Processo di verifica TLS per Cisco Email Security

Sommario

Introduzione

In questo documento vengono spiegate processo di verifica dell'identità del server Transport Layer Security (TLS) per Cisco Email Security Appliance (ESA)

Processo di verifica TLS per Cisco Email Security

Il processo di verifica TLS è essenzialmente un processo di convalida in due fasi:

I - CONVALIDA DEL CERTIFICATO

Ciò comporta la verifica di:

- periodo di validità del certificato - durata del certificato
- emittente catena di certificati
- elenco di revoche, ecc.

II - CONVALIDA IDENTITÀ SERVER

Processo di convalida dell'**identità presentata** dal server (contenuta nel certificato di chiave pubblica X.509) rispetto all'**identità di riferimento** del server.

Sfondo

Manteniamo la terminologia dei nomi di identità descritta nella RFC 6125.

Nota: L'**identità presentata** è un identificatore presentato da un certificato di chiave pubblica X.509 del server che può includere più identificatori presentati di tipi diversi. Nel caso del servizio SMTP, è contenuto come estensione subjectAltName di tipo dNSName o come CN (Nome comune) derivato dal campo del soggetto.

Nota: L'**identità di riferimento** è un identificatore costruito da un nome di dominio DNS completo che un client si aspetta da un servizio dell'applicazione di presentare nel certificato.

Il processo di verifica è importante soprattutto per un client TLS, in quanto in generale un client avvia una sessione TLS e un client deve autenticare la comunicazione. *A tale scopo, il client deve verificare se l'identità presentata corrisponde all'identità di riferimento.* La parte importante è capire che la sicurezza del processo di verifica TLS per il recapito della posta è quasi interamente basata sul client TLS.

Primo passo

Il primo passaggio della convalida dell'identità del server consiste nel determinare l'identità di riferimento da parte del client TLS. Dipende dall'applicazione quale elenco di identificatori di riferimento il client TLS considera accettabile. Anche un elenco di identificativi di riferimento accettabili deve essere costruito indipendentemente dagli identificativi presentati dal servizio. [rfs6125#6.2.1]

L'identità di riferimento deve essere un nome di dominio DNS completo e può essere analizzata da qualsiasi input (accettabile per un client e considerato sicuro). L'identità di riferimento deve essere un nome host DNS a cui il client sta tentando di connettersi.

Il nome di dominio di posta elettronica del destinatario è un'identità di riferimento espressa direttamente dall'utente, con l'intenzione di inviare un messaggio a un utente specifico in un particolare dominio e questo soddisfa anche il requisito di essere un FQDN a cui un utente sta tentando di connettersi. È coerente solo nel caso di un server SMTP autonomo in cui il server SMTP è di proprietà e gestito dallo stesso proprietario e il server non ospita troppi domini. Poiché ogni dominio deve essere elencato in certificato (come uno di SubjectAltName: valori dNSName). Dal punto di vista dell'implementazione, la maggior parte delle Autorità di certificazione (CA) limita il numero di nomi di dominio a un massimo di 25 voci (fino a un massimo di 100). Questo non è accettato nel caso dell'ambiente host, pensiamo ai provider di servizi di posta elettronica (ESP) in cui i server SMTP di destinazione ospitano migliaia e più di domini. Questo non è in scala.

L'identità di riferimento configurata in modo esplicito sembra essere la risposta, ma questo impone alcuni vincoli, in quanto è necessario associare manualmente un'identità di riferimento al dominio di origine per ogni dominio di destinazione o *"ottenere i dati da un servizio di mappatura dei domini di terze parti in cui un utente ha esplicitamente posto un trust e con cui il client comunica su una connessione o un'associazione che fornisce sia l'autenticazione reciproca che il controllo dell'integrità". [RFC6125#6.2.1]*

Dal punto di vista concettuale, questo può essere pensato come una "query MX sicura" da eseguire una sola volta al momento della configurazione, con il risultato memorizzato in modo permanente nell'MTA per proteggersi da eventuali compromessi del DNS quando è in stato di esecuzione. [2]

Ciò fornisce un'autenticazione più forte solo con i domini "partner", ma per i domini generici che non sono stati mappati questo non supera l'esame e questo non è immune dalle modifiche della

configurazione sul lato del dominio di destinazione (come le modifiche del nome host o dell'indirizzo IP).

