Cisco E メール セキュリティ用の TLS 確認プロセス

目次

概要

この資料は説明したものです Cisco E メール セキュリティ アプライアンス（ESA）のための Transport Layer Security （TLS）サーバ識別確認プロセスを

Cisco E メール セキュリティ用の TLS 確認プロセス

TLS 確認プロセスは本質的に 2 ステージ検証プロセスです:

I -認証の検証

これは確認をの含みます:

- 認証の妥当性期間-証明書ライフタイム
- 証明書 チェーン 発行元
- リボケーションリスト、等…

II -サーバ識別検証

これはサーバ**参照識別**に対してサーバによって**示される識別**の検証プロセス（X.509 公開鍵 証明書に含まれている）です。

背景説明

RFC 6125 に説明がある識別名前専門用語と保存しよう。

注: 示された識別は異なるタイプの複数示された識別名を含むことができるサーバ X.509 公開鍵 証明書によって示される識別名です。 SMTP サービスの場合には、それは型 dNSName の subjectAltName 拡張または Subject フィールドから得られる CN （ Common Name ）として含まれています。

注: 参照識別はクライアントがアプリケーションサービスが証明書で示すと期待すること完全修飾 DNS ドメイン名から組み立てられる識別名です。

確認プロセスは一般にクライアントが TLS セッションを始めるクライアントが通信を認証する必要があるので、TLS クライアントのために大抵重要であり。 *クライアントが示された識別は参照識別と一致するかどうか確認する必要があるこれを実現させるため。* 重要な部分は郵便配達のための TLS 確認プロセスのセキュリティが TLS クライアントにほとんど完全に基づいていることを理解することです。

ステップ 1

サーバ識別検証の第一歩は TLS クライアントによって参照識別を判別することです。 それはアプリケーションから参照識別 TLS クライアントのどんなリストが受諾可能であると考慮するか依存します。 また受諾可能な参照識別のリストはサービスによって示される識別とは関係なく組み立てる必要があります。 [rfs6125#6.2.1]

参照識別は完全修飾 DNS ドメイン名である必要があり、から解析するクライアントのために受諾可能および考慮するためにである）あらゆる入力（セキュアであるとことができます。 クライアントが接続することを試みている DNS ホスト名である参照識別必要。

受信者のメール ドメイン名は特定のユーザ特に送るためにインテントによるユーザによって直接、ドメインにメッセージを表現され、これがまたユーザが接続することを試みている FQDN のために要件を満たした参照識別です。 それは SMTP サーバが所有される同じオーナーおよびサーバによって管理されて余りにも多くのドメインをホストしていない自己ホストされた SMTP サーバの場合にはだけ一貫して。 証明書にリストされている各ドメイン必要性として（ subjectAltName の 1 つとして: dNSName 値）。 100）高くにインプリメンテーションの見通しから、証明書権限（ CA ）のほとんどは 25 のエントリ低くにドメイン名値の番号を制限します（。 これはメール サービス プロバイダー（ ESP ）についてホスト環境の場合には宛先 SMTP サーバが桁等々ドメインのホストするところ、考えよう受け入れられません。 これはどうしてもスケーリングしません。

明示的に設定された参照識別は返事のようですが、これは手動で各宛先 ドメインまたは*「クライアントが」チェックする相互認証および統合を両方提供するアソシエーションか接続に伝えるかどれをと人間ユーザが明示的に信頼を置いたサード・パーティ ドメイン マッピング サービスからのデータを得るためのソースドメインに*参照識別を関連付けることを必要とするので、いくつかの制約を課し。 *[RFC6125#6.2.1]*

概念的には、これはあらゆる DNS 妥協に対して保護するために永久に MTA でキャッシュされて結果が設定の時に一度だけ「セキュア MX クエリ」について間、走行状態で、考えることができます。 [2]

これは「パートナー」ドメインとのだけより強い認証を与えますが、これ合格しない検査にマップされなかったおよびこれまた宛先 ドメインの側のコンフィギュレーション変更に対して免疫がありません一般ドメインのために（ホスト名か IP アドレス変更のように）。

