如何繞過郵件安全裝置的DMARC檢查

目錄

簡介

本文說明如何繞過郵件安全裝置(ESA)上的基於域的郵件身份驗證、報告和一致性(DMARC)檢查。請參閱有關電子郵件身份驗證的簡介。

驗證DMARC

DMARC是一項技術規範，旨在降低電子郵件濫用可能性。DMARC使用發件人策略框架(SPF)和域金鑰識別郵件(DKIM)機制，對電子郵件接收者執行電子郵件身份驗證的方式進行標準化。為了通過DMARC驗證，電子郵件必須至少通過其中一個驗證機制，並且驗證識別符號必須符合RFC 5322。

裝置允許您：

- 使用DMARC驗證傳入的電子郵件。
- 定義配置檔案以覆蓋（接受、隔離或拒絕）域所有者的策略。
- 向域所有者傳送反饋報告，這有助於增強其身份驗證部署。
- 如果DMARC聚合報告大小超過10 MB或DMARC記錄的聚合報告(RUA)標籤中指定的大小，則向域所有者傳送傳遞錯誤報告。

AsyncOS可以處理在2013年3月31日提交給網際網路工程任務組(IETF)的符合DMARC規範的電子郵件。有關詳細資訊，請參閱http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02。

> **附註**：裝置不會對DMARC記錄格式錯誤的域中的郵件執行DMARC驗證。但是，裝置可以接收和處理此類消息。

配置DMARC旁路

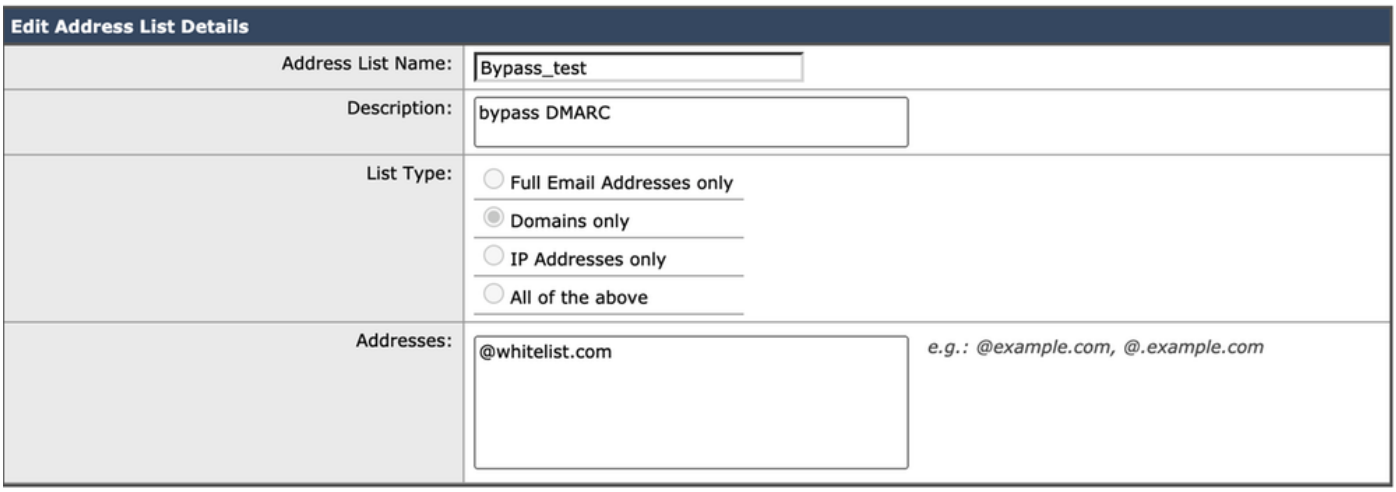
如果作為管理員，您的要求是跳過對來自特定發件人的郵件的DMARC驗證，您必須執行幾個步驟才能成功繞過該步驟。有關步驟的概述，請參閱以下內容：

> **附註**：使用完整電子郵件地址或域建立的地址清單只能用於繞過DMARC驗證。可以使用帶有**以上所有**選項的**地址清單**。但是，只有域/完整電子郵件地址或部分域地址的條目將發生異常。您必須使用**From標頭中提到的域**/完整電子郵件。