Secondo passo

Il passaggio successivo del processo consiste nel determinare un'identità presentata. L'identità presentata viene fornita da un certificato di chiave pubblica X.509 del server, come estensione subjectAltName di tipo dNSName o come nome comune (CN) trovato nel campo dell'oggetto. Dove è possibile che il campo relativo al soggetto sia vuoto, purché il certificato contenga un'estensione subjectAltName che include almeno una voce subjectAltName.

Sebbene l'utilizzo di Nome comune sia ancora in pratica, è considerato deprecato e la raccomandazione corrente è quella di utilizzare le voci subjectAltName. Il supporto per l'identità da Nome comune rimane per la compatibilità con le versioni precedenti. In tal caso, è necessario utilizzare prima dNSName di subjectAltName e solo quando è vuoto, viene selezionato Nome comune.

> **Nota:** Il nome comune non è fortemente tipizzato perché potrebbe contenere una stringa descrittiva per il servizio anziché una stringa il cui formato corrisponde a quello di un nome di dominio DNS completo

Alla fine, quando sono stati determinati entrambi i tipi di identità, il client TLS deve confrontare ciascuno dei suoi identificativi di riferimento con gli identificativi presentati al fine di trovare una corrispondenza.

Verifica ESA TLS

ESA consente di abilitare TLS e la verifica del certificato al momento della consegna a domini specifici (usando la pagina Controlli destinazione o il comando **destconfig** CLI). Quando è richiesta la verifica del certificato TLS, è possibile scegliere una delle due opzioni di verifica disponibili a partire dalla versione 8.0.2 di AsyncOS. Il risultato previsto della verifica può variare a seconda dell'opzione configurata. Tra le 6 diverse impostazioni per TLS, disponibili sotto controllo di destinazione, ci sono due importanti che sono responsabili della verifica del certificato:

1. **TLS obbligatorio - Verifica**
2. **TLS obbligatorio - Verifica dei domini ospitati**.

```
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 processo di verifica TLS per l'opzione (4) **Preferito - Verifica** è identico a (5) **Obbligatorio - Verifica**, ma l'azione intrapresa in base ai risultati differisce come illustrato nella tabella seguente. I risultati per l'opzione (6) **Obbligatorio - Verifica dei domini ospitati** è identico a (5) **Obbligatorio - Verifica** ma un flusso di verifica TLS è abbastanza diverso.

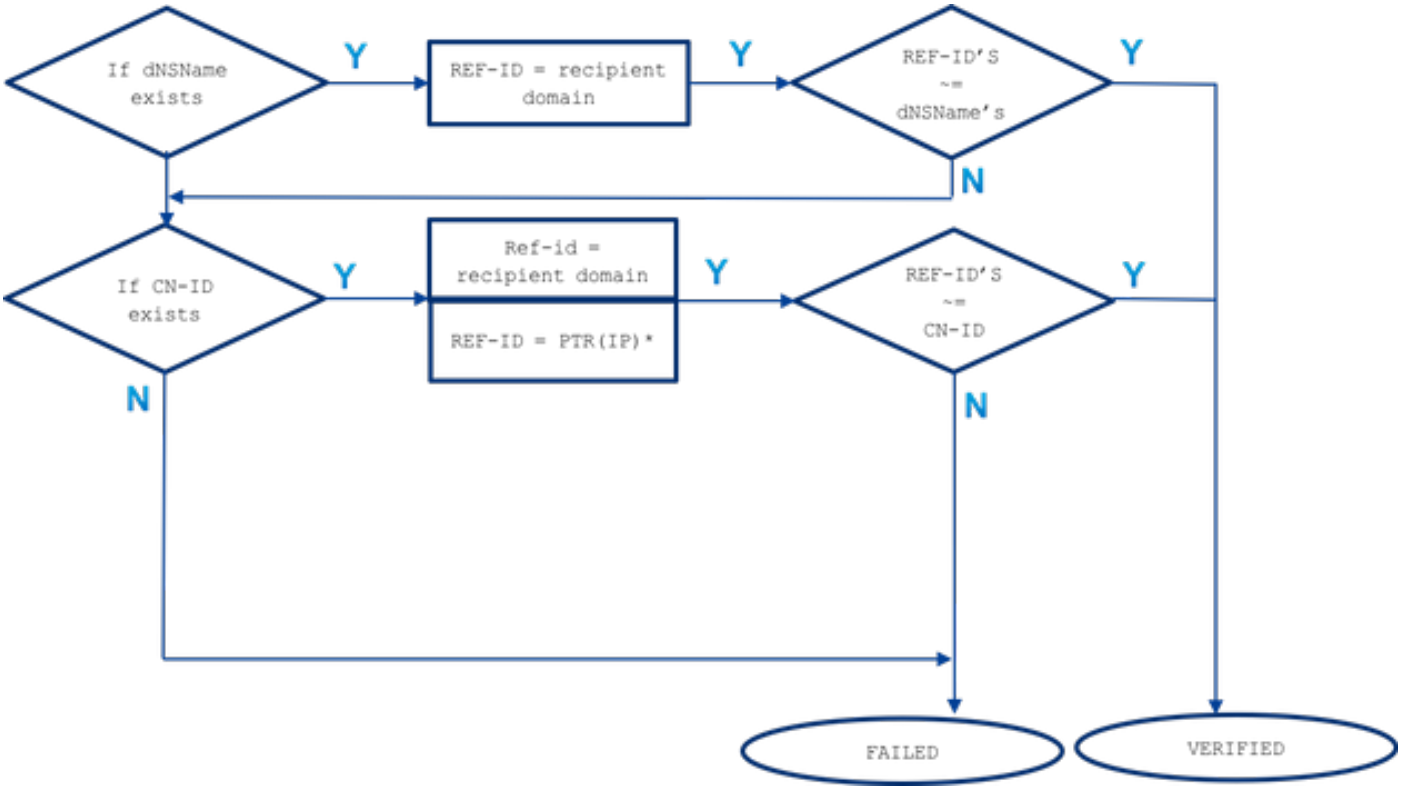
Impostazioni TLS	Significato
4. Preferito (Verifica)	Il protocollo TLS viene negoziato tra l'appliance Email Security e gli MTA del dominio. L'accessorio tenta di verificare il certificato dei domini. Sono possibili tre risultati: • TLS viene negoziato e il certificato verificato. La posta viene recapitata tramite una sessione crittografata. • TLS viene negoziato, ma il certificato non viene verificato. La posta viene recapitata tra una sessione crittografata. • Non viene stabilita alcuna connessione TLS e, di conseguenza, il certificato non viene verificato. Il messaggio e-mail viene recapitato in formato testo normale.
5. Obbligatorio (verifica)	Il protocollo TLS viene negoziato tra l'appliance Email Security e gli MTA del dominio. Verif del certificato dei domini obbligatoria. Sono possibili tre risultati: • Una connessione TLS viene negoziata e il certificato verificato. Il messaggio e-mail vie recapitato tramite una sessione crittografata. • Una connessione TLS viene negoziata ma il certificato non viene verificato da una CA attendibile. La posta non viene recapitata. • Connessione TLS non negoziata. La posta non viene recapitata.

La differenza tra le opzioni **TLS Required - Verify** e **TLS Required - Verify Hosted Domain** risiede nel processo di verifica dell'identità. Il modo in cui viene elaborata l'identità presentata e il tipo di identificativi di riferimento che è consentito utilizzare fanno la differenza per il risultato finale. Lo scopo della descrizione seguente e dell'intero documento è quello di avvicinare questo processo all'utente finale. Poiché la comprensione non corretta o non chiara di questo argomento può avere un impatto sulla protezione della rete degli utenti.

Verifica TLS obbligatoria

L'identità presentata deriva prima da subjectAltName - estensione dNSName e se non esiste alcuna corrispondenza o l'estensione subjectAltName non esiste rispetto a CN-ID - il campo Nome comune da oggetto è selezionato.

L'elenco di identità di riferimento (REF-ID) è costruito da un dominio destinatario o da un dominio destinatario e da un nome host derivato da una query DNS PTR eseguita sull'indirizzo IP a cui è connesso il client. Nota: In questo caso particolare, diverse identità di riferimento sono confrontate con diversi controlli di identità presentati.



~= rappresenta una corrispondenza esatta o con caratteri jolly

L'identità presentata (dNSName o CN-ID) viene confrontata con le identità di riferimento accettate finché non viene confrontata e nell'ordine in cui sono elencate di seguito.

- Se l'estensione dNSName di subjectAltName esiste: la corrispondenza esatta o con caratteri jolly viene eseguita solo nel dominio del destinatario

  L'identità di riferimento in caso di corrispondenza subjectAltName deriva solo dal dominio del destinatario. Se il dominio del destinatario non corrisponde ad alcuna delle voci dNSName, non viene verificata alcuna ulteriore identità di riferimento (come il nome host derivato dalla risoluzione DNS MX o PTR)

