邮件身份验证最佳实践 - 部署 SPF、DKIM 和 DMARC 的最佳方式

目录

简介

本指南介绍目前使用的三种主要邮件身份验证技术 - SPF、DKIM 和 DMARC，并讨论实施这些技术所涉及的各个方面。文中讨论了几种实际邮件架构情况，以及在思科邮件安全产品集中实施这些架构的准则。由于这是需要上手操作的最佳实践指南，因此本文将省略一些较为复杂的部分。为方便读者理解所呈现的内容，本文可能会在必要时简化或浓缩某些概念。

产品知识要求

本指南属于高级别文档。要完成所有演示内容，读者应具备思科邮件安全设备方面的产品知识，并达到思科邮件安全现场工程师认证级别。此外，读者应对 DNS 和 SMTP 及其操作非常了解。熟悉 SPF、DKIM 和 DMARC 的基础知识是加分项。

邮件身份验证 - 概述

发件人策略框架 (SPF)

Sender Policy Framework最初发布于2006年，即RFC4408。当前版本在RFC7208中指定，并在RFC7372中更新。实际上，它提供了一种简单的方法，使域所有者能够使用DNS向接收者通告其合法电子邮件源。虽然 SPF 主要是对返回路径 (MAIL FROM) 地址进行身份验证，但该规范建议（并提供机制）同时对 SMTP HELO/EHLO 参数（在 SMTP 会话期间传输的发件人网关的 FQDN）进行身份验证。

SPF 使用的是 TXT 类型的 DNS 资源记录，语法非常简单：

```
spirit.com       text = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.spirit.com
a:mx4.spirit.com include:spf.protection.outlook.com ~all"
```

上面的 Spirit Airlines 记录允许从 @spirit.com 地址发出的邮件来自特定的 /24 子网、由 FQDN 标识的两台计算机以及 Microsoft 的 Office365 环境。末尾的“~all”限定符指示收件人将任何其他来源视为 Soft Fail，即 SPF 的两种失败模式之一。请注意，发件人并不指定收件人针对失败邮件应执行的操作，而是仅指定邮件失败的程度。

Delta 则采用了不同的 SPF 方案：

```
delta.com       text = "v=spf1 a:smtp.hosts.delta.com
include:_spf.vendor.delta.com -all"
```

为最大限度减少所需的 DNS 查询数量，Delta 创建了一个单独的“A”记录，其中列出了所有 SMTP 网关。他们还在“_spf.vendor.delta.com”中为供应商提供了一个单独的 SPF 记录。他们还提供对未通过 SPF 身份验证的任何邮件执行 Hard Fail 的说明（“-all”限定符）。我们可以进一步查询供应商的 SPF 记录：

```
_spf.vendor.delta.com  text = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:skytel.com include:epsl1.com ?all"
```

例如，来自发件人 @delta.com 的邮件可以合法地从 Air France 的邮件网关发送。

United 使用的 SPF 方案则更为简单：

```
united.com     text = "v=spf1 include:spf.enviaremails.com.br
include:spf.usa.net include:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

除了公司自己的邮件网关外，他们还添加了邮件营销提供商（“usa.net”和“enviaremails.com.br”）、以前 Continental Air Lines 的网关，以及 MX 记录中列出的所有网关（“MX”机制）。请注意，MX（域的传入邮件网关）不一定与传出邮件网关完全相同。对于规模较小的企业，两者的邮件基础设施一般是相同的，而对于规模较大的组织，他们会采用单独的邮件基础设施分别处理传入和传出邮件。

值得注意的是，以上所有示例都广泛使用了其他 DNS 引用（“include”机制）。但出于性能考虑，SPF 规范将检索最终记录所需的 DNS 查询总数限制为 10 次。DNS 递归超过 10 次的任何 SPF 查询都会失败。

域名密钥识别邮件 (DKIM)

RFC 5585、6376和5863中指定的DKIM由雅虎的DomainKeys和思科的已识别互联网邮件这两个历史提议合并而成。它为发件人提供了一种对传出邮件进行加密签名的简单方法，并将签名（及其他验证元数据）添加到邮件头中（“DKIM-Signature”）。发件人将公钥发布在 DNS 中，使任何收件人都能轻松检索密钥和验证签名。DKIM 不会对物理邮件的来源进行身份验证，而是以这样一个事实为依据：如果邮件来源拥有发件人组织的私钥，则被隐式授权代表他们发送邮件。

要实施 DKIM，发件人组织需要生成一个或多个公钥对，并将这些公钥作为 TXT 记录发布在 DNS 中。每个密钥对都将由一个“选择器”引用，以便 DKIM 验证器对这些密钥加以区分。对传出邮件进行签名，并插入 DKIM-Signature 头：

```
DKIM签名：v=1； a=rsa-sha1； c=relaxed/relaxed； s=united； d=news.united.com；h=MIME-Version：Content-Type：Content-Transfer-Encoding：Date：To：From：Reply-To：Subject：List-Unsubscribe：Message-ID； i=MileagePlus@news.united.com；bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=；

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4DGmKhH1
```

签名格式非常简单。“a”标签指定用于签名的算法，“c”指定使用的规范化方案 [1]，“s”是选择器或密钥引用，“d”是签名域。此DKIM签名信头的其余部分特定于邮件：“h”列出签名信头，“i”列出签名用户的身份，最后信头以两个单独的散列结尾：“bh”是签名信头的散列，而“b”是邮件正文的散列值。

接收 DKIM 签名的邮件时，收件人将通过构建以下 DNS 查询来查询公钥：

