

在ESA上配置DKIM签名

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[确保DKIM签名已关闭](#)

[创建DKIM签名密钥](#)

[生成新的DKIM签名配置文件并将DNS记录发布到DNS](#)

[打开DKIM签名](#)

[测试邮件流以确认DKIM通过](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何在邮件安全设备(ESA)上配置DomainKeys识别邮件(DKIM)签名。

先决条件

要求

Cisco 建议您了解以下主题：

- 邮件安全设备(ESA)访问。
- 添加/删除TXT记录的DNS编辑访问。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

确保DKIM签名已关闭


您需要确保在所有邮件流策略中关闭DKIM签名。这允许您配置DKIM签名，而不会影响邮件流：

1. 导航到邮件策略>邮件流策略。
2. 导航到每个邮件流策略，并确保Domain Key/DKIM Signing设置为Off。

创建DKIM签名密钥

您需要在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，并生成新的私钥或粘贴到当前密钥中。


 注意：在大多数情况下，建议您选择2048位的私钥大小。

3. 确认更改。

生成新的DKIM签名配置文件并将DNS记录发布到DNS

接下来，您需要创建新的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. 导航至邮件策略(Mail Policies) >签名配置文件(Signing Profiles)，然后点击添加配置文件(Add Profile)。
 1. 在Profile Name字段中为配置文件指定描述性名称。
 2. 在Domain Name字段中输入您的域。
 3. 在选择器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。

4. 在Signing Key字段中选择上一部分中创建的DKIM签名密钥。
5. 单击“Submit”。
2. 在此处为您刚创建的签名配置文件单击DNS Text Record列中的Generate，然后复制生成的DNS记录。它必须类似于以下内容：

```
selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwmA
```

3. 提交更改。
4. 将步骤2中的DKIM DNS TXT记录提交到DNS。
5. 等待DKIM DNS TXT记录完全传播。
6. 转至Mail Policies > Signing Profiles。
7. 在测试配置文件列下，为新的DKIM签名配置文件单击测试。如果测试成功，请继续本指南。如果没有，请确认DKIM DNS TXT记录已完全传播。

打开DKIM签名

现在，ESA已配置为DKIM签名邮件，我们可以打开DKIM签名：

1. 导航到邮件策略>邮件流策略。
2. 转到具有中继的连接行为的每个邮件流策略，并将Domain Key/DKIM Signing设置为On。



注意：默认情况下，具有中继连接行为的唯一邮件流策略是名为中继的邮件流策略。您需要确保只有DKIM签名邮件是出站邮件。

3. 确认更改。

测试邮件流以确认DKIM通过

此时，DKIM已配置。但是，您需要测试DKIM签名，以确保它按预期对出站邮件签名，并且通过DKIM验证：

1. 通过ESA发送消息，并确保其获得ESA签署的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，查找报头Authentication-Results。查找报头的DKIM部分以确认其是否通过DKIM验证。报头必须类似于以下示例：

```
<#root>
```

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

```
dkim=pass
```

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

3. 查找信头“DKIM-Signature”，并确认使用了正确的选择器和域：

```
<#root>
```

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

```
d=domainsite
```

```
;
```

```
s=selector2
```

```
;
```

```
c=simple; q=dns/txt; i=@domainsite;
```

```
t=1117574938; x=1118006938;
```

```
h=from:to:subject:date;
```

```
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjMONTY3ODkwMTI=;
```

```
b=dzdVyOfAKCdLXdJ0c9G2q8LoXS1EniSbav+yuU4zGeeruD001szZ
```

```
VoG4ZHRNiYzR
```

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有针对此配置进行故障排除的特定方法。

相关信息

- [思科技术支持和下载](#)

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）。