ステップ 2

プロセスの次のステップは示された識別を判別することです。 示された識別はサーバ X.509 公開鍵 証明書によってタイプ dNSName のまたは Common Name （CN）として subjectAltName 拡張が Subject フィールドで見つけたように、提供されます。 Subject フィールドが空であることは全く問題がないところ証明書が少なくとも 1 つの subjectAltName エントリを含む subjectAltName 拡張が含まれている限り。

Common Name の使用がそれ実際にまだある非難されると考慮するおよびであるが現在の推奨事項は subjectAltName エントリを使用することです。 下位互換性のための Common Name 滞在からの識別のためのサポート。 このような場合 subjectAltName の dNSName は最初に使用する必要があり、空のときだけ Common Name はチェックされます。

> **注:** Common Name は形式が完全修飾 DNS ドメイン名のそれと一致するストリングよりもむしろ強く Common Name がサービスのための人間に適するストリングを示すかもしれませんので入力されません

端に両方識別の型が判別されたら、TLS クライアントは一致を見つけるために示された識別に対して参照識別のそれぞれを比較する必要があります。

ESA TLS 確認

ESA は特定のドメインに配達の TLS および証明書確認をイネーブルにすることを割り当てます（宛先を使用してページまたは **destconfig** CLI コマンドを制御します）。 TLS 証明書確認が必要となるとき、AsyncOS バージョン 8.0.2 以来の 2 つの確認オプションの 1 つを選択できます。 期待された確認結果は設定されたオプションによって変わることができます。 TLS の 6 つの異なる設定から、そこの利用可能な下宛先制御は重要な証明書確認に責任がある 2 です:

1. **必要な TLS -確認事項**
2. **必要な TLS が-ホストされたドメインを確認して下さい。**

```
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]>
```

好まれるオプション（4）のための TLS 確認プロセス**– Verify**（5）**必要とされる**と同一です**–**、しかしとられる結果に基づいて処置異なります示された下記の表として**確認して下さい。 必要な**オプション（6）がのための結果**–ホストされたドメインが**（5）**必要とされる**と同一であることを**確認して下さい–確認して下さい**しかし TLS 確認 フローはかなり異なっています。

