ESA에서 TLS에 대한 인증서 설정 가이드 만들기

목차

소개

이 문서에서는 TLS와 함께 사용할 인증서를 생성하고, 인바운드/아웃바운드 TLS를 활성화하고, Cisco ESA의 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ESA에서 TLS를 구현하면 암호화를 통해 이메일을 포인트-투-포인트 전송할 수 있는 프라이버시가 제공됩니다. 관리자가 CA(Certificate Authority) 서비스에서 인증서 및 개인 키를 가져오거나 자체 서명 인증서를 사용할 수 있습니다.

Cisco AsyncOS for Email Security는 SMTP(Simple Mail Transfer Protocol)에 대한 STARTTLS 확장(TLS를 통한 *보안 SMTP*)을 지원합니다.

> **팁**: TLS에 대한 자세한 내용은 RFC 3207을 참조하십시오.

> **참고**: 이 문서에서는 ESA에서 중앙 집중식 *관리* 기능을 사용하여 클러스터 레벨에서 인증서를 설치하는 방법에 대해 설명합니다. 인증서는 시스템 레벨에서도 적용할 수 있습니다. 그러나 시스템이 클러스터에서 제거된 후 다시 추가되면 시스템 레벨 인증서가 손실됩니다.

기능 개요 및 요구 사항

관리자는 다음과 같은 이유로 어플라이언스에 자체 서명 인증서를 생성하려고 합니다.

- TLS(인바운드 및 아웃바운드 대화 모두)를 사용하는 다른 MTA와의 SMTP 대화를 암호화하려면
- HTTPS를 통해 GUI에 액세스하기 위해 어플라이언스에서 HTTPS 서비스를 활성화하려면
- LDAP 서버에 클라이언트 인증서가 필요한 경우 LDAP(Lightweight Directory Access Protocol)에 대한 클라이언트 인증서로 사용합니다.
- 어플라이언스와 RSA(Rivest-Shamir-Addleman) Enterprise Manager for Data Loss Protection(DLP) 간 보안 통신을 허용하기 위해
- 어플라이언스와 Cisco AMP(Advanced Malware Protection) Threat Grid Appliance 간의 보안 통신을 허용합니다.

ESA에는 TLS 연결을 설정하는 데 사용할 수 있는 데모 인증서가 미리 구성되어 있습니다.

> **주의**: 데모 인증서는 보안 TLS 연결을 설정하기에 충분하지만, 확인 가능한 연결을 제공할 수 없다는 점에 유의하십시오.

Cisco에서는 CA로부터 X.509 또는 PEM(Privacy Enhanced Email) 인증서를 얻을 것을 권장합니다. 이를 *Apache* 인증서라고도 합니다. 자체 서명 인증서는 앞서 언급한 데모 인증서와 비슷하므로 확인 가능한 연결을 제공할 수 없으므로 CA의 인증서가 자체 서명 인증서보다 우선합니다.

> **참고**: PEM 인증서 형식은 RFC 1421~RFC 1424에서 추가로 정의됩니다. PEM은 공용 인증서(예: Apache 설치 및 CA 인증서 파일/*etc/ssl/certs*) 또는 전체 인증서 체인을 포함하여 공용 키, 개인 키 및 루트 인증서를 포함할 수 있는 컨테이너 형식입니다. 이름 *PEM*은 보안 이메일에 대해 실패한 메소드에서 가져온 것이지만, 사용한 컨테이너 형식은 여전히 활성 상태이며 X.509 ASN.1 키의 base-64 변환입니다.

개인 인증서 가져오기

자체 인증서를 가져오는 옵션은 ESA에서 사용할 수 있지만, 인증서가 PKCS *#12 형식이어야* 합니다. 이 형식에는 개인 키가 포함되어 있습니다. 관리자는 이 형식으로 사용할 수 있는 인증서를 자주 가지고 있지 않습니다. 이러한 이유로 Cisco에서는 ESA에서 인증서를 생성하고 CA에서 올바르게 서명하도록 권장합니다.

현재 인증서 업데이트

이미 존재하는 인증서가 만료된 경우 이 문서의 *Deploying Self-Signed Certificates 섹션*을 건너뛰고 존재하는 인증서를 다시 서명합니다.

