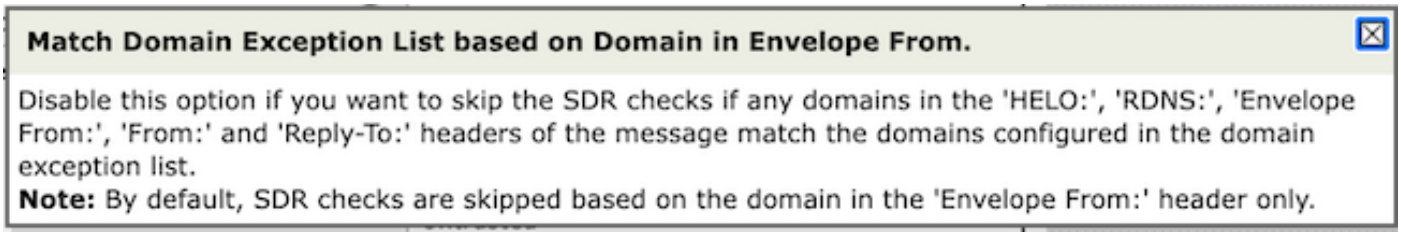
設定

本文的重點是新的域例外清單配置。使用手冊中提供了完整的SDR設定和配置。

在WebUI中導航到安全服務 > 域信譽。

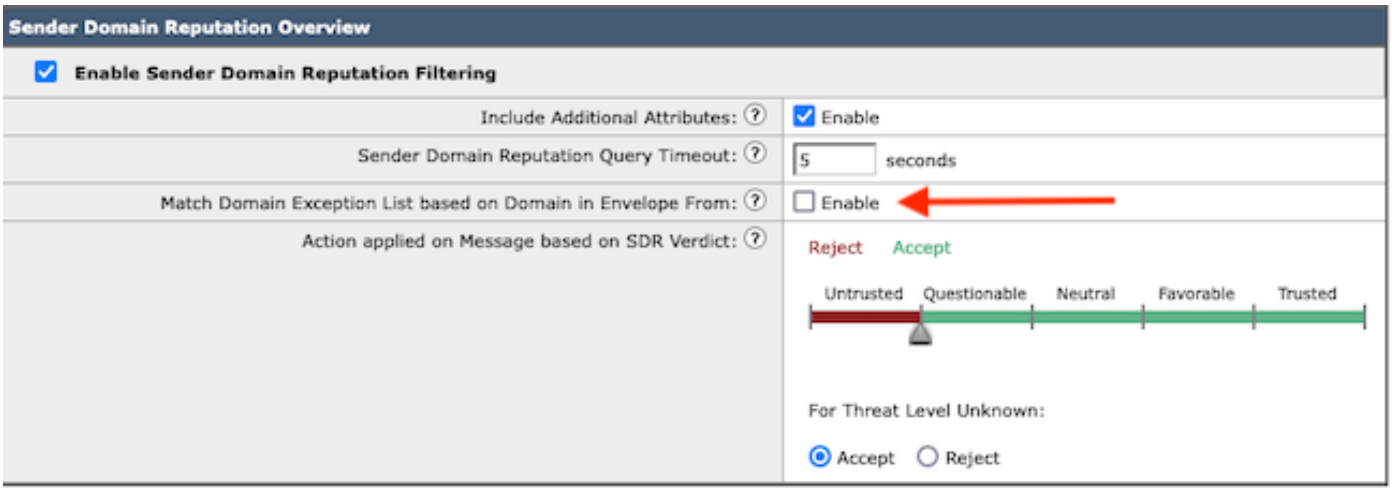
- 預設情況下，基於信封發件人的域名部分匹配域例外清單選項處於啟用狀態。
  - 如果啟用Checkbox，則只有「Envelope From， header」（信封發件人，信頭）值匹配，如果被定罪，則忽略郵件。
  - 如果Checkbox為空，則SDR域例外清單將匹配以下任何報頭欄位「HELO：」、「RDNS：」、「Envelope From：」、「From：」和「Reply-To：」報頭，如果被定罪，將匹配並繞過該消息。

如果選取相關的？資訊圖示，則會顯示設定詳細資訊。



注意：預設情況下，僅根據「信封發件人：」信頭中的域跳過SDR檢查。

選擇Edit Global Settings以刪除覈取方塊選項，如下圖所示：



域例外清單本身是包含域名的地址清單。

驗證

要使用新的Disable功能驗證功能是否正常工作，您需要向SEG傳送測試消息，並且在5個報頭值之一中具有匹配的域值。

在mail_logs的早期階段會出現一個示例日誌，該日誌指示全局異常清單內的異常以及在郵件流策略內匹配的異常：

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

指示異常的示例日誌將同時包含域和異常清單名稱。

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

疑難排解

如果對所選消息判定準確性產生疑問，則記錄這些值，並與消息跟蹤進行比較。

- 記錄全局域信譽設定 > 安全設定 > 域信譽。
- 驗證在全局域信譽設定中配置的關聯地址清單。
- 根據郵件跟蹤驗證匹配的郵件流策略。
- 檢查並記錄已配置域例外清單的任何郵件過濾器或內容過濾器的詳細資訊。

收集郵件跟蹤、郵件日誌和原始郵件信頭。

- 如果消息上的Global異常匹配，則沒有Domain Reputation的日誌條目，只是一行表示匹配的域。

- 如果消息上的「全局例外清單」不匹配，則存在域信譽的日誌條目，可從其中比較值。
    - 資訊：MID 16 SDR：請求SDR的域：反向DNS主機：不存在，helo：mail1.example.com，env-from：test2.example.com，header-from：te destination.example.com，回覆：test2.example.com
- 電子郵件標頭包含單個電子郵件中顯示的與設定進行比較的5個值中的任意一個。

收集所有資料後，檢查是否存在匹配項以確定功能是否正確。

相關資訊

- 電子郵件安全設定指南
- 用於支援指南的思科安全郵件網關啟動頁面

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）。