عملية التحقق من TLS لأمان البريد الإلكتروني من Cisco

المحتويات

المقدمة

يوضح هذا المستند عملية التحقق من هوية خادم أمان طبقة النقل (TLS) لأجهزة أمان البريد الإلكتروني من Cisco (ESA)

عملية التحقق من TLS لأمان البريد الإلكتروني من Cisco

عملية التحقق من صحة TLS هي أساسا عملية تحقق من مرحلتين:

I - التحقق من صحة الشهادة

ويشمل ذلك التحقق مما يلي:

- فترة صلاحية الشهادة - مدة صلاحية الشهادة
- مصدر سلسلة الشهادات
- قائمة الإبطال، إلخ ..

II - التحقق من هوية الخادم

هذه هي عملية تحقق من صحة **الهوية المقدمة** للخادم (الواردة في شهادة المفتاح العام X.509) مقابل **هوية مرجع** الخادم.

الخلفية

دعنا نبقي على مصطلحات اسم الهوية الموضحة في RFC 6125.

ملاحظة: **الهوية المعروضة** هي معرف تقدمه شهادة مفتاح عام للخادم X.509 يمكن أن تتضمن أكثر من معرفات مقدمة من أنواع مختلفة. في حالة خدمة SMTP، يتم احتواؤها إما كملحق AltName من النوع dNSName أو ك CN (الاسم الشائع) المشتق من حقل الموضوع.

ملاحظة: **هوية المرجع** عبارة عن معرف تم إنشاؤه من اسم مجال DNS مؤهل بالكامل يتوقع العميل أن تقدمه خدمة تطبيق في الشهادة.

تعد عملية التحقق مهمة في الغالب لعميل TLS، حيث يقوم العميل بشكل عام ببدء جلسة TLS ويحتاج العميل إلى مصادقة الاتصال. *لتحقيق ذلك، يحتاج العميل إلى التحقق مما إذا كانت الهوية المقدمة تطابق هوية المرجع.* والجزء المهم هو أن نفهم أن أمن عملية التحقق من خدمات الاتصالات السلكية واللاسلكية لتوصيل البريد يستند بشكل كامل تقريبا إلى عميل خدمات الاتصالات السلكية واللاسلكية.

الخطوة الأولى

تتمثل الخطوة الأولى في التحقق من هوية الخادم في تحديد هوية المرجع بواسطة عميل TLS. يعتمد ذلك على قائمة المعرفات المرجعية التي يعتبرها عميل TLS مقبولة من التطبيق. كما يجب إنشاء قائمة بمعرفات المراجع المقبولة بشكل مستقل عن المعرفات التي تقدمها الخدمة. [RFS6125#6.2.1]

يجب أن تكون هوية المرجع اسم مجال DNS مؤهلا بالكامل ويمكن تحليلها من أي إدخال (وهو مقبول للعميل ويعتبر آمنا). يجب أن تكون هوية المرجع اسم مضيف DNS يحاول العميل الاتصال به.

اسم مجال البريد الإلكتروني للمستلم هو هوية مرجعية يتم التعبير عنها مباشرة بواسطة المستخدم، بنية إرسال رسالة إلى مستخدم معين في مجال معين وهذا أيضا استوفى متطلب أن يكون FQDN الذي يحاول المستخدم الاتصال به. وهو متناسق فقط في حالة خادم SMTP المستضاف ذاتيا حيث يكون خادم SMTP مملوكا ومديرا بواسطة نفس المالك ولا يستضيف الخادم العديد من المجالات. حيث أن كل مجال يجب أن يكون مدرجا في الشهادة (كأحد قيم SubjectAltName: dNSName). من منظور التنفيذ، تحدد معظم مراجع الشهادات (CA) عدد قيم أسماء المجالات إلى 25 إدخالا (حتى 100). لا يتم قبول هذا في حالة البيئة المستضافة، فدعونا نفكر في موفري خدمة البريد الإلكتروني (ESP) حيث تستضيف خوادم SMTP الوجهة آلاف المجالات والمزيد. هذا فقط لا يتدرج.

