電子郵件驗證最佳作法 - 部署 SPF、DKIM 和 DMARC 的絕佳方法

目錄

簡介

本指南介紹了當前使用的三種主流電子郵件身份驗證技術 — SPF、DKIM和DMARC，並討論了其實施的各個方面。本文討論了幾種實際的電子郵件架構情況，以及在思科電子郵件安全產品集中實施這些情況的准則。由於這是實踐最佳做法指南，因此將省略一些比較複雜的材料。必要時，可以簡化或壓縮某些概念，以方便理解所介紹的事項。

產品知識要求

本指南是高級文檔。要完成演示材料，讀者應具備思科郵件安全裝置的產品知識，達到思科郵件安全現場工程師認證級別。此外，讀者應該對DNS和SMTP及其操作有強大的命令。熟悉SPF、DKIM和DMARC的基礎知識是一個優點。

電子郵件驗證 — 簡短概述

傳送者原則架構(SPF)

發件人策略框架最初於2006年發佈，稱為RFC4408。當前版本在RFC7208中指定，並在RFC7372中更新。本質上，它提供了一種簡單的方法，使域所有者能夠使用DNS將其合法電子郵件源通告給接收者。雖然SPF主要對返迴路徑(MAIL FROM)地址進行身份驗證，但規範建議（並提供機制）也對SMTP HELO/EHLO引數（在SMTP會話期間傳輸發件人網關的FQDN）進行身份驗證。

SPF使用語法非常簡單的TXT型別DNS資源記錄：

```
spirit.com        = "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記錄允許來自@spirit.com地址的電子郵件來自特定的/24子網、由FQDN標識的兩台電腦以及Microsoft的Office365環境。末尾的「~all」限定符指示接收方將任何其他源視為軟故障 — SPF兩種故障模式之一。請注意，發件人沒有指定接收者應對失敗消息做什麼，只是指定它們將失敗的程度。

另一方面，Delta使用不同的SPF方案：

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

為了最大限度地減少所需的DNS查詢數量，Delta建立了一個列出其所有SMTP網關的「A」記錄。它們還在"_spf.vendor.delta.com"中為供應商提供單獨的SPF記錄。這些指令還包含**Hard Fail**指令，用於識別未經SPF（「 — all」限定符）驗證的任何消息。 我們可以進一步查詢供應商的SPF記錄：

```
_spf.vendor.delta.com= "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"
```

因此，發自@delta.com的郵件可能來自法航的電郵網關。

另一方面，美聯航使用一種簡單得多的SPF方案：

```
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"
```

除了自己的企業郵件網關，還包括其電子郵件行銷提供商(「usa.net」和「enviaremails.com.br」)、舊版大陸航空網關以及MX記錄（「MX」機制）中列出的所有內容。 請注意，MX(域**的**傳入郵件網關)可能不同於傳出**網關**。對於較小的企業，它們通常是相同的，而較大的企業將有單獨的基礎架構來處理傳入郵件，有單獨的處理傳出郵件。

另外，值得注意的是，上述所有示例都廣泛使用了其他DNS推薦（「包括」機制）。 但是，由於效能原因，SPF規範將檢索最終記錄所需的DNS查詢總數限製為**10個**。任何具有超過10級DNS遞迴的SPF查詢都將失敗。

域金鑰識別郵件(DKIM)

在RFC 5585、6376和5863中指定的DKIM是兩個歷史建議的融合：Yahoo的DomainKeys和思科的Identified Internet Mail。它為發件人提供了對傳出郵件進行密碼簽名的簡單方法，並將簽名（連同其他驗證後設資料）包括在電子郵件標頭(「DKIM-Signature」)中。 發件人在DNS中發佈其公鑰，因此使得任何接收者都可以輕鬆檢索金鑰並驗證簽名。DKIM不對物理郵件的源進行身份驗證，但依賴於以下事實：如果源擁有發件人組織的私鑰，則隱式授權代表其傳送電子郵件。

為了實現DKIM，傳送組織將生成一個或多個公鑰對，並將公鑰作為TXT記錄在DNS中。每個金鑰對將由「選擇器」引用，因此DKIM驗證器可以區分金鑰。將對傳出郵件進行簽名，並插入DKIM簽名標頭：

```
DKIMv=1;a=rsa-sha1;c=/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+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKhH1MMTyYgwYqT01rEwL0V8MEY1MzxTrzijkLPGqt/sKK1K
WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJMRwxtgoWdfHU35CsFG2CNYLo=
```

簽名的格式相當簡單。"a"標籤指定用於簽名的演算法，"c"指定使用[1]的規範化方案，"s"是選擇器或金鑰引用，"d"是簽名域。此DKIM簽名標頭的其餘部分特定於郵件：「h」列出簽名信頭，「i」列出簽名使用者的身份，最後，信頭以兩個單獨的雜湊結束：「bh」是帶符號標頭的雜湊值，而「b」是消息正文的雜湊值。

接收者收到DKIM簽名的消息時，將通過構建以下DNS查詢來查詢公鑰：

