Processus de vérification de TLS pour la sécurité du courrier électronique de Cisco

Contenu

Introduction

Ce document décrit le processus de vérification d'identité de serveur de Transport Layer Security (TLS) pour l'appliance de sécurité du courrier électronique de Cisco (l'ESA)

Processus de vérification de TLS pour la sécurité du courrier électronique de Cisco

Le processus de vérification de TLS est essentiellement un processus de validation à deux étages :

I - VALIDATION DE CERTIFICAT

Ceci comporte la vérification de :

- période de validité de certificat - vie de certificat
- émetteur de chaîne de certificat
- liste de révocation, etc.…

II - VALIDATION D'IDENTITÉ DE SERVEUR

C'est un processus de validation de l'**identité présentée par** serveur (contenue dans le certificat de clé X.509 publique) contre l'**identité de référence de** serveur.

Fond

Gardons avec la terminologie de nom d'identité décrite dans RFC 6125.

> **Note**: **L'identité présentée** est un identifiant présenté par un certificat de clé publique du serveur X.509 qui peut inclure plus les identifiants présentés d'un de différents types. En cas de service smtp, il est contenu comme extension de subjectAltName de dNSName de type ou comme NC (nom commun) dérivée du domaine.

> **Note**: **L'identité de référence** est un identifiant construit du nom de domaine qualifié de DN a entièrement - qu'un client s'attend à ce qu'un service d'application se présente dans le certificat.

Le processus de vérification est en grande partie important pour un client de TLS, car en général un client initie une session de TLS et un client doit authentifier la transmission. *Pour réaliser ceci qu'un client doit vérifier si l'identité présentée apparie l'identité de référence.* La partie importante doit comprendre que la Sécurité du processus de vérification de TLS pour la distribution du courrier est presque entièrement basée sur le client de TLS.

Étape un

La première étape dans la validation d'identité de serveur est de déterminer l'identité de référence par le client de TLS. Il dépend de l'application quelle liste de client de TLS d'identifiants de référence considèrent acceptable. Également une liste d'identifiants acceptables de référence doit être construite indépendamment des identifiants présentés par le service. [rfs6125#6.2.1]

L'identité de référence doit être a entièrement - nom de domaine qualifié de DN et peut être analysée de n'importe quelle entrée (qui est acceptable pour un client et considérer sécurisée). La nécessité d'identité de référence d'être une adresse Internet de DN à laquelle le client essaye de se connecter.

Le nom de domaine d'email du destinataire est l'identité de référence qui est directement exprimée par l'utilisateur, par l'intention pour envoyer un message à un domaine d'utilisateur particulier en particulier et ceci a également répondu à une exigence d'être un FQDN auquel un utilisateur essaye de se connecter. Il est cohérent seulement en cas de serveur SMTP auto-hébergé où le serveur SMTP est possédé et géré par le même propriétaire et le serveur n'accueille pas trop de domaines. En tant que chaque besoin de domaine d'être répertorié dans le certificat (en tant qu'un de subjectAltName : valeurs de dNSName). D'un point de vue d'implémentation, la plupart d'autorités de certification (CA) limitent le nombre de valeur de noms de domaine aussi à bas que 25 entrées (aussi à élevé que 100). Ceci n'est pas reçu en cas d'environnement hébergé, permettez-nous pensent aux fournisseurs de services d'email (ESP) où les serveurs SMTP de destination héberge des milliers et plus de domaines. Ceci juste ne mesure pas.

