Cisco Email Security의 TLS 확인 프로세스

목차

소개

Cisco Email Security의 TLS 확인 프로세스

- I - 인증서 검증
- II - 서버 ID 검증

배경

- 1단계
- 2단계

ESA TLS 확인

TLS 필수 확인

TLS 필수 확인 - 호스트된 도메인

- 명시적으로 구성된 SMTPROUTES

예

관련 정보

소개

이 문서에서는 cisco ESA(Email Security Appliance)의 TLS(Transport Layer Security) 서버 ID 확인 프로세스

Cisco Email Security의 TLS 확인 프로세스

TLS 확인 프로세스는 기본적으로 2단계 검증 프로세스입니다.

I - 인증서 검증

여기에는 다음을 확인하는 작업이 포함됩니다.

- 인증서 유효 기간 - 인증서 수명
- 인증서 체인 발급자
- 취소 목록 등

II - 서버 ID 검증

서버 참조 ID에 대한 서버 표시 ID(X.509 공개 키 인증서에 포함)의 검증 프로세스입니다.

배경

RFC 6125에 설명된 ID 이름 용어를 계속 사용하겠습니다.

참고: 제시된 ID는 서버 X.509 공개 키 인증서에서 제시하는 식별자로, 서로 다른 유형의 제시된 식별자가 두 개 이상 포함될 수 있습니다. SMTP 서비스의 경우 dNSName 유형의 subjectAltName 확장명 또는 subject 필드에서 파생된 CN(Common Name)으로 포함됩니다.

참고: 참조 ID는 클라이언트에서 인증서에 애플리케이션 서비스가 있어야 하는 정규화된 DNS 도메인 이름으로 구성된 식별자입니다.

일반적으로 클라이언트가 TLS 세션을 시작하고 클라이언트가 통신을 인증해야 하므로 확인 프로세스는 TLS 클라이언트에 대해 대부분 중요합니다. 이를 위해 클라이언트는 제시된 ID가 참조 ID와 일치하는지 확인해야 합니다. 중요한 부분은 메일 전달을 위한 TLS 검증 프로세스의 보안성이 거의 전적으로 TLS 클라이언트를 기반으로 한다는 것을 이해하는 것이다.

1단계

서버 ID 검증의 첫 번째 단계는 TLS 클라이언트에서 참조 ID를 확인하는 것입니다. TLS 클라이언트가 허용 가능한 것으로 간주하는 참조 식별자 목록이 애플리케이션으로부터 달라집니다. 또한 허용 가능한 참조 식별자의 목록은 서비스에서 제공하는 식별자와 독립적으로 생성되어야 합니다. [rfs6125#6.2.1]

참조 ID는 정규화된 DNS 도메인 이름이어야 하며 어떤 입력에서도 구문 분석할 수 있습니다(클라이언트가 허용하고 안전하다고 간주할 수 있음). 참조 ID는 클라이언트가 연결하려는 DNS 호스트 이름이어야 합니다.

수신자 이메일 도메인 이름은 특정 도메인의 특정 사용자에게 메시지를 보낼 의도로 사용자가 직접 표시하는 참조 ID이며, 이는 사용자가 연결하려는 FQDN에 대한 요구 사항도 충족합니다. SMTP 서버가 동일한 소유자에 의해 소유 및 관리되고 서버가 너무 많은 도메인을 호스팅하지 않는 셀프 호스팅 SMTP 서버의 경우에만 일관성이 있습니다. 각 도메인을 인증서에 나열해야 하므로 (subjectAltName: dNSName 값 중 하나로), 구현 관점에서 볼 때 대부분의 CA(Certificate Authority)는 도메인 이름 값을 25개 이하로 제한합니다(최대 100개). 호스트된 환경에서는 허용되지 않습니다. 대상 SMTP 서버가 수천 개 이상의 도메인을 호스트하는 ESP(Email Service Providers)를 생각해 보겠습니다. 확장성이 없습니다.

