TLS-verificatieproces voor Cisco e-mail security

Inhoud

Inleiding

Dit document beschrijft het proces voor verificatie van de identiteit van de transportlaag security server (TLS) voor Cisco e-mail security applicatie (ESA)

TLS-verificatieproces voor Cisco e-mail security

Het TLS-verificatieproces is in wezen een valideringsproces in twee fasen:

I - VALIDATIE VAN CERTIFICATEN

Dit houdt in dat wordt gecontroleerd:

- geldigheidsduur van het certificaat - levensduur
- uitgevende instelling van certificaten
- lijst van herroeping enz .

II - VALIDATIE VOOR SERVERIDENTITEIT

Dit is een validatieproces van de **voorgestelde identiteit van de** server (vervat in X.509 publieke sleutelcertificaat) tegen de **referentie-identiteit van de** server.

Achtergrond

Laten we de terminologie van de naam, beschreven in RFC 6125, bij houden.

Opmerking: De **gepresenteerde identiteit** is een identificator die wordt gepresenteerd door een server X.509 openbaar sleutelcertificaat, dat meer dan één gepresenteerd identificator van verschillende typen kan bevatten. In het geval van een dienst voor het beheer van de smmtp, is deze opgenomen als een uitbreiding van het type AltName van het type dNSName of als de GN (Gemeenschappelijke Naam) afgeleid van het onderwerpveld.

Opmerking: De **referentie-identiteit** is een identificator die is samengesteld uit een volledig gekwalificeerde DNS-domeinnaam die een cliënt verwacht dat een toepassingsdienst in het certificaat aanwezig is.

Het verificatieproces is voornamelijk van belang voor een TLS-cliënt, aangezien een cliënt in het algemeen een TLS-sessie initieert en een cliënt de communicatie moet authenticeren. *Daartoe moet een cliënt nagaan of de aangeboden identiteit overeenkomt met de referentie-identiteit.* Het belangrijkste is te begrijpen dat de beveiliging van het TLS Verificatie-proces voor de postbezorging vrijwel geheel gebaseerd is op de TLS-cliënt.

Stap één

De eerste stap in de validatie van de serveridentiteit is het bepalen van de referentie-identiteit door de TLS-client. Het hangt af van de toepassing welke lijst van referentie-identificatoren TLS-client aanvaardbaar acht. Ook moet een lijst van aanvaardbare referentienummers worden opgesteld onafhankelijk van de identificatoren die door de dienst worden voorgesteld. [rfs6125#6.2.1]

De referentie-identiteit moet een volledig gekwalificeerde DNS-domeinnaam zijn en kan worden ontleend aan elke input (die voor een client aanvaardbaar is en als veilig wordt beschouwd). De referentie identiteit moet een DNS hostname zijn waaraan de client probeert verbinding te maken.

De naam van het ontvangende e-maildomein is een referentie-identiteit die rechtstreeks door de gebruiker wordt uitgedrukt, door de bedoeling een bericht naar een bepaalde gebruiker in een bepaald domein te sturen, en dit voldeed ook aan de eis om een FQDN te zijn waaraan een gebruiker probeert te verbinden. Het is consistent alleen in het geval van zelf-gehost MTP-server waar de MTP-server in het bezit is van en beheerd wordt door dezelfde eigenaar en de server niet te veel domeinen ontvangt. Zoals elk domein in certificaat moet worden vermeld (als één van subjectAltName: NNSName-waarden). Vanuit een implementatieperspectief beperkt de meeste certificaatautoriteiten (CA) het aantal domeinnamen tot maximaal 25 items (tot maximaal 100). Dit wordt niet geaccepteerd in het geval van de Hosted Environment, laten we denken aan E-mail Service Providers (ESP), waar de bestemmingservers in MTP duizenden en meer domeinen huisvesten. Dit schalen is gewoon niet.