يبدو أن هوية المرجع التي تم تكوينها بشكل صريح هي الإجابة ولكن هذا يفرض بعض القيود، حيث يلزم إقران هوية مرجعية يدويا بمجال المصدر لكل مجال وجهة أو *"الحصول على البيانات من خدمة تعيين مجال تابعة لجهة خارجية قام فيها المستخدم البشري بوضع الثقة بشكل صريح ويتصل بها العميل عبر اتصال أو اقتران يوفر المصادقة المتبادلة والتحقق من التكامل". [RFC6125#6.2.1]*

من الناحية المفاهيمية، يمكن التفكير في هذا "استعلام MX الآمن" لمرة واحدة في وقت التكوين، مع تخزين النتيجة مؤقتا بشكل دائم على MTA للحماية من أي تسوية DNS أثناء حالة التشغيل. [2]

وهذا يوفر مصادقة أقوى فقط مع مجالات "الشريك" ولكن للمجال العام الذي لم يتم تعيينه، فهذا لا يجتاز الاختبار وهذا أيضا ليس محصنا ضد تغييرات التكوين على جانب مجال الوجهة (مثل تغييرات اسم المضيف أو عنوان IP).

الخطوة الثانية

الخطوة التالية في العملية هي تحديد هوية مقدمة. يتم توفير الهوية المقدمة بواسطة شهادة مفتاح عام للخادم X.509، كملحق SubjectAltName من النوع dNSName أو كاسم شائع (CN) موجود في حقل الموضوع. حيث يكون من المقبول تماما أن يكون حقل الموضوع فارغا، طالما كانت الشهادة تحتوي على ملحق subjectAltName يتضمن إدخال SubjectAltName واحد على الأقل.

وعلى الرغم من أن إستخدام الاسم الشائع لا يزال في الممارسة العملية، فإنه يعتبر مهملا، والتوصية الحالية هي إستخدام إدخالات SubjectAltName. يبقى دعم الهوية من الاسم الشائع للتوافق مع الإصدارات السابقة. في مثل هذه الحالة يجب إستخدام dNSName الخاص ب subjectAltName أولا وفقط عندما يكون فارغا يتم التحقق من

"الاسم الشائع".

ملاحظة: لم يتم كتابة الاسم الشائع بقوة لأن الاسم الشائع قد يحتوي على سلسلة مناسبة للخدمة بدلا من سلسلة يطابق شكلها اسم مجال DNS المؤهل بالكامل

في النهاية عندما يكون كلا نوع الهويات محددا، يحتاج عميل TLS لمقارنة كل من معرفات المراجع الخاصة به مقابل المعرفات المقدمة بغرض العثور على تطابق.

التحقق من ESA TLS

يسمح ESA بتمكين TLS والتحقق من الشهادة على التسليم إلى مجالات معينة (باستخدام صفحة عناصر تحكم الوجهة أو أمر واجهة سطر الأوامر (CLI) **targetConfig**). عندما يكون التحقق من شهادة TLS مطلوبا، يمكنك إختيار أحد خيارين للتحقق من الصحة منذ إصدار 8.0.2 AsyncOS. يمكن أن تختلف نتيجة التحقق المتوقعة بناء على الخيار الذي تم تكوينه. من 6 إعدادات مختلفة ل TLS، متاح تحت تحكم الوجهة هناك إثنان مهمان مسؤولان عن التحقق من الشهادة:

1. **TLS مطلوب - التحقق من**
2. **TLS مطلوب - التحقق من المجالات المستضافة**.

```
CLI: destconfig

?Do you want to use TLS support

No .1

Preferred .2

Required .3

Preferred - Verify .4

Required - Verify .5

Required - Verify Hosted Domains .6

<[6]
```

عملية التحقق من TLS للخيار (4) **المفضل - التحقق** مطابق ل (5) **مطلوب - التحقق**، ولكن الإجراء المتخذ بناء على النتائج يختلف كما هو موضح في الجدول أدناه. النتائج الخاصة بالخيار (6) **مطلوبة - تحقق من** تطابق **المجالات المستضافة** مع (5) **مطلوب - تحقق** من أن تدفق التحقق من TLS مختلف تماما.

