TLS-Verifizierungsprozess für Cisco Email Security

Inhalt

Einführung

Dieses Dokument beschreibt der Transport Layer Security (TLS)-Serveridentitätsverifizierungsprozess für die Cisco E-Mail Security Appliance (ESA)

TLS-Verifizierungsprozess für Cisco Email Security

Bei der TLS-Verifizierung handelt es sich im Wesentlichen um einen zweistufigen Validierungsprozess:

I - ZERTIFIKATVALIDIERUNG

Dazu gehört die Überprüfung

- Gültigkeitsdauer des Zertifikats - Gültigkeitsdauer des Zertifikats
- Zertifikatsketten-Emittent
- Widerrufsliste usw.

II - VALIDIERUNG DER SERVERIDENTITÄT

Dies ist ein Validierungsprozess der **präsentierten Identität** des Servers (im öffentlichen X.509-Schlüsselzertifikat enthalten) für die **Referenzidentität** des Servers.

Hintergrund

Lassen Sie uns die in RFC 6125 beschriebene IdentitätsnamenTerminologie verwenden.

> **Hinweis**: Die **präsentierte Identität** ist ein Bezeichner, der durch ein öffentliches X.509-Schlüsselzertifikat des Servers dargestellt wird, das mehrere vorgestellte Bezeichner verschiedener Typen enthalten kann. Bei einem SMTP-Dienst ist er entweder als SubjectAltName-Erweiterung des Typs dNSName oder als vom Betrefffeld abgeleiteter CN (Common Name) enthalten.

> **Hinweis**: Die **Referenzidentität** ist ein Bezeichner, der aus einem vollqualifizierten DNS-Domänennamen erstellt wird, den ein Client von einem Anwendungsdienst im Zertifikat erwartet.

Der Verifizierungsprozess ist vor allem für einen TLS-Client wichtig, da ein Client im Allgemeinen eine TLS-Sitzung initiiert und die Kommunikation vom Client authentifiziert werden muss. *Hierzu muss ein Client überprüfen, ob die präsentierte Identität mit der Referenzidentität übereinstimmt.* Dabei ist zu beachten, dass die Sicherheit des TLS-Verifizierungsprozesses für die Zustellung von E-Mails fast ausschließlich auf dem TLS-Client basiert.

Schritt 1

Der erste Schritt bei der Validierung der Serveridentität besteht in der Bestimmung der Referenzidentität durch den TLS-Client. Von der Anwendung hängt ab, welche Liste von Referenzbezeichnern der TLS-Client für akzeptabel hält. Außerdem muss eine Liste zulässiger Referenzbezeichner unabhängig von den vom Dienst angegebenen Identifikatoren erstellt werden. [rfs6125#6.2.1]

Bei der Referenzidentität muss es sich um einen vollqualifizierten DNS-Domänennamen handeln, der von jeder Eingabe analysiert werden kann (die für einen Client akzeptabel ist und als sicher gilt). Bei der Referenzidentität muss es sich um einen DNS-Hostnamen handeln, mit dem der Client eine Verbindung herstellen möchte.

Der E-Mail-Domänenname des Empfängers ist eine Referenzidentität, die vom Benutzer direkt in der Absicht ausgedrückt wird, eine Nachricht an einen bestimmten Benutzer in einer bestimmten Domäne zu senden. Dies erfüllt auch die Anforderung, ein FQDN zu sein, mit dem ein Benutzer eine Verbindung herstellen möchte. Konsistent ist dies nur bei selbst gehosteten SMTP-Servern, auf denen der SMTP-Server im Besitz des gleichen Eigentümers ist und vom gleichen Besitzer verwaltet wird und der Server nicht zu viele Domänen hostet. Da jede Domäne im Zertifikat aufgeführt werden muss (als eine der BetreffzeilenAltName: dNSName-Werte). Im Hinblick auf die Implementierung beschränken die meisten Zertifizierungsstellen (Certificate Authority, CA) die Anzahl der Domänennamen-Werte auf 25 Einträge (auf bis zu 100). Dies wird in der gehosteten Umgebung nicht akzeptiert. Nehmen wir einmal an E-Mail-Service-Provider (ESP), wo die Ziel-SMTP-Server Tausende und mehr Domänen hosten. Das ist einfach nicht skalierbar.

