

配置安全邮件网关的发件人域例外列表

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[概述](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍对思科安全邮件网关(SEG)的发件人域信誉(SDR)设置选项“域例外列表”(Domain Exception List)的“新更改”。

作者：Chris Arellano Cisco TAC工程师。

先决条件

需要具备SEG设置和配置的一般知识。

思科安全邮件网关(SEG)的AsyncOS 15.0和更高版本。

对SDR功能的一般了解。

要求

启用发件人域信誉服务，并使用“仅域”(Domain Only)选项创建地址列表。

使用的组件

- 本文档中的信息基于以下软件和硬件版本：
 - 思科安全邮件网关(SEG) AsyncOS 15.5.1及更高版本。
- SEG发件人域信誉。
- 地址列表。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Sender Domain Reputation (发件人域信誉) 是一项云服务，用于收集多个发件人值、派生裁决并提供针对这些裁决采取行动的选项。SDR允许设置通过使用应用于域例外列表的地址列表绕过受信域。

在SEG 15.0之前的AsynOS版本中，SDR域例外列表有2个选项：

- 已启用=匹配信封发件人、域以绕过SDR操作。
- Disabled = Match only if all is present : Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC 。

SEG 15.0和更新版本的域例外列表：

- 已启用=匹配信封发件人、域以绕过SDR操作。
- Disabled = 匹配如果域存在于以下任何值中：
 - HELO
 - RDNS
 - 信封发件人
 - 从
 - 回复

配置

本文的重点是新的域例外列表配置。《用户指南》中提供了完整的SDR设置和配置。

在WebUI中导航到安全服务 > 域信誉。

- 默认情况下，Match Domain Exception List based on the Domain Name part of the Envelope From选项处于启用状态。
 - 如果启用该复选框，则只有值“Envelope From，header”（信封发件人，信头）才会匹配并绕过邮件（如果被定罪）。
 - 如果复选框为空，则SDR域例外列表将匹配以下任何报头字段“HELO：”、“RDNS：”、“Envelope From：”、“From：”和“Reply-To：”报头，如果被定罪，将匹配并绕过邮件。

如果选中关联的？信息图标，则会显示设置的详细信息。

Match Domain Exception List based on Domain in Envelope From. ✕

Disable this option if you want to skip the SDR checks if any domains in the 'HELO:', 'RDNS:', 'Envelope From:', 'From:' and 'Reply-To:' headers of the message match the domains configured in the domain exception list.

Note: By default, SDR checks are skipped based on the domain in the 'Envelope From:' header only.

 注意：默认情况下，仅根据“Envelope From：”信头中的域跳过SDR检查。


选择Edit Global Settings以删除复选框选项，如图所示：

Sender Domain Reputation Overview

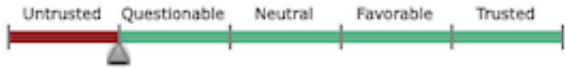
Enable Sender Domain Reputation Filtering

Include Additional Attributes: Enable

Sender Domain Reputation Query Timeout: seconds

Match Domain Exception List based on Domain in Envelope From: Enable 

Action applied on Message based on SDR Verdict: Reject Accept



For Threat Level Unknown: Accept Reject

域名例外列表本身是包含域名的地址列表。

验证

要使用新的Disable功能验证功能是否正常，您需要向SEG发送一条测试消息，在5个报头值之一中有一个匹配的域值。

在早期阶段，mail_logs中将出现一个示例日志，该日志指示全局例外列表内的例外并在邮件流策略内匹配：

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

指示异常的示例日志将同时包含域和异常列表名称。

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

故障排除

如果对所选邮件裁决的准确性存在疑问，则记录这些值，并与邮件跟踪进行比较。

- 记录全局域信誉设置 > 安全设置 > 域信誉。
- 验证在全局域信誉设置中配置的关联地址列表。
- 根据邮件跟踪验证匹配的邮件流策略。
- 检查并注意配置了域例外列表的所有邮件过滤器或内容过滤器的详细信息。

收集邮件跟踪、邮件日志和原始邮件信头。

- 如果消息上的Global exception匹配，则没有Domain Reputation的日志条目，只是表示匹配域的行。

- 如果邮件中的全局例外列表不匹配，则有域信誉的日志条目可用于比较值。
 - 信息：MID 16 SDR：请求SDR的域：反向DNS主机：不存在，helo：mail1.example.com，env-from：test2.example.com，header-from：te destination.example.com，回复：test2.example.com
- 邮件标题包含单个邮件中显示的与设置比较的5个值中的任意值。

收集所有数据后，请检查匹配项或不匹配项，以确定功能是否正确。

相关信息

- [邮件安全设置指南](#)
- [支持指南的思科安全电邮网关发布页面](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。