適用於思科電子郵件安全的TLS驗證流程

目錄

簡介

本檔案介紹 思科郵件安全裝置(ESA)的傳輸層安全(TLS)伺服器身份驗證流程

適用於思科電子郵件安全的TLS驗證流程

TLS驗證過程實質上是一個兩階段的驗證過程：

I — 證書驗證

這涉及驗證：

- 證書有效期 — 證書有效期
- 證書鏈頒發者
- 撤消清單等

II — 伺服器身份驗證

這是根據伺服器引用身份驗**證服務**器呈現的身份（包含在X.509公鑰證書中）的驗**證過程**。

背景

讓我們繼續使用RFC 6125中所述的身份名稱術語。

> **附註**：**呈現標識**是由伺服器X.509公鑰證書呈現的識別符號，該伺服器可以包含多個不同型別的呈現識別符號。在SMTP服務的情況下，它被包含為dNSName型別的subjectAltName副檔

名，或者作為從主題欄位派生的CN（一般名稱）副檔名。

附註：**引用標識**是從完全限定的DNS域名構造的識別符號，客戶端期望證書中存在應用程式服務。

驗證過程對於TLS客戶端來說最為重要，因為通常客戶端發起TLS會話，並且客戶端需要對通訊進行驗證。*為此，客戶端需要驗證提供的標識是否與參考標識匹配。*重點在於理解TLS驗證過程的安全性幾乎完全基於TLS客戶端。

第一步

伺服器身份驗證的第一步是通過TLS客戶端確定參考身份。這取決於應用程式中TLS使用者端認為可接受的參考識別符號的清單。此外，一個可接受的參考識別符號清單必須獨立於服務提供的識別符號來構建。[rfs6125#6.2.1]

引用標識必須是完全限定的DNS域名，並且可以從任何輸入解析（這對客戶端來說是可接受的，並且被認為是安全的）。 引用標識必須是客戶端嘗試連線的DNS主機名。

recipient email domain name是參考標識，由使用者直接表示，目的是向特定域中的特定使用者傳送消息，這也滿足了作為使用者試圖連線的FQDN的要求。只有在自託管SMTP伺服器的情況下（SMTP伺服器由同一所有者擁有和管理，並且伺服器沒有託管過多的域），該一致性才有效。因為每個域都需要列在證書中(作為subjectAltName之一：dNSName值)。 從實現角度來看，大多數證書頒發機構(CA)將域名值的數量限製為最少25個條目（最多100）。 在託管環境中則不接受，讓我們考慮一下電子郵件服務提供程式(ESP)，其中目標SMTP伺服器託管數千個域。這無法擴展。

顯式配置的參考標識似乎是解決方案，但這會施加一些限制，因為需要手動將參考標識與每個目標域的源域相關聯，*或「從第三方域對映服務獲取資料，在該服務中，使用者已顯式放置信任，並且客戶端通過連線或關聯進行通訊，該連線或關聯提供相互身份驗證和完整性檢查」。*
[RFC6125#6.2.1]

從概念上講，此查詢在配置時可以視為一次性的「安全MX查詢」，其結果永久快取在MTA上，以防止在運行狀態下受到任何DNS危害。[2]

這僅提供了對「合作夥伴」域的更強身份驗證，但對於尚未對映的泛型域，此身份驗證不會通過考試，並且也不能避免目標域一端的配置更改（如主機名或IP地址更改）。

第二步

該過程的下一步是確定呈現的身份。提供的身份由伺服器X.509公鑰證書提供，作為dNSName型別的subjectAltName擴展或在主題欄位中找到的公用名稱(CN)。其中，subject欄位為空是完全可以接受的，只要證書包含至少一個subjectAltName條目的使用者副檔名即可。

雖然公用名的使用仍然在實踐中，但會認為已棄用，目前的建議是使用subjectAltName條目。對公用名標識的支援保持向後相容性。在這種情況下，應首先使用subjectAltName的dNSName，並且僅當其為空時才檢查公用名。