إعدادات TLS	معنى
4. مفضل (تحقق)	يتم التفاو على TLS جهاز أمان الإلكتروني MTA (S للمجال. ي الجهاز الت من شهاد المجالات. وهناك ثلا نتائج محت • يتم

التفا
على
ويتم
التحق
الشه
يتم
البري
جلس
مشف

- يتم
التفا
على
ولكر
يتم
من
الشه
يتم
البري
جلس
مشف

- لم يت
إجرا
اتصا
TLS
وبالت
يتم
من
الشه
يتم
رسا
البري
الإلك
بنص
عادي

يتم التفاو
على TLS
جهاز أمان
الإلكتروني
MTA (S
للمجال. ا
من شهاد
المجالات
مطلوب.
وهناك ثلا
نتائج محت

- يتم
التفا
على
TLS

5. مطلوب (تحقق)

التحق
الشه
يتم
رسا
البري
الإلك
عبر
مشف

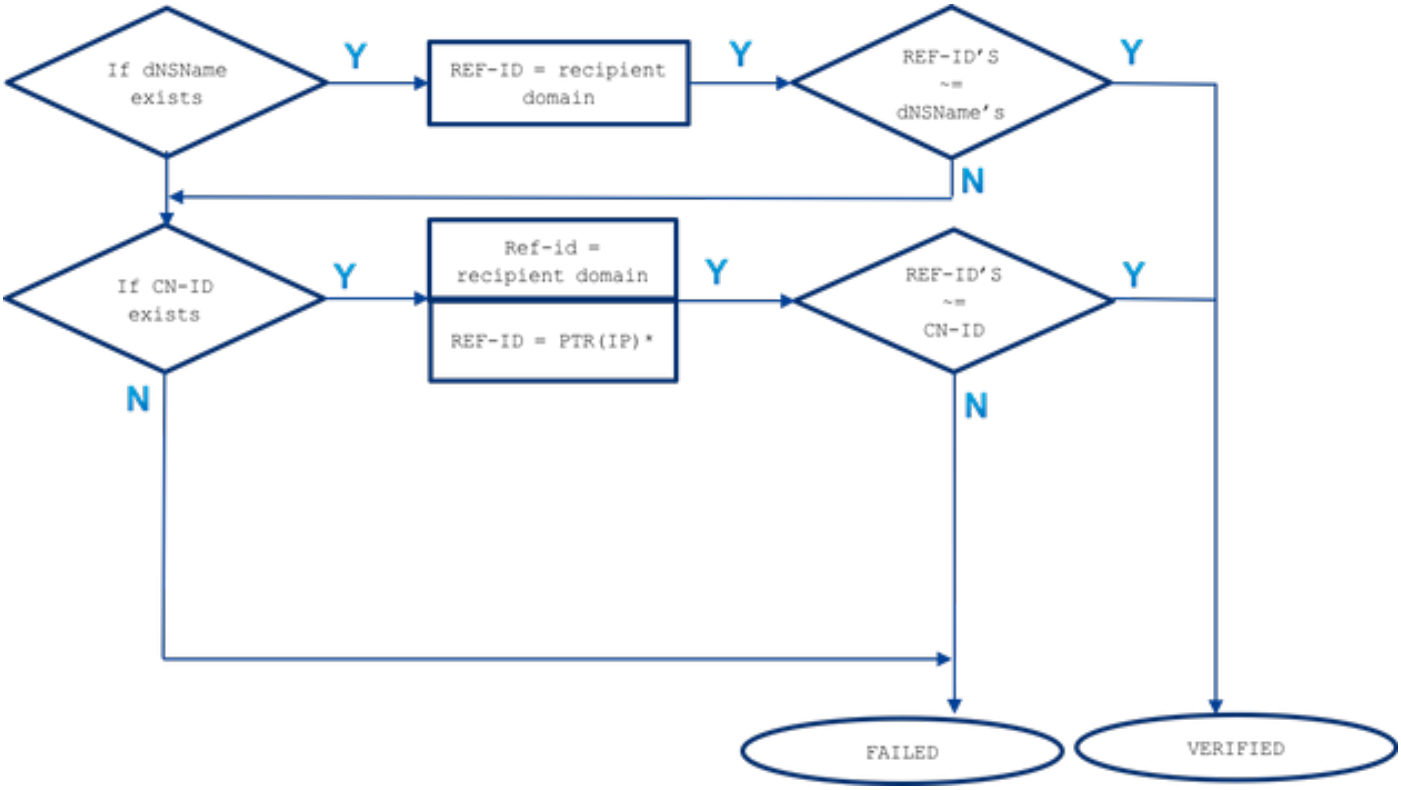
- يتم
التفا
على
TLS
لم ي
التحق
الشه
من
مرج
مصد
ثقة.
تسلي
البري
- لا يت
التفا
على
TLS
يتم
البري