명시적으로 구성된 참조 ID가 해답인 것처럼 보이지만, 이는 각 대상 도메인에 대해 소스 도메인에 참조 ID를 수동으로 연결하거나, "사용자가 명시적으로 신뢰를 두고 클라이언트가 상호 인증 및 무결성 검사 모두를 제공하는 연결 또는 연결을 통해 통신하는 타사 도메인 매핑 서비스에서 데이터를 얻는 것"을 필요로 하므로 몇 가지 제약을 부과합니다. [RFC6125#6.2.1]

개념적으로, 이는 컨피그레이션 시 일회성 "보안 MX 쿼리"로 간주될 수 있으며, 그 결과는 실행 상태에서 DNS 보안 침해로부터 보호하도록 MTA에 영구적으로 캐시됩니다. [2]

이렇게 하면 "파트너" 도메인에서만 더 강력한 인증이 제공되지만 매핑되지 않은 일반 도메인에서는 이 인증이 시험에 통과하지 않으며 대상 도메인(예: 호스트 이름 또는 IP 주소 변경)의 컨피그레이션 변경에도 영향을 받지 않습니다.

2단계

프로세스의 다음 단계는 제시된 ID를 확인하는 것입니다. 제시된 ID는 서버 X.509 공개 키 인증서에서 dNSName 유형의 subjectAltName 확장명 또는 주체 필드에 있는 CN(Common Name)으로 제공됩니다. 인증서에 하나 이상의 subjectAltName 항목이 포함된 subjectAltName 확장명이 포함되어 있는 한, 제목 필드가 비어 있을 수 있는 경우

Common Name의 사용은 아직 시행 중이지만 더 이상 사용되지 않는 것으로 간주되며 현재 권장 사항은 subjectAltName 항목을 사용하는 것입니다. 이전 버전과의 호환성을 위해 Common Name에서 ID를 계속 지원합니다. 이 경우 subjectAltName의 dNSName을 먼저 사용해야 하며, 이 이름이 비어 있는 경우에만 Common Name을 선택합니다.

참고: CN에는 정규화된 DNS 도메인 이름과 일치하는 형식의 문자열이 아니라 서비스에 대한 사용자 친화적 문자열이 포함될 수 있으므로 CN은 강력하게 형식화되지 않습니다

두 유형의 ID가 모두 결정된 경우, TLS 클라이언트는 일치를 찾기 위해 제시된 식별자와 각각의 참조 식별자를 비교해야 합니다.

ESA TLS 확인

ESA를 사용하면 특정 도메인에 전달할 때 TLS 및 인증서 확인을 활성화할 수 있습니다(Destination Controls(대상 제어) 페이지 또는 destconfig CLI 명령 사용). TLS 인증서 검증이 필요한 경우 AsyncOS 버전 8.0.2 이후 두 가지 확인 옵션 중 하나를 선택할 수 있습니다. 예상 확인 결과는 구성된 옵션에 따라 달라질 수 있습니다. TLS에 대한 6가지 설정 중에서 대상 제어에서 사용할 수 있는 두 가지 중요한 설정은 인증서 확인을 담당합니다.

1. TLS Required - Verify(TLS 필수 - 확인)
2. TLS Required(TLS 필수) - 호스팅된 도메인을 확인합니다.

```
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]>
```

옵션 (4) Preferred - Verify에 대한 TLS 확인 프로세스는 (5) Required - Verify와 동일하지만, 결과에 따라 수행되는 작업은 아래 표에 나와 있는 것과 다릅니다. 옵션 (6) Required - Verify Hosted

Domains is same (5) Required - Verify 그러나 TLS 확인 흐름은 매우 다릅니다.