> **팁**: 자세한 내용은 Email Security Appliance Cisco 문서에서 인증서 갱신을 참조하십시오.

자체 서명 인증서 구축

이 섹션에서는 자체 서명 인증서 및 CSR(Certificate Signing Request)을 생성하고, 서명을 위해 CA에 자체 서명 인증서를 제공하고, 서명된 인증서를 ESA에 업로드하고, ESA 서비스와 함께 사용할 인증서를 지정하고, 어플라이언스 컨피그레이션 및 인증서를 백업하는 방법에 대해 설명합니다.

자체 서명 인증서 및 CSR 생성

CLI를 통해 자체 서명 인증서를 생성하려면 certconfig 명령**을** 입력합니다.

GUI에서 자체 서명 인증서를 생성하려면

1. 어플라이언스 GUI에서 **Network(네트워크) > Certificates(인증서) > Add Certificate(인증서** 추가)로 이동합니다.
2. Create **Self-Signed Certificate** 드롭다운 **메뉴**를 클릭합니다.

   인증서를 생성할 때 *Common Name*이 수신 인터페이스의 호스트 이름과 일치하는지 또는 전달 인터페이스의 호스트 이름과 일치하는지 확인합니다.
   수신 *인터페이스*는 Network(**네트워크) > Listeners(리스너**)에 구성된 리스너에 **연결되는 인터페이스입니다**.deliveryconfig *명령*을 사용하여 CLI에서 명시적으로 구성하지 않은 경우 전달 인터페이스가 **자동으로** 선택됩니다.
3. 확인 가능한 인바운드 연결의 경우 다음 세 항목이 일치하는지 확인합니다.

MX 레코드(DNS(Domain Name System) 호스트 이름)

공용 이름

인터페이스 호스트 이름

참고: 시스템 호스트 이름은 확인 가능과 관련하여 TLS 연결에 영향을 미치지 않습니다. 시스템 호스트 이름은 어플라이언스 GUI의 오른쪽 상단 모서리에 표시되거나 CLI sethostname 명령 **출력에서** 표시됩니다.

주의: CSR을 **내보내기** 전에 변경 사항을 제출하고 커밋해야 합니다. 이 단계를 완료하지 않으면 새 인증서가 어플라이언스 컨피그레이션에 커밋되지 않으며 CA의 서명된 인증서가 이미 있는 인증서에 서명하거나 적용할 수 없습니다.

CA에 자체 서명 인증서 제공

서명을 위해 CA에 자체 서명된 인증서를 제출하려면

1. CSR을 PEM 형식으로 로컬 컴퓨터에 저장합니다. **Network(네트워크) > Certificates(인증서) > Certificate Name(인증서 이름) > Download Certificate Signing Request(인증서 서명 요청 다운로드)**.

2. 생성된 인증서를 서명을 위해 인식된 CA에 전송합니다.

3. X.509/PEM/Apache 형식의 인증서 및 중간 인증서를 요청합니다.

그런 다음 CA는 PEM 형식의 인증서를 생성합니다.

참고: CA 공급자 목록은 Certificate Authority Wikipedia 문서를 참조하십시오.

ESA에 서명된 인증서 업로드

CA가 개인 키로 서명된 신뢰할 수 있는 공개 인증서를 반환하면 서명된 인증서를 ESA에 업로드합니다.

그런 다음 퍼블릭 또는 프라이빗 리스너, IP 인터페이스 HTTPS 서비스, LDAP 인터페이스 또는 대상 도메인에 대한 모든 아웃바운드 TLS 연결과 함께 인증서를 사용할 수 있습니다.

서명된 인증서를 ESA에 업로드하려면

1. 수신된 신뢰할 수 있는 공개 인증서가 PEM 형식 또는 어플라이언스에 업로드하기 전에 PEM으로 변환할 수 있는 형식을 사용하는지 확인합니다. **팁**: 무료 소프트웨어 프로그램인 OpenSSL 툴킷을 사용하여 형식을 변환할 수 있습니다.
2. 서명된 인증서를 업로드합니다.