附註：公用名不是強型別，因為公用名可能包含服務的友好字串，而不是其形式與完全限定的DNS域名匹配的字串

最後，當已經確定兩種型別的標識時，TLS客戶端需要將其每個參考識別符號與提供的識別符號進

行比較以便找到匹配。

ESA TLS驗證

ESA允許在交付到特定域時啟用TLS和證書驗證(使用Destination Controls頁或**destconfig** CLI命令)。 當需要TLS證書驗證時，您可以從AsyncOS 8.0.2版開始選擇兩個驗證選項之一。預期驗證結果可能會因配置的選項而異。目標控制下提供的TLS有6個不同的設定，其中有兩個重要設定負責證書驗證：

1. **需要TLS — 驗證**
2. **需要TLS — 驗證託管域**。

```
CLI: destconfig

Do you want to use TLS support?

1. No

2. Preferred

3. Required

4. Preferred - Verify

5. Required - Verify

6. Required - Verify Hosted Domains

[6]>
```

選項(4)**首選 — 驗證**的TLS驗證過程與(5)**必需 — 驗證**相同，但基於結果而採取的操作因下表所示而異。選項(6)**Required** - Verify Hosted Domains與(5)**Required - Verify**的結果完全相同，但TLS驗證流程卻非常不同。

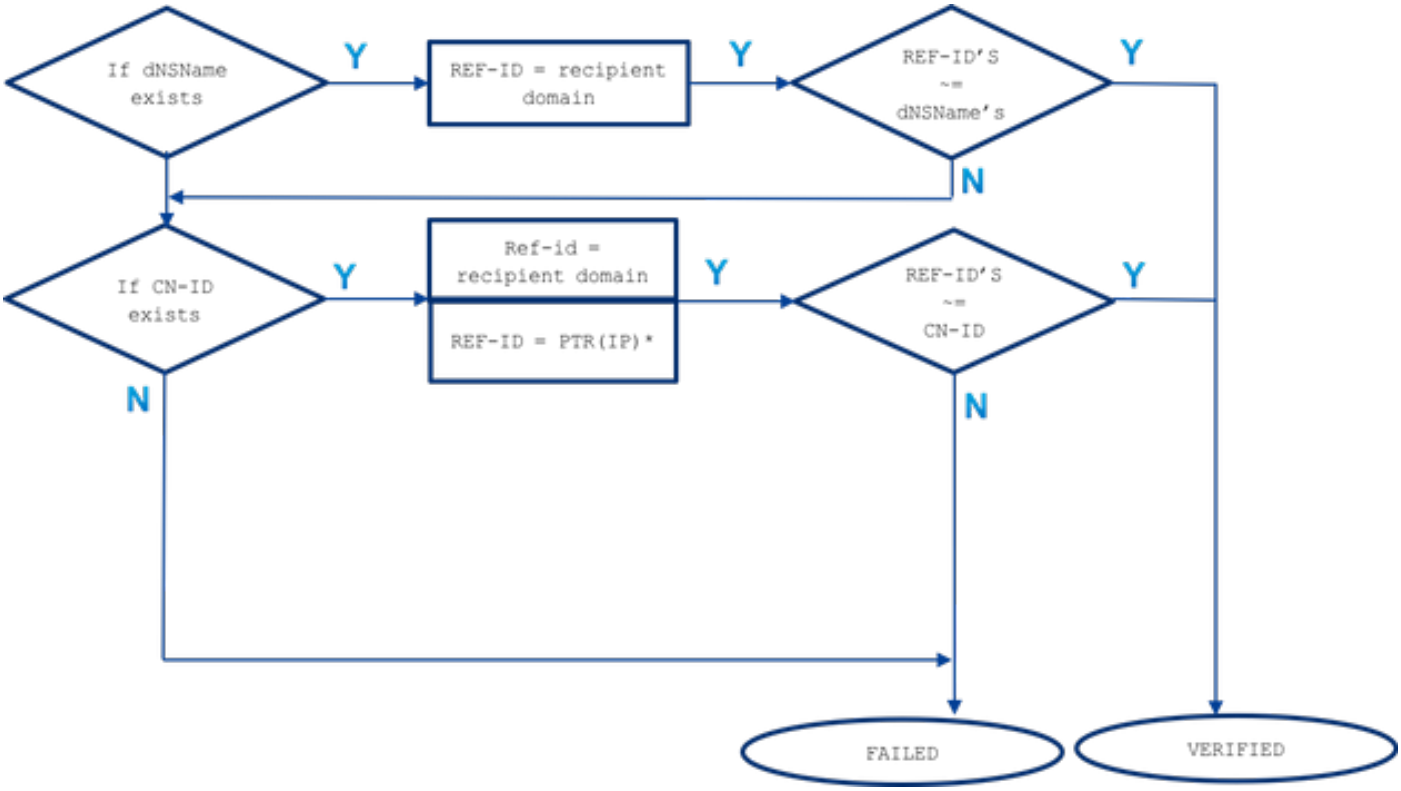
TLS設定	含義
4.首選（驗證）	TLS從郵件安全裝置協商到域的MTA。裝置會嘗試驗證域證書。 可能產生三種結果： • 將協商TLS並驗證證書。郵件通過加密會話傳送。 • 將協商TLS，但不會驗證證書。郵件通過加密會話傳送。 • 不建立TLS連線，隨後將不驗證證書。電子郵件以純文字檔案形式傳送。
5.必需（驗證）	TLS從郵件安全裝置協商到域的MTA。需要驗證域證書。 可能產生三種結果： • 協商一個TLS連線並驗證證書。該電子郵件是通過加密會話傳送的。 • TLS連線是經過協商的，但證書未經受信任CA驗證。郵件未送達。 • 不會協商TLS連線。郵件未送達。