```
<selector>._domainkey.<>
```

如DKIM簽名標頭中所指定。對於上述示例，我們的查詢是「united._domainkey.news.united.com」：

```
united._domainkey.news.united.com= "g=*\;k=rsa\;n=" ""
"postmaster@responsys.com" "" "" "" "" "" ""
"\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q
2KkWgl35hO4v6dTy5QmxcuV5AwqxLiz9d0jBaxtuvYALjlGkxmk5MemgAO
Cr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6OFzmw6Tp1t05NPWh0PbyUohZYt4qpcb
iz9Kc3UB2IBwIDAQAB\;
```

返回的DNS記錄包含金鑰以及其他可選引數。[2]

DKIM的主要問題是初始規範不允許通告傳送者使用DKIM。因此，如果一個郵件沒有簽名，接收者就沒有簡單的方法知道它應該被簽名，在這種情況下，它很可能是不真實的。由於單個組織可以（通常會）使用多個選擇器，因此「猜測」域是否支援DKIM並非易事。為此開發了一個獨立的標準，作者域簽名實踐，但由於使用率低和其他問題，在2013年被廢棄，沒有後繼者。

網域型訊息驗證、報告和一致性(DMARC)

DMARC是所涵蓋的三項電子郵件驗證技術中最年輕的一個，並且是專門為解決SPF和DKIM的缺點而開發的。與另外兩個不同，它驗證消息的Header From並連結到之前由另外兩個使用者執行的檢查。RFC7489中規定了DMARC。

DMARC over SPF和DKIM的附加值包括：

- 確保所有可用標識（HELO、MAIL FROM和/或DKIM簽名域）與From標頭對齊（完全匹配或從屬）
- 為發件人域所有者提供一種方法，以指定接收者必須如何處理**失敗**郵件的策略
- 為發件人域所有者提供反饋工具，使其獲知任何失敗的郵件，從而輕鬆識別SPF/DKIM/DMARC策略分配中的網路釣魚活動或錯誤

DMARC還使用簡單的基於DNS的策略分發機制：

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

DMARC策略規範中唯一的強制標籤是「p」，指定用於失敗消息的策略。它可以是以下三者之一：無、隔離、拒絕。

最常用的可選引數與報告有關："rua"指定URL(郵件至：或使用POST方法的http:// URL)，以傳送有關所有聲稱來自特定域的失敗消息的每日彙總報告。「ruf」指定一個URL，以便對每個失敗消息立即提交詳細的失敗報告。

根據規範，接收方**必須**遵守通告的策略。如果沒有，則它們必**須**在聚合報告中通知發件人域所有者。

DMARC的核心概念是所謂的識別符號對齊。識別符號對齊定義了消息如何通過DMARC驗證。SPF和DKIM識別符號單獨對齊，並且需要傳遞其中的任何一**個**消息才能整體傳遞DMARC。但是，有一個DMARC策略選項，傳送方可以請求生成失敗報告，即使一個對齊通過，但另一個失敗。在上面的「fo」標籤設定為「1」的示例中，我們可以看到這一點。

報文有兩種方法可遵守DKIM或SPF識別符號對齊方式，嚴格和放鬆。嚴格遵循意味著「發件人」的FQDN必須與SPF的DKIM簽名的簽名域ID（「d」標籤）或SMTP命令的MAIL FROM的FQDN完全匹配。另一方面，Relaxed允許Header From FQDN為前面提到的兩個子域。 在將您的電子郵件流量委託給第三方時，這將產生重要影響，本文檔稍後將對此進行討論。

SPF部署注意事項

接收器的SPF

在思科郵件安全裝置或雲郵件安全虛擬裝置上配置SPF驗證非常簡單。在本檔案的其餘部分，任何對ESA的提及也將包括CES。

SPF驗證在郵件流策略中配置 — 全域性運行它的最簡單方法是在相應偵聽程式的「預設策略引數」部分中開啟它。 如果對傳入和傳出郵件集合使用相同的偵聽程式，請確保您的「RELAYED」郵件流策略將SPF驗證設定為「Off」。

由於SPF不允許指定要採取的策略操作，因此SPF驗證（以及DKIM，稍後我們將看到）只驗證消息並為執行的每個SPF檢查插入一組標頭：

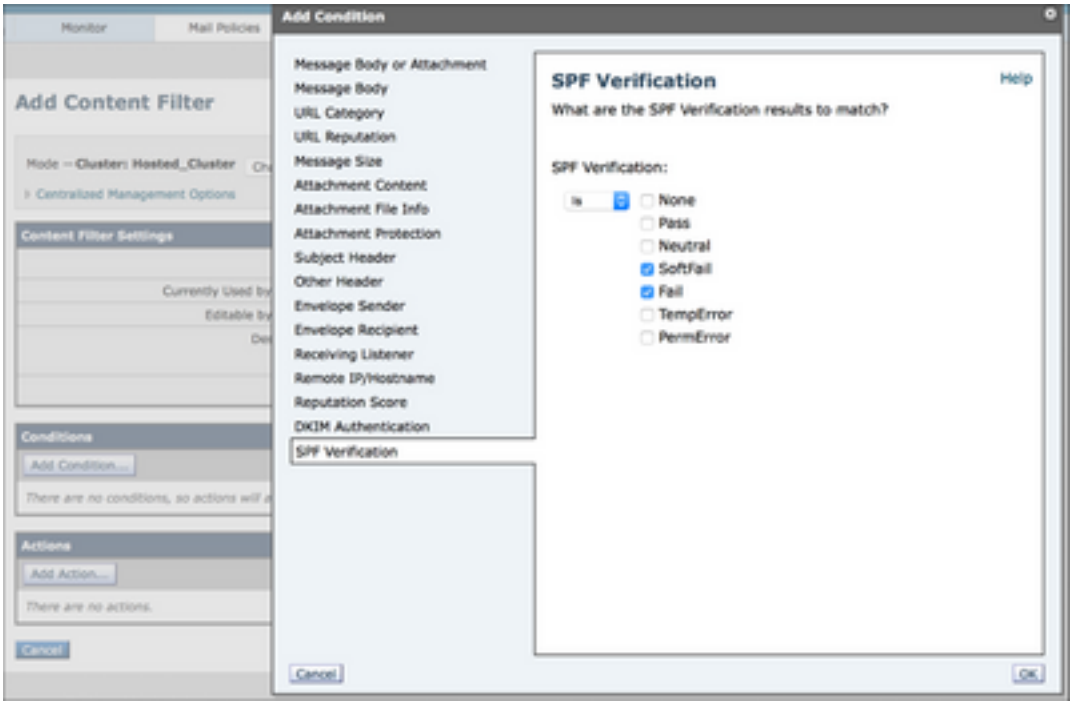
```
Received-SPF:(mx1.hc4-93.c3s2.smtpi.com:

  united.5765@envfrm.rsys2.com12.130.136.195

  )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:(mx1.hc4-93.c3s2.smtpi.com:


  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
```

請注意，對於此消息，SPF已驗證兩個「身份」：「mailfrom」由規範規定，而「helo」由規範建議。該消息將正式通過SPF，因為只有前者與SPF遵從性相關，但某些接收者可能會制裁不包含SPF記錄的發件人以確認其HELO身份。因此，最好在SPF記錄中包括您的傳出郵件網關的主機名。

郵件流策略驗證郵件後，由本地管理員來配置要執行的操作。這是使用郵件過濾器規則SPF-status()[3]完成的，或者通過使用規則建立傳入內容過濾器並將其應用於相應的傳入郵件策略來完成。

圖片1:SPF驗證內容篩選器條件



建議的過濾器操作是丟棄策略隔離區中失敗郵件（SPF記錄中為「— all」）和隔離軟失敗郵件

（SPF記錄中為「~all」），但這可能會因您的安全要求而異。有些接收者僅標籤失敗消息，或者不執行可見操作，但會向管理員報告。

最近，SPF的普及率大幅提高，但許多域發佈的SPF記錄不完整或不正確。要處於安全狀態，可能需要隔離所有SPF失敗的郵件，並監視隔離一段時間，以確保沒有「誤報」。

如果您為其他域或第三方提供電子郵件服務

如果您為第三方提供電子郵件傳送或託管服務，他們必須新增用於將郵件傳送至其自身SPF記錄的主機名和IP地址。最簡單的方法是提供商建立「umbrella」SPF記錄，並讓客戶在其SPF記錄中使用「include」機制。

```
suncountry.com= "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 ip4:107.247.57
ip4:2 7.87.182.66 ip4:199.66.248.0/22 include:cust-spf.exacttarget.com
~all"
```

我們可以看到，Sun Country的一些電子郵件由他們自己控制，但他們的行銷電子郵件外包給了第三方。展開引用的記錄會顯示其行銷郵寄服務提供商使用的當前IP地址清單：

```
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 ip4:209.43.22.0/28 245.80.0/20 147.128.0/20
147.176.0/20 111.0.0/18 ip4:198.nexus ip4:136.nexus ip4:136.nexus
ip4:13.nexus -all"
```

這種靈活性允許電子郵件服務提供商進行擴展，而無需聯絡每個客戶修改其DNS記錄。

如果您使用第三方電子郵件服務

與上一段類似，如果您使用任何第三方電子郵件服務，並且希望建立完全經SPF驗證的郵件流，則必須在您的郵件中包含他們自己的SPF記錄。