Network(네트워크) > Certificates(인증서)로 이동합니다.

서명을 위해 CA로 전송된 인증서의 이름을 클릭합니다.

로컬 컴퓨터 또는 네트워크 볼륨에 있는 파일의 경로를 입력합니다.

참고: 새 인증서를 업로드하면 현재 인증서를 덮어씁니다. 자체 서명 인증서와 관련된 중간 인증서도 업로드할 수 있습니다.

주의: 서명된 **인증서**를 업로드한 후 변경 사항을 제출하고 커밋해야 합니다.

ESA 서비스에 사용할 인증서 지정

이제 인증서가 생성, 서명 및 ESA에 업로드되었으므로 인증서 사용이 필요한 서비스에 사용할 수 있습니다.

인바운드 TLS

인바운드 TLS 서비스에 인증서를 사용하려면 다음 단계를 완료합니다.

1. Network(네트워크) **> Listeners(리스너)로 이동합니다**.
2. 리스너 이름을 클릭합니다.
3. *Certificate* 드롭다운 메뉴에서 인증서 이름을 선택합니다.
4. Submit(제출)**을 클릭합니다**.
5. 필요에 따라 추가 리스너에 대해 1~4단계를 반복합니다.
6. 변경 **사항**을 커밋합니다.

아웃바운드 TLS

아웃바운드 TLS 서비스에 인증서를 사용하려면 다음 단계를 완료하십시오.

1. Mail Policies(**메일 정책) > Destination Controls(대상 제어)로 이동합니다**.
2. Global **Settings(전역 설정) 섹션**에서 Edit *Global Settings...*를 클릭합니다.
3. *Certificate* 드롭다운 메뉴에서 인증서 이름을 선택합니다.
4. Submit(제출)**을 클릭합니다**.
5. 변경 **사항**을 커밋합니다.

HTTPS

HTTPS 서비스에 인증서를 사용하려면 다음 단계를 완료하십시오.

1. **Network(네트워크) > IP Interfaces(IP 인터페이스)로** 이동합니다.
2. 인터페이스 이름을 클릭합니다.
3. HTTPS Certificate 드롭다운 메뉴에서 *인증서* 이름을 선택합니다.
4. Submit(제출)**을 클릭합니다**.
5. 필요에 따라 추가 인터페이스에 대해 1~4단계를 반복합니다.
6. 변경 **사항**을 커밋합니다.

LDAP

LDAP에 인증서를 사용하려면 다음 단계를 완료합니다.

1. **System Administration(시스템 관리) > LDAP로** 이동합니다.
2. LDAP **Global Settings(LDAP 전역 설정) 섹션**에서 Edit *Settings...를* 클릭합니다.
3. *Certificate* 드롭다운 메뉴에서 인증서 이름을 선택합니다.
4. Submit(제출)**을 클릭합니다**.
5. 변경 **사항**을 커밋합니다.

URL 필터링

URL 필터링에 인증서를 사용하려면

1. CLI에 **websecurityconfig** 명령을 입력합니다.
2. 명령 프롬프트를 진행합니다. 이 프롬프트에 도달할 때 **Y**를 선택해야 합니다.

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. 인증서와 연결된 번호를 선택합니다.
4. 컨피그레이션 **변경** 사항을 커밋하려면 commit 명령을 입력합니다.

어플라이언스 컨피그레이션 및 인증서 백업

현재 어플라이언스 컨피그레이션이 저장되었는지 확인합니다. 어플라이언스 컨피그레이션에는 이전에 설명한 프로세스를 통해 적용된 완료된 인증서 작업이 포함되어 있습니다.

어플라이언스 컨피그레이션 파일을 저장하려면 다음 단계를 완료합니다.

1. 보거나 **저장하려면 System Administration(시스템 관리) > Configuration File(컨피그레이션 파**

일) > Download file to local computer(로컬 컴퓨터로 파일 다운로드)로 이동합니다.

2. 인증서 내보내기:

   Network(네트워크) > Certificates(인증서)로 이동합니다.

   Export Certificate(인증서 내보내기)를 클릭합니다.

   내보낼 인증서를 선택합니다.