TLS Required -Verify和**TLS Required - Verify Hosted Domain**選項之間的區別位於身份驗證過程中。處理呈現標識的方式以及允許使用何種型別的參考識別符號對最終結果有影響。以下描述以及整個文檔的用途是使此流程更接近終端使用者。由於不正確或不清楚理解本主題可能會對使用者網路造成安全影響。

需要TLS驗證

提供的標識首先從subjectAltName - dNSName副檔名匯出，如果沒有match或subjectAltName副檔名不存在，則會選中CN-ID - Common Name from subject欄位。

參考身份(REF-ID)清單由收件人域或收件人域和主機名構建，該主機名是從針對客戶端所連線的IP地址運行的PTR DNS查詢派生的。 附註：在特定情況下，不同參考身份與不同的呈現身份檢查相比較。



~=表示完全匹配或萬用字元匹配

所提供的身份（dNSName或CN-ID）與接受的參考身份進行比較，直到其匹配並按其列出的順序進行匹配。

- 如果存在subjectAltName的dNSName擴展： 僅針對收件人域執行完全匹配或萬用字元匹配

  subjectAltName匹配情況下的引用標識僅從收件人域派生。如果收件人域與任何dNSName條目不匹配，則不會檢查進一步的參考標識（如從DNS解析MX或PTR派生的主機名）

- 如果主題DN的CN存在(CN-ID): 對收件人域執行完全匹配或萬用字元匹配根據從對目標伺服器的IP執行的PTR查詢派生的主機名執行完全匹配或萬用字元匹配

  其中PTR記錄保持轉發器和解析器之間的DNS一致性。此處需要提到是，僅當PTR記錄存在時，才會將CN欄位與PTR的主機名進行比較，並且此主機名的已解析A記錄（轉發器）（參考標識）返回的IP地址與執行PTR查詢所依據的目標伺服器IP匹配。

  A(PTR(IP))== IP

  如果CN-ID是從收件人域派生的，並且當不存在匹配時，會對目標IP的PTR記錄執行DNS查詢以獲取主機名。如果PTR存在，將對從PTR派生的主機名上的A記錄執行額外查詢，以確認DNS一致性是否保留！未檢查進一步的引用（如從MX查詢派生的主機名）