De expliciet gedefinieerde referentie-identiteit lijkt het antwoord te zijn, maar dit legt enige beperkingen op, aangezien het vereist is om handmatig een referentie-identiteit te koppelen aan brondomein voor elk doeldomein of *"het verkrijgen van de gegevens van een derdeads domeinkaartmakerij waarin een menselijke gebruiker expliciet vertrouwen heeft gesteld en waarmee de client communiceert over een verbinding of vereniging die zowel wederzijdse authenticatie als integriteitscontrole biedt". [RFC6125#6.2.1]*

Conceptueel kan dit worden gezien als een eenmalige "beveiligde MX query" op het moment van configuratie, waarbij het resultaat permanent op de MTA wordt gecached om te beschermen tegen een DNS compromis tijdens de run status. [2]

Dit geeft alleen een sterkere authenticatie met "partner"-domeinen maar voor generiek domein dat

niet in kaart is gebracht, gaat dit niet door het examen en dit is ook niet immuun tegen configuratieveranderingen aan de kant van het bestemmingsterrein (zoals hostname of IP adresveranderingen).

Stap twee

De volgende stap in het proces is het bepalen van een identiteit die wordt gepresenteerd. De gepresenteerde identiteit wordt verschaft door een server X.509 publieke sleutelcertificaat, als subjectAltName extensie van type dNSName of als Common Name (CN) die in het onderwerpveld wordt gevonden. Wanneer het voor het onderwerpveld perfect aanvaardbaar is dat het leeg is, zolang het certificaat een subjectAltName-extensie bevat die ten minste één onderwerpAltName-vermelding bevat.

Hoewel het gebruik van de gemeenschappelijke naam in de praktijk nog steeds bestaat, wordt het geacht te zijn afgekeurd en wordt in de huidige aanbeveling verwezen naar de vermelding van de naam subjectAltName. De ondersteuning van de identiteit van Common Name blijft voor compatibiliteit met de achterzijde. In een dergelijk geval dient eerst een naam van subjectAltName te worden gebruikt en alleen wanneer deze naam leeg is, wordt de Common Name gecontroleerd.

> Opmerking: de Common Name wordt niet sterk getypt omdat een Common Name een menselijke vriendelijke string voor de service zou kunnen bevatten, in plaats van een string waarvan de vorm overeenkomt met die van een volledig gekwalificeerde DNS-domeinnaam

Aan het einde van het jaar waarin beide soorten identificaties zijn vastgesteld, moet de TLS-cliënt elk van zijn referentienummers vergelijken met de voorgestelde identificatoren om een match te vinden.

ESA-TLS-verificatie

De ESR laat TLS en certificatenverificatie bij levering aan specifieke domeinen toe (met behulp van de Destination Control-pagina of de **deconfiguratie** CLI-opdracht). Wanneer de TLS-certificeringscontrole vereist is, kunt u één van twee verificatieopties kiezen sinds AsyncOS versie 8.0.2. Het verwachte verificatieresultaat kan afhankelijk van de ingestelde optie verschillen. Van 6 verschillende instellingen voor TLS, beschikbaar onder bestemmingscontrole, zijn er twee belangrijke die verantwoordelijk zijn voor de certificatencontrole:

1. **TLS vereist - Controleer**
2. **TLS vereist - controleer Hosted domein**.

```
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]>
```

Een TLS-verificatieprocedure voor optie (4) **Voorkeurd - Verifieer** is identiek aan (5) **Vereiste - Controleer**, maar de op resultaten gebaseerde actie verschilt zoals in onderstaande tabel weergegeven. De resultaten voor optie (6) **vereist - Controleer of de Hosted Domain** identiek is aan (5) **vereist - Controleer** maar een TLS-verificatiestroom is een heel andere.