Die explizit konfigurierte Referenzidentität scheint die Antwort zu sein, aber dies erlegt einige Einschränkungen auf, da es erforderlich ist, eine Referenzidentität manuell für jede Zieldomäne zuzuordnen oder *"die Daten von einem Drittanbieter-Domänenzuordnungsdienst abzurufen, in dem ein Benutzer explizit Vertrauen gesetzt hat und mit dem der Client über eine Verbindung oder Verbindung kommuniziert, die sowohl gegenseitige Authentifizierung als auch Integritätsprüfung ermöglicht". [RFC6125#6.2.1]*

Dies kann konzeptionell an eine einmalige "sichere MX-Abfrage" zum Zeitpunkt der Konfiguration

gedacht werden, bei der das Ergebnis dauerhaft auf der MTA zwischengespeichert wird, um im laufenden Zustand vor DNS-Kompromittierungen zu schützen. [2]

Dies bietet eine stärkere Authentifizierung nur mit "Partner"-Domänen, aber für generische Domänen, die noch nicht zugeordnet wurden, besteht diese Prüfung nicht, und dies ist auch nicht immun gegen Konfigurationsänderungen auf der Seite der Ziel-Domäne (wie Hostname oder IP-Adressänderungen).

Schritt 2

Der nächste Schritt des Prozesses besteht in der Bestimmung einer angezeigten Identität. Die präsentierte Identität wird von einem öffentlichen X.509-Schlüsselzertifikat des Servers bereitgestellt, entweder als subjectAltName-Erweiterung des Typs dNSName oder als Common Name (CN), der im Betrefffeld gefunden wird. Wenn es für das Betrefffeld vollkommen akzeptabel ist, leer zu sein, solange das Zertifikat eine subjectAltName-Erweiterung enthält, die mindestens einen subjectAltName-Eintrag enthält.

Obwohl die Verwendung von Common Name noch in der Praxis ist, wird sie als veraltet angesehen und die aktuelle Empfehlung lautet, subjectAltName-Einträge zu verwenden. Die Unterstützung für die Identität von Common Name dient weiterhin der Abwärtskompatibilität. In einem solchen Fall sollte zunächst ein dNSName von subjectAltName verwendet werden, und nur wenn dieser leer ist, wird der Common Name aktiviert.

> **Hinweis**: Der Common Name ist nicht stark typisiert, da ein Common Name möglicherweise eine Zeichenfolge für den Dienst enthält, die für den Benutzer geeignet ist, und nicht eine Zeichenfolge, deren Form mit der eines vollqualifizierten DNS-Domänennamen übereinstimmt.

Wenn am Ende beide Identitätstypen bestimmt wurden, muss der TLS-Client alle seine Referenzbezeichner mit den angegebenen Identifikatoren vergleichen, um eine Übereinstimmung zu finden.

ESA-TLS-Verifizierung

Die ESA ermöglicht die Aktivierung von TLS und der Zertifikatsverifizierung bei der Zustellung an bestimmte Domänen (mithilfe der Seite "Zielsteuerelemente" oder des CLI-Befehls **destconfig**). Wenn eine TLS-Zertifikatsüberprüfung erforderlich ist, können Sie eine von zwei Überprüfungsoptionen seit AsyncOS Version 8.0.2 wählen. Das erwartete Überprüfungsergebnis kann je nach konfigurierter Option variieren. Von den sechs verschiedenen Einstellungen für TLS, die unter Zielkontrolle verfügbar sind, gibt es zwei wichtige Einstellungen, die für die Zertifikatsüberprüfung verantwortlich sind:

1. **TLS erforderlich - Verifizieren**
2. **TLS erforderlich - Überprüfen von gehosteten Domänen**.

```
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]>
```

Ein TLS-Verifizierungsprozess für Option (4) **Preferred - Verify** ist mit (5) **Required - Verify**, wobei sich die auf den Ergebnissen basierenden Maßnahmen jedoch von den in der nachfolgenden Tabelle aufgeführten unterscheiden. Die Ergebnisse für die Option (6) **Erforderlich - Überprüfen Sie, ob gehostete Domänen** mit (5) **Erforderlich** identisch sind **- Überprüfen -** doch ein TLS-Verifizierungsablauf ist ganz anders.