```
<selector>._domainkey.<signing domain>
```

（如 DKIM-Signature 头中所指定的那样）。对于上面的示例，查询将是“united._domainkey.news.united.com”：

```
united._domainkey.news.united.com文本= "g=*\； k=rsa\； n=" "联系" "postmaster@responsys.com" "有" "任何" "问题" "涉及" "此" "签署" "\；
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2KkWgl35h
Cr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6OFZMW6Tp1t05NPWh0PbyUohZYt4qpcbiz9Kc3
```

返回的 DNS 记录包含密钥及其他可选参数。[2]

DKIM 的主要问题是，其最初制定的规范不允许通告发件人使用了 DKIM。因此，如果邮件不含签名，发件人也很难知道该邮件应该含有签名，而一旦邮件不含签名，该邮件很可能就是虚假邮件。由于一个组织可以（且通常会）使用多个选择器，因此很难“猜测”是否对某个域启用了 DKIM。为解决这个问题，业界发布了一个独立标准《作者域签名实践》，但由于使用率较低和其他问题，该标准在 2013 年已被废弃，且不再有后续版本。

基于域的邮件身份验证、报告和一致性 (DMARC)

DMARC 是三种邮件身份验证技术中最新的一种，专门用于解决 SPF 和 DKIM 存在的问题。与其他两种技术不同，DMARC 会对邮件的 Header From 进行身份验证，同时涵盖其他两种技术之前执行的相关检查。DMARC 由 RFC7489 指定。

DMARC 优于 SPF 和 DKIM 的方面还包括：

- 确保所有可用身份（HELO、MAIL FROM 和/或 DKIM 签名域）与 From 信头一致（完全匹配或从属）
- 为发件人域所有者提供了一种方法，让他们能够为收件人指定必须如何处理失败邮件的策略
- 为发件人域所有者提供了一种反馈工具，让他们能够获得有关任何失败邮件的通知，以轻松识别网络钓鱼活动或 SPF/DKIM/DMARC 策略分发中的错误

DMARC 也使用简单的基于 DNS 的策略分发机制：

```
_dmarc.aa.com text = "v=DMARC1\; p=none\; fo=1\; ri=3600\;
rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

DMARC 策略规范中唯一的强制标签是“p”，用于指定要对失败邮件使用的策略。它可以是以下三种类型之一：无、隔离、拒绝。

最常用的可选参数与报告有关：“rua”指定一个URL(使用POST方法的mailto：或http:// URL)来发送有关所有声称来自特定域的失败邮件的每日汇总报告。“ruf”指定另一个 URL，用于立即提交有关每封失败邮件的详细失败报告。

根据规范，收件人必须遵守通告的策略。否则，他们必须在汇总报告中通知发件人域所有者。

DMARC 的核心概念是所谓的标识符一致性。标识符一致性定义了邮件如何才能通过 DMARC 验证。SPF 和 DKIM 标识符的一致性是独立的，邮件需要通过其中任何一个一致性验证，以通过 DMARC 整体检查。但是，即使一个一致性验证已通过，另一个一致性验证已失败，发件人仍可利用其中的一个 DMARC 策略选项，继续请求生成失败报告。比如在上面的示例中，“fo”标签被设置为“1”。

邮件遵循 DKIM 或 SPF 标识符一致性的方法有两种：Strict 和 Relaxed。Strict 意味着 Header From 的 FQDN 必须完全匹配 DKIM 签名的签名域 ID（“d”标签）或 SPF 的 MAIL FROM SMTP 命令的 FQDN。Relaxed 则允许 Header From FQDN 属于上面提到的两种规范的子域。 这在将邮件流量委派给第三方时具有重要意义，本文稍后将对此进行讨论。

SPF 部署注意事项

面向收件人的 SPF

为思科邮件安全设备或云邮件安全虚拟设备配置 SPF 验证非常简单。在本文档的剩余部分，对 ESA（邮件安全设备）的任何引用也将包括 CES（云邮件安全）。

SPF 验证是在“邮件流策略”中配置的。要实现全局运行，最简单的方法是在相应侦听器的“默认策略参数”部分将其开启。如果正在使用同一侦听器收集传入和传出邮件，请确保将“RELAYED”邮件流策略中的 SPF 验证设置为“关闭”。