```
jetblue.comv=spf1 include:_spf.qualtrics.com ?all
```

JetBlue使用Qualtrics分析服務，他們唯一需要做的事情就是提供來自Qualtrics的正確SPF記錄。同樣，大多數其他ESP都會提供SPF記錄以包括在客戶記錄中。

如果您的ESP或電子郵件行銷人員不提供SPF記錄，您將不得不直接在您的中列出其傳出郵件網關。但是，您有責任保證這些記錄的準確性，如果提供商新增額外的網關或更改IP地址或主機名，您的郵件流可能會受到危害。

不具有SPF意識的第三方的其他風險來自共用資源：如果ESP使用同一個IP地址來傳送多個客戶的電子郵件，則從技術上講，一個客戶可以生成SPF有效消息，偽裝成通過同一介面傳送的另一客戶。因此，在設定任何SPF限制之前，您應調查您的MSP的安全策略和電子郵件身份驗證意識。如果客戶沒有您的問題答案，考慮到SPF是網際網路上的基本信任機制之一，強烈建議您重新考慮您選擇的MSP。 它不僅與安全性有關 — MSP採用的SPF、DKIM、DMARC和其他發件人最佳做法[4]是交付性的保證。如果您的MSP未遵循他們或錯誤地遵循他們，這將降低他們在大型接收系統中的可信度，並可能延遲甚至阻止您的郵件。

沒有電子郵件流量的（子）域

目前，大多陣列織都擁有多個域用於行銷目的，但僅使用一個域用於企業電子郵件流量。即使SPF正確部署在生產域上，不良參與者仍可使用未主動用於電子郵件的其他域來欺騙組織的身份。SPF可以通過特殊的「deny all」 SPF記錄來防止此情況發生 — 對於不生成電子郵件流量的任何域（和子域！），在DNS中發佈「v=spf1 -all」。一個絕佳例子是openspf.org — SPF委員會的網站。

由於SPF委派僅對單個域有效，因此還針對您可能正在使用的未生成電子郵件的任何子域發佈「拒絕所有」SPF記錄非常重要。即使您的生產域具有「常規」SPF記錄，也不要費力將「deny all」記錄新增到沒有流量的子域。再一次 — 不要忘記接收與傳送不同：域很可能接收電子郵件，但永遠不會成為來源。對於短期行銷域（例如，活動、限時促銷、產品發佈.....），情況尤其如此，傳入這些域的電子郵件將傳送到您的生產域，而對這些電子郵件的所有響應將從生產域傳送。這些短期域將具有有效的MX記錄，但應具有SPF記錄，以便將其標識為不**是**電子郵件源。

DKIM部署注意事項

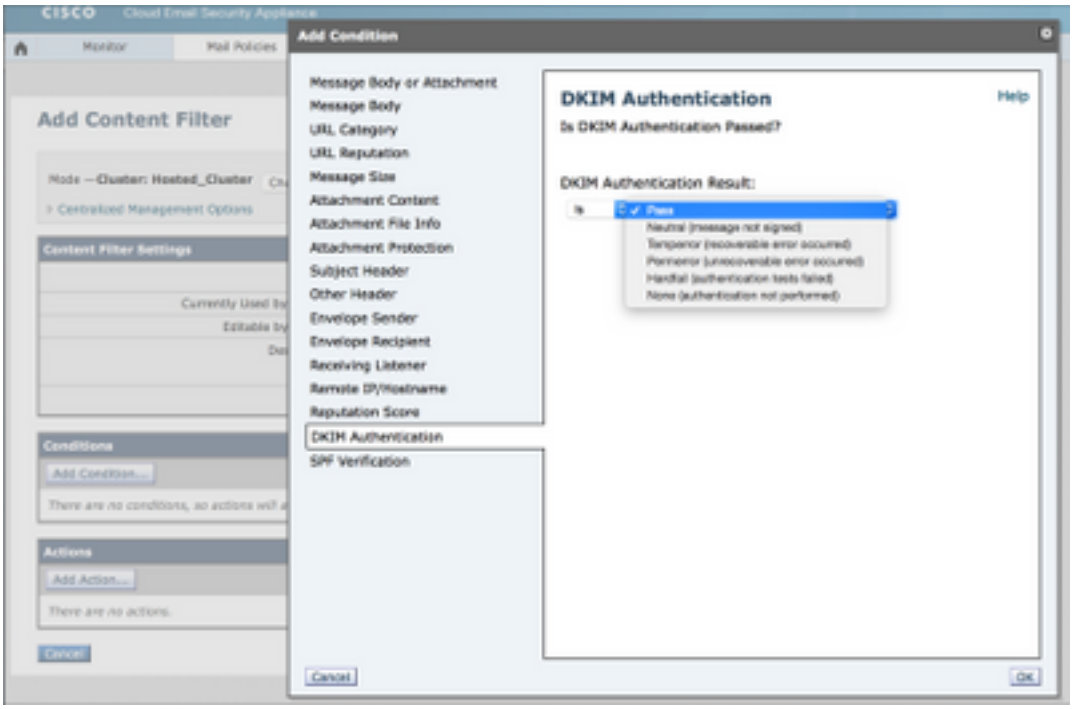
接收器的DKIM

在ESA上配置DKIM驗證與SPF驗證類似。在郵件流策略的預設策略引數中，只需將DKIM驗證設定為「開啟」。同樣地，由於DKIM不允許任何策略規範，這將只是驗證簽名並插入「Authentication-Results」標頭：

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

任何基於DKIM驗證結果的操作都必須由內容過濾器執行：

圖片2:DKIM驗證內容過濾器條件