TLS-Einstellungen	Bedeutung
4. Bevorzugt (Verifizieren)	TLS wird von der E-Mail-Security-Appliance an die MTA(s) für die Domäne ausgehandelt. Die Appliance versucht, das Domänenzertifikat zu überprüfen. Drei Ergebnisse sind möglich: • TLS wird ausgehandelt, und das Zertifikat wird verifiziert. Die Post wird verschlüsselt zugestellt. • TLS wird ausgehandelt, das Zertifikat wird jedoch nicht verifiziert. Die Post wird verschlüsselt zugestellt. • Es wird keine TLS-Verbindung hergestellt, und anschließend wird das Zertifikat nicht verifiziert. Die E-Mail-Nachricht wird als einfacher Text zugestellt.
5. Erforderlich (Verifizieren)	TLS wird von der E-Mail-Security-Appliance an die MTA(s) für die Domäne ausgehandelt. Es ist eine Überprüfung des Domänenzertifikats erforderlich. Drei Ergebnisse sind möglich: • Es wird eine TLS-Verbindung ausgehandelt, und das Zertifikat wird verifiziert. Die E-Mail-Nachricht wird verschlüsselt gesendet. • Eine TLS-Verbindung wird ausgehandelt, das Zertifikat wird jedoch nicht von einer vertrauenswürdigen CA überprüft. Die Post wird nicht zugestellt. • Eine TLS-Verbindung wird nicht ausgehandelt. Die Post wird nicht zugestellt.

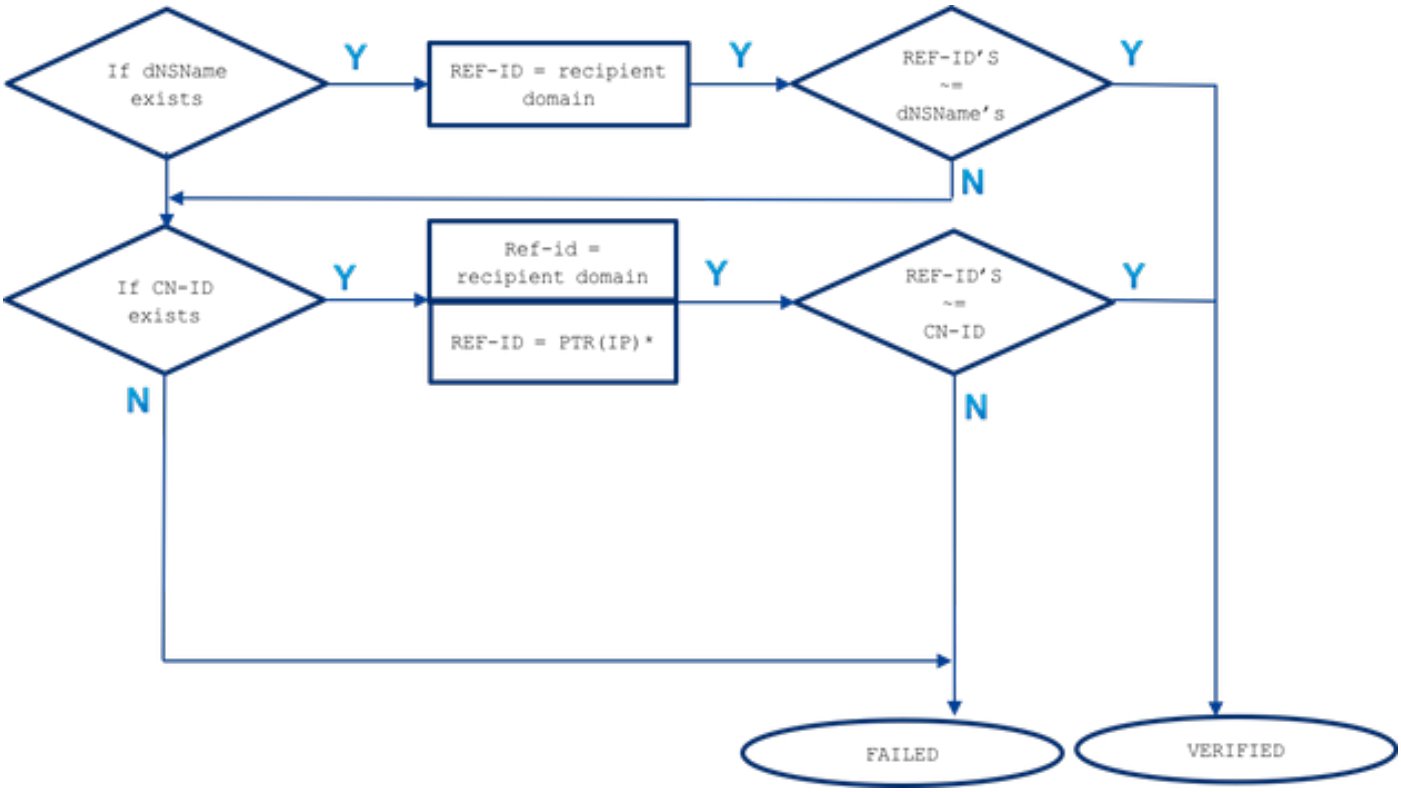
Der Unterschied zwischen **TLS Required - Verify** und **TLS Required - Verify Hosted Domain** options (**TLS erforderlich** und **TLS erforderlich - Verifizieren gehosteter Domänen**) wird im Identitätsüberprüfungsprozess gespeichert. Die Art und Weise, wie die präsentierte Identität verarbeitet wird und welcher Typ von Referenzbezeichnern verwendet werden darf, beeinflusst das Endergebnis. Der Zweck der unten stehenden Beschreibung sowie des gesamten Dokuments besteht darin, diesen Prozess dem Endbenutzer näher zu bringen. Da das falsche oder unklare Verständnis dieses Themas Auswirkungen auf die Sicherheit des Benutzernetzwerks haben kann.