   인증서의 파일 이름을 입력 합니다.

   인증서 파일의 비밀번호를 입력합니다.

   Export(내보내기)를 클릭합니다.

   파일을 로컬 또는 네트워크 시스템에 저장합니다.

   추가 인증서를 지금 내보낼 수 있습니다. 또는 Network(네트워크) > Certificates(인증서) 위치로 돌아가려면 Cancel(취소)을 클릭합니다.

   참고: 이 프로세스에서는 인증서를 PKCS#12 형식으로 저장합니다. 그러면 비밀번호 보호 기능이 있는 파일이 생성되고 저장됩니다.

인바운드 TLS 활성화

모든 인바운드 세션에 대해 TLS를 활성화하려면 웹 GUI에 연결하고 구성된 인바운드 리스너에 대해 Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책)를 선택한 후 다음 단계를 완료합니다.

1. 정책을 수정해야 하는 리스너를 선택합니다.

2. 정책을 수정하려면 정책의 이름 링크를 클릭합니다.

3. *Security Features*(*보안 기능*) 섹션에서 다음 *암호화 및 인증* 옵션 중 하나를 선택하여 해당 리스너 및 메일 플로우 정책에 필요한 TLS 레벨을 설정합니다.

   꺼짐 - 이 옵션을 선택하면 TLS가 사용되지 않습니다.

   Preferred(기본 설정) - 이 옵션을 선택하면 TLS는 원격 MTA에서 ESA로 협상할 수 있습니다. 그러나 원격 MTA가 협상하지 않으면(*220* 응답 수신 전) SMTP 트랜잭션이 암호화되지 않은 *일반 상태로* 계속됩니다. 인증서가 신뢰할 수 있는 인증 기관에서 시작되었는지 확인하기 위해 시도되지 않습니다. 220 응답을 수신한 후 오류가 발생하면 SMTP 트랜잭션이 일반 텍스트로 돌아가지 않습니다.

   필수 - 이 옵션을 선택하면 원격 MTA에서 ESA로 TLS를 협상할 수 있습니다. 도메인의 인증서를 확인하기 위한 시도가 없습니다. 협상이 실패하면 연결을 통해 이메일이 전송되지 않습니다. 협상이 성공하면 메일은 암호화된 세션을 통해 전달됩니다.

4. Submit(제출)**을 클릭합니다**.

5. Commit Changes(**변경 사항 커밋) 버튼**을 클릭합니다. 원하는 경우 지금 선택 사항인 코멘트를 추가할 수 있습니다.

6. 변경 **사항**을 저장하려면 Commit Changes를 클릭합니다.

리스너에 대한 메일 플로우 정책이 이제 선택한 TLS 설정으로 업데이트됩니다.

선택한 도메인 집합에서 도착한 인바운드 세션에 대해 TLS를 활성화하려면 다음 단계를 완료하십시오.

1. 웹 GUI에 연결하고 **Mail Policies(메일 정책) > HAT Overview(HAT 개요)를** 선택합니다.

2. 적절한 발신자 그룹에 발신자 IP/FQDN을 추가합니다.

3. 이전 단계에서 수정한 발신자 그룹과 연결된 메일 플로우 정책의 TLS 설정을 수정합니다.

4. Submit(제출)**을 클릭합니다**.

5. Commit Changes(**변경 사항 커밋) 버튼**을 클릭합니다. 원하는 경우 지금 선택 사항인 코멘트를 추가할 수 있습니다.

6. 변경 **사항**을 저장하려면 Commit Changes를 클릭합니다.

이제 발신자 그룹에 대한 메일 플로우 정책이 선택한 TLS 설정으로 업데이트됩니다.

> **팁**: ESA에서 TLS 검증을 처리하는 방법에 대한 자세한 내용은 이 문서를 참조하십시오. ESA에서 인증서 검증을 위한 알고리즘은 무엇입니까?

아웃바운드 TLS 활성화

아웃바운드 세션에 대해 TLS를 활성화하려면 웹 GUI에 연결하고 **Mail Policies(메일 정책) > Destination Controls(대상 제어)**를 선택한 다음 다음 다음 단계를 완료합니다.