L'identité explicitement configurée de référence semble être la réponse mais ceci imposent quelques contraintes, car on l'exige pour associer manuellement une identité de référence au domaine de source pour chaque domaine ou *« obtenir de* destination les *données d'un tiers service de mappage de domaine dans lequel un utilisateur humain a explicitement placé la confiance et avec ce que le client communique au-dessus d'une connexion ou d'une association qui fournissent l'authentification mutuelle et l'intégrité vérifiant ». [RFC6125#6.2.1]*

Conceptuellement, ceci peut être considéré « une requête sécurisée MX » une fois au moment de la configuration, avec le résultat de manière permanente caché sur le MTA pour protéger contre tous les DN compromettent tandis que dans l'état de passage. [2]

Ceci donne une authentification plus forte seulement avec des domaines de « partenaire » mais pour le domaine générique qui n'a pas été tracé ceci ne passe pas l'examen et ceci n'est également pas immunisé contre des modifications de configuration du côté du domaine de destination (comme l'adresse Internet ou les modifications d'adresse IP).

Étape deux

L'étape suivante dans le processus est de déterminer une identité présentée. L'identité présentée est fournie par un certificat de clé publique du serveur X.509, comme extension de subjectAltName de dNSName de type ou en tant que nom commun (NC) trouvé dans le domaine. Là où il est parfaitement acceptable que le domaine soit vide, tant que le certificat contient une extension de subjectAltName qui inclut au moins une entrée de subjectAltName.

Bien que l'utilisation du nom commun soit dans la pratique lui soit toujours considèrent être désapprouvées et la recommandation en cours est d'utiliser des entrées de subjectAltName. Le soutien de l'identité du séjour commun de nom pour la compatibilité ascendante. En pareil cas un dNSName de subjectAltName devrait être utilisé d'abord et seulement quand il est vide le nom commun est vérifié.

> **Note**: le nom commun n'est pas fortement tapé parce qu'un nom commun pourrait contenir une chaîne qui respecte humaines pour le service, plutôt qu'une chaîne dont les correspondances de forme qui a du nom de domaine qualifié de DN entièrement -

À l'extrémité quand les deux le type d'identités ont été déterminés, le client de TLS doit comparer chacun de ses identifiants de référence contre les identifiants présentés afin de trouver une correspondance.

Vérification de TLS ESA

L'ESA permet activer le TLS et la vérification de certificat sur la livraison aux domaines spécifiques (utilisant la destination contrôle la commande CLI de page ou de **destconfig**). Quand la vérification de certificat de TLS est exigée, vous pouvez choisir une de deux options de vérification depuis la version 8.0.2 d'AsyncOS. Le résultat prévu de vérification peut varier selon l'option configurée. De 6 configurations différentes pour le TLS, le contrôle de dessous disponible de destination là sont deux importants qui sont responsables de la vérification de certificat :

1. **TLS exigé - Vérifiez**
2. **TLS exigé - Vérifiez les domaines hébergés**.

```
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]>
```

Un processus de vérification de TLS pour l'option (4) **préférée – Verify** est identique (5) à **requis – vérifiez**, mais la mesure prise basée sur des résultats diffère en tant que dedans présentée table ci-dessous. Les résultats pour l'option (6) **exigée – Vérifiez les domaines hébergés** est identique (5) à **requis – vérifiez** mais un écoulement de vérification de TLS est très différent.