TLS erforderlich Überprüfung

Die präsentierte Identität wird zuerst von subjectAltName - dNSName-Erweiterung abgeleitet, und wenn keine Übereinstimmung oder SubjectAltName-Erweiterung existiert nicht als CN-ID - Common Name aus dem Betreff-Feld wird überprüft.

Die REF-ID-Liste (Reference Identity) wird aus einer Empfängerdomäne oder Empfängerdomäne erstellt, und der Hostname wird aus einer PTR-DNS-Abfrage abgeleitet, die mit der IP-Adresse

ausgeführt wird, mit der der Client verbunden ist. Hinweis: In diesem speziellen Fall werden unterschiedliche Referenzidentitäten mit unterschiedlichen angegebenen Identitätskontrollen verglichen.



~= steht für die exakte Übereinstimmung oder die Platzhalterangabe.

Die präsentierte Identität (dNSName oder CN-ID) wird mit akzeptierten Referenzidentitäten verglichen, bis sie abgeglichen ist und in der nachfolgend aufgeführten Reihenfolge aufgeführt wird.

- Wenn die dNSName-Erweiterung subjectAltName vorhanden ist: exakte Übereinstimmung oder Platzhalterabgleich erfolgt nur mit der Empfängerdomäne.

  Die Referenzidentität im Falle einer subjectAltName-Übereinstimmung wird nur von der Empfängerdomäne abgeleitet. Wenn die Empfängerdomäne mit keinem der dNSName-Einträge übereinstimmt, wird keine weitere Referenzidentität geprüft (z. B. der aus der DNS-Auflösung MX oder PTR abgeleitete Hostname).

- Wenn CN des Betreff-DN vorhanden ist (CN-ID): exakte Übereinstimmung oder Übereinstimmung mit Platzhalter für Empfängerdomäne vorgenommendie exakte Übereinstimmung oder die Übereinstimmung mit dem Platzhalter erfolgt anhand des Hostnamens, der von einer PTR-Abfrage abgeleitet wurde, die mit einer IP-Adresse des Zielservers durchgeführt wurde.