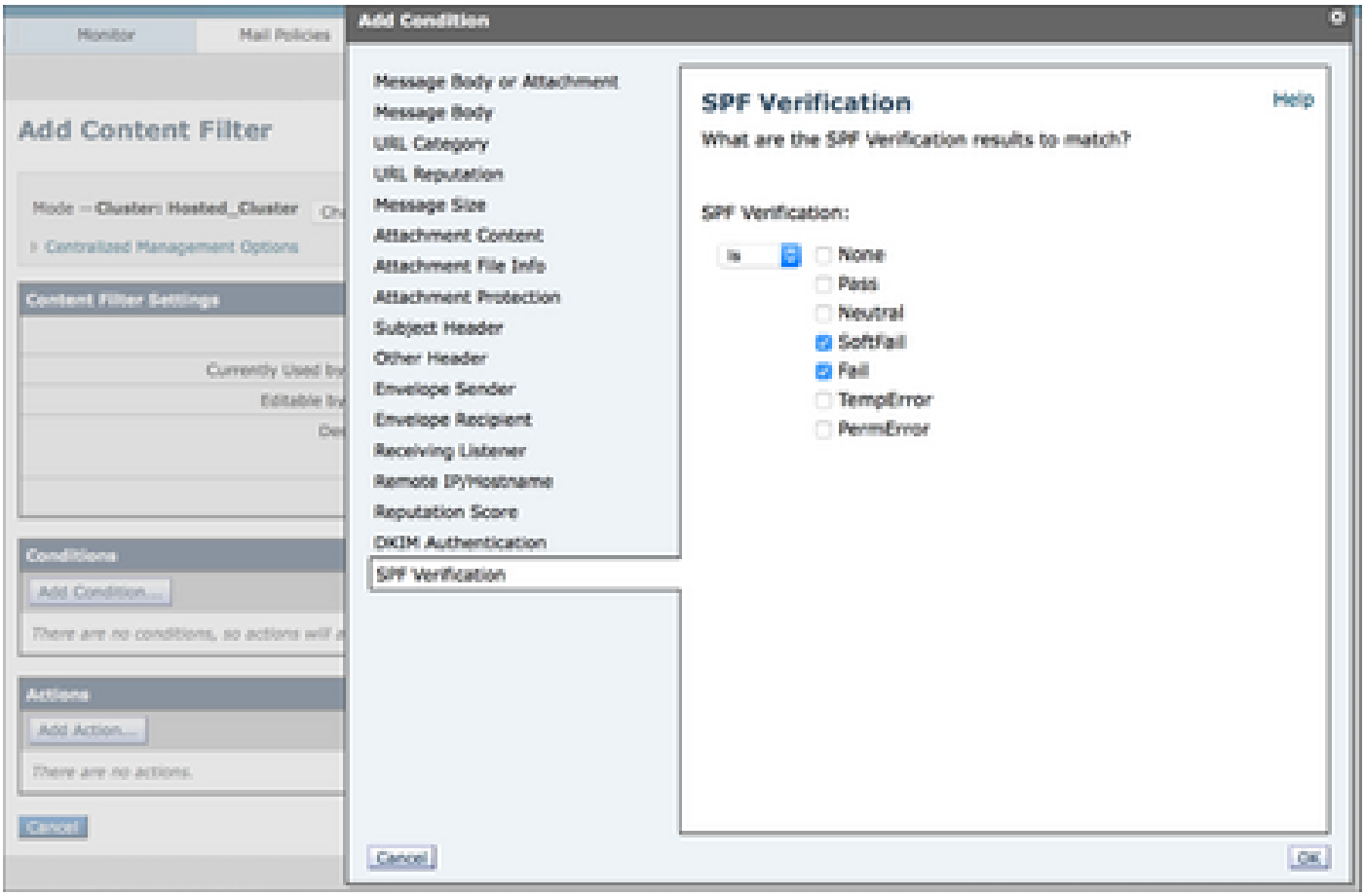
由于 SPF 不允许指定要采取的策略操作，因此 SPF 验证（以及 DKIM，我们稍后将对此进行介绍）将仅验证邮件并为执行的每项 SPF 检查插入一组信头：

```
Received-SPF：通过(mx1.hc4-93.c3s2.smtpi.com：域
    united.5765@envfrm.rsys2.com designates 12.130.136.195 as
    permitted sender) identity=mailfrom;
  client-ip=12.130.136.195； receiver=mx1.hc4-93.c3s2.smtpi.com；
    envelope-from="united.5765@envfrm.rsys2.com";
    x-sender="united.5765@envfrm.rsys2.com";
  x-conformance=sidf_compatible； x-record-type="v=spf1"
Received-SPF：无(mx1.hc4-93.c3s2.smtpi.com：无发件人
    authenticity information available from domain of
    postmaster@omp.news.united.com) identity=helo;
  client-ip=12.130.136.195； receiver=mx1.hc4-93.c3s2.smtpi.com；
    envelope-from="united.5765@envfrm.rsys2.com";
    x-sender="postmaster@omp.news.united.com";
    x-conformance=sidf_compatible
```

请注意，对于此邮件，SPF验证了两种“身份”：规范规定的“mailfrom”和规范建议的“helo”。该邮件将正式通过 SPF 验证，因为只有前者与 SPF 合规性有关，但有些收件人可能也会批准 SPF 记录中不包含 HELO 身份的发件人。因此，建议在 SPF 记录中包含传出邮件网关的主机名。

邮件流策略对邮件进行验证后，将由本地管理员配置要采取的操作。管理员可以使用邮件过滤器规则 SPF-status() [3] 完成此步骤，或使用该规则创建一个传入内容过滤器，并将其应用于相应的传入邮件策略。

图片1：SPF验证内容过滤器条件



建议的过滤操作是丢弃 Fail 邮件（SPF 记录中的“-all”），并在策略隔离区中隔离 Softfail 邮件（SPF 记录中的“~all”），但也可根据您的安全要求自行调整。有些收件人只是标记了失败邮件，或不采取任何可见操作，但会向管理员报告。

最近，SPF 的使用率大幅增长，但许多域发布的 SPF 记录不完整或不正确。为安全起见，您需要隔离所有 SPF-failing 邮件，并持续监控隔离区一段时间，确保不存在“误报”问题。