綜上所述，使用「需要TLS — 驗證」選項，與dNSName或CN相比，沒有MX主機名，僅對CN檢查

DNS PTR RR，並且僅在保留DNS一致性時匹配A(PTR(IP))= IP，對dNSName和CN執行精確和萬用字元測試。

需要TLS驗證 — 託管域

呈現的標識首先從dNSName型別的subjectAltName擴展派生。如果dNSName與接受的一個引用標識(REF-ID)之間不匹配，則無論主題欄位中是否存在CN，驗證都會失敗，並且可以通過進一步的身份驗證。僅當證書不包含任何dNSName型別的subjectAltName副檔名時，才會驗證從subject欄位派生的CN。

回想一下，將呈現的身份（dNSName或CN-ID）與接受的參考身份進行比較，直到它匹配為止，並按照它們列出的順序排列。

- 如果存在subjectAltName的dNSName擴展：

  如果dNSName與下面列出的一個接受的引用標識之間沒有匹配，則標識驗證將失敗
  對收件人域執行完全匹配或萬用字元匹配： 其中一個dNSName必須與收件人域匹配使用SMTPROUTES(*)對顯式配置的主機名執行精確或萬用字元匹配根據收件人域名從（不安全的）DNS查詢派生的MX主機名，完成精確或萬用字元匹配

  如果收件人域沒有使用FQDN條目顯式配置SMTP路由，並且收件人域不匹配，則使用來自針對收件人域的（不安全的）DNS查詢的MX記錄返回的FQDN。如果沒有匹配項，則不再執行進一步的測試，不會檢查任何PTR記錄
- 如果主題DN的CN存在(CN-ID):
  僅當證書中不存在dNSName時，才會驗證CN。CN-ID與下面接受的引用標識清單進行比較。

  對收件人域執行完全匹配或萬用字元匹配完全匹配或萬用字元匹配是針對在SMTPROUTES(*)中明確配置的主機名進行的根據收件人域名從（不安全的）DNS查詢派生的MX主機名，完成精確或萬用字元匹配

明確配置的SMTPROUTES

當配置了SMTP路由且提供的標識與電子郵件收件人域不匹配時，則會比較所有FQDN路由名稱，如果不匹配，則不會進行進一步的檢查。使用顯式配置的SMTP路由時，不會將MX主機名與提供的標識進行比較。此處的例外情況使設定為IP地址的SMTP路由成為異常。

以下規則適用於顯式配置的SMTP路由：

- 當收件人域存在SMTP路由且它是完全限定DNS域名(FQDN)時，該路由被視為引用標識。將此主機名（路由名稱）與從證書中收到的呈現的標識進行比較，證書是從該主機名指向的目標伺服器派生的。