- Se esiste un CN del DN soggetto (CN-ID): corrispondenza esatta o con caratteri jolly nel dominio del destinatarioLa corrispondenza esatta o con caratteri jolly viene eseguita sul nome host derivato dalla query PTR eseguita su un indirizzo IP del server di destinazione

  In cui il record PTR mantiene una coerenza nel DNS tra il server di inoltro e il resolver. A questo proposito, il campo CN viene confrontato con un nome host di PTR solo quando esiste un record PTR e un record A risolto (un server d'inoltro) per questo nome host (identità di riferimento) restituisce un indirizzo IP corrispondente all'indirizzo IP del server di destinazione con cui è stata eseguita una query PTR.

  A(PTR(IP)) == IP

  L'identità di riferimento nel caso di CN-ID deriva dal dominio del destinatario e, in assenza di corrispondenza, viene eseguita una query DNS su un record PTR dell'IP di destinazione per ottenere un nome host. Se esiste una PTR, viene eseguita un'ulteriore query su un record A di un nome host derivato da una PTR per confermare che la coerenza DNS viene mantenuta.

Non vengono controllati ulteriori riferimenti (come il nome host derivato dalla query MX)

Per riassumere, con l'opzione 'TLS obbligatorio - Verifica' non esiste alcun nome host MX confrontato con dNSName o CN, un record di risorse PTR DNS viene controllato solo per CN e viene confrontato solo se la coerenza DNS viene mantenuta A(PTR(IP)) = IP, vengono eseguiti sia il test esatto che il test con caratteri jolly per dNSName e CN.

Verifica richiesta TLS - Dominio ospitato

L'identità presentata deriva innanzitutto dall'estensione subjectAltName di tipo dNSName. Se non c'è corrispondenza tra dNSName e una delle identità di riferimento accettate (REF-ID), la verifica non riesce indipendentemente dal fatto che nel campo dell'oggetto esista un CN e potrebbe superare un'ulteriore verifica dell'identità. Il CN derivato dal campo del soggetto viene convalidato solo quando il certificato non contiene estensioni subjectAltName di tipo dNSName.

Tenere presente che l'identità presentata (dNSName o CN-ID) viene confrontata con le identità di riferimento accettate finché non viene confrontata e nell'ordine in cui sono elencate di seguito.

- Se l'estensione dNSName di subjectAltName esiste:

  Se non esiste corrispondenza tra dNSName e una delle identità di riferimento accettate elencate di seguito, la convalida dell'identità non riesce
  la corrispondenza esatta o con caratteri jolly viene eseguita nel dominio del destinatario: Uno di dNSName deve corrispondere a un dominio del destinatariouna corrispondenza esatta o con caratteri jolly viene eseguita su un nome host configurato in modo esplicito con SMTPROROUTE (*)una corrispondenza esatta o con caratteri jolly viene eseguita sul nome host MX derivato da una query DNS (non sicura) sul nome di dominio del destinatario

  Se il dominio del destinatario non dispone di una route SMTP configurata in modo esplicito con voci FQDN e il dominio del destinatario non ha una corrispondenza con un FQDN restituito da un record MX da una query DNS (non protetta) su un dominio del destinatario. In assenza di corrispondenza, non vengono eseguiti altri test e non viene controllato alcun record PTR
- Se esiste un CN del DN soggetto (CN-ID):
  CN convalidato solo quando dNSName non esiste nel certificato. Il CN-ID viene confrontato con l'elenco di identità di riferimento accettate riportato di seguito.

