Cisco电子邮件安全的TLS验证进程

目录

简介

本文描述Cisco电子邮件安全工具的(ESA)传输层安全(TLS)服务器身份验证进程

Cisco电子邮件安全的TLS验证进程

TLS验证进程根本是一个两阶段验证过程：

我-证书确认

这介入验证：

- 证书有效性周期-认证寿命
- 证书链签发人
- 撤消清单，等等。

II -服务器身份验证

这是服务器**被提交的身份的**验证过程(包含在X.509公开密钥认证)服务器**参考身份**。

背景

请保留与身份描述的名字术语在RFC 6125。

> **Note**:**被提交的身份**是能包括超过一个不同的类型被提交的标识的服务器X.509公开密钥认证提交的标识。在SMTP服务的情况下，它包含作为类型dNSName subjectAltName扩展名或作为

从Subject字段(共同名称)派生的CN。

Note:**参考身份**是从一个完全合格的DNS域名修建的标识客户端在认证盼望一项应用服务出席。

验证进程对TLS客户端是主要重要，因为客户端一般来说起动TLS会话，并且客户端需要验证通信。*达到客户端需要验证的此被提交的身份是否匹配参考身份。*重要部分将了解TLS验证进程安全邮件发送的根据TLS客户端几乎完全地。

第一步

在服务器身份验证的第一步将确定参考身份由TLS客户端。它从应用程序取决于参考标识TLS客户端什么列表认为可接受的。并且必须独立服务提交的标识修建可接受的参考标识列表。[rfs6125#6.2.1]

参考身份必须是一个完全合格的DNS域名，并且可以从解析为客户端是可接受的和认为安全)的所有输入(。 参考身份需要是客户端设法连接的DNS主机名。

接收电子邮件域名是由用户直接地表示，由目的特别是传送信息到特定用户域，并且这也符合要求是FQDN用户设法连接的参考身份。它在SMTP服务器拥有的自主机的SMTP服务器的情况下是仅一致，并且管理由同一个责任人和服务器不主机许多域。作为每域需要列出在认证(作为一个subjectAltName ：dNSName值)。从实施的角度看，大多认证权限(CA)限制域名值的编号低到25个条目(高达100)。它没有在主机的环境的情况下被认可，请考虑电子邮件服务供应商(ESP)其中目的地SMTP服务器主机千位等等域。这就是不扩展。

明确配置的参考身份似乎是答案，但是这强加一些约束，因为要求手工关联参考身份到每个目的地域或*“获取的数据源域从一个人的用户明确地放置了信任的第三方域映射服务，并且与哪些客户端在提供检查的相互验证和的完整性”的连接或关联传达。[RFC6125#6.2.1]*

概念上，这在MTA可以被重视一次一次性“安全的MX查询”在配置时，当结果永久被缓存预防所有DNS妥协，当在运转状态时。[2]

这产生一个仅强力身份验证与“合作伙伴”域，但是对于未被映射这不通过检查的通用域和此也不是免疫的配置更改在目的地域一边(类似主机名或IP地址更改)。

第二步

下一步在进程中是确定一个被提交的身份。服务器X.509公开密钥认证提供被提交的身份，类型dNSName subjectAltName扩展名或作为共同名称(CN)在Subject字段查找。那里是空的Subject字段是完全可接受的，只要认证包含包括至少一个subjectAltName条目的一个subjectAltName扩展名。

虽然使用共同名称是仍然实践上它是考虑贬抑，并且当前推荐是使用subjectAltName条目。身份的技术支持从后向兼容性的共同名称逗留。在这种情况下应该首先使用subjectAltName dNSName，并且，只有当是空的时共同名称被检查。

Note:共同名称不是强类型的，因为共同名称也许包含服务的人友好的串，而不是表匹配那一个完全合格的DNS域名的串

在末端，当两确定了时身份的类型， TLS客户端需要对出席的标识比较其参考标识中的每一个为查

找匹配的目的。

ESA TLS验证

ESA允许启用TLS和证书验证在发运对特定域(使用目的地控制CLI命令的页或的**destconfig**)。当需要时TLS证书验证，您能选择两个验证选项之一从AsyncOS版本8.0.2。期望的验证结果能根据被配置的选项变化。从TLS的6个不同的设置，那里可用的下面目的地控制是对证书验证负责的两重要：