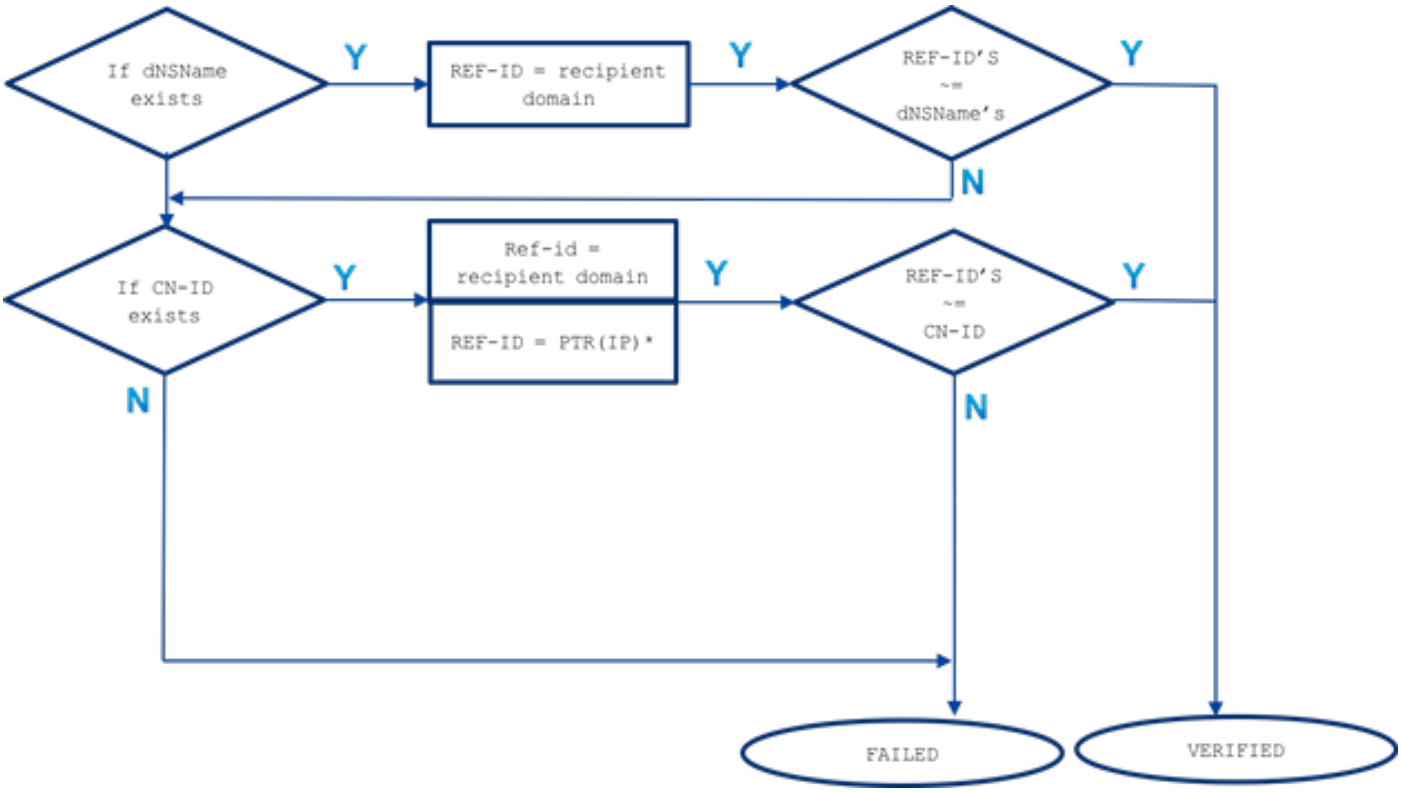
TLS 설정	의미
4. 기본 설정(확인)	TLS는 Email Security Appliance에서 도메인에 대한 MTA로 협상됩니다. 어플라이언스는 도메인 인증서를 확인하려고 시도합니다. 다음과 같은 세 가지 결과를 얻을 수 있습니다. • TLS가 협상되고 인증서가 검증됩니다. 메일은 암호화된 세션을 통해 전달됩니다. • TLS가 협상되지만 인증서는 확인되지 않습니다. 메일은 암호화된 세션을 통해 전달됩니다. • 어떤 TLS 연결도 이루어지지 않으며, 그 후에는 인증서가 검증되지 않습니다. 이메일 메시지는 일반 텍스트로 전달됩니다.
5. 필수(확인)	TLS는 Email Security Appliance에서 도메인에 대한 MTA로 협상됩니다. 도메인 인증서를 확인해야 합니다. 다음과 같은 세 가지 결과를 얻을 수 있습니다. • TLS 연결이 협상되고 인증서가 검증됩니다. 이메일 메시지는 암호화된 세션을 통해 전달됩니다. • TLS 연결이 협상되지만 인증서는 신뢰받는 CA에 의해 검증되지 않습니다. 우편물이 배달되지 않습니다 • TLS 연결은 협상되지 않습니다. 우편물이 배달되지 않습니다