如果您为其他域或第三方提供邮件服务

如果您为第三方提供邮件传送或托管服务，他们必须将您用于传送其邮件所使用的主机名和 IP 地址添加到他们自己的 SPF 记录中。最简单的实现方法是让提供商创建一个“umbrella”SPF 记录，并让客户在其 SPF 记录中使用“include”机制。

```
suncountry.com    text = "v=spf1 mx ip4:207.238.249.242
ip4:146.88.177.148 ip4:146.88.177.149 ip4:67.109.66.68
ip4:198.179.134.238 ip4:107.20.247.57 ip4:207.87.182.66
ip4:199.66.248.0/22 include:cust-spf.exacttarget.com ~all"
```

可以看到，Sun Country 有一部分邮件由其自己控制，但将营销邮件外包给了第三方。展开引用的记录后，可以看到其营销邮件服务提供商当前使用的 IP 地址列表：

```
cust-spf.exacttarget.com      text = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
```

```
ip4:207.250.68.0/24 ip4:209.43.22.0/28 ip4:198.245.80.0/20
ip4:136.147.128.0/20 ip4:136.147.176.0/20 ip4:13.111.0.0/18 -all"
```

这种灵活性使邮件服务提供商可以自行扩展，而无需联系每个客户修改 DNS 记录。

如果您使用第三方邮件服务

与上一段类似，如果您正在使用任何第三方邮件服务，并希望建立完整的 SPF-verified 邮件流，则必须将他们的 SPF 记录添加到您自己的记录中。

```
jetblue.com descriptive text "v=spf1 include:_spf.qualtrics.com ?all"
```

JetBlue 使用 Qualtrics 分析服务，他们只需通过 Qualtrics 添加正确的 SPF 记录。同样，其他大多数 ESP 都提供要添加到客户记录中的 SPF 记录。

如果您的 ESP 或邮件营销商不提供 SPF 记录，您必须在自己的记录中直接列出他们的传出邮件网关。但是，您有责任确保这些记录的准确性，如果提供商添加了其他网关、更改了 IP 地址或主机名，您的邮件流可能会面临危险。

不具有SPF意识的第三方的其他危险来自共享资源：如果ESP使用同一IP地址发送多个客户的电子邮件，则从技术上讲，一个客户可以生成SPF有效的邮件，伪装成通过同一界面传送的另一客户。因此，在实施任何 SPF 限制之前，应全面调查 MSP 的安全策略以及他们对邮件身份验证的了解程度。如果您的问题没有答案，考虑到SPF是Internet上的基本信任机制之一，强烈建议您重新考虑您对MSP的选择。这不仅仅关乎安全性- SPF、DKIM、DMARC和MSP采用的其他发件人最佳实践[4]可保证可交付性。如果您的 MSP 没有或未能正确遵循这些实践，他们在大型接收系统中的可信度就会大打折扣，这可能会导致您的邮件出现延迟甚至被阻止。

不生成邮件流量的（子）域

出于营销需要，大多数组织现在都拥有多个域，但主要将其中一个域用于企业邮件流量。即使已经在生产域中正确部署了 SPF，攻击者仍可利用其他不经常用于传送邮件的域，以伪装组织的身份。SPF 可以防止这种情况发生，方法是利用一个特别的“deny all”SPF 记录，对于不生成邮件流量的任何域（包括子域！），请在 DNS 中发布“v=spf1 –all”。SPF 理事会的网站 openspf.org 就是一个最佳示例。

由于 SPF 委派仅对单个域有效，因此必须为可能使用但不一定会生成邮件的任何子域发布“deny all”SPF 记录。即使生产域已有“regular”SPF 记录，也一定要将“deny all”记录添加到不生成邮件流量的子域中。再强调一次-不要忘记接收并不等同于发送：域很可能接收电子邮件，但永远不会成为来源。特别是短期营销域（例如活动、限时促销、产品发布等），传入这些域的邮件会被传送到生产域，对这些邮件的任何回复也会从生产域传出。这些短期域将拥有一个有效的 MX 记录，但也应具有可将其标识为没有邮件来源的 SPF 记录。