與SPF不同的是，DKIM直接處理實際的消息文本，因此某些引數可能會受到限制。或者，您可以建立DKIM驗證配置檔案，並將不同的驗證配置檔案分配給不同的郵件流策略。它們允許您限制要接受的特徵碼的關鍵大小，設定關鍵檢索失敗操作，並配置DKIM驗證的深度。

當消息經過多個網關時，可以對其進行多次簽名，從而攜帶多個簽名。若要使郵件通過DKIM驗證，**需要**驗證任何簽名。預設情況下，ESA最多將驗證五個簽名。

由於SMTP和電子郵件的歷史開放性，以及整個Internet不願意適應（積極）的變化，仍有幾種DKIM簽名可能合法失敗，例如郵件清單管理員直接轉發但修改郵件，或者直接轉發郵件而不是作為新郵件的附件。因此，一般來說，DKIM失敗的郵件的最佳做法仍然是隔離或標籤，而不是丟棄它們。

準備與DKIM簽名

在中繼郵件流策略中啟用DKIM簽名之前，需要生成/匯入金鑰、建立DKIM簽名配置檔案並在DNS中發佈公鑰。

如果要為單個域進行簽名，則過程非常簡單。生成金鑰對，在「郵件策略」的「域金鑰」部分建立單個簽名配置檔案，並在配置檔案就緒後按一下「DNS文本記錄」下的「生成」選項。發佈在DNS中生成的金鑰。最後，在郵件流策略中啟用DKIM簽名。

如果您要簽署多個不同的域，情況會更加複雜。在這種情況下，您有兩個選擇：

1. 使用單個簽名配置檔案對所有域進行簽名。您將在「主」域的DNS區域中儲存（單個）公鑰，您的DKIM簽名將引用該金鑰。在過去，ESP經常採用這種技術 — 它允許他們大規模簽名，同時不需要與單個客戶的DNS空間進行互動[5]。
2. 為您簽署的每個域建立單獨的簽名配置檔案。這使得初始配置更加複雜，但是向前發展提供了更大的靈活性。為每個域建立一個金鑰對，在「配置檔案使用者」部分建立只指定一個域（及其子域）的配置檔案，並在該特定域的DNS區域中發佈相關公鑰。

雖然選#1的開始比較容易，但請記住，它最終會破壞DMARC。由於DMARC要求簽名域ID與標題來自對齊，因此您的識別符號與DKIM對齊將失敗。如果正確配置您的SPF，並依靠對SPF識別符號的校準通過DMARC驗證，您也許能夠順利完成該過程。

但是，通過從頭開始實施選項#2，您無需擔心DMARC，並且對於單個域撤銷或重新配置簽名服務非常容易。 此外，如果您為第三方域提供某些電子郵件服**務，則很可能需要從這些域獲取要使用的金鑰（並將其匯入ESA）。** 該金鑰將特定於域，因此您需要建立單獨的配置檔案。

如果您使用第三方電子郵件服務

通常，如果您使用DKIM簽名並將您的某些電子郵件處理（如行銷電子郵件）解除安裝給第三方，則您不希望他們使用您在生產中使用的相同金鑰。這是DKIM中存在選擇器的主要原因之一。相反，您應該生成一個新的金鑰對，在DNS區域中發佈公共部分，並將金鑰傳遞給另一方。這還允許您在出現問題時快速撤銷該特定金鑰，同時保持生產DKIM基礎架構不變。

雖然DKIM沒有必要（同一域的郵件可使用多個不同的金鑰進行簽名），但最好為第三方處理的任何電子郵件提供單獨的子域。它將使追蹤報文更容易，並且允許以後更乾淨地實施DMARC。例如，請考慮來自漢莎航空多條消息的這五個DKIM簽名信頭：