TLS Required - Verify 및 TLS Required - Verify Hosted Domain 옵션 간의 차이는 ID 확인 프로세스에 있습니다. 제시된 ID가 어떻게 처리되는지, 어떤 유형의 참조 식별자가 사용되도록 허용되는지가 최종 결과에 대한 차이를 만든다. 전체 문서와 함께 아래 설명의 목적은 이 프로세스를 최종 사용자에게 더 가까이 다가가는 것입니다. 이 주제에 대한 오해 또는 불명확한 이해는 사용자 네트워크에 보안에 영향을 미칠 수 있습니다.

TLS 필수 확인

제시된 ID는 subjectAltName - dNSName 확장에서 먼저 파생되며, 일치하는 항목이 없거나 subjectAltName 확장명이 CN-ID - Common Name from subject(주체의 CN-ID - 공용 이름) 필드에 없는 경우 선택됩니다.

참조 ID(REF-ID) 목록은 클라이언트가 연결된 IP 주소에 대해 실행된 PTR DNS 쿼리에서 파생된 수신자 도메인 또는 수신자 도메인 및 호스트 이름에서 생성됩니다. 참고: 이 경우 다른 참조 ID를 다른 표시 ID 검사와 비교합니다.



~= 일치 또는 와일드카드 일치 표시

제공된 ID(dNSName 또는 CN-ID)는 매칭될 때까지 그리고 아래에 나열된 순서대로 수락된 참조 ID와 비교됩니다.

- subjectAltName의 dNSName 확장명이 있는 경우:
  - 수신자 도메인에 대해서만 정확한 일치 또는 와일드카드 일치 수행

    subjectAltName 일치의 경우 참조 ID는 수신자 도메인에서만 파생됩니다. 수신자 도메인이 dNSName 항목과 일치하지 않으면 추가 참조 ID가 검사되지 않습니다(예: DNS 확인 MX 또는 PTR에서 파생된 호스트 이름).

- 주체 DN의 CN이 존재하는 경우(CN-ID):
  - 수신자 도메인에 대해 정확한 일치 또는 와일드카드 일치 수행
  - 대상 서버의 IP에 대해 수행된 PTR 쿼리에서 파생된 호스트 이름에 대해 정확한 일치 또는 와일드카드 일치가 수행됩니다

    PTR 레코드가 전달자와 확인자 간의 DNS 일관성을 유지했습니다. 여기서 CN 필드는 PTR 레코드가 존재하고 이 호스트 이름(참조 ID)에 대해 확인된 A 레코드(전달자)가 PTR 쿼리가 수행된 대상 서버 IP와 일치하는 IP 주소를 반환하는 경우에만 PTR의 호스트 이름과 비교됩니다.

    A(PTR(IP)) == IP

    CN-ID의 경우 참조 ID는 수신자 도메인에서 파생되며 일치하는 항목이 없는 경우 호스트 이름을 가져오기 위해 대상 IP의 PTR 레코드에 대해 DNS 쿼리가 수행됩니다. PTR이 있는 경우 PTR에서 파생된 호스트 이름의 A 레코드에 대해 추가 쿼리를 수행하여 DNS 일관성이 유지되는지 확인합니다. 더 이상 참조되지 않음(예: MX 쿼리에서 파생

된 호스트 이름)

요약하면, 'TLS Required - Verify' 옵션을 사용하면 dNSName 또는 CN과 비교한 MX 호스트 이름이 없으므로 DNS PTR RR은 CN에 대해서만 확인되며 DNS 일관성이 유지된 경우에만 확인됩니다. A(PTR(IP)) = IP, dNSName 및 CN에 대해 정확한 테스트와 와일드카드 테스트가 모두 수행됩니다.

TLS 필수 확인 - 호스트된 도메인

제시된 ID는 먼저 dNSName 유형의 subjectAltName 확장에서 파생됩니다. dNSName과 허용된 참조 ID(REF-ID) 중 하나가 일치하지 않으면 주체 필드에 CN이 있는지 여부에 관계없이 확인이 실패하고 추가 ID 확인을 통과할 수 있습니다. 주체 필드에서 파생된 CN은 인증서에 dNSName 유형의 subjectAltName 확장이 포함되어 있지 않은 경우에만 검증됩니다.