DKIM 部署注意事项

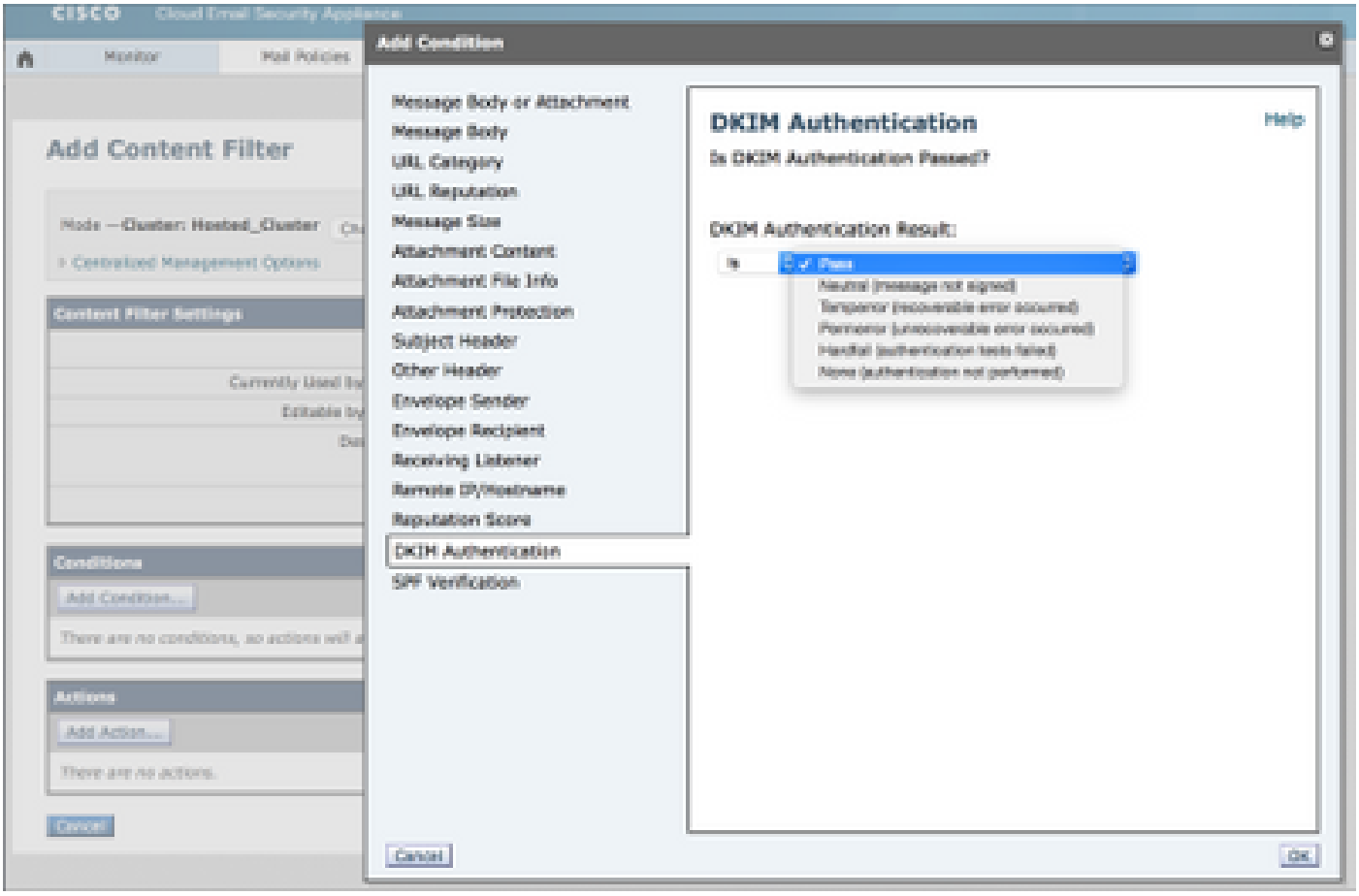
面向收件人的 DKIM

为 ESA 配置 DKIM 验证策略类似于配置 SPF 验证策略。在“邮件流策略”的“默认策略参数”中，只需将“DKIM 验证”设置为“开启”。同样，由于 DKIM 不支持指定任何策略，因此将只验证签名并插入“Authentication-Results”头：

`Authentication-Results`： mx1.hc4-93.c3s2.smtpi.com； dkim=pass (signature verified) header.i=MileagePlus@news.united.com

任何基于 DKIM 验证结果的操作都必须由内容过滤器执行：

图片2：DKIM验证内容过滤器条件



与简单直观的 SPF 不同，DKIM 是针对实际邮件文本进行操作，因此某些参数可能会受到限制。您也可以创建 DKIM 验证配置文件，并将不同的验证配置文件分配给不同的邮件流策略。通过这些配置文件，您可以限制可接受的签名密钥大小、设置密钥检索失败操作次数以及配置 DKIM 验证的深度。

邮件通过多个网关传送时，由于可对邮件进行多次签名，因此该邮件将含有多个签名。要让这样的邮件通过 DKIM 验证，需要对任何签名进行验证。默认情况下，ESA 最多验证五个签名。

由于 SMTP 和邮件一直以来的开放性，加之整个互联网用户并未积极适应这些变化（正面的），DKIM 签名仍存在很多合法失败的情况，例如邮件列表管理器直接中继但修改了邮件时，或直接转发邮件而不是作为新邮件的附件传送时。因此，针对未通过 DKIM 验证的邮件，最佳做法仍然是隔离或标记，而不是将其丢弃。

准备使用 DKIM 进行签名

在 RELAYED 邮件流策略中开启 DKIM 签名之前，需要生成/导入密钥，创建 DKIM 签名配置文件并在 DNS 中发布公钥。

为单个域创建签名的过程非常简单。生成密钥对，在“邮件策略”的“域密钥”部分创建一个签名配置文件。该配置文件准备就绪后，点击“DNS 文字记录”下的“生成”选项。将生成的密钥发布在 DNS 中。最后，在“邮件流策略”中开启 DKIM 签名。

为多个不同的域创建签名的过程会复杂一些。要实现此操作，您有两种选择：

1. 用单个签名配置文件为所有域创建签名。需要将（单个）公钥存储在 DNS 的“主”域中，DKIM 签名将引用该公钥。ESP 过去经常使用此技术，这可以让他们实现规模化签名，而不必与每个客户的 DNS 空间交互 [5]。
2. 为要签名的每个域创建独立的签名配置文件。这会让初始配置变得复杂一些，但可以在未来提供更大灵活性。为每个域创建一个密钥对，在“配置文件用户”部分创建仅指定一个域（及其子域）的配置文件，并将相关公钥发布在该特定域的 DNS 区域中。

选项 #1 的初始配置更简单，但它最后无法通过 DMARC 验证。由于 DMARC 要求签名域 ID 与 Header From 一致，因此 DKIM 的标识符一致性验证将失败。如果正确配置了 SPF，并依靠 SPF 标识符一致性通过 DMARC 验证，有可能避开此问题。

