在ESA上配置无中断的DKIM密钥替换

目录

[简介](#)

[先决条件](#)

[创建新的DKIM签名密钥](#)

[生成新的DKIM签名配置文件](#)

[将DNS记录发布到DNS](#)

[删除旧签名配置文件并从新签名配置文件中删除占位符用户](#)

[测试邮件流以确认DKIM通过](#)

简介

本文档介绍如何在不停机的情况下替换ESA上现有的DKIM签名密钥和DNS中的DKIM公钥。

先决条件

1. 访问邮件安全设备(ESA)。
2. 访问DNS以添加/删除TXT记录。
3. ESA必须已使用DKIM配置文件对邮件签名。

创建新的DKIM签名密钥

您首先需要在ESA上创建新的DKIM签名密钥：

1. 导航到邮件策略>签名密钥，然后选择添加密钥。
2. 为DKIM密钥命名，并生成新私钥或粘贴到现有私钥中。

> 注意：在大多数情况下，建议选择2048位的私钥大小。

3. 提交更改。

> 注意：此更改不会影响DKIM签名或邮件流。我们只是在添加DKIM签名密钥，尚未将其应用于任何DKIM签名配置文件。

生成新的DKIM签名配置文件

接下来，确保创建新的DKIM签名配置文件，从该DKIM签名配置文件生成DKIM DNS记录并将该记录发布到DNS:

1. 导航到邮件策略>签名配置文件，然后选择添加配置文件。

2. 在Profile Name字段中为配置文件指定描述性名称。
3. 在域名字段中输入您的域。
4. 在Selector字段中输入新的选择器字符串。

> 注意： 选择器是一个任意字符串，用于允许给定域的多个DKIM DNS记录。我们将使用选择器为您的域在DNS中允许多个DKIM DNS记录。必须使用不同于现有DKIM签名配置文件的新选择器。

5. 在Signing Key字段中选择上一节中创建的DKIM签名密钥。
6. 在签名配置文件的底部，添加新的用户。此用户必须是未使用的占位符电子邮件地址。

> 警告：您必须添加未使用的电子邮件地址作为此签名配置文件的用户。否则，此配置文件可能会在发布DKIM TXT记录之前对出站邮件进行签名，从而导致DKIM验证失败。将未使用的电子邮件地址添加为用户可确保此签名配置文件不对任何出站邮件签名。

7. 选择 Submit。

将DNS记录发布到DNS

1. 在此处，为您刚创建的签名配置文件选择DNS文本记录列生成，并复制生成的DNS记录。其外观必须类似于：

```
selector2._domainkey.example.com. IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw
```

2. 提交更改。
3. 在第2步中向DNS提交DKIM DNS TXT记录。
4. 等待DKIM DNS TXT记录完全传播。

删除旧签名配置文件并从新签名配置文件中删除占位符用户

将DKIM TXT记录提交到DNS并确保已传播后，下一步是删除旧的签名配置文件并从新的签名配置文件中删除占位符用户：

> 注意： 极力建议您先备份ESA配置文件，然后再继续执行这些步骤。这是因为，如果您删除了旧的DKIM签名配置文件，并且需要恢复为以前的配置，则可以轻松加载已备份的配置文件。

1. 依次导航邮件策略(Mail Policies)>签名配置文件(Signing Profiles)，选择旧DKIM签名配置文件，然后选择删除(Delete)。
2. 导航到新的DKIM签名配置文件，选择当前占位符用户，然后选择删除。
3. 选择 Submit。
4. 在测试配置文件列下，为新的DKIM签名配置文件选择测试。如果测试成功，请继续下一步。如果不是，请确认DKIM DNS TXT记录已完全传播。
5. 提交所做的更改。

测试邮件流以确认DKIM通过

此时，您已完成进一步配置DKIM。但是，您必须测试DKIM签名，以确保它按预期对出站邮件进行签名并通过DKIM验证：

1. 通过ESA发送消息，确保其获得ESA签名的DKIM和另一台主机验证的DKIM。
2. 在另一端收到消息后，检查消息的报头中是否存在报头Authentication-Results。查找报头的DKIM部分以确认它是否通过DKIM验证。报头必须类似于
   <#root>

   ```
   Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
   ```

   dkim=pass

   ```
    header.i=none; dmarc=fail (p=none dis=none) d=example.net
   ```

3. 查找报头DKIM-Signature，并确认使用了正确的选择器和域：

   <#root>

   ```
   DKIM-Signature: a=rsa-sha256;
   ```

   d=example.net

   ;

   s=selector2

   ;

   ```
      c=simple; q=dns/txt; i=@example.net;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
               VoG4ZHRNiYzR
   ```

4. 一旦您确信DKIM按预期工作，请至少等待一个星期再删除旧DKIM TXT记录。这可确保已处理由旧DKIM密钥签名的所有邮件。

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）。