  corrispondenza esatta o con caratteri jolly nel dominio del destinatariouna corrispondenza esatta o con caratteri jolly viene eseguita su un nome host configurato in modo esplicito in SMTPROUTES (*)una corrispondenza esatta o con caratteri jolly viene eseguita sul nome host MX derivato da una query DNS (non sicura) sul nome di dominio del destinatario

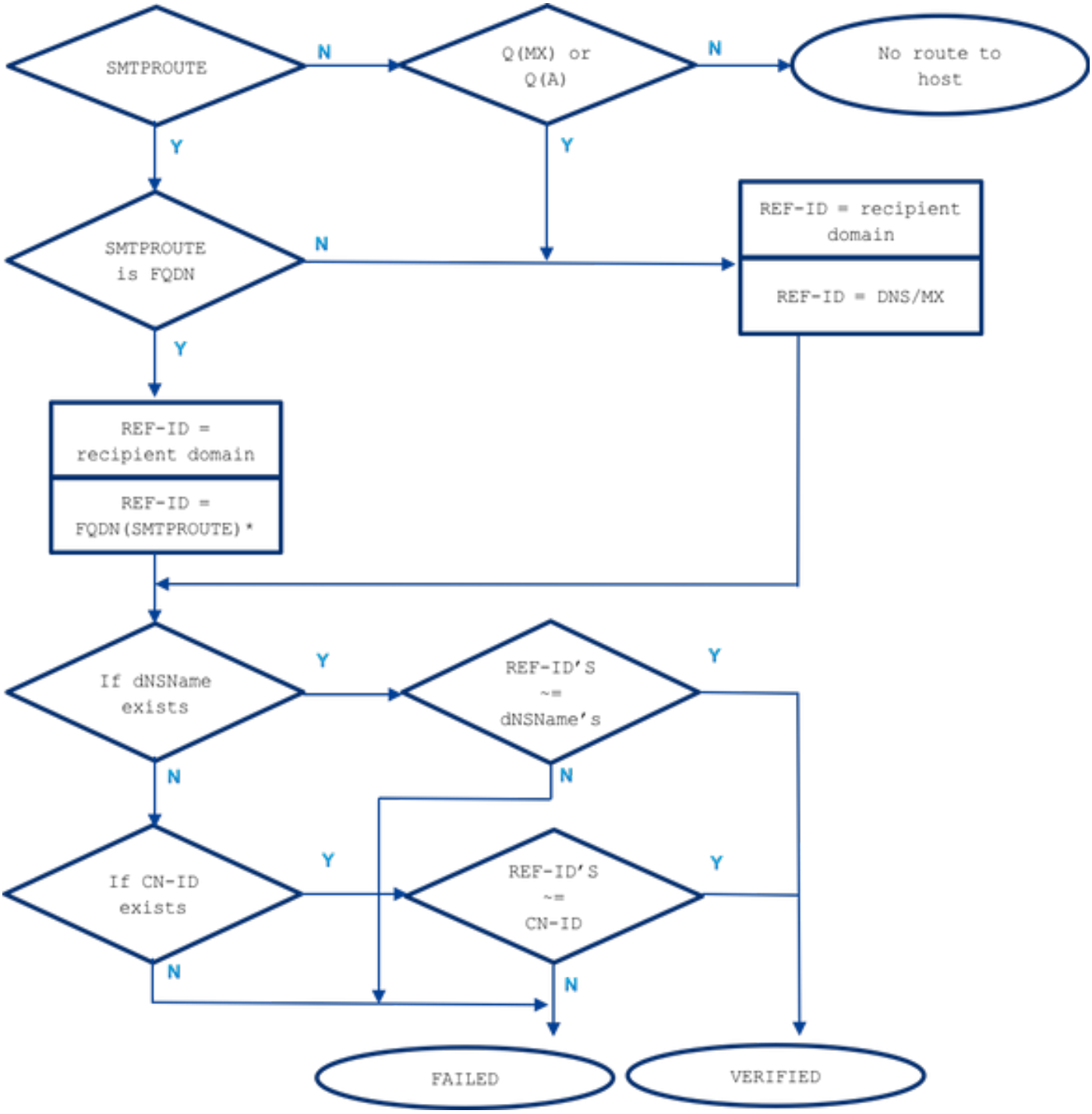
ROUTE SMT configurate in modo esplicito

Quando la route SMTP è configurata e l'identità presentata non corrisponde al dominio del destinatario della posta elettronica, tutti i nomi di route FQDN vengono confrontati e, se non corrispondono, non vengono eseguiti ulteriori controlli. Con route SMTP configurate in modo esplicito, nessun nome host MX viene considerato confrontato con un'identità presentata. L'eccezione qui fa una route SMTP che è stata impostata come indirizzo IP.

In caso di route SMTP configurate in modo esplicito, si applicano le regole seguenti:

- Quando esiste una route SMTP per un dominio del destinatario ed è un nome di dominio DNS completo (FQDN), viene considerata come identità di riferimento. Questo nome host (un nome di route) viene confrontato con l'identità presentata ricevuta da un certificato derivato da un server di destinazione a cui punta.
- Sono consentite più route per un dominio del destinatario. Se il dominio del destinatario dispone di più route SMTP, queste vengono elaborate finché gli identificatori presentati dal certificato del server di destinazione non corrispondono al nome della route alla quale è stata stabilita la connessione. Se gli host nella lista hanno priorità diverse, vengono elaborati per primi quelli con la priorità più alta (0 è il valore più alto e quello predefinito). Se tutte hanno la stessa priorità, l'elenco delle route viene elaborato nell'ordine in cui sono state impostate dall'utente.
- Nel caso in cui l'host non risponde (non è disponibile) o risponde ma la verifica TLS non è riuscita, viene elaborato l'host successivo dell'elenco. Quando il primo host è disponibile e supera la verifica, gli altri non vengono utilizzati.
- Se più route vengono risolte negli stessi indirizzi IP, viene stabilita una sola connessione all'IP e l'identità presentata derivata dal certificato inviato dal server di destinazione deve corrispondere a uno di questi nomi di route.
- Se la route SMTP esiste per i domini dei destinatari ma è stata configurata come indirizzo IP, viene ancora utilizzata per effettuare una connessione ma un'identità presentata dal certificato viene confrontata con il dominio del destinatario e più avanti con il nome host derivato dal record di risorse DNS/MX.

Quando si parla dell'opzione di verifica TLS obbligatoria per i domini ospitati, il modo in cui ESA si è connessa a un server di destinazione è importante per il processo di verifica TLS a causa delle route SMTP configurate in modo esplicito che forniscono un'identità di riferimento aggiuntiva da considerare nel processo.



~= rappresenta una corrispondenza esatta o con caratteri jolly

Esempio

Prendiamo ad esempio la vita reale, ma per il dominio del destinatario: example.com. Di seguito sono riportate tutte le operazioni necessarie per verificare manualmente l'identità del server.

In primo luogo, verranno raccolte tutte le informazioni necessarie sul server destinatario.

Nomi host 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):