但是，如果一开始就实施选项 2，就无需再担心 DMARC 验证失败问题，而且为单个域撤销或重新配置签名服务也会非常简单。 此外，如果您为第三方域提供部分邮件服务，则很可能需要从他们那里获得要使用的密钥（并将其导入到您自己的 ESA 中）。该密钥是特定于域的，因此需要创建单独的配置文件。

如果您使用第三方邮件服务

通常，如果您使用 DKIM 签名并将部分邮件处理任务（例如营销邮件）外包给第三方，您不希望他们使用的密钥与你在生产域中使用的密钥相同。这是 DKIM 提供选择器的主要原因之一。与之前的操作不同，您应生成一个新的密钥对，在 DNS 区域发布公钥，并向另一方传送私钥。这也可以让您在出现问题时快速撤销该特定密钥，同时保持 DKIM 生产基础设施不变。

虽然对于 DKIM 不是必需（同一域的邮件可以使用多个不同的密钥进行签名），但最好为第三方处理的任何邮件提供单独子域。这可以让您更轻松地跟踪邮件，并在以后更清晰地实施 DMARC。例如，请考虑以下来自 Lufthansa 的多封邮件的五个 DKIM-Signature 头：

```
DKIM签名：v=1；a=rsa-sha1；c=relaxed/relaxed；s=汉莎航空
；d=newsletter.milesandmore.com；

DKIM签名：v=1；a=rsa-sha1；c=relaxed/relaxed；s=汉莎航空
2；d=newsletter.lufthansa.com；

DKIM签名：v=1；a=rsa-sha1；c=relaxed/relaxed；s=汉莎航空3；d=lh.lufthansa.com；

DKIM签名：v=1；a=rsa-sha1；c=relaxed/relaxed；s=汉莎航空4；d=e.milesandmore.com

DKIM签名：v=1；a=rsa-sha1；c=relaxed/relaxed；s=汉莎航空5；d=fly-
```

lh.lufthansa.com；

可以看到，Lufthansa 将五个不同的密钥（选择器）分别用于两个主生产域（lufthansa.com 和 millisandmore.com）的五个独立子域中。这意味着您可以独立控制每个域，并可将每个域外包给不同的邮件服务提供商。

DMARC 部署注意事项

面向收件人的 DMARC

针对 ESA 的 DMARC 验证是基于配置文件的，但与 DKIM 不同，默认配置文件必须经过编辑，以符合规范要求。ESA 的默认行为是从不丢弃任何邮件（除非客户有明确指示），因此默认 DMARC 验证配置文件会将所有操作设置为“无操作”。此外，要生成正确的报告，需要编辑“邮件策略”DMARC 部分的“全局设置”。

完成配置文件的设置后，与其他两种验证机制一样，在“邮件流策略”的“默认策略设置”部分设置 DMARC 验证。确保选中发送汇总反馈报告的复选框，这应该是 DMARC 为发件人提供的最重要的功能。撰写本文时，ESA 还不支持生成每封邮件的失败报告（DMARC 策略的“ruf”标签）。

与 SPF 或 DKIM 不同，由于 DMARC 策略操作是由发件人设置的，因此在配置文件的配置之外，没有可配置的特定操作。无需创建任何内容过滤器。

DMARC 验证会向 Authentication-Results 头添加其他字段：

Authentication-Results： mx1.hc4-93.c3s2.smtpi.com； dkim=pass (signature verified) header.i=MileagePlus@news.united.com； dmarc=pass (p=none dis=none) d=news.united.com

在上面的示例中，我们看到基于 DKIM 标识符一致性对 DMARC 进行了验证，且发件人要求策略为“none”。这表示它们当前处于 DMARC 部署的“监控”阶段。

如果您为其他域或第三方提供邮件服务

ESP 实现 DMARC 合规性的一个最主要问题是实现适当的标识符一致性。规划 DMARC 时，请确保 SPF 设置正确，所有其他相关域在您的 SPF 记录中都有您的传出网关，并且它们不会提交未通过一致性验证的邮件，这主要通过为 MAIL FROM 和 Header From 身份使用不同的域来实现。此错误最常见于发送邮件通知或警告的应用，因为很多应用作者并不知道邮件身份不一致带来的后果。

正如前面提到的，请确保为每个域使用单独的 DKIM 签名配置文件，且签名配置文件正确引用了您要签名的域（将在 Header From 中使用）。如果使用自己的子域，可以使用单个密钥进行签名，但请确保在 DMARC 策略中将 DKIM 的遵守情况设置为“relaxed” (“adkim=r”)。

通常，如果您为很多第三方提供邮件服务且无法直接对其进行控制，建议编写一份指南，介绍如何提交最有可能传送的邮件。由于用户对用户的邮件通常不会存在此问题，因此该指南主要用作上述示例中的应用作者的策略文档。

如果您使用第三方邮件服务

如果您通过第三方传送部分邮件流量，最佳方式是向第三方提供商委派单独的子域（或完全不同的域）。这样，他们就可以根据需要管理 SPF 记录、拥有独立的 DKIM 签名基础设施，并且不会干扰您的生产流量。此外，外包邮件的 DMARC 策略可以不同于内部邮件。前面已经提到，在考虑第三方传送的邮件时，请始终确保标识符的一致性，并确保在 DMARC 策略中对 DKIM 和 SPF 的遵守情况进行了合理地设置。