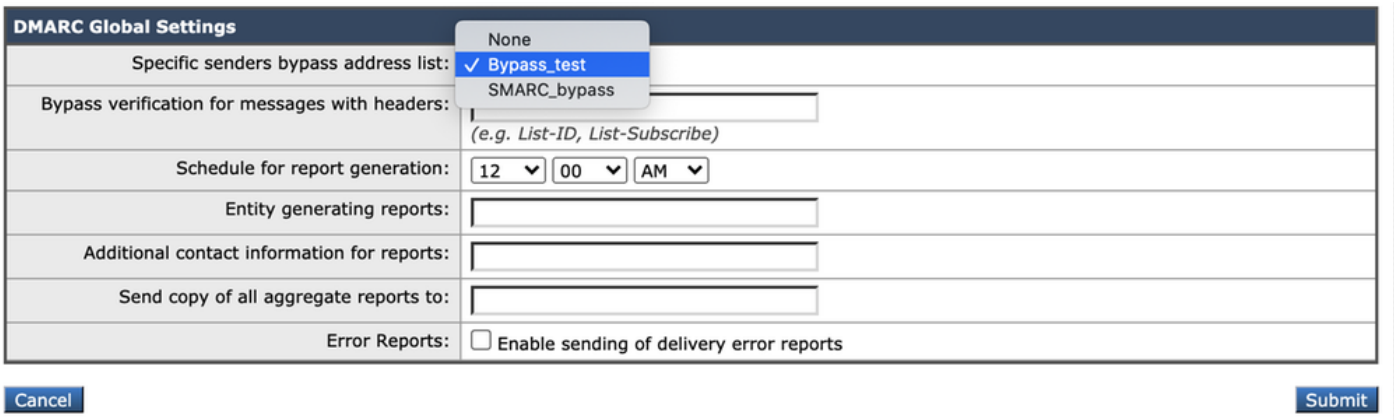
1. 確保為關聯的郵件流策略啟用**DMARC驗證**。
2. 導航到**Mail Policies > Address List**。
3. 點選**Add Address List**。
4. 通過填**寫詳細**資訊建立地址清單。
5. 按一下**Submit**。
6. **Address List**建立後，您必須將該清單呼叫到**DMARC Specific Senders Bypass Address List**。

以下是如何設定旁路組態以及如何進行記錄的一個範例：

建立地址清單時以「**僅域**」為例，並將其新增到**From**標頭詳細資訊。



成功建立包含所有所需條目的地址清單後，您必須呼叫**DMARC特定發件人旁路地址清單**下的**地址清單**。您需要導航到**Mail Policies > DMARC > Edit Global Settings**，然後點選下拉選單呼叫新建立的**Address List**，如下所示：



Mail_Logs中的差異

此處顯示了mail_logs的表示形式，它將有助於理解在驗證域的DMARC和將其配置為跳過時日誌記錄之間的區別。

選中DMARC時的郵件日誌：

```
Sat Mar 20 21:14:22 2021 Info: ICID 57 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable
```

```
Sat Mar 20 21:14:22 2021 Info: Start MID 76571 ICID 57

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 From:

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 RID 0 To:

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC: Verification skipped (No record found for the sending domain)

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC:

Sat Mar 20 21:14:23 2021 Info: MID 76571 Message-ID '<613a1e1b-998a-6375-8887-ab2c6d430256@whitelist.com>'

Sat Mar 20 21:14:23 2021 Info: MID 76571 Subject 'Test 4'
```

附註：沒有針對域@whitelist.com發佈記錄，因此我們看到「未找到傳送域的記錄」。

繞過DMARC檢查的郵件日誌

```
Sat Mar 20 21:15:36 2021 Info: ICID 58 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not applicable

Sat Mar 20 21:15:37 2021 Info: Start MID 76572 ICID 58

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 From:

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 RID 0 To:

Sat Mar 20 21:15:37 2021 Info: MID 76572 DMARC: Verification skipped (Local bypass configuration)

Sat Mar 20 21:15:37 2021 Info: MID 76572 Message-ID '<2ba742a2-f8ba-9ff0-7dc9-362421f5177e@whitelist.com>'

Sat Mar 20 21:15:37 2021 Info: MID 76572 Subject 'Test Bypass DMARC'
```

相關資訊

- 瞭解DMARC工作流
- 如何使用DMARC驗證傳入消息
- 篩選器以處理跳過DMARC驗證的郵件
- 技術支援與文件 - Cisco Systems