الفرق بين **TLS مطلوب - التحقق** و**TLS مطلوب - التحقق من** وجود خيارات **المجال المستضاف** في عملية التحقق من الهوية. الطريقة التي تتم بها معالجة الهوية المقدمة ونوع المعرفات المرجعية المسموح باستخدامها، تصنع فرقا حول النتيجة النهائية. والغرض من الوصف الوارد أدناه وكذلك المستند بالكامل هو تقريب هذه العملية من المستخدم النهائي. حيث إن الفهم غير الصحيح أو غير الواضح لهذا الموضوع يمكن أن يكون له تأثير أمني على شبكة المستخدم.

التحقق المطلوب من TLS

يتم اشتقاق الهوية المقدمة أولا من ملحق SubjectAltName - dNSName وإذا لم يكن هناك تطابق أو لم يكن ملحق SubjectAltName موجودا من CN-ID - يتم التحقق من Common Name من حقل الموضوع.

يتم إنشاء قائمة معرف المرجع (REF-ID) من مجال مستلم أو مجال مستلم واسم المضيف المشتق من تشغيل استعلام PTR DNS مقابل عنوان IP المتصل به العميل. ملاحظة: في هذه الحالة بالذات، تقارن الهويات المرجعية المختلفة بأشكال مختلفة من التحقق من الهوية المقدمة.



~= يمثل تطابق حرف بدل أو مطابق دقيق

تتم مقارنة الهوية المقدمة (dNSName أو CN-ID) بهويات المراجع المقبولة حتى تتم مطابقتها وترتيب سردها أدناه.

- إذا كان ملحق dNSName ل subjectAltName موجودا: تم إجراء تطابق تام أو حرف بدل مقابل مجال المستلم فقط

يتم اشتقاق هوية المرجع في حالة مطابقة subjectAltName فقط من مجال المستلم. إذا لم يتطابق مجال المستلم مع أي من إدخالات dNSName، فلن يتم التحقق من أي هوية مرجع أخرى (مثل اسم المضيف المشتق من DNS Resolution MX أو PTR)

- إذا كان CN للموضوع DN موجودا (CN-ID): تم إجراء تطابق تام أو حرف بدل مقابل مجال المستلميتم إجراء تطابق تام أو أحرف بدل مقابل اسم المضيف المشتق من استعلام PTR الذي يتم إجراؤه مقابل IP الخاص بخادم الوجهة

حيث حافظ سجل PTR على تناسق في DNS بين الموجه والمحل. ما يجب ذكره هنا، أنه تتم مقارنة حقل CN باسم المضيف من PTR فقط عند وجود سجل PTR وسجل تم حله (موجه) لاسم المضيف (هوية المرجع) هذا إرجاع عنوان IP الذي يطابق عنوان IP لخادم الوجهة الذي تم إجراء استعلام PTR ضمنه.

a(ptr(ip)) == ip

يتم اشتقاق هوية المرجع في حالة معرف CN من مجال المستلم وعندما لا يكون هناك تطابق في استعلام DNS يتم إجراؤه مقابل سجل PTR لمعرف IP الوجهة للحصول على اسم المضيف. في حالة وجود PTR يتم إجراء استعلام إضافي مقابل سجل على اسم مضيف مشتق من PTR لتأكيد حفظ تناسق DNS ! لم يتم التحقق من أي مرجع آخر (مثل اسم المضيف المشتق من استعلام MX)
للتلخيص، باستخدام خيار "TLS مطلوب - التحقق" لا يوجد اسم مضيف MX مقارنة ب dNSName أو CN، يتم التحقق من DNS PTR RR فقط ل CN ويتم مطابقته فقط إذا تم الحفاظ على اتساق IP = (PTR(IP))A DNS، يتم إجراء إختبار أحرف البدل والحديد ل dNSName و CN.

التحقق من TLS المطلوب - المجال المستضاف

يتم اشتقاق الهوية المقدمة أولا من ملحق subjectAltName من النوع dNSName. إذا لم يكن هناك تطابق بين dNSName وأحد الهويات المرجعية المقبولة (REF-ID)، يفشل التحقق بغض النظر عن وجود CN في حقل الموضوع ويمكن أن يمر بالمزيد من التحقق من الهوية. يتم التحقق من صحة CN المستمد من حقل الموضوع فقط عندما لا تحتوي الشهادة على أي من ملحق subjectAltName من النوع dNSName.