제시된 ID(dNSName 또는 CN-ID)가 매칭될 때까지 그리고 아래에 나열된 순서대로 수락된 참조 ID와 비교됩니다.

- subjectAltName의 dNSName 확장명이 있는 경우:

  dNSName과 아래에 나열된 수락된 참조 ID 중 하나가 일치하지 않으면 ID 검증이 실패합니다

  - 수신자 도메인에 대해 정확한 일치 또는 와일드카드 일치 완료: dNSName 중 하나가 수신자 도메인과 일치해야 합니다.
  - SMTPROUTES(*)를 사용하여 명시적으로 구성된 호스트 이름에 대해 정확한 일치 또는 와일드카드 일치 수행
  - 수신자 도메인 이름에 대해 (안전하지 않은) DNS 쿼리에서 파생된 MX 호스트 이름에 대해 정확한 일치 또는 와일드카드 일치가 수행됩니다

    받는 사람 도메인에 FQDN 항목이 있는 SMTP 경로가 명시적으로 구성되지 않았고 받는 사람 도메인이 받는 사람 도메인에 대한 (안전하지 않은) MX 레코드의 FQDN에 의한 반환보다 일치하지 않는 경우 DNS 쿼리가 사용됩니다. 일치 항목이 없으면 추가 테스트가 수행되지 않으며 PTR 레코드가 검사되지 않습니다
- 주체 DN의 CN이 존재하는 경우(CN-ID):

  CN은 dNSName이 인증서에 없을 때만 검증됩니다. CN-ID는 아래 허용 참조 ID 목록과 비교됩니다.

  - 수신자 도메인에 대해 정확한 일치 또는 와일드카드 일치 수행
  - SMTPROUTES(*)에서 명시적으로 구성된 호스트 이름에 대해 정확한 일치 또는 와일드카드 일치가 수행됩니다
  - 수신자 도메인 이름에 대해 (안전하지 않은) DNS 쿼리에서 파생된 MX 호스트 이름에 대해 정확한 일치 또는 와일드카드 일치가 수행됩니다

명시적으로 구성된 SMTPROUTES

SMTP 경로가 구성되고 제시된 ID가 이메일 수신자 도메인과 일치하지 않으면 모든 FQDN 경로 이름이 비교되며 일치하지 않으면 더 이상 확인하지 않습니다. 명시적으로 구성된 SMTP 경로를 사용하는 경우 MX 호스트 이름은 제공된 ID와 비교되는 것으로 간주되지 않습니다. 여기서는 예외로 IP 주소로 설정된 SMTP 경로를 만듭니다.

명시적으로 구성된 SMTP 경로의 경우 다음 규칙이 적용됩니다.

- SMTP 경로가 수신자 도메인에 대해 존재하고 FQDN(정규화된 DNS 도메인 이름)인 경우 참조 ID로 간주됩니다. 이 호스트 이름(경로 이름)은 자신이 가리키는 대상 서버에서 파생된 인증서에서 받은 제공된 ID와 비교됩니다.