1. 대상 **추가...를 클릭합니다.**.

2. 대상 도메인을 추가합니다.

3. TLS *Support(TLS 지원)* 섹션에서 드롭다운 메뉴를 클릭하고 다음 옵션 중 하나를 선택하여 구성할 TLS의 유형을 활성화합니다.

   None(없음) - 이 옵션을 선택하면 인터페이스에서 도메인의 MTA로의 아웃바운드 연결에 대해 TLS가 협상되지 않습니다.

   Preferred(기본 설정) - 이 옵션을 선택하면 ESA 인터페이스에서 도메인에 대한 MTA로 TLS가 협상됩니다. 그러나 TLS 협상이 실패하면(220 응답 수신 전) SMTP 트랜잭션이 *암호화되지 않은 일반 상태로* 계속됩니다. 인증서가 신뢰할 수 있는 CA에서 시작되었는지 확인하기 위해 시도되지 않습니다. 220 응답을 수신한 후 오류가 발생하면 SMTP 트랜잭션이 일반 텍스트로

돌아가지 않습니다.

필수 - 이 옵션을 선택하면 ESA 인터페이스에서 도메인에 대한 MTA로 TLS가 협상됩니다. 도메인의 인증서를 확인하기 위한 시도가 없습니다. 협상이 실패하면 연결을 통해 이메일이 전송되지 않습니다. 협상이 성공하면 메일은 암호화된 세션을 통해 전달됩니다.

Preferred-Verify - 이 옵션을 선택하면 TLS가 ESA에서 도메인에 대한 MTA로 협상되고 어플라이언스에서 도메인 인증서 확인을 시도합니다. 이 경우 다음과 같은 세 가지 결과가 가능합니다.

TLS가 협상되고 인증서가 검증됩니다. 메일은 암호화된 세션을 통해 전달됩니다.

TLS가 협상되지만 인증서는 확인되지 않습니다. 메일은 암호화된 세션을 통해 전달됩니다.

어떤 TLS 연결도 수행되지 않으며 인증서도 확인되지 않습니다. 이메일 메시지는 일반 텍스트로 전달됩니다.**Required-Verify** - 이 옵션을 선택하면 TLS가 ESA에서 도메인에 대한 MTA로 협상되며 도메인 인증서를 확인해야 합니다. 이 경우 다음과 같은 세 가지 결과가 가능합니다.

TLS 연결이 협상되고 인증서가 검증됩니다. 이메일 메시지는 암호화된 세션을 통해 전달됩니다.

TLS 연결이 협상되지만 인증서는 신뢰할 수 있는 CA에 의해 검증되지 않습니다. 우편물이 배달되지 않습니다

TLS 연결은 협상되지 않지만 메일은 전달되지 않습니다.

4. 대상 도메인의 대상 도메인*에* 필요한 *추가* 변경을 수행합니다.

5. Submit(제출)**을 클릭합니다**.

6. Commit Changes(**변경 사항 커밋) 버튼**을 클릭합니다. 원하는 경우 지금 선택 사항인 코멘트를 추가할 수 있습니다.

7. 변경 **사항**을 저장하려면 Commit Changes를 클릭합니다.

ESA 인증서 컨피그레이션 오류 증상

TLS는 자체 서명 인증서와 함께 작동하지만, 발신자가 TLS 확인이 필요한 경우 CA 서명 인증서를 설치해야 합니다.

CA 서명 인증서가 ESA에 설치되었더라도 TLS 확인은 실패할 수 있습니다.

이러한 경우에는 Verify(확인) 섹션의 단계를 통해 인증서를 확인하는 것이 좋습니다.

다음을 확인합니다.

웹 브라우저에서 TLS 확인

CA 서명 인증서를 확인하려면 ESA GUI HTTPS 서비스에 인증서를 적용합니다.