不生成邮件流量的（子）域

与前面两种邮件身份验证技术相比，DMARC 的另一大改进是其处理子域的方式。默认情况下，特定域的 DMARC 策略将应用于所有子域。 检索 DMARC 策略记录时，如果在 Header From FQDN 级别找不到任何记录，则收件人必须确定发件人的组织域 [6]，并在其中查找策略记录。

但是，组织域的 DMARC 策略也可指定单独的子域策略（DMARC 记录的“sp”标签），该策略将应用于未发布明确 DMARC 策略的任何子域。

在前面的 SPF 章节所讨论的场景中，您需要执行以下操作：

1. 为属于合法邮件来源的任何子域发布明确的 DMARC 记录。
2. 在组织域策略记录中发布“reject”子域策略，以自动拒绝任何伪装成非发送域的邮件。

这种邮件身份验证结构可以为您的基础设施和品牌提供最佳保护。

DMARC 特定问题

DMARC 存在一些潜在问题，这些问题源自它所依赖的其他身份验证技术的固有特性和缺陷。由于 DMARC 会主动推送拒绝邮件的策略，并关联邮件中所有不同发件人的标识符，因此将这些问题充分暴露出来。

大多数问题出现在邮件列表和邮件列表管理软件上。将邮件发送至邮件列表时，系统会将该邮件重新分发给所有收件人。但是，生成的邮件（带有原始发件人的发件人地址）将由邮件列表管理器的托管基础设施传送，因此无法通过 SPF 的 Header From 检查（大多数邮件列表管理器使用列表地址作为 Envelope From (MAIL FROM)，并使用原始发件人地址作为 Header From）。

由于 DMARC 的 SPF 验证将失败，因此需要依靠 DKIM 验证，但大多数邮件列表管理器还会向邮件添加页脚，或使用列表名称标记主题，从而导致 DKIM 签名验证失败。

对于此问题，DKIM 的创作者们提出了几种解决方案，所有这些解决方案最终都归结为，邮件列表管理器必须在所有 From 地址中使用列表地址，并通过其他方式指示原始发件人地址。

仅通过 SMTP 复制原始邮件并转发给新收件人的邮件也会出现类似问题。但是，目前使用的大多数邮件用户代理都能正确生成新邮件，并以内联形式或作为新邮件的附件来添加转发邮件。如果转发用户通过了 DMARC 验证，那么以这种方式转发的邮件也能通过 DMARC 验证（当然，无法确定原始邮件的真实性）。

实施邮件身份验证的操作计划示例

技术本身没有多少难度，但要实施完整的邮件身份验证基础设施，整个过程可能漫长而曲折。对于规模较小且具有受控邮件流的组织，实施过程会非常简单，而对于规模较大的组织，实施过程可能

充满挑战。因此，大型企业常常聘请咨询团队来管理实施项目。

第1步：DKIM

实施 DKIM 相对简单，因为未签名的邮件不会导致任何邮件拒绝问题。在真正实施之前，请考虑前面提到的所有要点。联系您可能委托签名的任何第三方，确保第三方支持 DKIM 签名，并考虑好选择器管理策略。有些组织会针对不同的组织单位保留单独密钥（选择器）。为提升安全性，您可以考虑定期轮换密钥，但请确保在成功传送所有邮件之前不要删除旧密钥。

您还需要特别注意密钥大小。虽然通常是“越多越好”，但必须考虑到，为每封邮件创建两个数字签名（包括规范化等）会占用大量 CPU 资源，同时也会影响传出邮件网关的性能。考虑到计算开销，2048 位是可供使用的最大实际密钥大小，不过对于大多数部署，1024 位密钥就能很好地兼顾性能和安全性。

为成功实施后续的 DMARC，您应完成以下操作：

1. 标识您发送邮件用到的所有域，包括子域
2. 为每个域生成 DKIM 密钥并创建签名配置文件
3. 将相关私钥传送给所有第三方
4. 在相关 DNS 区域中发布所有公钥
5. 验证第三方是否已准备好开始签名
6. 为所有 ESA 的 RELAYED 邮件流策略启用 DKIM 签名
7. 通知第三方开始签名

第2步：SPF

正确实施 SPF 可能是任何邮件身份验证基础设施实施中最耗时、最麻烦的部分。由于邮件的使用和管理非常简单，而且从安全和访问角度来看是完全开放的，因此组织一直以来都没有对使用邮件的人员和方式实施严格的策略。这导致当今大多数组织无法全面了解来自内部和外部的所有不同邮件来源。实施 SPF 的一个最大问题是识别谁正在代表您合法发送邮件。

需要查找的邮件来源：

1. 明显目标 - Exchange 或其他组件服务器或传出邮件网关
2. 可能生成外部通知的任何 DLP 解决方案或其他邮件处理系统
3. 向客户发送交互信息的 CRM 系统
4. 可能发送邮件的各种第三方应用
5. 可能发送邮件的实验、测试或其他服务器
6. 被配置为直接发送外部邮件的个人计算机和设备

由于组织所处的环境不尽相同，因此上述列表并不完整，但应将其视为查找邮件来源的一般性准则。确定所有或大部分邮件来源后，您需要先清理邮件来源列表，而不是对每一个现有邮件来源进行授权。理想情况下，所有传出邮件都应通过传出邮件网关传送，只有少数合理情况除外。如果有自己的或使用第三方营销邮件解决方案，应为其使用与生产邮件网关不同的独立基础设施。如果您的邮件传送网络非常复杂，可以继续在 SPF 中记录当前状态，但请务必在未来留出时间解决此问题。