1. **需要的TLS -验证**
2. **需要的TLS -验证主机的域。**

```
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]>
```

(4)一个TLS验证进程**首选的**选项的**– Verify**与(5)**要求**是相同的**–请验证**，但是根据结果的执行的操作有所不同作为被提交的下面的表。(6)结果**需要的**选项的**–验证主机的域**与(5)**要求**是相同的**–请验证**，但是TLS验证流是相当不同的。

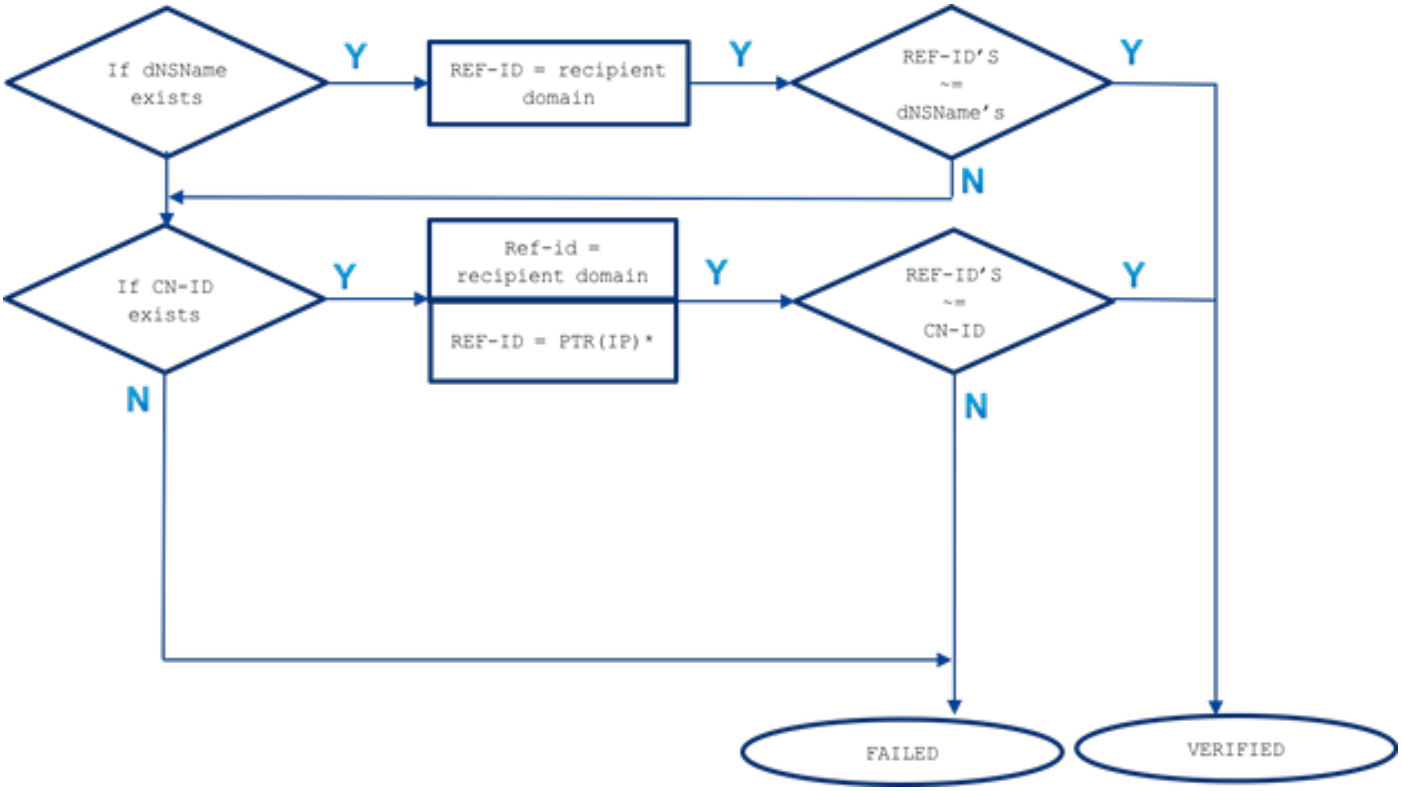
TLS设置	含义
4. 更喜欢(请验证)	TLS从电子邮件安全工具协商到域的MTA。工具尝试验证域认证。 三种结果是可能的： • TLS协商，并且认证被验证。邮件通过加密的会话被提供。 • TLS协商，但是认证没有被验证。邮件通过加密的会话被提供。 • TLS联系没有被建立，并且，认证随后没有被验证。电子邮件消息在纯文本被提供。
5. 必需(请验证)	TLS从电子邮件安全工具协商到域的MTA。需要域认证的验证。 三种结果是可能的： • TLS连接协商，并且认证被验证。电子邮件消息通过加密的会话被提供。 • TLS连接协商，但是认证没有由委托的CA验证。没有提供邮件。 • TLS连接没有协商。没有提供邮件。