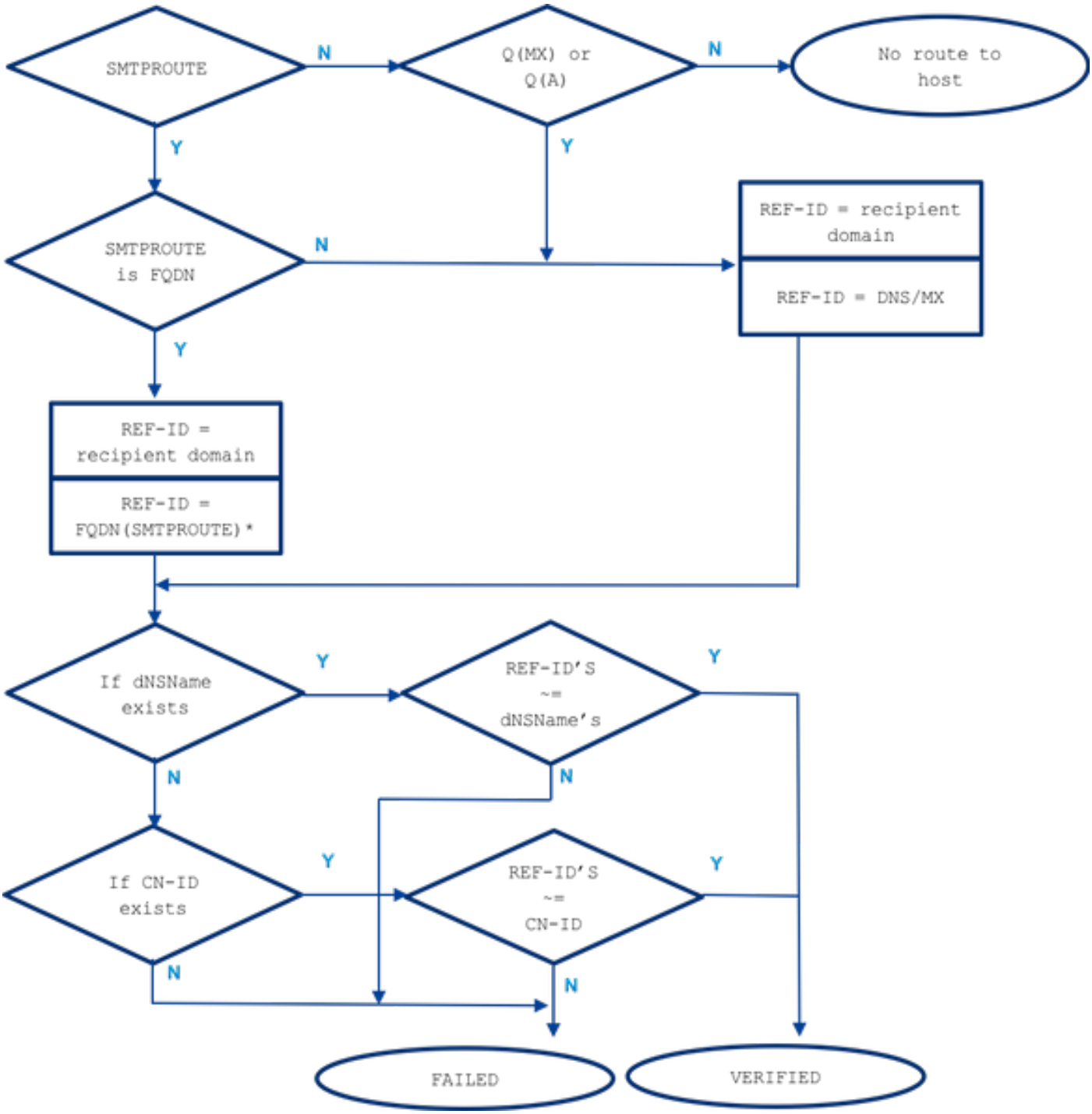
- 수신자 도메인에 대해 여러 경로가 허용됩니다. 수신자 도메인에 둘 이상의 SMTP 경로가 있는 경우, 대상 서버의 인증서에서 제공된 식별자가 연결이 설정된 경로의 이름과 일치할 때까지 경로가 처리됩니다. 목록의 호스트의 우선순위가 서로 다른 경우, 가장 높은 호스트(0이 가장 높은 호스트, 기본값)가 먼저 처리됩니다. 모두 우선순위가 동일한 경우 사용자가 경로를 설정한 순서대로 경로 목록이 처리됩니다.

- 호스트가 응답하지 않거나(사용할 수 없음) 응답하지만 TLS 확인에 실패한 경우 목록의 다음 호스트가 처리됩니다. 첫 번째 호스트가 사용 가능하고 검증을 통과하면 다른 호스트는 사용되지 않습니다.

- 여러 경로가 동일한 IP 주소로 확인되는 경우 이 IP에 대한 하나의 연결만 설정되고 대상 서버에서 보낸 인증서에서 파생된 제공된 ID가 이러한 경로 이름 중 하나와 일치해야 합니다.