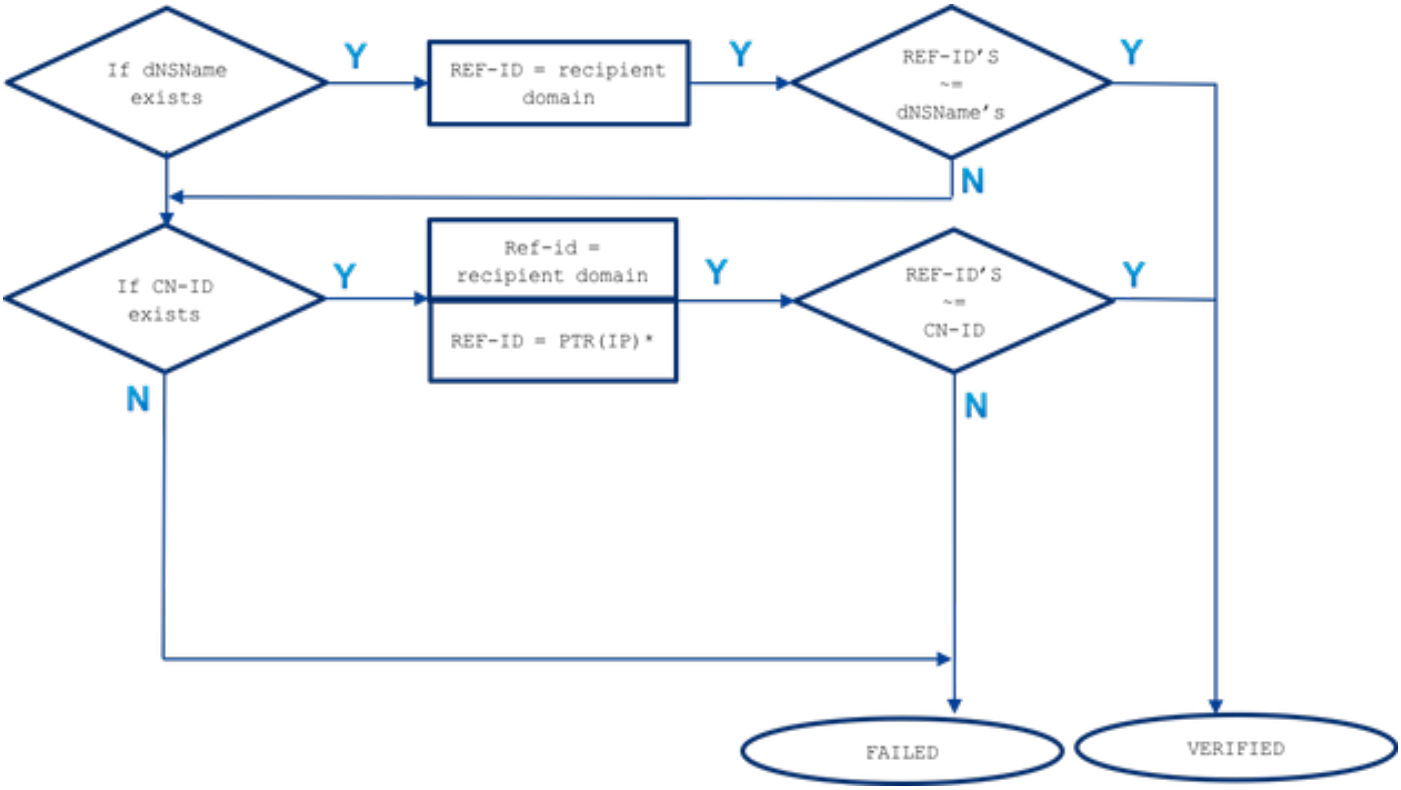
TLS 設定	意味
4. Preferred (Verify)	TLS は E メール セキュリティ アプライアンスからドメインのための MTA へのネゴシエーれます。 機器はドメイン証明書を確認するように試みます。 次の 3 つの結果が考えられます。 • TLS がネゴシエートされ、証明書が検証される。 暗号化されたセッションによってメー配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。 暗号化されたセッションにてメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。 電子メール メッセージがプレーン テトで配信される。
5. Required (Verify)	TLS は E メール セキュリティ アプライアンスからドメインのための MTA へのネゴシエーれます。 ドメイン証明書の確認が必要となります。 次の 3 つの結果が考えられます。 • TLS 接続がネゴシエートされ、証明書が検証される。 暗号化されたセッションによってメール メッセージが配信される。 • TLS 接続はネゴシエートされますが、証明書は信頼された CA によって確認されません。ールは配信されない。 • TLS 接続がネゴシエートされない。 メールは配信されない。

必要な TLS 間の違いが**-確認すれば必要な TLS -ホステッド ドメインが**識別確認プロセスでオプション置くことを**確認して下さい**。 どのような参照識別が使用されることができるか方法は示された識別がどのように処理され、最終結果かについての違いを生じる。 下記の説明、また全体資料の目的はエンドユーザにより密接へこのプロセスです。 このサブジェクトの不正確か明白でない知識はユーザネットワークのセキュリティ への影響がある場合があるように。

必要な TLS が確認します

示された識別は subjectAltName から最初に-あれば dNSName 拡張は CN-ID より一致または subjectAltName 拡張ないし、- Subject フィールドからの Common Name チェックされます得られます。

参照識別（REF-ID）リストは受信者のドメインから組み立てられますまたは IP アドレスに対して PTR DNS クエリ実行から得られる受信者ドメインおよびホスト名はクライアントに接続されます。 注： その特別な場合では、異なる参照識別は異なる示された識別チェックと比較されます。



~= は正確なまたはワイルドカード一致を表します

示された識別はで（dNSName か CN-ID）一致するおよびそれらによってが下記にリストされている順序比較されますまで受け入れられた参照識別で。

- subjectAltName 存在の dNSName 拡張: 正確なまたはワイルドカード一致は受信者のドメインだけに対して行われます

  subjectAltName 一致の場合には参照識別は受信者のドメインからだけ得られます。 受信者のドメインが dNSName エントリのうちのどれも一致するそれ以上の参照識別はチェックされません（DNS 解決 MX か PTR から得られるホスト名のように）

