

如何DKIM签署代表其他域发送的电子邮件

目录

[简介](#)

[背景信息](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍当邮件代表其他域发送时，如何在邮件安全设备(ESA)和云邮件安全(CES)上使用域密钥识别的邮件(DKIM)签名邮件。

背景信息

从[RFC2822](#)

“发起方字段指示邮件源的邮箱。“发件人：”字段指定邮件的作者，即负责撰写邮件的人或系统的邮箱。“发件人：”字段指定负责邮件实际传输的代理的邮箱。例如，如果秘书要向另一个人发送邮件，则该秘书的邮箱将出现在“发件人：”字段中，而实际作者的邮箱将出现在“发件人：”字段中。如果邮件的发起者可以由单个邮箱指示，且作者和发送者相同，则不应使用“发件人：”字段。否则，应显示两个字段。”

根据[最终用户指南14.0](#)

“当用于发送消息（出站）的侦听程序收到消息时，邮件网关会检查是否存在域配置文件。如果在邮件网关上创建了域配置文件（并为邮件流策略实施），则会扫描邮件以查找有效的发件人：或从：地址。如果两者都存在，则发送方：报头始终用于域密钥和DKIM签名，但是从：报头也是必需的，即使它不用于DKIM签名。仅发送方时：报头存在，DomainKeys或DKIM签名配置文件不匹配。
"发件人:"报头仅在以下情况下使用：

- 没有发件人：标题。
- 在Web界面的DKIM全局设置页面中，选择Use From Header for DKIM Signing选项。”

先决条件

要求

本文档没有任何特定的要求。

使用的组件

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。

配置

1. [配置DKIM签名](#)

2. 导航至Mail Policies > Signing Profiles > DKIM Global Settings > Use From Header for DKIM Signing:关闭

注意：如果Use From Header for DKIM Signing设置为On，则ESA始终会查看From报头字段，并且代表其他域发送的消息不是DKIM签名的，因为**Sender**报头填充了Envelope From 值，因此这些消息与DKIM配置文件中建立的域不匹配。

验证

1. 启动SMTP对话

```
ESA-C690-K9.MX> telnet 15.0.0.59 25
Trying 15.0.0.59...
Connected to 15.0.0.59.
Escape character is '^]'.
220 mail.mxesa.com ESMTTP
hello
250 mail.mxesa.com
MAIL FROM: amacorra@mxesa.com
250 sender <amacorra@mxesa.com> ok
RCPT TO: amacorra@cloudesa.com
250 recipient <amacorra@cloudesa.com> ok
data
354 go ahead
From: amacorra@cloudesa.com
To: amacorra@cloudesa.com
Sender: amacorra@mxesa.com
Subject: Adding Sender Header Manually

Adding Sender Header Manually.
.
```

```
250 ok: Message 640880 accepted
```

2. 验证日志

DKIM:通过签名验证(d= mxesa.com s=selector i=@ mxesa.com)

3. 验证报头

dkim=pass (签名验证) header.i=@mxesa.com

在收件箱中，您会收到包含下一行的电子邮件：

```
amacorra@mxesa.com <amacorra@ mxesa.com;代表 ; amacorra@cloudesa.com
<amacorra@cloudesa.com>
```

相关信息

- [RFC2822](#)
- [最终用户指南14.0](#)
- [配置DKIM签名](#)