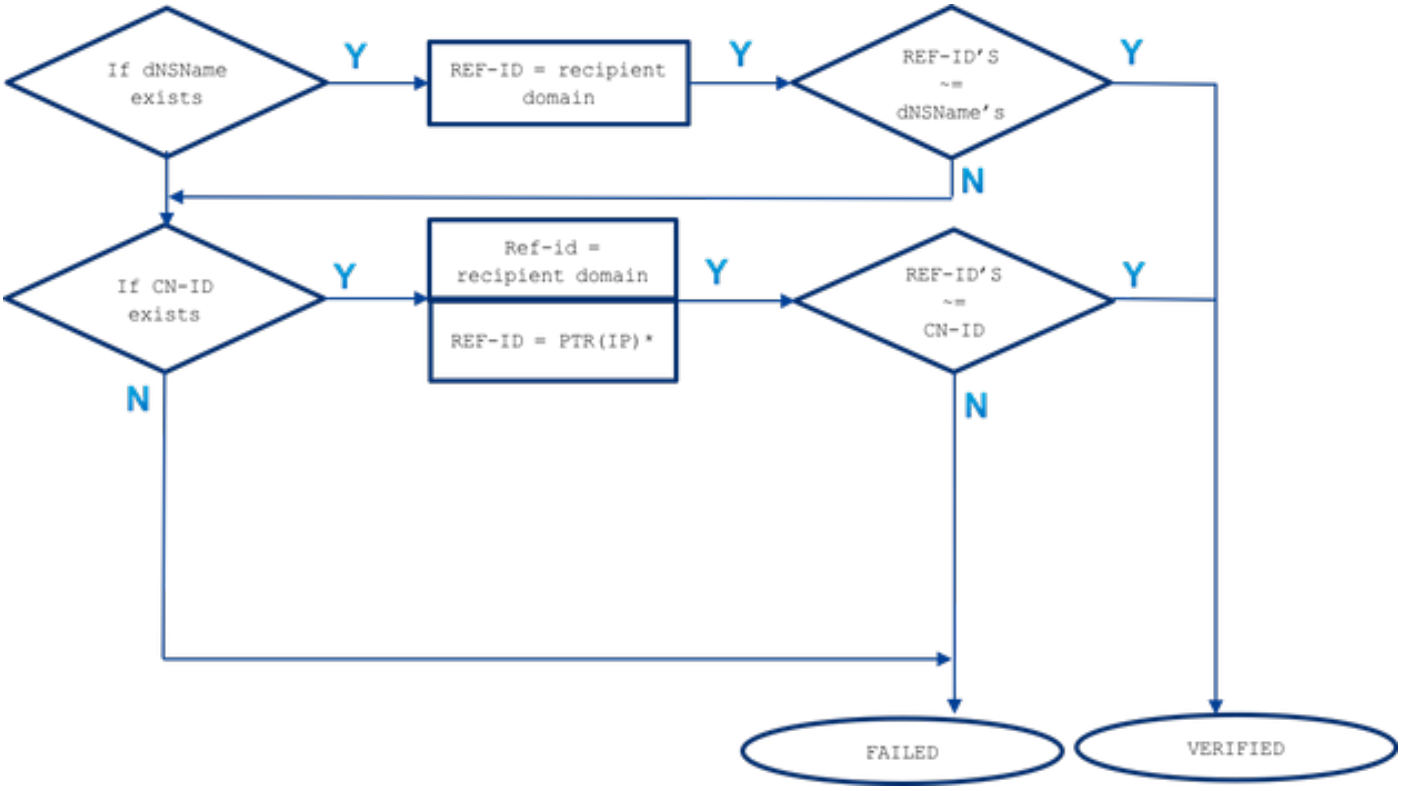
Configurations de TLS	Signification
4. Préféré (vérifiez)	Le TLS est négocié de l'appliance de sécurité du courrier électronique au MTA pour le domaine. Les tentatives d'appareils de vérifier le certificat de domaines. Trois résultats sont possibles : • Le TLS est négocié et le certificat est vérifié. La messagerie est fournie par l'intermédiaire d'une session chiffrée. • Le TLS est négocié, mais le certificat n'est pas vérifié. La messagerie est fournie par l'intermédiaire d'une session chiffrée. • Aucun rapport de TLS n'est établi et, ultérieurement le certificat n'est pas vérifié. Le message électronique est fourni en texte brut.
5. Requis (vérifiez)	Le TLS est négocié de l'appliance de sécurité du courrier électronique au MTA pour le domaine. La vérification du certificat de domaines est exigée. Trois résultats sont possibles : • Une connexion de TLS est négociée et le certificat est vérifié. Le message électronique est fourni par l'intermédiaire d'une session chiffrée. • Une connexion de TLS est négociée mais le certificat n'est pas vérifié par un CA de confiance. La messagerie n'est pas fournie. • Une connexion de TLS n'est pas négociée. La messagerie n'est pas fournie.