تذكر أنه يتم مقارنة الهوية المقدمة (dNSName أو CN-ID) مع الهويات المرجعية المقبولة حتى تتم مطابقتها بالترتيب الوارد أدناه.

- إذا كان ملحق dNSName ل subjectAltName موجودا:

في حالة عدم وجود تطابق بين dNSName وفشل التحقق من صحة هوية أحد الهويات المرجعية المقبولة المدرجة
تم إجراء تطابق تام أو حرف بدل مقابل مجال المستلم: يجب أن يطابق أحد DNSName مجال مستلميتم إجراء تطابق تام أو أحرف بدل مقابل اسم المضيف الذي تم تكوينه بشكل صريح باستخدام SMTPROUTES (*)يتم إجراء تطابق دقيق أو حرف بدل مقابل اسم مضيف MX مشتق من استعلام DNS (غير آمن) مقابل اسم مجال المستلم

إذا لم يكن مجال المستلم قد قام بتكوين مسار SMTP بشكل صريح مع إدخالات FQDN ولم يكن مجال المستلم مطابقا مع إرجاع FQDN بواسطة سجل MX من استعلام DNS (غير آمن) مقابل مجال مستلم يتم إستخدامه. في حالة عدم وجود تطابق لم يتم إجراء أي إختبارات إضافية، لا يتم التحقق من أي سجلات PTR
- إذا كان CN للموضوع DN موجودا (CN-ID):
يتم التحقق من صحة CN فقط في حالة عدم وجود dNSName في الشهادة. تتم مقارنة معرف CN مع قائمة الهويات المرجعية المقبولة أدناه.

تم إجراء تطابق تام أو حرف بدل مقابل مجال المستلميتم إجراء تطابق تام أو أحرف بدل مقابل اسم المضيف الذي تم تكوينه بشكل صريح في SMTPROUTES (*)يتم إجراء تطابق دقيق أو حرف بدل مقابل اسم مضيف MX مشتق من استعلام DNS (غير آمن) مقابل اسم مجال المستلم

الشركات الصغيرة التي تم تكوينها بشكل صريح

عند تكوين مسار SMTP وعدم تطابق الهوية المقدمة مع مجال مستلم البريد الإلكتروني، تتم مقارنة جميع أسماء مسارات FQDN وإذا لم تتطابق مع ذلك، فلا توجد عمليات تحقق أخرى. باستخدام مسارات SMTP التي تم تكوينها بشكل صريح، لا يتم إعتبار اسم المضيف MX مقارنا بهوية مقدمة. يصنع الاستثناء هنا مسار SMTP الذي تم تعيينه كعنوان IP.

تنطبق القواعد التالية في حالة موجهات SMTP التي تم تكوينها بشكل صريح:

- عندما يكون مسار SMTP موجودا لمجال مستلم وهو اسم مجال DNS مؤهل بالكامل (FQDN)، يتم اعتباره هوية مرجع. ويقارن اسم المضيف هذا (اسم مسار) بالهوية المقدمة التي تم تلقيها من شهادة مشتقة من خادم وجهة يشير إليها.