需要的TLS之间的区别**-验证**和**需要的TLS -验证主机的域**选项在身份验证进程放置。方式被提交的身份如何处理和允许使用什么类型的参考标识产生关于最终结果的变化。下面的说明以及全部的文件的目的是对接近此进程终端用户。对此主题的不正确或不清楚的了解能有在客户网络的一个安全影响。

需要的TLS验证

被提交的身份首先从subjectAltName派生- dNSName扩展名，并且，如果没有匹配或subjectAltName扩展名比CN-ID不存在-从Subject字段的共同名称被检查。

参考身份(REF-ID)列表从一个接收域被修建或从PTR DNS查询和主机名派生的接收人域运行客户端连接的IP地址。 **注意**：在该特别情形中，不同的参考身份与不同的被提交的身份检查比较。



~=表示确切或通配符匹配

被提交的身份(dNSName或CN-ID)比较以被接受的参考身份，被匹配和按他们下面是列出的顺序。

- 如果subjectAltName dNSName扩展名存在： 确切或通配符匹配完成仅接收域

  在subjectAltName匹配的情况下参考身份从接收域仅派生。如果接收域不匹配dNSName条目中的任一个进一步参考身份没有被检查(类似从DNS解析MX或PTR派生的主机名)

- 如果主题DN CN存在(CN-ID) ： 确切或通配符匹配完成接收域确切或通配符匹配完成从PTR查询派生的主机名执行目标服务器的IP

  那里PTR记录保留在DNS的一致性在转发器和解析器之间。什么需要是提及此处，该CN字段对从PTR的一个主机名比较，只有当PTR记录存在，并且一个被解决的A记录(转发器)此主机名(参考身份)回归的匹配目标服务器IP PTR查询执行的IP地址。

  A (PTR(IP)) == IP

  在CN-ID的情况下参考身份从接收域派生，并且，当没有匹配时DNS查询执行目的地IP PTR记录获得主机名。如果PTR存在一次另外的查询执行在从PTR派生的主机名的一个A记录确认DNS一致性保留!进一步参考没有被检查(类似从MX查询派生的主机名)

要总结，当'TLS需要-请验证'那里选项是没有MX主机名比较dNSName或CN， DNS PTR RR仅被检查CN和被匹配，只有当DNS一致性是保留的A (PTR(IP)) = IP，请苛求，并且dNSName的通配符测试和CN执行。

需要的TLS验证-主机的域

被提交的身份从类型首先派生dNSName subjectAltName扩展名。如果没有在dNSName和那个的匹配被接受的参考身份之间(REF-ID)，验证不发生故障问题，如果CN在Subject字段存在，并且可能通过进一步身份验证。只有当认证不包含其中任一个类型dNSName时， subjectAltName扩展名从Subject字段派生的CN被验证。

收回被提交的身份(dNSName或CN-ID)比较以被接受的参考身份，被匹配和按他们下面是列出的顺序。

- 如果subjectAltName dNSName扩展名存在：

  如果没有matchbetween dNSName，并且其中一个被接受的参考身份列出了belowthan身份验证是失败的
  确切或通配符匹配完成接收域： 一dNSName必须匹配一个接收域确切或通配符匹配明确地完成与SMTPROUTES的配置的主机名(*)确切或通配符匹配完成从(不安全)接收域名的DNS查询派生的MX主机名

  如果接收域未用FQDN条目明确地配置SMTP路由，并且接收域未被匹配比从(不安全)一个接收域的DNS查询使用由MX纪录的FQDN回归。如果没有匹配进一步测试没有被执行，无PTR记录被检查
- 如果主题DN CN存在(CN-ID) ：
  只有当dNSName在认证时，不存在CN被验证。CN-ID与被接受的参考身份比较下面列出。