  Der PTR-Datensatz bewahrte eine Konsistenz im DNS zwischen Forwarder und Resolver auf. Es muss hier erwähnt werden, dass das CN-Feld nur dann mit einem Hostnamen von PTR verglichen wird, wenn ein PTR-Datensatz vorhanden ist und ein aufgelöster A-Datensatz (ein Forwarder) für diesen Hostnamen (Referenzidentität) eine IP-Adresse zurückgibt, die mit einer Ziel-Server-IP-Adresse übereinstimmt, für die eine PTR-Abfrage durchgeführt wurde.

A(PTR(IP)) == IP

Die Referenzidentität im Fall einer CN-ID wird von der Empfängerdomäne abgeleitet und bei Nichtübereinstimmung wird eine DNS-Abfrage mit einem PTR-Datensatz der Ziel-IP durchgeführt, um einen Hostnamen zu erhalten. Wenn ein PTR vorhanden ist, wird eine zusätzliche Abfrage für einen A-Datensatz auf einem Hostnamen durchgeführt, der von einem PTR abgeleitet wurde, um zu bestätigen, dass eine DNS-Konsistenz erhalten bleibt. Es werden keine weiteren Verweise geprüft (wie der Hostname, der von der MX-Abfrage abgeleitet wurde).

Zusammenfassend lässt sich sagen, dass mit der Option "TLS Required - Verify" (TLS erforderlich - Verifizieren) kein MX-Hostname im Vergleich zu dNSName oder CN angegeben wird, dass ein DNS-PTR-RR nur für CN aktiviert und zugeordnet wird, wenn die DNS-Konsistenz erhalten bleibt A(PTR(IP)) = IP, sowohl der exakte als auch der Platzhaltertest für dNSNName und CN durchgeführt wird.

TLS erforderlich Verifizieren - gehostete Domäne

Die präsentierte Identität wird zunächst von der Erweiterung subjectAltName des Typs dNSName abgeleitet. Wenn keine Übereinstimmung zwischen dem dNSN-Namen und einer der akzeptierten Referenzidentitäten (REF-ID) besteht, schlägt die Überprüfung fehl, unabhängig davon, ob es sich um eine CN im Betrefffeld handelt, und kann eine weitere Identitätsüberprüfung durchlaufen. Die aus dem Betrefffeld abgeleitete CN wird nur validiert, wenn das Zertifikat keine der subjectAltName-Erweiterungen vom Typ dNSName enthält.

Denken Sie daran, dass die präsentierte Identität (dNSName oder CN-ID) mit akzeptierten Referenzidentitäten verglichen wird, bis sie zugeordnet ist und in der nachfolgend aufgeführten Reihenfolge aufgeführt wird.

- Wenn die dNSName-Erweiterung subjectAltName vorhanden ist:

  Wenn keine Übereinstimmung zwischen dem dNSName und einer der unten aufgeführten akzeptierten Referenzidentitäten besteht, ist die Identitätsvalidierung fehlgeschlagen.
  exakte Übereinstimmung oder Übereinstimmung mit Platzhalter für Empfängerdomäne: Einer der dNSName muss mit einer Empfängerdomäne übereinstimmen.die exakte Übereinstimmung oder die Übereinstimmung mit einem Platzhalter erfolgt mit dem explizit konfigurierten Hostnamen mit SMTPROUTES (*)die exakte Übereinstimmung oder die Übereinstimmung mit einem Platzhalter erfolgt mit dem MX-Hostnamen, der von einer (unsicheren) DNS-Abfrage mithilfe des Empfängerdomänennamen abgeleitet wurde.