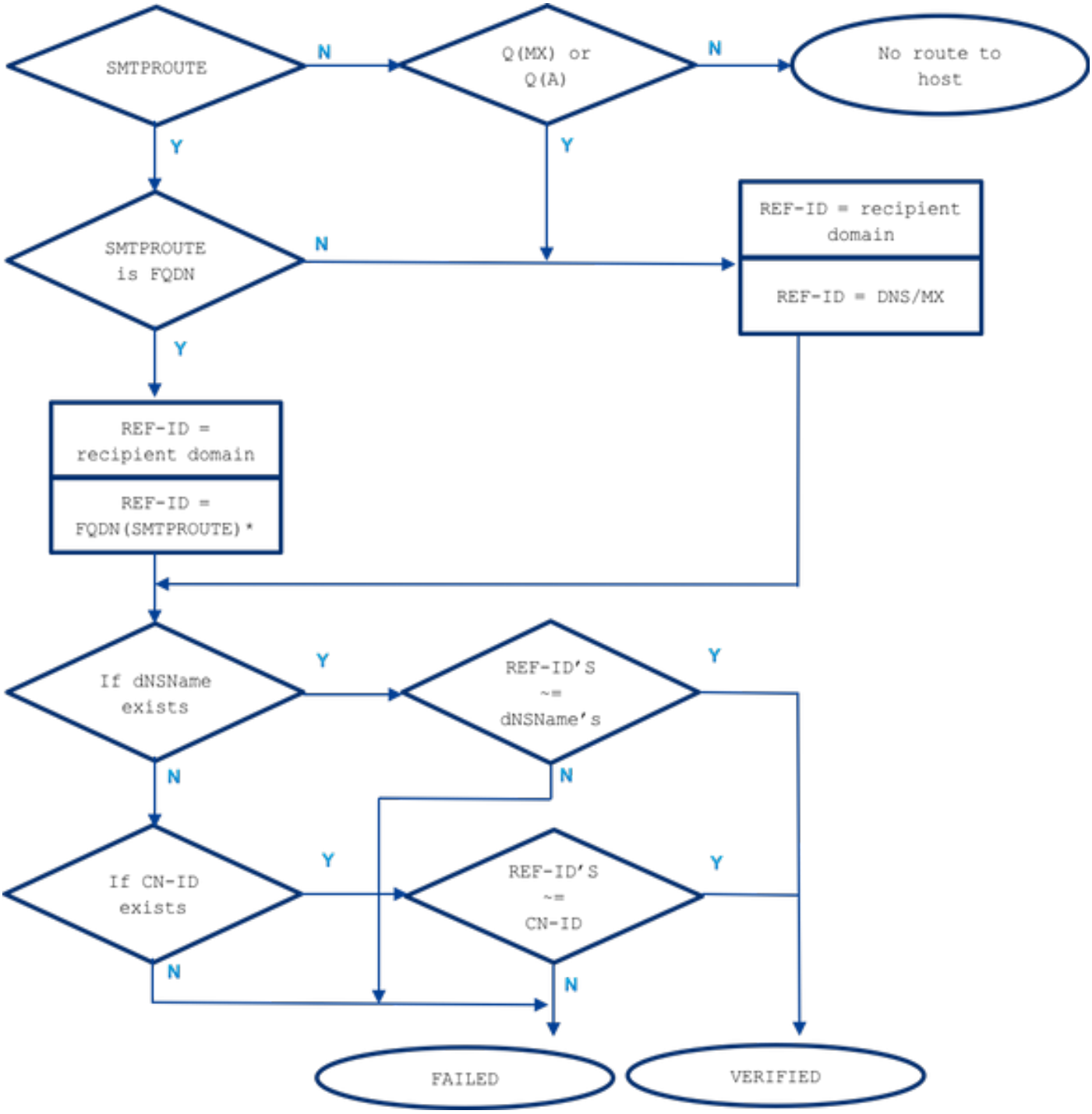
- مسموح بمسارات متعددة لمجال مستلم. إذا كان مجال المستلم يحتوي على أكثر من مسار SMTP، فسيتم معالجة المسارات حتى تتطابق المعرفات المقدمة من الشهادة من الخادم الوجهة مع اسم المسار الذي تم إنشاء الاتصال إليه. إذا كان للمضيفين في القائمة أولويات مختلفة، فإن الأجهزة المضيفة الأعلى (0 هو الأعلى و الافتراضي) تتم معالجتها أولا. إذا كانت لدى الجميع نفس الأولوية، تتم معالجة قائمة المسارات بالترتيب الذي تم فيه تعيين المسارات بواسطة المستخدم.

- في حالة عدم إستجابة المضيف (غير متوفر) أو إستجابته ولكن فشل التحقق من TLS في المضيف التالي من القائمة التي تمت معالجتها. عندما يكون المضيف الأول متاحا ويتجاوز التحقق من أن الآخرين لا يتم إستخدامهم.

- إذا تم حل عدة مسارات إلى عناوين IP نفسها، يتم إنشاء اتصال واحد فقط ب IP هذا ويجب أن تتطابق الهوية المقدمة المشتقة من الشهادة المرسلة من الخادم الوجهة مع أحد أسماء المسارات هذه.

- إذا كان مسار SMTP موجودا لمجالات المستلم ولكن تم تكوينه كعنوان IP، فلا يزال المسار يستخدم لإجراء اتصال ولكن تتم مقارنة هوية مقدمة من الشهادة مع مجال المستلم وأيضا مع اسم المضيف المستمد من سجل مورد DNS/MX.