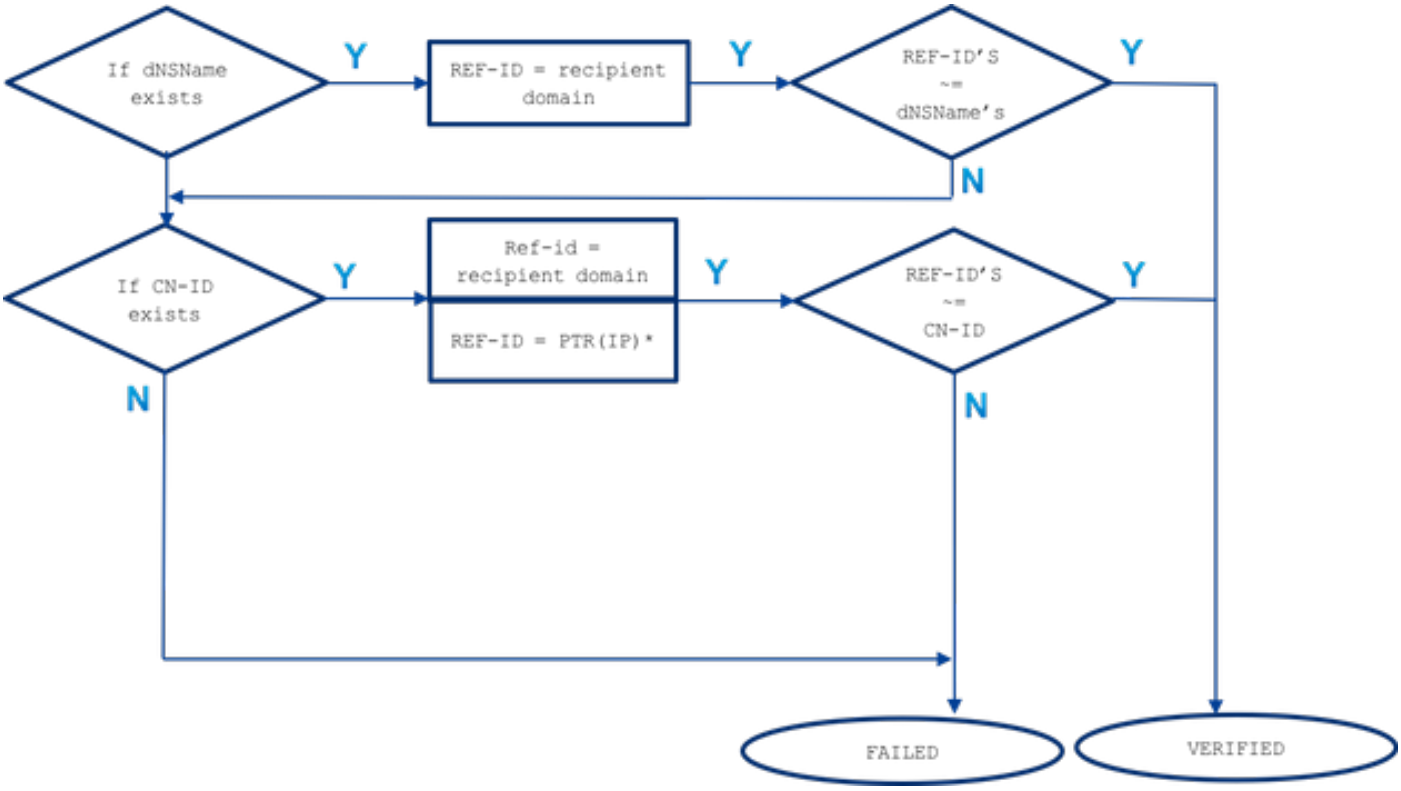
TLS-instellingen	Betekenis
4. Voorkeuren (Verifiëren)	TLS wordt via onderhandelingen gesloten van het e-mailsecurity apparaat naar de MTA(s) voor het domein. Het apparaat probeert het certificaat van de domeinnaam te controleren. Er zijn drie uitkomsten mogelijk: • Het TLS wordt onderhandeld en het certificaat wordt geverifieerd. De post wordt afgeleverd via een versleutelde sessie. • Het TLS wordt onderhandeld, maar het certificaat wordt niet geverifieerd. De post wordt afgeleverd via een versleutelde sessie. • Er wordt geen TLS-verbinding gemaakt en vervolgens wordt het certificaat niet geverifieerd. Het e-mailbericht wordt in onbewerkte tekst verzonden.
5. Vereiste (controle)	TLS wordt via onderhandelingen gesloten van het e-mailsecurity apparaat naar de MTA(s) voor het domein. Verificatie van het domeincertificaat is vereist. Er zijn drie uitkomsten mogelijk: • Er wordt onderhandeld over een TLS-verbinding en het certificaat wordt geverifieerd Het e-mailbericht wordt afgeleverd via een versleutelde sessie. • Er is onderhandeld over een TLS-verbinding, maar het certificaat is niet geverifieerd door een vertrouwde CA. De post is niet afgeleverd. • Een TLS-verbinding is niet onderhandeld. De post is niet afgeleverd.