  Wenn die Empfängerdomäne keine explizit konfigurierte SMTP-Route mit FQDN-Einträgen aufweist und die Empfängerdomäne nicht zugeordnet wurde, wird eine FQDN-Rückgabe eines MX-Datensatzes von einer (unsicheren) DNS-Abfrage für eine Empfängerdomäne verwendet. Wenn keine Übereinstimmung vorhanden ist, werden keine weiteren Tests durchgeführt, es werden keine PTR-Datensätze überprüft.
- Wenn CN des Betreff-DN vorhanden ist (CN-ID):
  CN wird nur validiert, wenn dNSName im Zertifikat nicht vorhanden ist. Die CN-ID wird mit der folgenden Liste der zulässigen Referenzidentitäten verglichen.

exakte Übereinstimmung oder Übereinstimmung mit Platzhalter für Empfängerdomäne vorgenommenDie exakte Übereinstimmung oder die Platzhalterabstimmung wird mit dem explizit konfigurierten Hostnamen in SMPROUTES (*) durchgeführt.die exakte Übereinstimmung oder die Übereinstimmung mit einem Platzhalter erfolgt mit dem MX-Hostnamen, der von einer (unsicheren) DNS-Abfrage mithilfe des Empfängerdomänennamen abgeleitet wurde.

Explizit konfigurierte SMTPROUTES

Wenn die SMTP-Route konfiguriert ist und die angegebene Identität nicht mit der E-Mail-Empfängerdomäne übereinstimmt, werden alle Namen der FQDN-Routen verglichen, und wenn diese nicht übereinstimmen, werden keine weiteren Prüfungen durchgeführt. Bei explizit konfigurierten SMTP-Routen wird kein MX-Hostname als mit einer angegebenen Identität verglichen. Die Ausnahme bildet hier eine SMTP-Route, die als IP-Adresse festgelegt wurde.

Die folgenden Regeln gelten für explizit konfigurierte SMTP-Routen:

- Wenn eine SMTP-Route für eine Empfängerdomäne existiert und es sich um einen vollqualifizierten DNS-Domänennamen (FQDN) handelt, wird sie als Referenzidentität betrachtet. Dieser Hostname (ein Routenname) wird mit der angezeigten Identität verglichen, die von einem Zertifikat empfangen wird, das von einem Zielserver abgeleitet ist, auf den er verweist.