- サブジェクト DN 存在の CN （CN-ID）: 正確なまたはワイルドカード一致は受信者のドメインに対して行われます正確なまたはワイルドカード一致は宛先 サーバの IP に対して実行された PTR クエリから得られるホスト名に対して行われます

  PTR レコードがフォワーダとリゾルバ間の DNS の一貫性を維持したところ。 PTR レコードがおよびある時だけ言及であるどんな必要をここに、その CN フィールドが PTR からのホスト名に対して比較されるかこのホスト名（参照識別）戻りのための解決された A レコード（フォワーダ） PTR クエリが実行された 宛先 サーバ IP を一致する IP アドレス。

  A（PTR（IP））== IP

  CN-ID の場合には参照識別は受信者のドメインから得られ、ホスト名を得るために一致するないとき DNS クエリは宛先IP の PTR レコードに対して実行された。 DNS 一貫性は維持されることを追加クエリを存在 する PTR が確認するために PTR から得られるホスト名の A レコードに対して実行された! それ以上の参照はチェックされません（MX クエリから得られるホスト名のように）

、「必要な TLS 要約するために-」がそこのオプションが dNSName か CN と比較される MX ホ

スト名ではないことを確認して下さい DNS PTR RR は CN があるようにだけ確認され、ときだけ DNS 一貫性なら維持された A（PTR（IP））= IP 一致します、強要すれば両方 dNSName および CN のためのワイルドカード テストは実行された。

必要な TLS が確認します-ホステッド ドメイン

示された識別は型 dNSName の subjectAltName 拡張から最初に得られます。 受け入れられた参照識別（REF-ID）の dNSName ともの間に一致がなければ、確認は CN が Subject フィールドにあり、それ以上の識別確認を渡すことができれば関係を失敗しません。 Subject フィールドから得られる CN は証明書がタイプ dNSName の subjectAltName 拡張のうちのどれも含まれていないときだけ検証されます。

一致するおよびそれらによってが下記にリストされている順序比較されるまで示された識別がで（dNSName か CN-ID）受け入れられた参照識別でことを再呼び出しして下さい。

- subjectAltName 存在の dNSName 拡張:

  matchbetween dNSName をおよびなければ受け入れられた参照識別の 1 つは belowthan 識別検証を失敗しますリストしました
  正確なまたはワイルドカード一致は受信者のドメインに対して行われます: dNSName の 1 つは受信者のドメインを一致する必要があります正確なまたはワイルドカード一致は SMTPROUTES の設定された ホストネームに対して明示的に行われます（*）正確なまたはワイルドカード一致は（不確かの）受信者のドメイン名に対する DNS クエリから得られる MX ホスト名に対して行われます

  受信者のドメインが FQDN エントリで明示的に SMTP ルートを設定しないし、受信者のドメインがより一致しなかったら（不確かの）受信者のドメインに対する DNS クエリからの MXレコードによる FQDN 戻りは使用されます。 一致するなければそれ以上のテストは、どれも実行された PTR レコードはチェックされます
- サブジェクト DN 存在の CN（CN-ID）:
  CN は検証され dNSName がときだけ証明書で存在 しません。 CN-ID は受け入れられた参照識別の下記のリストと比較されます。

  正確なまたはワイルドカード一致は受信者のドメインに対して行われます正確なまたはワイルドカード一致は SMTPROUTES の設定された ホストネームに対して明示的に行われます（*）正確なまたはワイルドカード一致は（不確かの）受信者のドメイン名に対する DNS クエリから得られる MX ホスト名に対して行われます

明示的に設定された SMTPROUTES

SMTP ルートがおよび設定されるとき示された識別は一致する eメール受信者 ドメインをそして名前が比較されるそれ以上のチェックがありませんすべての FQDN ルーティング一致するし。 明示的に設定された SMTP を使うと MX ホスト名を示された識別に対して比較されると考慮されますルーティングしません。 IP アドレスとして設定されたここの例外は SMTP ルートを作ります。

次のルールは明示的に設定された SMTP ルーティングの場合には適用されます:

- SMTP ルートが受信者のドメインのためにおよびあるときそれは完全修飾 DNS ドメイン名

（FQDN）それが参照識別として考慮されるです。 このホスト名-（ルート名前）から指している宛先 サーバ得られる証明書から届く示された識別で比較されます。

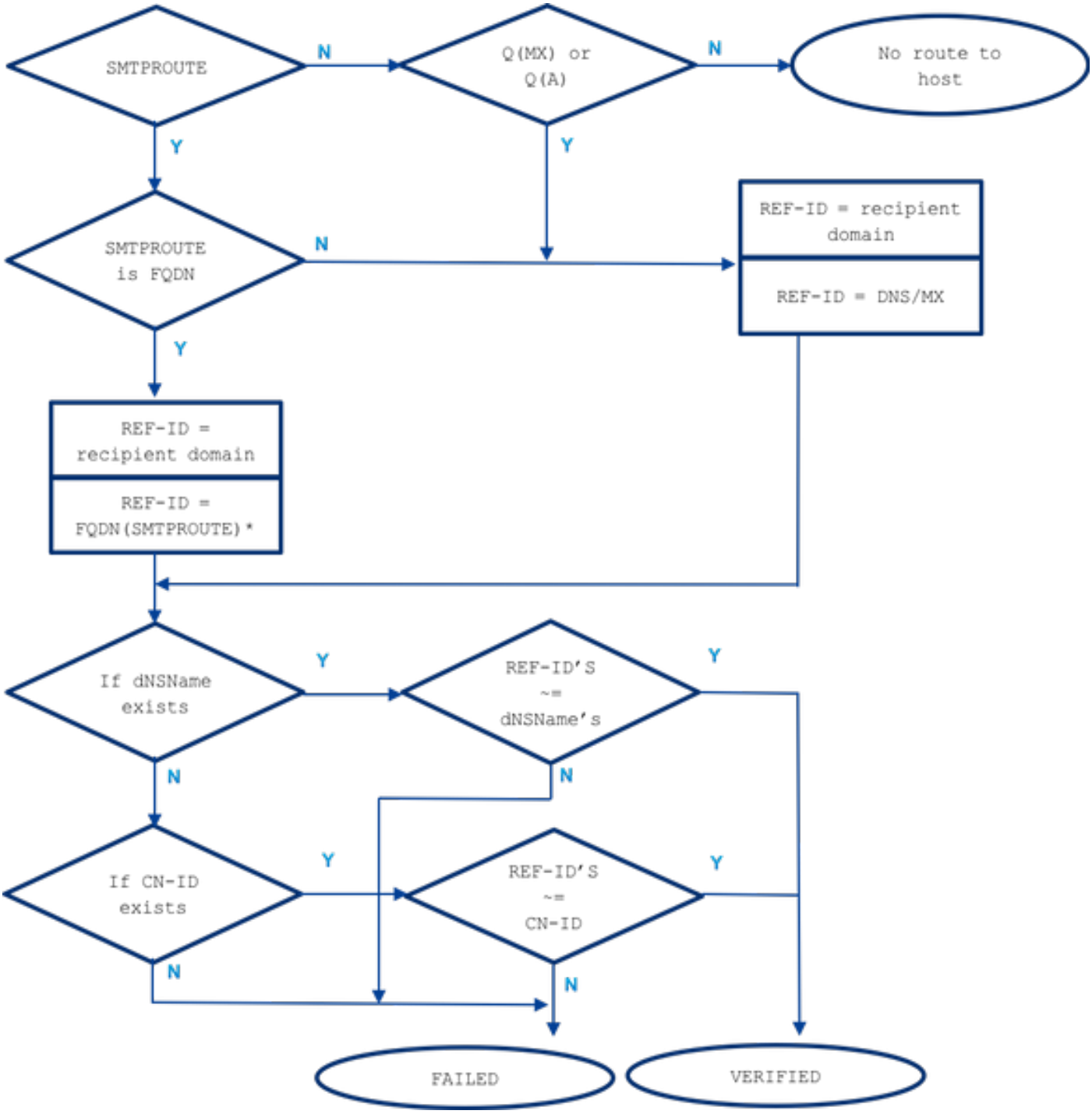
- 受信者のドメインのためのいくつものルートは許可されます。 受信者のドメインに複数の SMTP ルートがある場合、ルートは宛先 サーバからの証明書からの示された識別名まで一致します接続が確立されたルートの名前と処理されます。 リストのホストに最も高いのの異なる優先順位が物（あれば 0 は最も高く、デフォルトは）最初に処理されます。 すべてに同じ優先順位があればルーティングのリストはルーティングがユーザによって設定された順序で処理されます。