Het verschil tussen **TLS vereist - Controleer** en **TLS vereist - Controleer de** opties van de **Hosted Domain** in het proces van identiteitscontrole. De wijze waarop de gepresenteerde identiteit wordt verwerkt en het type referentienummers dat mag worden gebruikt, maken een verschil over het eindresultaat. Het doel van onderstaande beschrijving en het gehele document is om dit proces dichter bij de eindgebruiker te brengen. Aangezien een onjuist of onduidelijk begrip van dit onderwerp van invloed kan zijn op het gebruikersnetwerk.

TLS verplicht te controleren

De gepresenteerde identiteit wordt eerst afgeleid van de onderwerpregel AltName - dNSName extensie en indien er geen match of subjectAltName extensie bestaat dan CN-ID - Common Name van het onderwerpveld wordt gecontroleerd.

De lijst met referentie-identiteit (REF-ID) is geconstrueerd vanaf een ontvankelijk domein of een ontvankelijk domein en hostname afgeleid van een PTR DNS-query uitgevoerd tegen het IP-adres waarop de client is aangesloten. Opmerking: In dat specifieke geval worden verschillende referentie - identiteiten vergeleken met de verschillende aangeboden identiteitscontroles.



~= geeft de exacte of wilde kaartovereenkomende waarde weer

De aangeboden identiteit (dNSName of CN-ID) wordt vergeleken met aanvaarde referentie-identiteiten totdat deze is genormaliseerd en in de onderstaande volgorde zijn ze opgenomen.

- Als NSName-extensie van subjectAltName bestaat: de exacte of natuurkaartwedstrijd wordt alleen tegen het ontvangende domein uitgevoerd

  Referentietsidentiteit in het geval van subjectAltName match wordt alleen afgeleid van het ontvangende domein. Als het ontvangende domein geen van de dNSName-items correspondeert, wordt er geen verdere referentie-identiteit gecontroleerd (zoals hostname afgeleid van DNS resolutie MX of PTR)

- Indien GN van onderwerp DN bestaat (GN-ID): de exacte of natuurkaartwedstrijd wordt uitgevoerd tegen het ontvangende domeinDe exacte of wildkaartmatch wordt uitgevoerd tegen hostname afgeleid van PTR query uitgevoerd tegen een IP van de doelserver

  Wanneer het PTR-record een consistentie in DNS tussen expediteur en oplosmiddel heeft bewaard. Wat hier moet worden vermeld, wordt dat GN-veld alleen vergeleken met een hostname uit PTR wanneer er een PTR-record bestaat en een opgelost A record (een expediteur) voor deze hostname (referentie-identiteit) een IP-adres dat overeenkomt met een IP-server waartegen een PTR-query is uitgevoerd.

  A(PTR(IP)) = IP

  Referentie-identiteit in het geval van CN-ID wordt afgeleid van het ontvangende domein en wanneer er geen match is, wordt een DNS-query uitgevoerd tegen een PTR-record van bestemming IP om een hostname te krijgen. Als een PTR bestaat wordt er een extra query uitgevoerd tegen een A record op een hostname afgeleid van een PTR om te bevestigen dat

een DNS consistentie wordt bewaard! Er wordt geen verdere referentie gecontroleerd (zoals hostname afgeleid van MX query)

Samengevat, met de optie "TLS Requirements - verify" is er geen MX hostname in vergelijking met dNSName of CN, dan wordt een DNS PTR RR alleen gecontroleerd voor CN en wordt deze alleen gematcht als de DNS consistentie A(PTR(IP)) = IP bewaard blijft, zowel de exacte als de wilde test voor NSName en CN uitgevoerd wordt.

TLS verplicht te controleren - Hosted domein

De gepresenteerde identiteit is voor het eerst afgeleid van de subjectAltName extensie van type dNSName. Indien de naam van de NSN en een van de aanvaarde referentie-identiteiten (REF-ID) niet met elkaar overeenkomen, geeft de controle geen aanleiding tot het ontbreken van GN in het onderwerpveld en kan zij een verdere identiteitscontrole ondergaan. De van het onderwerpveld afgeleide GN wordt alleen gevalideerd indien het certificaat geen enkele van de onderwerpregel of naam van het type dNSName bevat.