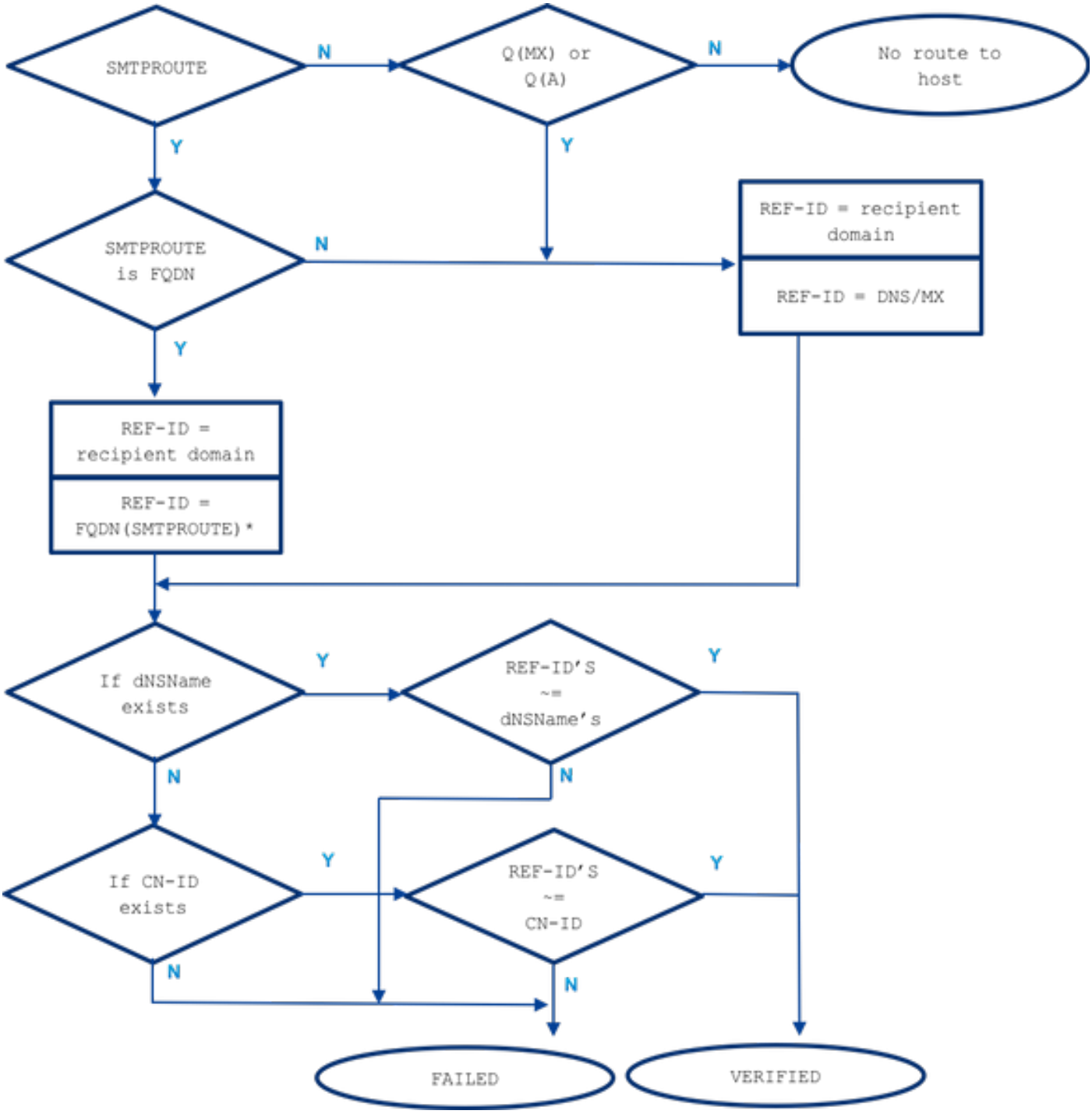
- Mehrere Routen für eine Empfängerdomäne sind zulässig. Wenn die Empfängerdomäne über mehr als eine SMTP-Route verfügt, werden die Routen verarbeitet, bis die angezeigten Bezeichner vom Zertifikat des Zielservers mit dem Namen der Route übereinstimmen, zu der die Verbindung hergestellt wurde. Wenn die Hosts in der Liste unterschiedliche Prioritäten haben, werden zuerst die Hosts mit den höchsten (0 ist die höchste und der Standardwert) verarbeitet. Wenn alle dieselbe Priorität haben, wird die Routenliste in der Reihenfolge verarbeitet, in der die Routen vom Benutzer festgelegt wurden.

- Wenn der Host nicht antwortet (nicht verfügbar ist) oder antwortet, die TLS-Überprüfung jedoch fehlgeschlagen ist, wird der nächste Host aus der Liste verarbeitet. Wenn der erste Host verfügbar ist und die Überprüfung besteht, werden die anderen nicht verwendet.

- Wenn mehrere Routen zu denselben IP-Adressen aufgelöst werden, wird nur eine Verbindung zu dieser IP hergestellt, und die präsentierte Identität, die aus dem vom Zielserver gesendeten Zertifikat abgeleitet wird, muss mit einem dieser Routennamen übereinstimmen.

- Wenn eine SMTP-Route für Empfängerdomänen existiert, aber als IP-Adresse konfiguriert wurde, wird die Route immer noch für die Herstellung einer Verbindung verwendet. Eine präsentierte Identität aus dem Zertifikat wird jedoch mit der Empfängerdomäne und weiter mit dem Hostnamen verglichen, der aus dem DNS/MX-Ressourcendatensatz abgeleitet wurde.

Wenn wir von der Option "TLS Required Verify" (TLS-Überprüfung erforderlich) für gehostete Domänen sprechen, ist die Art und Weise, wie die ESA mit einem Zielserver verbunden ist, für den TLS-Verifizierungsprozess wichtig, da die explizit konfigurierten SMTP-Routen zusätzliche Referenzidentität bereitstellen, die im Prozess zu berücksichtigen ist.