- ホストが（応答しないとき利用可能）またはそれが応答すればではないが、TLS 確認はリストからの次のホストを処理されます失敗しました。 最初のホストが利用でき、確認を渡すとき他は使用されません。

- いくつものルートが同じ IP アドレスに解決する場合、この IP への 1 つの接続だけが確立され、宛先 サーバが送信 する 証明書から得られる示された識別がこれらのルート名前の 1 と一致する必要がある。

- SMTP ルートが受信者のドメインのためにあるが、IP アドレスで設定される場合、ルートは今でも接続をする使用ですが、証明書からの示された識別は受信者のドメインに対しておよび DNS/MX リソースレコードから得られるホスト名とそれ以上-比較されます。

必要な TLS 述べているとき ESA が宛先 サーバとである明示的に設定された SMTP ルーティングが理由でプロセスで考慮されるべき追加参照識別を提供する TLS 確認プロセスのために重要どのように接続したかホストされたドメインのためのオプションを、方法確認して下さい。



~= は正確なまたはワイルドカード一致を表します

例

実質ライフからの、受信者のドメインのための例を使って考えよう: example.com など。 の下で すべてのステップを記述することを試みました手動でサーバ識別を確認して必要である。

最初に、受信者のサーバについてのすべての必要とされる情報を収集しよう。

MX ホスト名:

```
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
```

注: MX ホスト名および revDNS 名前はこの場合一致する

この場合証明書によって示される識別を得るために割り当てます:

証明書識別:

```
$ 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
```

宛先 サーバは両方とも同じ証明書をインストールしてもらいます。 2 つの検証オプションを検討しよう、確認結果を比較する。

必要な TLS の使用の場合には **確認して下さい:**

TLS セッションは MX サーバの 1 つと設定され、識別検証は望ましい示された識別のチェックから開始します:

- 示された識別: **dNSName はあります** (許可された参照識別との比較に続いて下さい)

  参照識別は = 受信者のドメイン (example.com) チェックされ、dNSName DNS を一致する: *.emailhosted.not、DNS: emailhosted.not
- 示された識別: **CN は**前のものに関しては一致がなかった**あります** (次に示された identiy と

続けて下さい）

参照識別は = 受信者のドメイン（**example.com** ）チェックされ、**CN *.emailhosted.not を一致する**

参照識別 = PTR（IP）: PTR クエリーは TLS クライアント（ESA）は確立された接続がおよび証明書受け取られてある、およびこのクエリー リターン実行されたサーバの IP に対して: **mx0a.emailhosted.not.**

DNS 一貫性は有効な参照識別としてこのホスト名を考慮するためにチェックされます:

```
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 の値は CN ***.emailhosted.not** に対して比較され、そこに一致します。PTR ドメイン名は証明書が CA証明であるので識別をそれ検証します全証明書を検証し、TLS セッションは設定されます。

必要な TLS の使用の場合にはこの同じ受信者の **ホステッド ドメインのために確認して下さい**:

- 示された識別: **dNSName はあります**（従って CN はそのケースで処理されません）参照識別は = 受信者のドメイン（example.com）チェックされます
  dNSName DNS を一致する: *.emailhosted.not、DNS: emailhosted.not参照識別 = FQDN（smtp ルート）は-そこにこの受信者のドメインのための smtproutes ではないです

  その上に使用される SMTPROUTES ないように:

  参照識別 = MX（受信者のドメイン）は受信者のドメインに対して- DNS MX クエリ実行された
  そして戻り: **mx01.subd.emailhosted.not** -これは **dNSName DNS を一致する: *.emailhosted.not、DNS: emailhosted.not**
- 示された識別: **CN は** dNSName が同様にあると同時に**ありますが、スキップされます。**

CN が処理されると考慮されないので TLS 識別検証はそのケースに失敗します、また証明書確認はその結果接続確立され。

関連情報

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 リリース ノート
- テクニカル サポートとドキュメント – Cisco Systems