```
DKIMv=1;a=rsa-sha1;c=/s=d=newsletter.milesandmore.com;

DKIMv=1;a=rsa-sha1;c=/s=2;d=newsletter.lufthansa.com;

DKIMv=1;a=rsa-sha1;c=/s=3;d=lh.lufthansa.com;

DKIMv=1;a=rsa-sha1;c=/s=4;d=e.milesandmore.com

DKIMv=1;a=rsa-sha1;c=/s=5;d=fly-lh.lufthansa.com;
```

我們可以看到，漢莎航空使用五個不同的鍵（選擇器），拆分為兩個主要生產域(lufthansa.com和milesandmore.com)的五個獨立的子域。 這意味著每個報文傳送服務均可獨立控制，並可外包給不同的報文傳送服務提供商。

DMARC部署注意事項

接收器的DMARC

ESA上的DMARC驗證基於配置檔案，但與DKIM不同，必須編輯預設配置檔案才能符合規範。ESA的預設行為是除非客戶明確指示，否則從不丟棄任何消息，因此預設DMARC驗證配置檔案的所有操作都設定為「無操作」。此外，要生成正確的報告，您需要編輯「郵件策略」的DMARC部分的「全域性設定」。

配置檔案設定完成後，DMARC驗證就像其他兩個一樣，在「郵件流策略」的「預設策略設定」部分設定。確保選中此框以傳送彙總反饋報告 — 這可以說是DMARC對發件人最重要的功能。在編寫本報告時，ESA不支援生成每條消息的故障報告（DMARC策略的「ruf」標籤）。

由於DMARC策略操作由傳送者建議，與SPF或DKIM不同，在配置檔案配置之外沒有可配置的特定操作。無需建立任何內容過濾器。

DMARC驗證將在Authentication-Results標題中新增其他欄位：

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

在以上示例中，我們看到基於DKIM識別符號對齊方式驗證了DMARC，並且傳送方請求了「無」策略。這表明它們當前處於DMARC部署的「監控」階段。

如果您為其他域或第三方提供電子郵件服務

ESP對於DMARC合規性的最大關注點是實現適當的識別符號對齊。在規劃DMARC時，請確保您的SPF設定正確，所有其他相關域在SPF記錄中都有您的傳出網關，並且它們不會提交將不能對齊的郵件，這主要是通過為MAIL FROM和Header From標識使用不同的域來實現的。此錯誤通常由傳送電子郵件通知或警告的應用程式完成，因為應用程式編寫者大多不知道其電子郵件標識不一致的結果。

如前所述，請確保為每個域使用單獨的DKIM簽名配置檔案，並且簽名配置檔案正確引用了報頭髮件人中使用的要簽名的域。如果您使用自己的子域，可以使用單個金鑰進行簽名，但是請確保在DMARC策略中將對DKIM的遵守設定為鬆動(「adkim="r」)。

一般而言，如果您為大量無法直接控制的第三方提供電子郵件服務，那麼最好編寫一份指導性文檔，說明如何提交最可能發出的電子郵件。由於使用者到使用者電子郵件通常表現良好，因此，在以上示例中，這主要用作應用程式作者的策略文檔。

如果您使用第三方電子郵件服務

如果您使用第三方傳送您的某些電子郵件流量，最佳方法是將單獨的子域（或完全不同的域）委託給第三方提供商。這樣，他們就可以根據需要管理SPF記錄，具有單獨的DKIM簽名基礎結構，而不會干擾您的生產流量。然後，外包電子郵件的DMARC策略可能與內部不同。如前所述，在考慮第三方傳送的電子郵件時，請始終確保您的識別符號將保持一致，並且您的DMARC策略中適當設定

了對DKIM和SPF的遵守情況。

沒有電子郵件流量的（子）域

DMARC相對於以前電子郵件驗證技術的另一個改進是它如何處理子域。預設情況下，特定域的DMARC策略適用於其所有子域。檢索DMARC策略記錄時，如果在標頭的FQDN級別上找不到記錄，則接收方有義務確定傳送方的組織域[6]，並在此查詢策略記錄。

但是，組織域的DMARC策略還可以指定單獨的子域策略（「DMARC記錄的sp」標籤），該標籤將適用於未發佈顯式DMARC策略的任何子域。

在SPF章節前面討論的場景中，您將：

1. 為作為合法電子郵件源的任何子**域**發佈顯式DMARC記錄。
2. 在組織域策略記錄中發佈「拒絕」的子域策略，以自動拒絕欺騙非傳送域的任何電子郵件

這種電子郵件身份驗證的結構化可最大程度地保護您的基礎架構和品牌。

DMARC特定問題

DMARC存在一些潛在問題，所有這些問題都源於它所依賴的其他身份驗證技術的性質和缺點。問題在於DMARC通過主動推送拒絕電子郵件的策略，並通過將郵件中的所有不同發件人識別符號關聯起來，使這些問題浮出水面。