- SMTP 경로가 수신자 도메인에 대해 존재하지만 IP 주소로 구성된 경우, 이 경로는 연결에 여전히 사용되지만 인증서의 제시된 ID는 수신자 도메인 및 DNS/MX 리소스 레코드에서 파생된 호스트 이름과 비교됩니다.

호스팅 도메인에 대한 TLS 필수 확인 옵션에 대해 설명할 때, 프로세스에서 고려될 추가 참조 ID를 제공하는 명시적으로 구성된 SMTP 경로 때문에 ESA가 대상 서버에 연결된 방법은 TLS 확인 프로세스에 중요합니다.



~= 일치 또는 와일드카드 일치 표시

예

실제 상황을 예로 들어 보겠습니다. 수신자 도메인: example.com. 아래에서는 서버 ID를 수동으로 확인하는 데 필요한 모든 단계를 설명하려고 했습니다.

먼저 수신자 서버에 대해 필요한 모든 정보를 수집합니다.

MX 호스트 이름:

<#root>

```
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
```

참고: 이 경우 MX 호스트 이름과 revDNS 이름이 일치하지 않습니다

이제 인증서 제공 ID를 가져옵니다.

인증서 ID:

<#root>

```
$ 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

<#root>

```
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

두 대상 서버 모두에 동일한 인증서가 설치되어 있습니다. 두 검증 옵션을 검토하고 검증 결과를 비교해봅시다.
TLS Required Verify를 사용하는 경우:
TLS 세션은 MX 서버 중 하나로 설정되며 ID 검증은 원하는 표시 ID를 확인하는 것으로 시작됩니다.

- 제시된 id: dNSName이 존재합니다(허용되는 참조 id와 계속 비교).
  - reference identity = recipient domain (example.com)(참조 ID = 수신자 도메인 (example.com))이 선택되었으며 dNSName DNS:*.emailhosted.not, DNS:emailhosted.not과 일치하지 않습니다.
- 제시된 id: CN 존재(일치하는 항목이 없었던 이전 id와 마찬가지로 다음 제시된 id 계속)
  - reference identity = recipient domain(example.com)이 확인되었으며 CN *.emailhosted.not과 일치하지 않습니다.
  - 참조 ID = PTR(IP) : PTR 쿼리는 TLS 클라이언트(ESA)가 연결을 설정하고 인증서를 수신한 서버의 IP에 대해 수행되며 이 쿼리는 다음을 반환합니다. mx0a.emailhosted.not.
    - 이 호스트 이름을 유효한 참조 ID로 간주하기 위해 DNS 일관성이 검사됩니다.

      일관성 있음: A(PTR(IP)) = IP

<#root>

```
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.의 값은 CN *.emailhosted.not과 비교되며 여기서 일치합니다.

PTR 도메인 이름은 ID를 검증하며, 인증서가 CA 서명 인증서이므로 전체 인증서를 검증하고 TLS 세션이 설정됩니다.

이 동일한 수신자에 대해 호스팅된 도메인에 대해 TLS Required Verify를 사용하는 경우

- 제시된 id: dNSName이 존재하므로 이 경우 CN이 처리되지 않습니다.
  - reference identity = recipient domain (example.com)(참조 id = 수신자 도메인())을 선택하고
    dNSName DNS:*.emailhosted.not, DNS:emailhosted.not과 일치하지 않습니다.
  - 참조 ID = FQDN(smtp 경로) - 이 받는 사람 도메인에 대한 smtproutes가 없습니다.

    추가로 사용되는 SMTPROUTES가 없으므로:

  - 참조 ID = MX(recipient domain) - DNS MX 쿼리가 수신자 도메인에 대해 수행됩니다.
    반환값: mx01.subd.emailhosted.not - dNSName DNS:*.emailhosted.not,
    DNS:emailhosted.not과 일치하지 않습니다.
- 제시된 id: CN이 존재하지만 dNSName이 존재하므로 건너뜁니다.

CN이 처리되지 않은 것으로 간주되므로 이 경우 TLS ID 검증과 인증서 검증이 실패하고 결과적으로 연결을 설정할 수 없습니다.

관련 정보

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

- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 릴리스 노트초
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.