  确切或通配符匹配完成接收域确切或通配符匹配明确地完成在SMTPROUTES的配置的主机名(*)确切或通配符匹配完成从(不安全)接收域名的DNS查询派生的MX主机名

明确配置的SMTPROUTES

当配置SMTP路由，并且时被提交的身份没有匹配电子邮件接收方域然后名字比较的所有FQDN路由，并且，如果他们不配比没有进一步检查。使用明确配置的SMTP不路由MX主机名考虑比较一个被提交的身份。此处例外做设置作为IP地址的一个SMTP路由。

以下规则在明确配置的SMTP路由的情况下适用：

- 当SMTP路由为一个接收域存在，并且时它是一个完全合格的DNS域名(FQDN)考虑作为参考身份。此主机名(路由名字)与从认证接收的被提交的身份比较派生从指向的目标服务器。

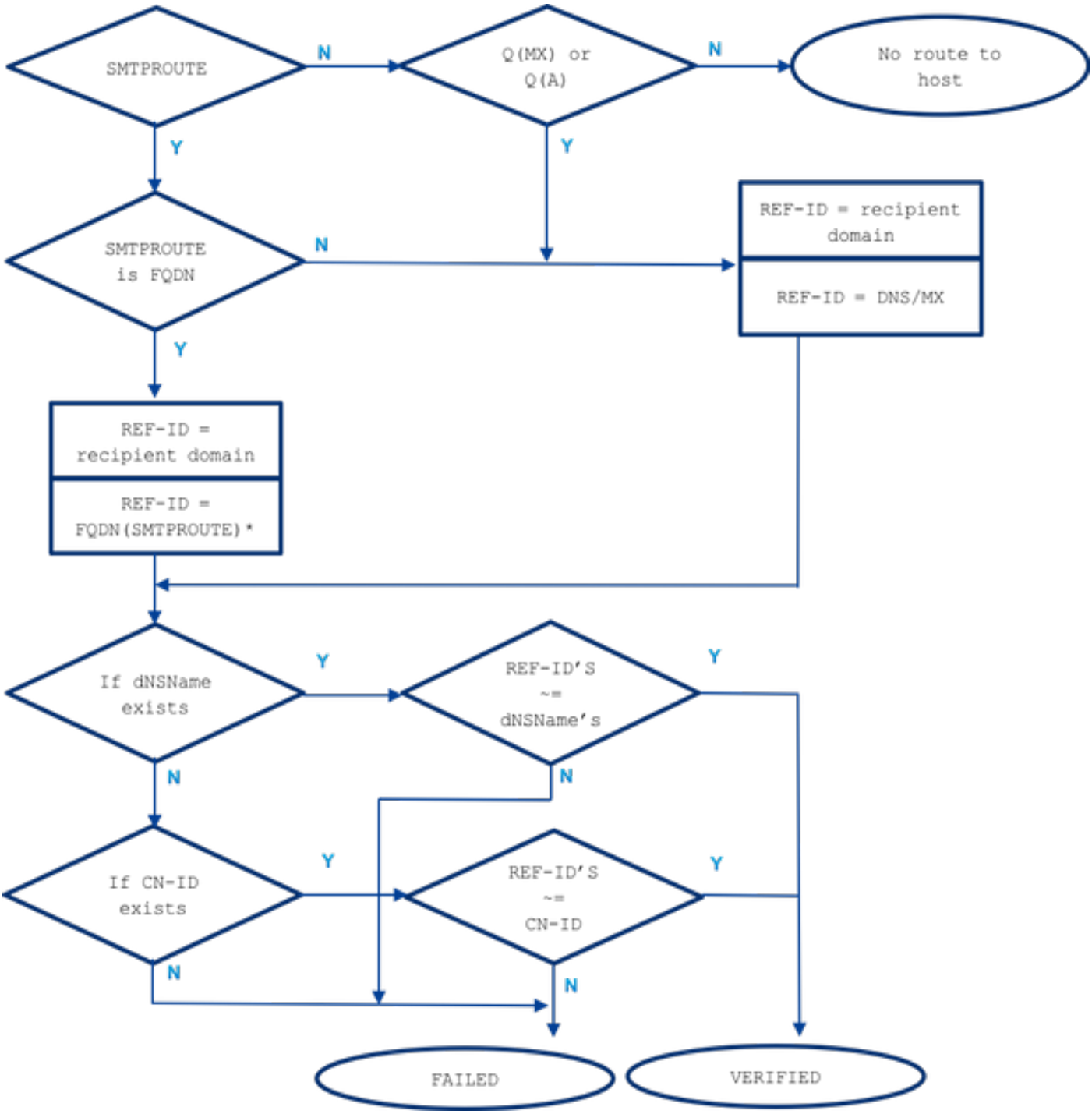
- 一个接收域的多个路由允许。如果接收域有超过一个SMTP路由，路由处理直到从认证的被提交的标识从目标服务器将匹配连接被建立路由的名字。如果在列表的主机有不同的优先级那个与最高(0最高，并且默认值)首先处理。如果所有有同一优先级路由列表按用户设置路由的顺序处理。