大多數問題發生在郵件清單和郵件清單管理軟體上。當電子郵件傳送到郵件清單時，會將其重新分發給所有收件人。但是，生成的電子郵件（帶有原始發件人的發件人地址）將通過郵件清單管理器的宿主基礎設施傳遞，從而無法通過SPF檢查郵件頭髮件人(大多數郵件清單管理器將清單地址用作信封發件人(MAIL FROM)，將原始發件人的地址用作郵件頭髮件人)。

由於DMARC會對SPF失敗，我們可以依賴DKIM，但是，大多數郵件清單管理員也會向郵件新增頁尾，或用清單名稱標籤主題，從而中斷DKIM簽名驗證。

DKIM的作者提出了幾種解決此問題的方法，所有這些方法都歸結為郵件清單的管理者必須在所有「發件人」地址中使用清單的地址，並用另一種方法指明原始發件人地址。

僅通過SMTP將原始郵件複製到新收件人的郵件也會出現類似的問題。但是，目前使用的大多數郵件使用者代理將正確形成新郵件，並將已轉發的郵件以內聯方式或作為新郵件的附件包括在內。如果轉發使用者通過（當然，無法建立原始報文的真實性），以此方式轉發的報文將通過DMARC。

實施電子郵件身份驗證的行動計畫示例

儘管技術本身很簡單，但實施完整電子郵件身份驗證基礎設施的道路可能會漫長而曲折。對於較小的組織和郵件流量受控的組織而言，這種方法相當簡單，而較大的環境可能會發現它極具挑戰性。大型企業聘請諮詢幫助來管理實施專案的情況並不少見。

第1步：DKIM

DKIM相對不具侵入性，因為未簽名的消息不會遭到任何拒絕。在實際執行之前，考慮到前面提到的所有要點。聯絡您可能委託簽署的任何第三方，確保您的第三方支援DKIM簽署，並考慮您的選擇器管理策略。有些組織會為不同的組織單位保留不同的鍵（選擇器）。為了增強安全性，您可以考慮金鑰的定期輪替，但是請確保在傳送所有郵件之前不刪除舊金鑰。

應特別考慮關鍵尺寸。雖然一般情況下「更多更好」，但您必須考慮為每封郵件建立兩個數位簽章（包括規範化等）是一項非常昂貴的CPU任務，而且會影響外發郵件網關的效能。由於計算開銷，2048位是可使用的最大的實用金鑰大小，但對於大多數部署而言，1024位金鑰在效能和安全性之間實現了很好的折衷。

為了成功隨後實施DMARC，您應該：

1. 標識作為傳送的所有域，包括子域
2. 為每個域生成DKIM金鑰和建立簽名配置檔案
3. 向任何第三方提供相關私鑰
4. 發佈相關DNS區域中的所有公鑰
5. 驗證第三方是否準備好開始簽名
6. 在所有ESA上啟用DKIM登入中繼郵件流策略
7. 通知第三方開始簽名

第2步：SPF

正確實施SPF可能是任何電子郵件身份驗證基礎設施實施中最耗時最麻煩的部分。由於該電子郵件的使用和管理非常簡單，而且從安全性和訪問的角度完全開放，組織過去一直沒有對使用者和使用方式實施嚴格的策略。這導致如今大多陣列織無法完整地檢視所有不同的電子郵件來源，包括來自內部和外部的電子郵件來源。實施SPF的一個最大問題是發現目前誰正代表您合法傳送電子郵件。

要查詢的內容：

1. 明顯的目標 — Exchange或其他元件伺服器或傳出郵件網關
2. 可能會生成外部通知的任何DLP解決方案或其他電子郵件處理系統
3. CRM系統傳送與客戶互動的資訊
4. 可能傳送電子郵件的各種第三方應用程式
5. 實驗室、測試或其他可能傳送電子郵件的伺服器
6. 配置為直接傳送外部電子郵件的個人電腦和裝置

以上清單並不完整，因為各組織的環境各不相同，但應將其視為關於應尋找目標的一般性指南。一旦（大多數）您的電子郵件源被識別出來，您可能會想要後退一步，清理清單而不是授權每個現有的電子郵件源。理想情況下，所有傳出電子郵件都應當通過您的傳出郵件網關傳送，只有少數合理的例外。如果您有自己的或使用了第三方行銷郵件解決方案，則應使用獨立於生產郵件網關的基礎架構。如果您的郵件傳送網路異常複雜，您可以繼續在SPF中記錄當前狀態，但需要在將來清理該情況時花費時間。

如果通過同一基礎結構為多個域提供服務，則可能要建立一個通用SPF記錄，並在各個域中使用「包括」機制引用它。確保SPF記錄不是太寬；例如，如果一個/24網路中只有五台電腦傳送SMTP，則將這些五個IP地址新增到SPF，而不是整個網路。力求使您的記錄儘可能具體，以最大程度地減少惡意電子郵件損害您身份的可能性。

從非匹配發件人(「~all」)的softfail選項開始。 只有在100%確定您已識別所有電子郵件源之後才將其更改為「硬失敗」(-all)，否則您可能會丟失生產電子郵件**源**。稍後，在實施DMARC並在監控模式下運行一段時間後，您將能夠識別您錯過的任何系統，並更新您的SPF記錄以完成操作。只有到那時，將您的SPF設定為硬故障才安全。

步驟3:DMARC