La différence entre le **TLS exigé - Vérifiez** et **TLS requis - Vérifiez les** options **hébergées de domaine** s'étend dans le processus de vérification d'identité. La manière comment l'identité présentée est traitée et quel type d'identifiants de référence sont permis pour être utilisés font une différence au sujet d'un résultat final. Le but de la description ci-dessous aussi bien que du document entier est à plus proche ce processus de l'utilisateur final. Comme la compréhension incorrecte ou peu claire de ce sujet peut avoir une incidence de Sécurité sur le réseau utilisateur.

Le TLS exigé vérifie

L'identité présentée est dérivée d'abord du subjectAltName - l'extension de dNSName et s'il y a aucune extension de correspondance ou de subjectAltName n'existe pas que CN-ID - nom commun de domaine est vérifiée.

La liste de l'identité de référence (REF-ID) est construite d'un domaine réceptif ou le domaine et l'adresse Internet de destinataire dérivés d'un passage de requête DNS PTR contre l'adresse IP le client est connecté à. Remarque: Dans ce cas particulier, différentes identités de référence sont comparées à différents contrôles présentés d'identité.



le ~= représente la correspondance précise ou de masque

L'identité présentée (dNSName ou CN-ID) est comparée aux identités reçues de référence jusqu'à ce qu'elle soit appariée et dans la commande qu'ils sont répertoriés ci-dessous.

- Si l'extension de dNSName du subjectAltName existe : la correspondance précise ou de masque est faite contre le domaine réceptif seulement

  L'identité de référence en cas de correspondance de subjectAltName est dérivée seulement du domaine réceptif. Si le domaine réceptif n'apparie pas les entrées l'unes des de dNSName aucune autre identité de référence n'est vérifiée (comme l'adresse Internet dérivée du MX ou du PTR de résolution de DN)

- Si la NC du DN soumis existe (CN-ID) : la correspondance précise ou de masque est faite contre le domaine réceptifla correspondance précise ou de masque est faite contre l'adresse Internet dérivée de la requête PTR exécutée contre un IP du serveur cible

  Là où l'enregistrement PTR a préservé une cohérence dans des DN entre l'expéditeur et le résolveur. Quel besoin d'être mention ici, ce champ NC est comparé contre une adresse Internet de PTR seulement quand un enregistrement PTR existent et un enregistrement résolu A (un expéditeur) pour ce retour d'adresse Internet (identité de référence) une adresse IP qui apparient un IP de serveur cible contre lequel une requête PTR a été exécutée.

  IP DE == A (PTR(IP))

  L'identité de référence en cas de CN-ID est dérivée du domaine réceptif et quand il n'y a aucune correspondance une requête DNS est exécutée contre un enregistrement PTR d'IP de destination pour obtenir une adresse Internet. Si un PTR existe une requête supplémentaire est exécutée contre un enregistrement A sur une adresse Internet dérivée

d'un PTR pour confirmer qu'une cohérence de DN est préservée ! Aucune référence supplémentaire ne sont vérifiées (comme l'adresse Internet dérivée de la requête MX)

Pour résumer, avec le « TLS requis - vérifiez » l'option là n'est aucune adresse Internet MX comparée au dNSName ou à la NC, un PTR rr de DN est examiné seulement pour assurer la NC et est apparié seulement si des DN que la cohérence est A préservé (PTR(IP)) = IP, exigez et l'essai de masque pour le dNSName et la NC sont réalisés.

Le TLS exigé vérifie - Domaine hébergé

L'identité présentée est d'abord dérivée de l'extension de subjectAltName du dNSName de type. S'il n'y a aucune correspondance entre le dNSName et celui d'identités reçues de référence (REF-ID), la vérification échoue aucune matière si la NC existent dans le domaine et pourraient passer davantage de vérification d'identité. La NC dérivée du domaine est validée seulement quand le certificat ne contient pas d'extension de subjectAltName de dNSName de type.