~= steht für die exakte Übereinstimmung oder die Platzhalterangabe.

Beispiel

Nehmen wir ein Beispiel aus dem realen Leben, aber für die Empfängerdomäne: example.com. Im Folgenden habe ich versucht, alle Schritte zu beschreiben, die erforderlich sind, um die Serveridentität manuell zu überprüfen.

Lassen Sie uns zunächst alle erforderlichen Informationen über den Empfängerserver sammeln.

MX-Hostnamen:

```
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
```

Hinweis: Die MX-Hostnamen und die revDNS-Namen stimmen in diesem Fall nicht überein.

Lassen Sie uns nun eine präsentierte Identität des Zertifikats abrufen:

ZERTIFIKATIDENTITÄTEN:

```
$ 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
```

Beide Zielserver haben dasselbe Zertifikat installiert. Lassen Sie uns zwei Validierungsoptionen überprüfen und die Prüfergebnisse vergleichen.

Bei Verwendung von **TLS erforderlich Überprüfen:**

Die TLS-Sitzung wird mit einem der MX-Server eingerichtet, und die Identitätsvalidierung beginnt mit der Überprüfung der gewünschten präsentierten Identität:

- präsentierte Identität: **dNSName existiert** (siehe Vergleich mit zulässiger Referenzidentität)

  Referenz-Identität = Empfängerdomäne (**example.com**) ist geprüft und **stimmt nicht mit** dem **dNSName DNS:*.emailhosted.not, DNS:emailhosted.not überein.**
- präsentierte Identität: **CN vorhanden** (Fortsetzung mit der nächsten präsentierten Identität, wie für die vorherige vorhanden war keine Übereinstimmung)

  Referenz-Identität = Empfängerdomäne (**example.com)** wird geprüft und **stimmt nicht mit** der **CN *.emailhosted.not überein.**

Referenz-Identität = PTR(IP): Eine PTR-Abfrage wird für die IP-Adresse des Servers durchgeführt, zu dem der TLS-Client (ESA) eine Verbindung hergestellt und ein Zertifikat erhalten hat. Diese Abfrage gibt Folgendes zurück: **mx0a.emailhosted.not.**

Die DNS-Konsistenz wird überprüft, um diesen Hostnamen als gültige Referenzidentität zu betrachten:

```
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
```

Der Wert von **mx0a.emailhosted.not.** wird mit CN ***.emailhosted.not** verglichen und dort **stimmt** es **überein.**

Der PTR-Domänenname validiert die Identität. Da es sich bei dem Zertifikat um ein Zertifizierungsstellen-signiertes Zertifikat handelt, wird das gesamte Zertifikat validiert, und es wird eine TLS-Sitzung eingerichtet.

Bei Verwendung von **TLS Required Verify** für **die gehostete Domäne** für denselben Empfänger:

- präsentierte Identität: **dNSName vorhanden** (in diesem Fall wird die CN nicht verarbeitet) Referenz-Identität = Empfängerdomäne (example.com) wird überprüft und entspricht nicht dem DNS-Namen dNSN:*.emailhosted.not, DNS:emailhosted.notReferenz-Identität = FQDN(SMTP-Route) - für diese Empfängerdomäne gibt es keine SMTP-Protokolle

  Da keine SMTPROUTES zusätzlich verwendet werden:

  Referenz-Identität = MX(Empfängerdomäne) - Für die Empfängerdomäne wird eine DNS-MX-Abfrage ausgeführt
  und gibt zurück: **mx01.subd.emailhosted.not** - dies **stimmt nicht mit** dem **dNSName DNS:*.emailhosted.not, DNS:emailhosted.not überein.**
- präsentierte Identität: **CN ist vorhanden, wird aber** auch **übersprungen**, da dNSName vorhanden ist.

Da CN nicht als verarbeitet angesehen wird, schlägt die TLS-Identitätsvalidierung in diesem Fall fehl, ebenso die Zertifikatsüberprüfung, und infolgedessen kann keine Verbindung hergestellt werden.

Zugehörige Informationen

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC 2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2, Versionshinweiss
- Technischer Support und Dokumentation - Cisco Systems