如果通过同一基础设施为多个域提供服务，需要创建一个通用 SPF 记录，并使用“include”机制在各个域中引用该记录。确保您的SPF记录不是太宽；例如，如果/24网络中只有5台计算机发送

SMTP，请将这5个单独的IP地址添加到SPF中，而不是添加到整个网络。SPF 记录应尽可能具体，以最大限度减少威胁您身份的恶意邮件。

先从不匹配发件人的 softfail 选项 (“~all”) 开始。只有在 100% 确定已识别所有邮件来源后，才能将其更改为 hardfail (-all)，否则可能会丢失生产邮件。实施 DMARC 并在监控模式下运行一段时间后，您就能识别遗漏的任何系统，并更新 SPF 记录以使其完整。只有这样，将 SPF 设置为 hardfail 才是安全的。

第3步：DMARC

尽可能完整设置 DKIM 和 SPF 后，就可以创建 DMARC 策略了。请考虑前面章节中提到的所有不同情况，如果您的邮件基础设施比较复杂，请准备好部署多个 DMARC 记录。

创建用于接收报告的邮件别名，或创建可以接收报告的 Web 应用。对于该邮件别名的地址没有严格要求，但其最好具有一定描述性，以方便识别。例如 rua@domain.com、dmarc.rua@domain.com、mailauth-rua@domain.com。确保您拥有一套完整流程，方便操作人员监控这些地址并对 SPF、DKIM 和 DMARC 配置进行相应修改，或在出现欺骗活动时及时提醒安全团队。最初，工作负载可能很大，因为您需要对记录不断调整，以添加 SPF 和 DKIM 配置期间可能遗漏的任何内容。一段时间后，报告可能仅指示欺骗活动。

最初，将 DMARC 策略设置为“none”，并将调查分析选项设置为发送任何未通过检查的报告 (“fo=1”)，这有助于快速发现 SPF 和 DKIM 中存在的任何错误，而且不会影响流量。提交的报告内容达到您的要求后，请根据您的安全策略和偏好，将该策略更改为“Quarantine”或“reject”。同样，请确保指派操作人员持续分析收到的 DMARC 报告，以判断是否存在任何误报。

完整而正确地实施 DMARC 不是一项可短时间内完成的简单任务。发布不完整的记录集和将策略设置为“none”也许能够获得部分结果（以及 DMARC 的正式“实施”），但相关各方全面实施该策略符合发件人组织和整个互联网的最大利益。

下面是为某个典型项目实施各个步骤的大概时间表。由于每个组织所处的环境各不相同，因此下面的这个时间表并非完全准确：

1. 计划和准备 DKIM	2-4 周
2. 运行 DKIM 测试	2 周
3. SPF - 确定合法发件人	2-4 周
4. 准备 DMARC 策略	2 周
5. 运行 SPF 和 DMARC 记录测试	4-8 周

6. 运行 SPF hardfail 测试	2 周
7. 运行 DMARC quarantine/reject 测试	4 周
8. 监控 DMARC 报告并对 SPF/DKIM 进行相应调整	持续

较小的组织可能会经历大多数步骤的较短持续时间，尤其是第3步和第4步。无论您认为电邮基础设施多么简单，在测试运行期间始终分配充足的时间，并密切监控您可能错过的任何问题的反馈报告。

规模较大的组织可能需要较长时间才能完成相同步骤，测试要求也会更加严格。邮件基础设施较为复杂的企业常常寻求外部帮助，其中不仅涉及邮件身份验证实施的技术方面，还涉及整个项目的管理以及各团队和部门的协调。

其他参考

- SPF参考站点：http://www.openspf.org
- DKIM委员会：http://www.dkim.org
- DMARC主网站，由受信任域项目运行：http://www.dmarc.org
- dmarcian - 帮助和资源网站，由 DMARC 的作者之一 Tim Draegen 运营。确保访问“工具”部分：http://www.dmarcian.com
- 在线信任Alliance的记录验证程序工具：https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant -另一个帮助您创建DMARC记录的工具：http://www.kitterman.com/dmarc/assistant.html
- SPF记录测试工具：http://www.kitterman.com/spf/validate.html
- “不要成为网络钓鱼：深入探讨电子邮件身份验证技术”，Cisco Live 2014年演示文稿 BRKSEC-3770：https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] 规范化不在本文档的讨论范围内。有关 DKIM 规范化的详细信息，请参阅“其他参考”部分中的资料。

[2] DKIM DNS 记录参数也不在本文档的讨论范围内。

[3] 创建邮件过滤器不在本文档的讨论范围内。如需获得相关帮助，请参阅《AsyncOS for Email 用户指南》。

[4] M3AAWG 制定了一系列优秀的最佳实践，被行业大多数组织所采用并获得广泛认可。您可以通过以下网址获取他们发布的《发件人最佳常见做法》文档：https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5] 此行为利用了以下事实：DKIM 最初完全不验证 MAIL FROM 或 Header From 中声明的邮件来源。它仅验证签名域 ID（DKIM 签名的“d”参数和签名配置文件中的“Domain Name”参数）是否确实托管用于对邮件进行签名的密钥对的公钥。通过对“From”信头进行签名来表示发件人的真实性。只

需确保在“配置文件用户”部分列出为其签名的任何和所有域（和子域）。

[6] 通常是比 TLD 低一级的域或相关的 ccTLD 前缀（.ac.uk、.com.sg 等）

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）。