عندما نتحدث عن خيار TLS للتحقق المطلوب للمجالات المستضافة، فإن الطريقة التي تتصل بها ESA بخادم الوجهة تعتبر مهمة لعملية التحقق من TLS بسبب مسارات SMTP التي تم تكوينها بشكل صريح والتي توفر هوية مرجعية إضافية ليتم مراعاتها في العملية.



=~ يمثل تطابق حرف بدل أو مطابق دقيق

مثال

لنأخذ مثال من الحياة الحقيقية، لكن لمجال المستلم: example.com. حاولت أدناه وصف كافة الخطوات الضرورية للتحقق يدويا من هوية الخادم.

أولا، دعنا نجمع كافة المعلومات المطلوبة حول خادم المستلم.

أسماء مضيفات MX:

```
.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

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

:(((A(PTR(IP

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

ملاحظة: لا تتطابق أسماء مضيف MX وأسماء RevDNS في هذه الحالة

الآن دعونا نحصل على هوية الشهادة المقدمة:

هويات الشهادة (الشهادات):

```
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
```

تم تثبيت نفس الشهادة على الخادمين الوصفين. دعنا نستعرض خيارين للتحقق من الصحة ومقارنة نتائج التحقق من الصحة.

في حالة إستخدام **TLS المطلوب التحقق:**

يتم إنشاء جلسة TLS باستخدام أحد خوادم MX ويبدأ التحقق من الهوية بالتحقق من الهوية المقدمة المطلوبة:

- الهوية المقدمة: **NSName موجود** (متابعة المقارنة مع هوية المرجع المسموح بها)

تم التحقق من هوية المرجع = مجال المستلم (**example.com**) ولا **تطابق** DNS **NSNname:*.emailhosted.not، DNS:EmailHosted.not**
- الهوية المقدمة: **CN موجود** (متابعة المعرف التالي المقدم كما هو الحال بالنسبة للهوية السابقة لا يوجد تطابق)

هوية المرجع = مجال المستلم (**example.com**) محددة ولا **تتطابق مع CN *.emailhosted.not**

الهوية المرجعية = PTR(IP)): يتم إجراء استعلام PTR مقابل IP الخاص بالخادم الذي قام عميل ESA) TLS) بإنشاء اتصال إليه وتلقي شهادة، ويرجع هذا الاستعلام: **mx0a.emailhosted.not.**

يتم التحقق من تناسق DNS لاعتبار اسم المضيف هذا هوية مرجعية صالحة:

```
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
```

تتم مقارنة قيمة **mx0a.emailhosted.not.** مقابل CN ***.emailhosted.not** وهناك **تطابق.**
يتحقق اسم مجال PTR من الهوية، وبما أن الشهادة هي شهادة CA موقعة، فإنه يتحقق من صحة الشهادة بأكملها ويتم إنشاء جلسة TLS.

في حالة إستخدام **TLS مطلوب التحقق للمجال المستضاف** لنفس المستلم:

- الهوية المقدمة: **NSName موجود** (لذلك لن تتم معالجة CN في هذه الحالة) الهوية المرجعية = مجال المستلم (example.com) تم فحصه و
لا يطابق DNS:*.emailhosted.not، DNS:EmailHosted.NOTهوية المرجع = FQDN(smtp route) - لا توجد مشاكل لمجال المستلم هذا

حيث أنه لا يوجد أي إستخدام للأجزاء الصغيرة كأدوات إضافية:

هوية المرجع = MX(مجال المستلم) - يتم إجراء استعلام DNS MX مقابل مجال المستلم
وعمليات الإرجاع: **mx01.subd.emailhosted.not - لا يتطابق** مع **dNSNname DNS:*.emailhosted.not، DNS:emailhosted.not**
- الهوية المقدمة: **CN موجود ولكن تم تخطيه** نظرا لوجود dNSName أيضا.
بما أن CN لا يعتبر أنه تتم معالجته، فإن التحقق من صحة هوية TLS يفشل في هذه الحالة وكذلك لا يمكن تأسيس التحقق من الشهادة ونتيجة لذلك الاتصال.

معلومات ذات صلة

- **المعيار** https://tools.ietf.org/html/rfc6125 - RFC6125
- **المعيار** https://tools.ietf.org/html/rfc2818 - RFC2818
- ملاحظة الإصدار AsyncOS 8.0.2s
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).