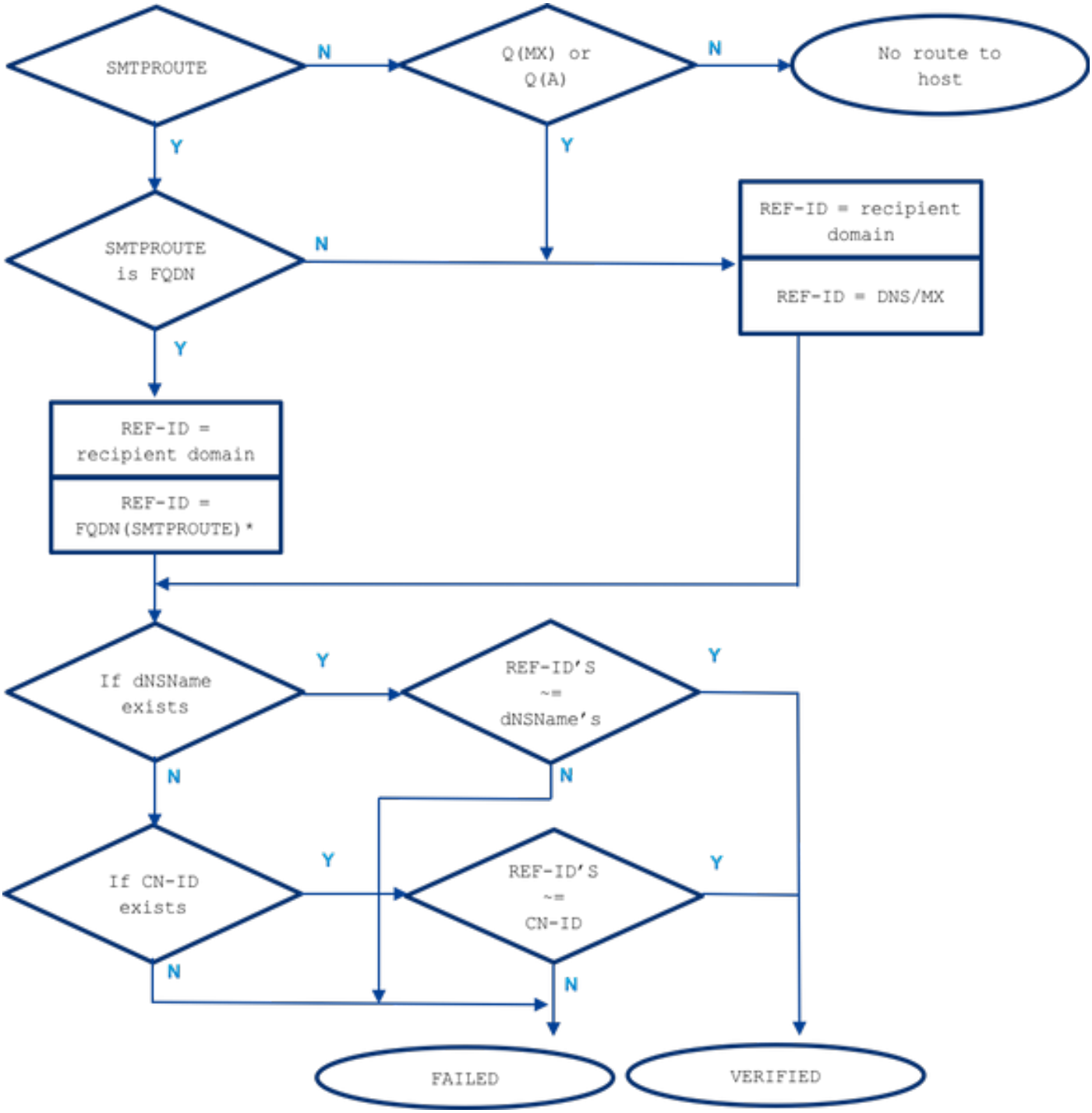
- 允許一個收件人域使用多個路由。如果收件人域有多個SMTP路由，則處理路由，直到來自目標伺服器的證書提供的識別符號與建立連線的路由的名稱相匹配。如果清單中的主機具有不同的優先順序，則會首先處理優先順序最高（0為最高且為預設值）的主機。如果所有路由的優先順序相同，則路由清單將按照使用者設定的順序進行處理。

- 如果主機沒有響應（不可用）或者它響應但TLS驗證失敗，則處理清單中的下一台主機。當第一台主機可用並通過驗證時，其它主機則未使用。

- 如果多個路由解析為相同的IP地址，則僅建立與此IP的一個連線，且從目標伺服器傳送的證書中派生的呈現身份必須與這些路由名稱之一匹配。

- 如果收件人域存在SMTP路由，但已配置為IP地址，則該路由仍用於建立連線，但來自證書的呈現身份會與收件人域進行比較，並進一步與源自DNS/MX資源記錄的主機名進行比較。

當我們討論託管域的「TLS必需驗證」選項時，ESA如何與目標伺服器連線對於TLS驗證過程非常重要，因為顯式配置的SMTP路由提供了要在該過程中考慮的額外參考標識。



