DMARC体系结构-标识对准线

Contents

Introduction

本文与发送方政策架构(SPF)和DomainKeys被识别的邮件(DKIM)对准线需求一起描述一般基于域的信息验证，报告和符合(DMARC)体系结构概念，关于DMARC。

术语

此部分记述并提供定义给在本文内使用的某些关键术语。

- **EHLO/HELO** -在SMTP会话初始化时供应SMTP客户端的身份如对RFC 5321定义的命令。
- **从报头**-从：字段指定消息的作者。它与包含一个本地部件和域名的电子邮件地址一起将典型地包括显示名字(什么显示终端用户由邮件客户端)，(例如，“张三” < johndoe@example.com >)如对RFC 5322定义。
- **邮件从**-这从MAIL命令派生在SMTP会话的开始并且提供发送方证明如对RFC5321定义。也一般叫作包发送方、回归PATH或者跳动地址。

DMARC -标识对准线

DMARC附加什么DKIM和SPF请验证对什么在列出从报头。这由*对准线*完成。 对准线要求域身份由SPF和DKIM匹配验证在可视的电子邮件地址的域对终端用户。

请从标识开始是，并且他们为什么是重要的关于DMARC。

标识

标识识别将验证的一个域名。

关于DMARC的标识：

- SPF ：

  SPF验证出现于邮件或SMTP会话的EHLO/HELO部分的域，或者两个。这些可能是不同的域，并且他们不典型地是可视的对终端用户。

- DKIM ：

  DKIM验证被添加在*d*=标记内的一个签名的签署的域。

这些(SPF和DKIM)标识利用在派生的域标识验证从报头。从报头域使用，因为它是消息的创建人的最普通的邮件用户代理(MUA)字段并且是终端用户用于的那个识别消息(发送方)的来源，由报头也做滥用的一个头等目标。

警告：DMARC能仅保护滥用以防止有效免受报头。

DMARC不能起作用：

- 畸形，缺少或者被重复的RFC 5322报头
- 固执的报头，因为他们不会被验证
- 当有超过在报头的一个域身份(*)

所以，除DMARC之外的一个进程应该存在识别与固执的畸形的报头的消息和实现方式标记和使他们可视作为非DMARC合格报头。

(*) DMARC需要从报头提取单个域身份。如果有超过在报头的一个电子邮件地址比此报头在多数DMARC实施将被跳过。处理报头以超过一个域身份陈述作为在DMARC规格的外范围。

当Cisco ESA能发现超过时一个域身份在邮件日志留下一个适当的消息：

```
(Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs

Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be determined)
```

标识对准线

标识对准线定义了SPF验证的域并且/或者DKIM之间的一个关系和从报头。对准线是需要在SPF和

DKIM以后成功验证另外满足的配比的进程。 DMARC认证过程要求SPF或DKIM (域身份)使用的其中至少一个标识将对齐与域部分的从报头地址。

DMARC引入两个对准线模式：

- **严格的**模式要求完全匹配(请对齐)在域名之间
- **轻松的**模式允许同一个域的子域

标识对准线，因为消息能带有从所有域的一个有效签名，包括邮件列表甚至一名坏演员，使用的域需要。所以，仅仅带有一个有效签名不是推断作者域的真实性的足够。

DKIM对准线

DKIM域标识通过查看在DKIM签名的*d=*标记得到，并且与比较从报头域顺利地验证DKIM签名。

为例，消息可以代表域d=blog.cisco.com签字，识别域blog.cisco.com*作为签署人*。 DMARC使用此域并且它与域部份的比较从报头(例如， noreply@cisco.com)。使用轻松的模式，在这些标识之间的对准线失效strictmode，但是通过。

> **Note**:单个电子邮件能包含多个DKIM签名，并且认为DMARC “通行证”，如果任何DKIM签名对齐并且验证。

SPF对准线

SPF (spfv1)机制验证域标识传送从：

- 从身份的邮件(mail from命令)
- HELO/EHLO身份(HELO/EHLO命令)

从域身份的默认情况下邮件设法验证。直升机域身份由仅DMARC验证与空邮件的消息的从身份，类似信号反跳信息。

此的一个普通的示例是消息用不同的邮件传送从地址(noreply@blog.cisco.com)的地方与什么比较在从报头(noreply@cisco.com)。从域noreply **@blog.cisco.com的**身份零件的邮件**与将对齐**从报头domainof noreply @cisco.com在relaxedmode，但是不在严格的模式下。

对准线模式标记

使用**adkim**和**aspf**对准线模式标记， DMARC对准线模式在DMARC策略记录可以被定义。 这些标记指示什么模式对于DKIM或SPF标识是必需的对准线。

如果标记不存在，模式可以设置到轻松或严格，以轻松是默认值。这可以设置在TAG值下如下：

- **r ：轻松的模式**
- **s ：严格的模式**

参考

- RFC5321 -简单邮件转发协议
- RFC5322 -互联网消息格式
- RFC6376 - DomainKeys识别邮件(DKIM)签名
- RFC7208 -发送方政策架构(SPF)为核准的使用在电子邮件的域
- RFC7489 -基于域的信息验证，报告和符合(DMARC)