Herinnert u zich dat de voorgestelde identiteit (NSName of CN-ID) wordt vergeleken met aanvaarde referentie-identiteiten totdat deze is genormaliseerd en in de onderstaande volgorde is opgenomen.

- Als NSName-extensie van subjectAltName bestaat:

  Indien er geen verband bestaat tussen de dNSName en één van de aanvaarde hieronder vermelde referentienummers, is validatie mislukt
  de exacte of natuurkaartwedstrijd wordt uitgevoerd tegen het ontvangende domein : Een van de dNSName moet overeenkomen met een ontvanger domeinDe exacte of vervanging van een jokerteken gebeurt tegen expliciet ingestelde hostname met SMTPROUTES (*)De exacte of wildkaartwedstrijd wordt uitgevoerd tegen MX hostname afgeleid van (een onveilige) DNS-query tegen de ontvangende domeinnaam

  Als het ontvangende domein geen expliciet geconfigureerde route voor TCP met FQDN-ingangen heeft en het ontvangende domein niet is afgesloten dan een FQDN-terugkeer door een MX-record van (een onveilig) DNS-query tegen een ontvankelijk domein wordt gebruikt. Als er geen match is, worden geen PTR-records gecontroleerd
- Indien GN van onderwerp DN bestaat (GN-ID):
  De GN wordt alleen gevalideerd indien de naam van de NSN niet in het certificaat voorkomt. De GN-ID wordt vergeleken met de onderstaande lijst van erkende referentie-identiteiten.

  de exacte of natuurkaartwedstrijd wordt uitgevoerd tegen het ontvangende domeinDe exacte of vervanging van een jokerteken gebeurt tegen expliciet ingestelde hostname in SMTPROUTES (*)De exacte of wildkaartwedstrijd wordt uitgevoerd tegen MX hostname afgeleid van (een onveilige) DNS-query tegen de ontvangende domeinnaam

Expliciet geconfigureerd SMTPROUTES

Wanneer de route voor het midden- en kleinbedrijf is ingesteld en de aangeboden identiteit niet overeenkomt met het domein van de e-mail-ontvanger, worden alle namen van de FQDN-routes vergeleken en als ze niet overeenkomen, zijn er geen verdere controles. Met uitdrukkelijk gevormde MX-hostname-routes worden niet vergeleken met een voorgestelde identiteit. De

uitzondering maakt hier een route die werd geplaatst als IP adres.

De volgende regels zijn van toepassing in het geval van uitdrukkelijk gedefinieerde MTP-routes:

- Wanneer er een MTP-route voor een ontvankelijk domein bestaat en het een volledig gekwalificeerde DNS-domeinnaam (FQDN) is, wordt deze als referentie-identiteit beschouwd. Deze hostname (een routenaam) wordt vergeleken met de voorgestelde identiteit die ontvangen is van een certificaat afgeleid van een server waarop het wijst.