~=表示完全匹配或萬用字元匹配

範例

讓我們從現實生活中舉一個例子，但是對於收件人域：example.com。下面我嘗試介紹手動驗證伺服器身份所需的所有步驟。

首先，讓我們收集有關收件人伺服器的所有必要資訊。

MX主機名：

```
example.com -> IN MX mx01.subd.emailhosted.not.
example.com -> IN MX mx02.subd.emailhosted.not.

mx01.subd.emailhosted.not. -> IN A 192.0.2.1
mx02.subd.emailhosted.not. -> IN A 192.0.2.2
```

PTR(IP):

```
192.0.2.1 -> IN PTR mx0a.emailhosted.not.
192.0.2.2 -> IN PTR mx0b.emailhosted.not.
```

A(PTR(IP)):

```
mx0a.emailhosted.not. -> IN A 192.0.2.1
mx0b.emailhosted.not. -> IN A 192.0.2.2
```

附註：在這種情況下，MX主機名和revDNS名稱不匹配

現在讓我們獲取一個證書顯示的身份：

證書標識：

```
$ echo QUIT |openssl s_client -connect mx0a.emailhosted.not:25 -starttls smtp 2>/dev/null|
openssl x509 -text | grep -iEo 'DNS:.*|CN=.*'

CN=thawte SHA256 SSL CA
CN=*.emailhosted.not
DNS:*.emailhosted.not, DNS:emailhosted.not
```

```
echo QUIT |openssl s_client -connect mx0b.emailhosted.not:25 -starttls smtp 2>/dev/null| openssl
x509 -text | grep -iEo 'DNS:.*|CN=.*'

CN=thawte SHA256 SSL CA
CN=*.emailhosted.not
DNS:*.emailhosted.not, DNS:emailhosted.not
```

兩個目標伺服器都安裝了相同的證書。現在來檢查兩個驗證選項，比較驗證結果。
如果使用 TLS Required Verify:
使用其中一個MX伺服器建立TLS會話，身份驗證通過檢查所需的呈現身份開始：

- 呈現標識：dNSName exist（繼續與允許的引用標識進行比較）

  引用標識=收件人域(example.com)已選中，並且與dNSName DNS:*.emailhosted.not、DNS:emailhosted.not不匹配
- 呈現標識：CN存在（繼續下一個呈現標識與上一個標識沒有匹配）

引用標識=收件人域(example.com)已選中，且**與CN *.emailhosted.not**不匹配

參考身份= PTR(IP):對TLS客戶端(ESA)已建立連線並收到證書的伺服器的IP執行PTR查詢，並且此查詢返回： **mx0a.emailhosted.not。**

檢查DNS一致性，以將此主機名視為有效的參考標識：

```
mx01.subd.emailhosted.not. -> IN A 192.0.2.1

PTR(IP):      192.0.2.1  -> IN PTR  mx0a.emailhosted.not.
A(PTR(IP)):   mx0a.emailhosted.not. -> IN A 192.0.2.1
```

mx0a.emailhosted.not的值。與CN***.emailhosted.not比較，**它匹配**了。**
PTR域名驗證身份，由於證書是CA簽名的證書，它驗證整個證書並建立TLS會話。

對於同一收件人 **的託管域使用TLS必需**驗證的情況下：

- 呈現身份：**dNSName存**在（因此在這種情況下將不處理CN）已檢查引用標識=收件人域(example.com)，且
  與dNSName DNS:*.emailhosted.not、DNS:emailhosted.not不匹配引用標識= FQDN(smtp route) — 此收件人域沒有smtproutes

  由於並未額外使用SMTPROUTES:

  引用標識= MX（收件人域）— 針對收件人域執行DNS MX查詢
  和返回： **mx01.subd.emailhosted.not** — 此值與**dNSName DNS:*.emailhosted.not、DNS:emailhosted.not**不匹配
- 呈現身份：**CN存在，但由於dNSName**也存在，因此被跳過。

由於CN不被視為要處理，在此情況下，TLS身份驗證以及證書驗證失敗，因此無法建立連線。

相關資訊

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2版本說明s
- 技術支援與文件 - Cisco Systems