Rappelez-vous que l'identité présentée (dNSName ou CN-ID) est comparée aux identités reçues de référence jusqu'à ce qu'elle soit appariée et dans la commande qu'ils sont répertoriés ci-dessous.

- Si l'extension de dNSName du subjectAltName existe :

  S'il y a aucun matchbetween le dNSName et une d'identités reçues de référence a répertorié la validation belowthan d'identité est manquée
  la correspondance précise ou de masque est faite contre le domaine réceptif : Un du dNSName doit apparier un domaine réceptifla correspondance précise ou de masque est faite contre l'adresse Internet explicitement configurée avec SMTPROUTES (*)la correspondance précise ou de masque est faite contre l'adresse Internet MX dérivée (de la requête DNS un non sécurisé) contre le nom de domaine réceptif

  Si le domaine réceptif n'a pas explicitement configuré l'artère de SMTP avec des entrées FQDN et le domaine réceptif n'était pas apparié qu'un retour FQDN par un MX Record (de requête DNS un non sécurisé) contre un domaine réceptif est utilisé. S'il n'y a aucune correspondance aucun autre essai n'est réalisé, qu'aucun des enregistrements PTR sont vérifiés
- Si la NC du DN soumis existe (CN-ID) :
  La NC est validée seulement quand le dNSName ne fait pas existe dans le certificat. Le CN-ID est comparé à la liste ci-dessous d'identités reçues de référence.

  la correspondance précise ou de masque est faite contre le domaine réceptifla correspondance précise ou de masque est faite contre l'adresse Internet explicitement configurée dans SMTPROUTES (*)la correspondance précise ou de masque est faite contre l'adresse Internet MX dérivée (de la requête DNS un non sécurisé) contre le nom de domaine réceptif

SMTPROUTES explicitement configuré

Quand l'artère de SMTP est configurée et l'identité présentée n'a pas apparié le domaine de destinataire de courriel alors que tout le FQDN conduit des noms sont comparés et s'ils ne

s'assortissent pas il n'y a aucun autre contrôle. Avec le SMTP explicitement configuré ne conduit aucune adresse Internet MX sont considérés comme pour être comparés contre une identité présentée. L'exception ici fait une artère de SMTP qui a été placée comme adresse IP.

Les règles suivantes s'appliquent en cas d'artères explicitement configurées de SMTP :

- Quand l'artère de SMTP existent pour un domaine réceptif et c'est a entièrement - le nom de domaine qualifié de DN (FQDN) il est considéré comme identité de référence. Cette adresse Internet (un nom d'artère) est comparée à l'identité présentée reçue d'un certificat dérivé d'un serveur cible lequel il indique.