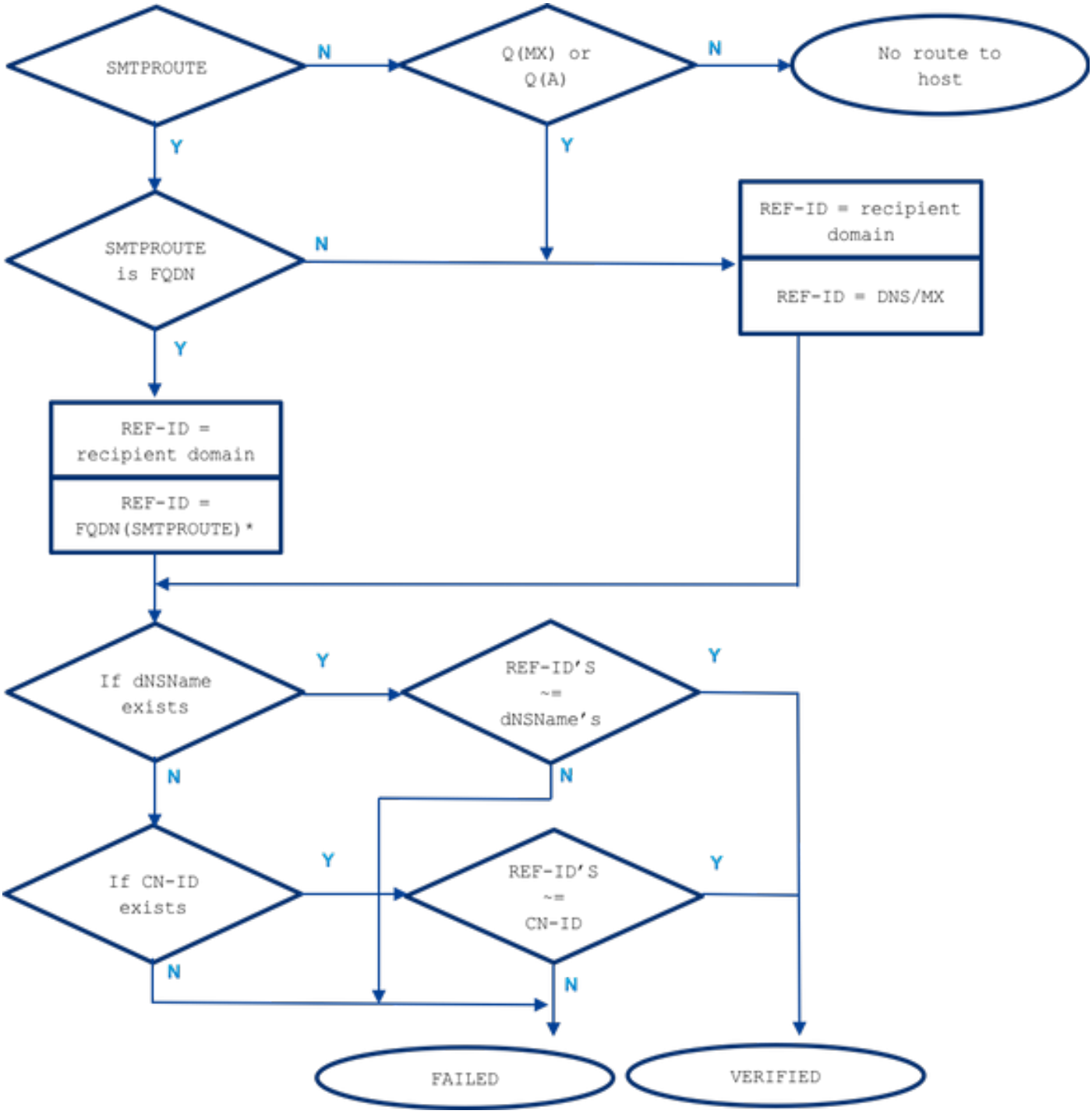
- Meervoudige routes voor een begunstigd domein zijn toegestaan. Als het ontvangende domein meer dan één route in het midden- en kleinbedrijf heeft, worden de routes verwerkt tot de gepresenteerde identificatoren van het certificaat van de server van bestemming overeenkomen met de naam van de route waarop de verbinding werd ingesteld. Als de gastheren op de lijst verschillende prioriteiten hebben worden degenen met het hoogste (0 is het hoogste en standaard) eerst verwerkt. Indien alle routes dezelfde prioriteit hebben, wordt de lijst van routes in de volgorde verwerkt, werden de routes door de gebruiker vastgesteld.

- Indien de gastheer niet reageert (is niet beschikbaar) of reageert, maar de TLS-verificatie heeft gefaald, wordt de volgende host uit de lijst verwerkt. Wanneer de eerste host beschikbaar is en de verificatie doorgeeft, worden de andere niet gebruikt.

- Als meerdere routes naar dezelfde IP adressen oplossen, wordt slechts één verbinding met deze IP gevestigd en moet de voorgestelde identiteit afgeleid van het certificaat dat door de doelserver wordt verzonden één van deze routenaam overeenkomen.

- Als er een MTP-route voor ontvangende domeinen bestaat maar als IP-adres is geconfigureerd, wordt de route nog gebruikt om een verbinding te maken, maar een gepresenteerde identiteit van het certificaat wordt vergeleken met het ontvangende domein en verder met de hostnaam die is afgeleid van het DNS/MX-bronrecord.

