如何在邮件安全设备上绕过DMARC检查

目录

简介

本文档介绍如何绕过邮件安全设备(ESA)上基于域的邮件身份验证、报告和一致性(DMARC)检查。请参阅关[于电子邮件身份验证的简](#)介。

验证DMARC

DMARC是为降低基于电子邮件的滥用的可能性而创建的技术规范。DMARC使用发件人策略框架(SPF)和域密钥识别邮件(DKIM)机制，对邮件接收方执行邮件身份验证的方式进行了标准化。为了通过DMARC验证，电子邮件必须至少通过其中一种身份验证机制，并且身份验证标识符必须符合RFC 5322。

设备允许您：

- 使用DMARC验证传入的电子邮件。
- 定义配置文件以覆盖（接受、隔离或拒绝）域所有者的策略。
- 向域所有者发送反馈报告，这有助于加强其身份验证部署。
- 如果DMARC聚合报告大小超过10 MB或DMARC记录的聚合报告(RUA)标签中指定的大小，则向域所有者发送交付错误报告。

AsyncOS可以处理符合DMARC规范的邮件，这些邮件已于2013年3月31日提交至互联网工程任务组(IETF)。有关详细信息，请参[阅http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02](#)。

> **注意**：设备不会对来自DMARC记录格式错误的域的邮件执行DMARC验证。但是，设备可以接收和处理此类消息。

配置DMARC绕行

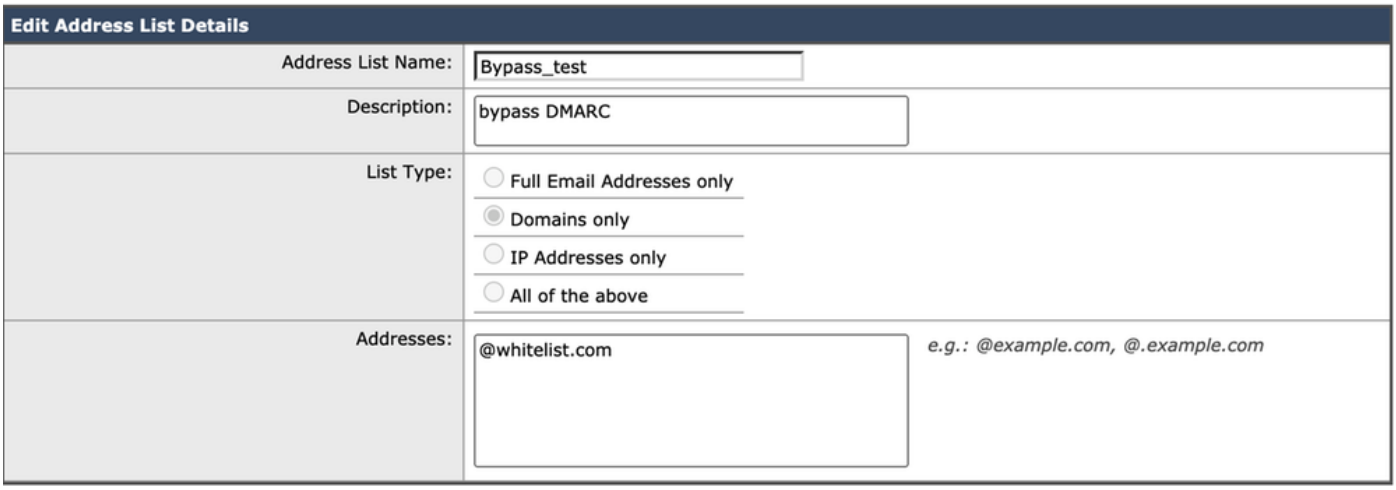
如果作为管理员，您的要求是跳过对来自特定发件人的邮件的DMARC验证，则您必须执行几个步骤才能成功绕过。有关这些步骤的概述，请参阅：

> **注意**：使用完整电子邮件地址或域创建的地址列表只能用于绕过DMARC验证。可以使用带有**上面**“全部”选**项的地址列表**。但是，仅包含域/完整邮件地址或部分域地址的条目将适用于异常。您必须使用“发件人”**标题中提及的域**/完整电**子邮**件地址。

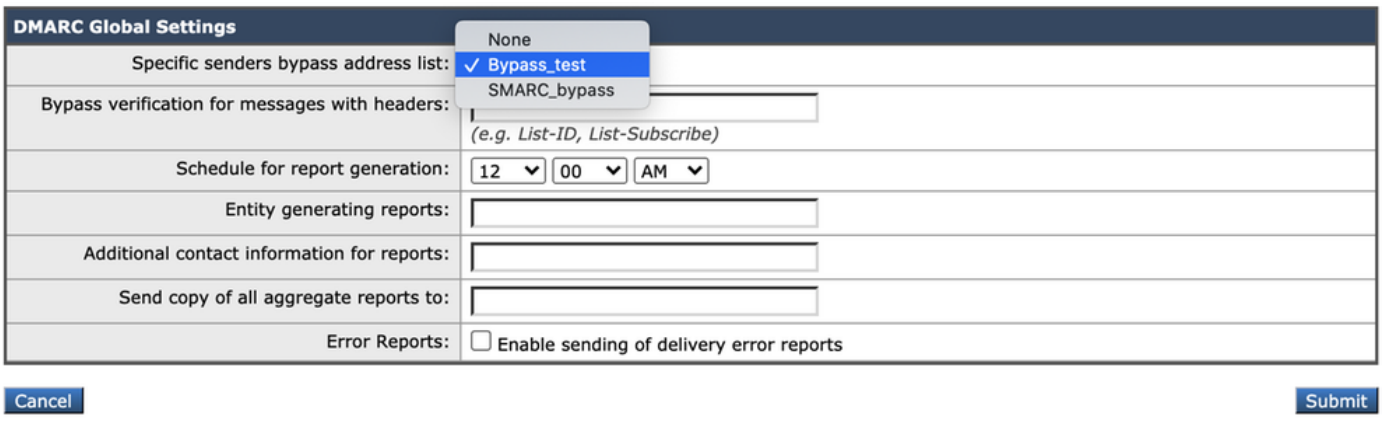
1. 确保**已为关**联的邮**件**流策略打开DMARC验证。
2. 导航至**邮件策略>地址列表**。
3. 单击“添**加地址列表”**。
4. 通过填写**详细信息**创建地址列表。
5. 单击 **Submit**。
6. 创建地**址列表**后，您必须将该列表调用到DMARC特定发**件人绕行地址列表**。

以下是如何配置旁路配置以及如何完成日志记录的示例：

地址列表以“仅域”**为例**创建，并添加到“发件人”报**头详细**信息中。



成功创建包含所有所需条目的地址列表后，您必须调用DMARC特定发件人旁**路地址**列表**下的地址列表**。您需要导航至“邮件策**略”>“DMARC”>“编辑全局设置”**，并通过单击下拉**列表**来调用新创建的地址列表，如下所示：



Mail_Logs中的差异

此处显示了mail_logs的表示形式，这有助于了解在验证域的DMARC时和配置为跳过时，日志记录之间的区别。

选中DMARC时的邮件日志：

```
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'
```

注意：没有为域@whitelist.com发布记录，这是我们看到“发送域未找到记录”的原因。

绕过DMARC检查的邮件日志

```
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'
```

相关信息

- 了解DMARC工作流
- 如何使用DMARC验证传入邮件
- 用于处理跳过DMARC验证的邮件的过滤器
- 技术支持和文档 - Cisco Systems