```
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
```

Nota: i nomi host MX e i nomi revDNS non corrispondono in questo caso

Ottieni ora un'identità di certificato presentata:

IDENTITÀ CERTIFICATO/I:

```
$ 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
```

In entrambi i server di destinazione è installato lo stesso certificato. Esaminiamo due opzioni di convalida e confrontiamo i risultati della verifica.

In caso di utilizzo di **TLS Required Verify:**

La sessione TLS viene stabilita con uno dei server MX e la convalida dell'identità inizia controllando l'identità presentata desiderata:

- identità presentata: **esiste dNSName** (continuare il confronto con l'identità di riferimento consentita)

  l'identità di riferimento = dominio destinatario (**example.com**) è selezionata e **non corrisponde** al **nome DNS dNSN:*.emailhosted.not, DNS:emailhosted.not**
- identità presentata: **CN** (continuare con l'identità presentata successiva, come per l'identità precedente, senza corrispondenza)

  l'identità di riferimento = dominio del destinatario (**example.com)** è selezionata e **non corrisponde** alla **CN *.emailhosted.not**

identità di riferimento = PTR(IP) : viene eseguita una query PTR sull'indirizzo IP del server a cui il client TLS (ESA) ha stabilito la connessione e ricevuto un certificato. La query restituisce: **mx0a.ospitato.non.**

Èstata verificata la coerenza DNS per considerare questo nome host come identità di riferimento valida:

```
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
```

Il valore di **mx0a.emailhosted.not.** viene confrontato con CN ***.emailhosted.not** e qui **corrisponde.**

Il nome di dominio PTR convalida l'identità e, poiché il certificato è un certificato firmato dalla CA, convalida l'intero certificato e viene stabilita una sessione TLS.

In caso di utilizzo di **TLS Required Verify per il dominio ospitato** per lo stesso destinatario:

- identità presentata: **dNSName esiste** (in questo caso la CN non verrà elaborata) identità di riferimento = dominio destinatario (example.com) è selezionato e
  non corrisponde a dNSName DNS:*.emailhosted.not, DNS:emailhosted.notidentità di riferimento = FQDN(route smtp) - non esistono smtproute per questo dominio destinatario

  Poiché non sono disponibili SMTPROUTE, vengono utilizzate anche le seguenti opzioni:

  identità di riferimento = MX(dominio destinatario) - viene eseguita una query DNS MX sul dominio destinatario
  e restituisce: **mx01.subd.emailhosted.not** - **non corrisponde** al **DNS dNSName:*.emailhosted.not, DNS:emailhosted.not**
- identità presentata: **CN esiste ma viene ignorato** perché esiste anche dNSName.

Poiché il CN non viene considerato elaborato, la convalida dell'identità TLS non riesce in questo caso, così come la verifica del certificato e di conseguenza non è possibile stabilire la connessione.

Informazioni correlate

- RFC 6125 - https://tools.ietf.org/html/rfc6125
- RFC 2818 - https://tools.ietf.org/html/rfc2818
- Nota sulla release di AsyncOS 8.0.2s
- Documentazione e supporto tecnico – Cisco Systems