Wanneer we het hebben over TLS Benodigd Verifiëren van de optie voor Hosted Domain, is de manier waarop ESA met een doelserver is verbonden van belang voor het proces van TLS-verificatie vanwege de expliciet gedefinieerde MTP-routes die voorzien in een bijkomende referentie-identiteit die in het proces in aanmerking moet worden genomen.



~= geeft de exacte of wilde kaartovereenkomende waarde weer

Voorbeeld

Laten we een voorbeeld nemen uit het echte leven, maar voor het ontvangende domein: voorbeeld.com. Hieronder probeerde ik alle stappen te beschrijven die nodig zijn om de serveridentiteit handmatig te controleren.

Eerst verzamelen we alle benodigde informatie over de ontvanger server.

MX hostname:

```
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
```

Opmerking: de MX-hostnamen en de revDNS-namen komen in dit geval niet overeen

Laten we nu een legitimatiebewijs zien:

IDENTITEIT(EN):

```
$ 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 doelservers hebben hetzelfde certificaat geïnstalleerd. Laten we twee validatieopties bekijken en de verificatieresultaten vergelijken.

Als u **TLS** gebruikt, **dient u te controleren:**

De TLS-sessie wordt vastgesteld met één van de MX-servers en de identiteitsvalidatie begint met het controleren van de gewenste identiteit:

- voorgestelde identiteit: **dNSName bestaat** (blijft vergelijken met de toegestane referentie-identiteit)

  referentie-identiteit = ontvanger domein (**voorbeeld.com**) wordt gecontroleerd en **komt niet overeen met** de **DNSdNSName:*.emailHosted.not, DNS:emailHosted.not**
- voorgestelde identiteit: **GN bestaat** (blijven bestaan met de volgende gepresenteerde identiteit zoals voor de vorige, er was geen match)

  referentie-identiteit = begunstigde domein (**voorbeeld.com)** wordt gecontroleerd en komt **niet**

overeen met de **GN *.e.mailhosted.not**

referentie-identiteit = PTR(IP) : Er wordt een PTR-query uitgevoerd tegen het IP van de server waarop de TLS-client (ESA) een verbinding heeft ingesteld en een certificaat heeft ontvangen, en deze query geeft terug: **mx0a.emailhosted.niet.**

DNS Consistentie wordt gecontroleerd om deze hostname als geldige referentie-identiteit te beschouwen:

```
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
```

De waarde van **mx0a.emailhosted.not.** is vergeleken met GN ***.e-mailhosted.not** en daar **komt** het **overeen.**

De PTR-domeinnaam bevestigt de identiteit en aangezien het certificaat een CA-ondertekend certificaat is, wordt het gehele certificaat geldig en wordt de TLS-sessie vastgesteld.

Als u **TLS** gebruikt **, dient u te controleren of het opgeslagen domein** voor dezelfde ontvanger **is**:

- voorgestelde identiteit : **dNSName bestaat** (dus de GN zal in dat geval niet worden verwerkt) referentie identiteit = ontvanger domein (voorbeeld.com) wordt gecontroleerd en komt niet overeen met de DNS voor dezelfde naam:*.emailHosted.not, DNS:emailHosted.notreferentie-identiteit = FQDN (smtp-route) - er zijn geen protocollen voor dit begunstigde domein

  Aangezien SMTPROUTES niet daarnaast wordt gebruikt:

  referentie-identiteit = MX (ontvanger domein) - er wordt een DNS MX-query uitgevoerd tegen het ontvangende domein
  en retourneert: **mx01.subd.e.mailhosted.not** - dit **komt niet overeen met** de **dNSName DNS:*.e-mailhosted.not, DNS:e-mailHosted.not**
- voorgestelde identiteit : **GN bestaat, maar wordt genegeerd** omdat DNSName ook bestaat.

Aangezien de GN niet wordt geacht te worden verwerkt, is de geldigheid van de TLS-identificatievalidatie in dat geval niet toereikend, evenals de verificatie van de certificaten en kan bijgevolg de verbinding niet worden vastgesteld.

Gerelateerde informatie

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 release-opmerkingS
- Technische ondersteuning en documentatie – Cisco Systems