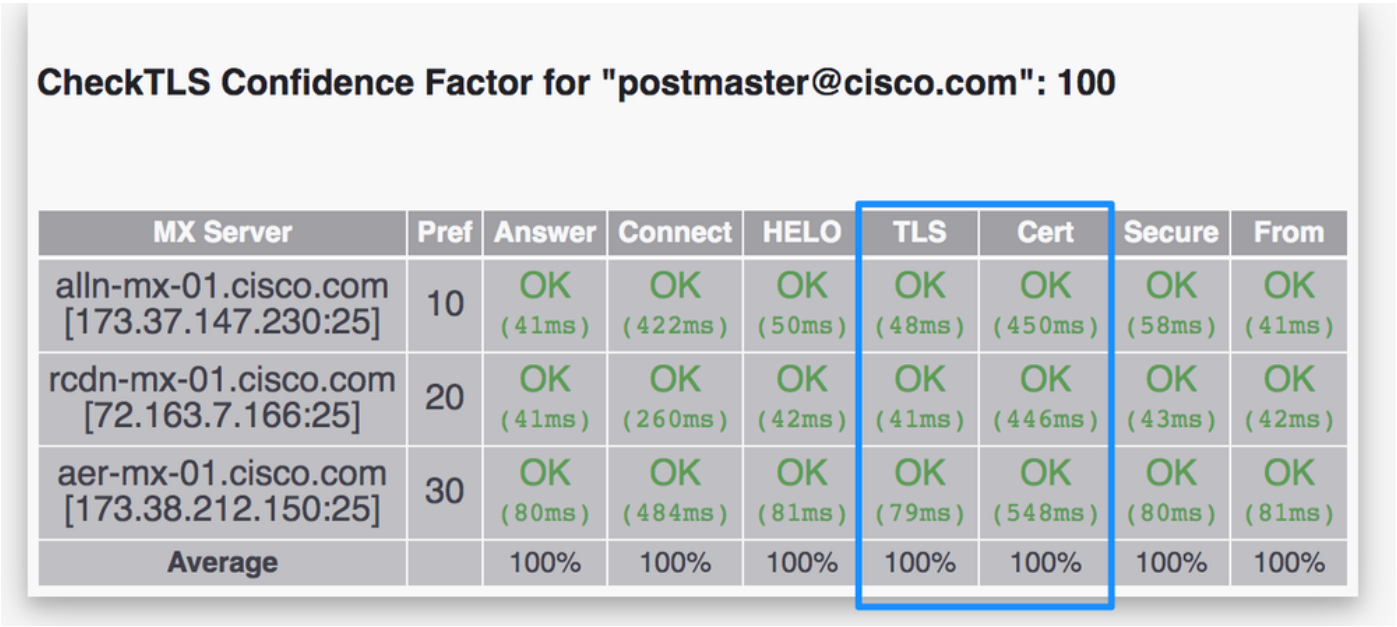
그런 다음 웹 브라우저에서 ESA의 GUI로 이동합니다. https://youresa으로 이동할 때 경고가 있는 경우 중간 인증서가 누락되는 등 인증서가 부적절하게 연쇄된 상태일 수 있습니다.

서드파티 툴을 사용하여 TLS 확인

테스트 전에 어플라이언스가 인바운드 메일을 수신하는 리스너에 테스트할 인증서가 적용되었는지 확인합니다.