- 万一，当主机不回应(时不是可用的)或它回应，但是TLS验证发生了故障从列表的下台主机处理。当第一台主机是可用的并且通过时的验证没有使用其他。

- 如果多个路由解决对同样IP地址，只有与此IP的一连接被建立和从认证派生的被提交的身份发送由目标服务器必须匹配一这些路由名字。

- 如果SMTP路由为接收域存在，但是被配置了作为IP地址，路由仍然是使用建立联系，但是从认证的一个被提交的身份对接收域比较和更加进一步与从DNS/MX资源记录派生的主机名。

当我们谈论需要时的TLS请验证主机的域的选项，方式ESA如何用目标服务器连接对提供在进程中将考虑的另外的参考身份的TLS验证进程是重要由于明确配置的SMTP路由。



~=表示确切或通配符匹配

示例

请采取一个示例从实际生活，但是接收域的：example.com。在我之下设法描述是必要手工验证服务器身份的所有步骤。

首先，请收集关于接收服务器的所有需要信息。

MX主机名：

```
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) ：

```
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
```

A (PTR(IP)) ：

```
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
```

Note:MX主机名和revDNS名字在这种情况下不配比

现在让获得认证被提交的身份：

认证身份：

```
$ 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
```

两目标服务器有安装的同一个认证。请查看两个验证选项和比较验证结果。
在使用 **需要的TLS的情况下请验证：**
TLS会话建立与其中一个MX服务器，并且身份验证通过检查期望被提交的身份开始：

- 被提交的身份： **dNSName存在**(请继续和允许参考身份相比)

  参考身份=接收域(example.com)被检查和不**匹配**dNSName DNS: *.emailhosted.not， DNS:

emailhosted.not

- 被提交的身份： **CN存在**(请继续其次被提交的identiy至于对于上一个一个匹配)

  参考身份=接收域(**example.com**)被检查和不**匹配CN *.emailhosted.not**

  参考身份= PTR(IP) ：PTR查询执行TLS客户端服务器(ESA)有建立的连接和接收认证和此查询回归的IP ：**mx0a.emailhosted.not.**

  DNS一致性被检查此主机名把有效参考身份视为：

```
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的值对CN ***.emailhosted.not**比较，**并且**那里配比。
PTR域名验证身份，并且，因为认证是CA证书它验证全部的认证，并且TLS会话建立。

在使用 **需要的TLS的情况下为**此同样接收人的 **主机的域请验证**：

- 被提交的身份：**dNSName存在**(因此CN不会处理在那种情况下) 参考身份=接收域(example.com)被检查和
  不匹配dNSName DNS: *.emailhosted.not， DNS: emailhosted.not参考身份= FQDN (smtp路由) -那里是此接收域的没有smtproutes

  尽管没有另外使用的SMTPROUTES ：

  参考身份= MX (接收域) - DNS MX查询执行接收域
  并且回归： **mx01.subd.emailhosted.not** -这不**匹配dNSName DNS: *.emailhosted.not， DNS: emailhosted.not**
- 被提交的身份：当dNSName存在， **CN存在，但是被跳过**。

因为CN没有认为处理TLS身份验证失败在那种情况下以及结果证书验证和连接不可能设立。

相关信息

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2版本注释
- 技术支持和文档 - Cisco Systems