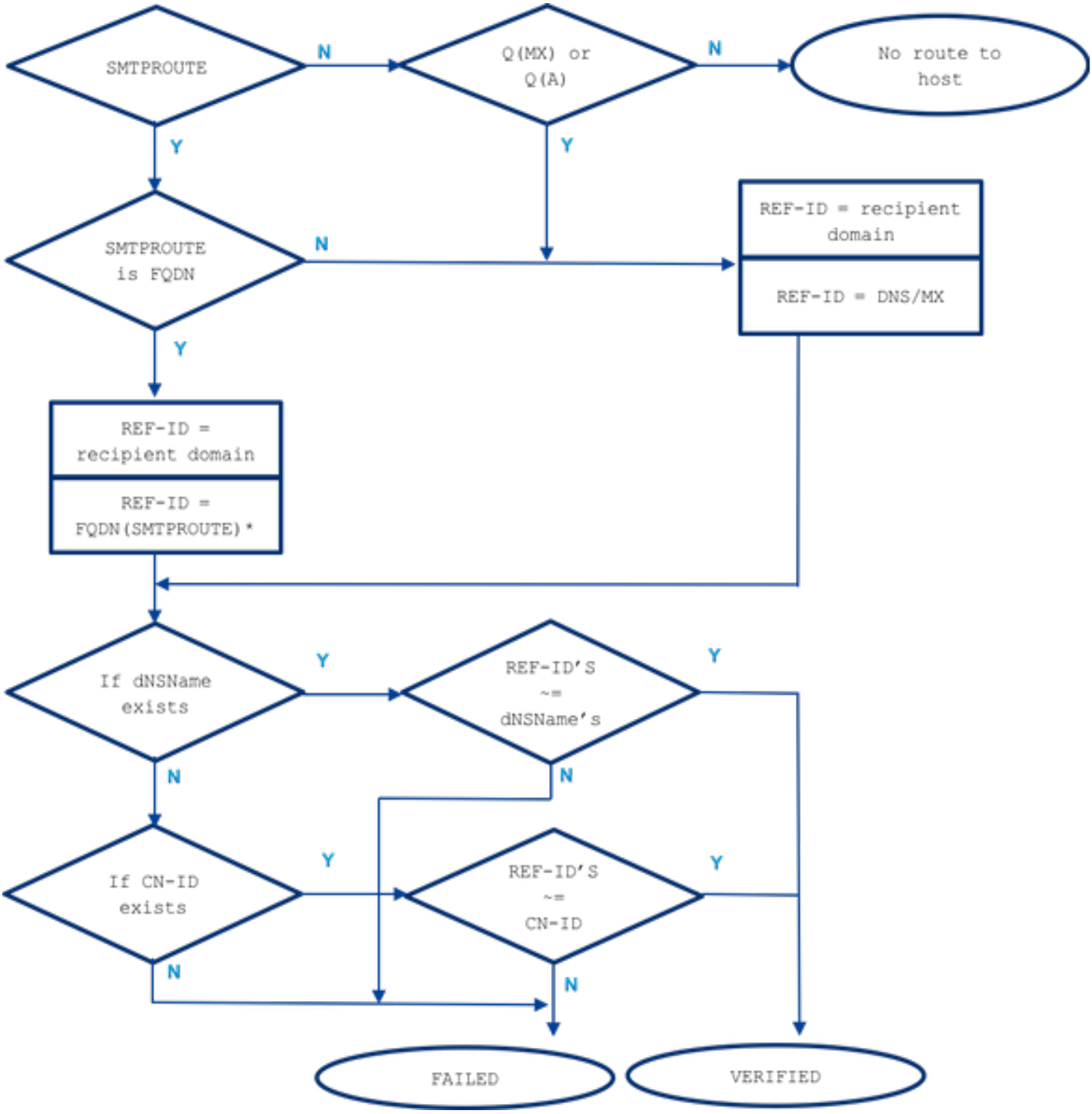
- On permet de plusieurs artères pour un domaine réceptif. Si le domaine réceptif a plus d'une artère de SMTP, les artères sont traitées jusqu'aux identifiants présentés du certificat du serveur cible apparieront le nom de l'artère à laquelle la connexion a été établie. Si les hôtes sur la liste ont différentes priorités celles avec le plus élevé (0 est le plus élevé et le par défaut) sont traités d'abord. Si tous ont la même priorité la liste d'artères est traitée dans la commande que les artères ont été placées par l'utilisateur.

- Au cas où quand l'hôte ne répond pas (ne serait pas disponible) ou il répondent mais la vérification de TLS a manqué le prochain hôte de la liste est traitée. Quand le premier hôte est disponible et passe la vérification d'autres ne sont pas utilisés.

- Si le multiple conduit des résolutions aux mêmes adresses IP, seulement une connexion à cet IP est établie et l'identité présentée dérivée du certificat envoyé par le serveur cible doit apparier un du nom de ces artères.