一旦設定了DKIM和SPF並儘可能完整，就應該建立DMARC策略。考慮前面章節中提到的所有不同

情況，如果您擁有複雜的電子郵件基礎架構，請準備部署多個DMARC記錄。

建立將接收報告的電子郵件別名，或建立可以接收報告的Web應用程式。沒有嚴格定義的電子郵件地址用於此目的，但如果它們是描述性的，例如rua@domain.com、dmarc.rua@domain.com、mailauth-rua@domain.com等，則會有幫助。確保您有一個操作員監控這些地址並適當修改SPF、DKIM和DMARC配置的流程，或在出現欺騙活動時向安全團隊發出警報。最初，工作量會非常大，因為您需要調整記錄以涵蓋您在SPF和DKIM配置期間可能遺漏的任何內容。過了一會兒，報告可能只顯示欺騙企圖。

最初，將DMARC策略設定為「無」，並將您的取證選項設定為傳送任何失敗檢查的報**告(**「fo=1」) — 這將快速發現SPF和DKIM中的任何錯誤，同時不影響流量。一旦您對提交的報告的內容感到滿意，請將策略更改為「隔離」或「拒絕」，具體取決於您的安全策略和首選項。同樣地，請確保您的操作員持續分析您收到的DMARC報告是否有任何誤報。

完整、正確地實施DMARC不是一項小任務，也不是一項短任務。儘管發佈不完整的記錄集和「無」政策可能獲得一些結果（以及DMARC的正式「實施」），但無論是從傳送方還是整個網際網路來說，每個人都盡其所能地實施它最符合其利益。

關於時間表，下面是一個典型專案的單個步驟的非常粗略的概述。同樣，由於每個組織都不同，這些都不準確：

1. DKIM的規劃和準備	2-4週
2. DKIM測試運行	2週
3. SPF — 合法發件人標識	2-4週
4. DMARC政策編制	2週
5. SPF和DMARC記錄測試運行	4-8週
6. SPF測試運行，硬體失敗	2週
7. DMARC測試運行，隔離/拒絕	4週
8.監測DMARC報告並相應調整SPF/DKIM	連續

較小的組織可能會經歷大多數步驟的較短持續時間，尤其是步驟3和4。無論您認為電子郵件基礎架構多麼簡單，在測試運行期間始終分配充足的時間，並且嚴密監控您可能錯過的任何內容的反饋報告。

較大的組織可能會經歷更長的相同步驟持續時間，以及更嚴格的測試要求。擁有複雜電子郵件基礎架構的公司往往會僱用外部幫助（不僅用於電子郵件身份驗證實施的技術方面，還用於管理整個專案以及跨團隊和部門進行協調），這種情況屢見不鮮。

其他參考

- SPF的參考站點：http://www.openspf.org
- DKIM理事會：http://www.dkim.org
- DMARC主網站，由受信任域專案運行：http://www.dmarc.org
- dmarcian — 一個幫助和資源網站，由DMARC的作者之一Tim Draegen經營。確保訪問「工具」部分：http://www.dmarcian.com
- Online Trust Alliance的記錄驗證器工具：https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC記錄助手 — 另一個有助於建立DMARC記錄的工具：http://www.kitterman.com/dmarc/assistant.html
- SPF記錄測試工具：http://www.kitterman.com/spf/validate.html
- 「不要像個網路釣魚者：深入瞭解電子郵件身份驗證技術」，Cisco Live 2014簡報BRKSEC-

3770:https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1]規範化不在本檔案的範圍之內。有關DKIM規範化的詳細資訊，請參閱「其他參考」一節中的資料。

[2] DKIM DNS記錄引數也超出了本文檔的範圍。

[3]創建郵件過濾器超出本文檔的範圍。如需幫助，請參閱AsyncOS for Email使用手冊。

[4] M3AWG定義了行業中大多數企業應用和認可的優秀最佳實踐。其發件人最佳常見實踐文檔位於https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5]此行為利用了以下事實：最初DKIM根本沒有按照MAIL FROM或Header From所述驗證郵件源。它僅驗證簽名域ID（「DKIM簽名」的「d」引數以及簽名配置檔案中的「域名」引數）是否的確承載用於對消息進行簽名的對的公鑰。對「發件人」標題進行簽名意味著發件人的真實性。確保列出您在「配置檔案使用者」部分登入的所有域（和子域）。

[6]通常，域低於TLD或相關的ccTLD字首（.ac.uk、.com.sg等……）