- Si l'artère de SMTP existent pour les domaines réceptifs mais ont été configurées comme adresse IP, l'artère est toujours utilisation d'établir un rapport mais une identité présentée de certificat est comparée contre le domaine réceptif et autre à l'adresse Internet dérivée de l'enregistrement de ressource DNS/MX.

Quand nous parlons le TLS exigé vérifie l'option pour les domaines hébergés, la manière comment l'ESA s'est connecté à un serveur cible est important pour le processus de vérification de TLS en raison des artères explicitement configurées de SMTP qui fournit l'identité supplémentaire de référence à considérer dans le processus.



le ~= représente la correspondance précise ou de masque

Exemple

Prenons un exemple de la vie réelle, mais pour le domaine réceptif : example.com. Au-dessous d'l essayé pour décrire toute l'étape qui sont nécessaires pour vérifier manuellement l'identité de serveur.

D'abord, recueillons toute l'information nécessaire au sujet du serveur destinataire.

Adresses Internet 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) :

```
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: les adresses Internet MX et les noms de revDNS ne s'assortissent pas dans ce cas

Permet maintenant d'obtenir une identité présentée par certificat :

IDENTITÉS DE CERTIFICATS :

```
$ 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
```

Les deux serveurs cibles font installer le même certificat. Passons en revue deux options de validation et comparer la vérification résulte.
En cas d'utiliser le **TLS requis vérifiez :**
La session de TLS est établie avec un des serveurs MX et les débuts de validation d'identité en vérifiant l'identité présentée désirée :

- identité présentée : **le dNSName existent** (continuez rivaliser avec l'identité permise de référence)

  l'identité de référence = domaine réceptif (**example.com**) est vérifiée et **n'apparie pas les DN de dNSName : *.emailhosted.not, DN : emailhosted.not**

- identité présentée : **La NC existent** (continuez identiy ensuite présenté quant à la précédente il n'y avait aucune correspondance)

  l'identité de référence = domaine réceptif (**example.com)** est vérifiée et **n'apparie pas la NC *.emailhosted.not**

  identité de référence = PTR(IP) : une requête PTR est exécutée contre l'IP du serveur auquel le client de TLS (ESA) a la connexion établie et reçu un certificat, et des retours de cette requête : **mx0a.emailhosted.not.**

  La cohérence de DN est vérifiée pour considérer cette adresse Internet en tant qu'identité valide de référence :

```
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
```

  La valeur de **mx0a.emailhosted.not** est comparée contre NC ***.emailhosted.not et** là elle s'assortit**.**

Le nom de domaine PTR valide l'identité et car le certificat est un certificat signé CA il valide le certificat de totalité et la session de TLS est établie.

En cas d'utiliser le **TLS requis vérifiez pour assurer le domaine hébergé** pour ce même destinataire :

- identité présentée : **le dNSName existent** (ainsi la NC ne sera pas traitée dans ce cas) l'identité de référence = le domaine réceptif (example.com) est vérifiée et n'apparie pas les DN de dNSName : *.emailhosted.not, DN : emailhosted.notl'identité de référence = le FQDN (artère de SMTP) - là n'est aucun smtproutes pour ce domaine réceptif

  Comme il y a aucun SMTPROUTES supplémentaire utilisé :

  l'identité de référence = le MX (domaine réceptif) - une requête MX de DN est exécutée contre le domaine réceptif
  et retours : **mx01.subd.emailhosted.not** - ceci **n'apparie pas les DN de dNSName : *.emailhosted.not, DN : emailhosted.not**
- identité présentée : **La NC existent mais sont ignorées** pendant que le dNSName existent aussi bien.

Car la NC n'est pas considérée pour être traitée la validation d'identité de TLS manque dans ce cas aussi bien que la vérification de certificat et en conséquence connexion ne peut pas être établie.

Informations connexes

- RFC6125 - https://tools.ietf.org/html/rfc6125

- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 notes de mise à jour
- Support et documentation techniques - Cisco Systems