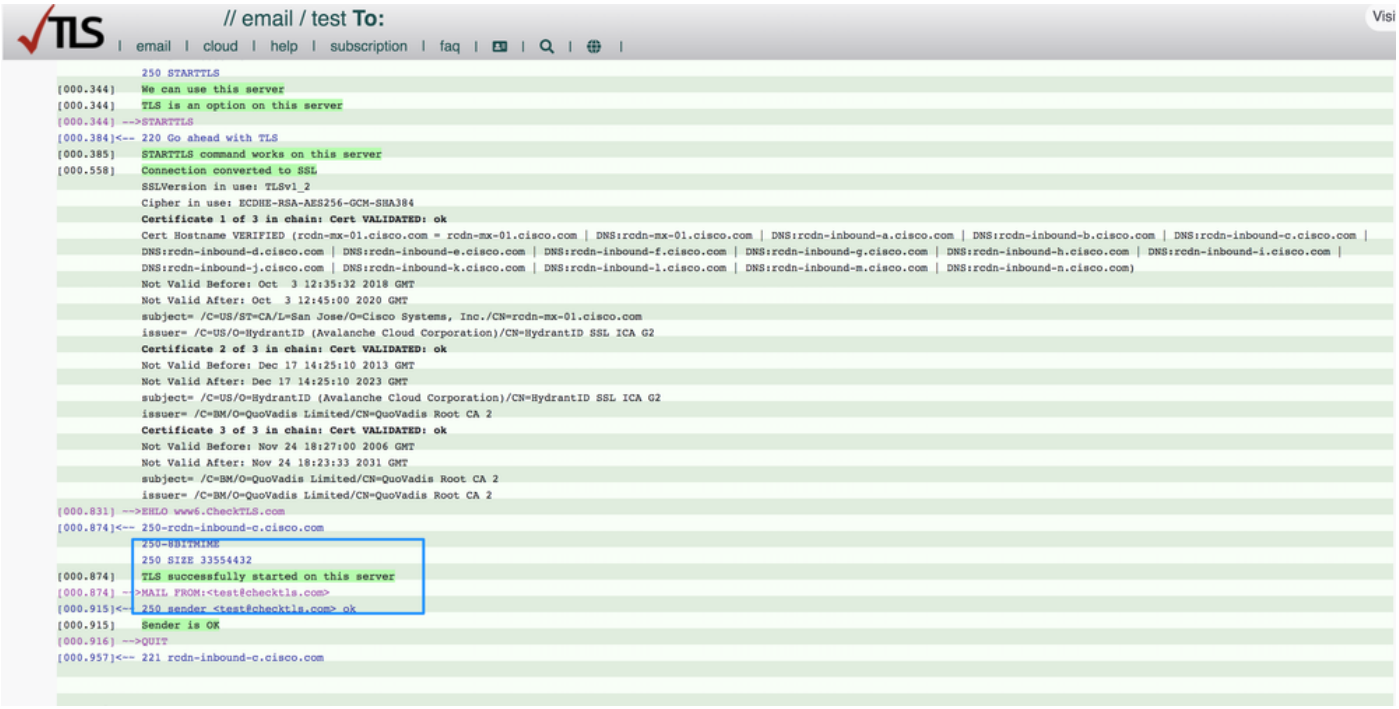
CheckTLS.com 및 SSL-Tools.net과 같은 타사 툴을 사용하여 인증서의 올바른 체인을 확인할 수 있습니다.

TLS-Verify Success에 대한 CheckTLS.com 출력의 예



CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



TLS // email / test To:

email | cloud | help | subscription | faq

```
250 STARTTLS
[000.344]   We can use this server
[000.344]   TLS is an option on this server
[000.344] -->STARTTLS
[000.384]<-- 220 Go ahead with TLS
[000.385]   STARTTLS command works on this server
[000.558]   Connection converted to SSL
            SSLVersion in use: TLSv1_2
            Cipher in use: ECDHE-RSA-AES256-GCM-SHA384
            Certificate 1 of 3 in chain: Cert VALIDATED: ok
            Cert Hostname VERIFIED (rcdn-mx-01.cisco.com = rcdn-mx-01.cisco.com | DNS:rcdn-mx-01.cisco.com | DNS:rcdn-inbound-a.cisco.com | DNS:rcdn-inbound-b.cisco.com | DNS:rcdn-inbound-c.cisco.com |
            DNS:rcdn-inbound-d.cisco.com | DNS:rcdn-inbound-e.cisco.com | DNS:rcdn-inbound-f.cisco.com | DNS:rcdn-inbound-g.cisco.com | DNS:rcdn-inbound-h.cisco.com | DNS:rcdn-inbound-i.cisco.com |
            DNS:rcdn-inbound-j.cisco.com | DNS:rcdn-inbound-k.cisco.com | DNS:rcdn-inbound-l.cisco.com | DNS:rcdn-inbound-m.cisco.com | DNS:rcdn-inbound-n.cisco.com)
            Not Valid Before: Oct  3 12:35:32 2018 GMT
            Not Valid After: Oct  3 12:45:00 2020 GMT
            subject= /C=US/ST=CA/L=San Jose/O=Cisco Systems, Inc./CN=rcdn-mx-01.cisco.com
            issuer= /C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID SSL ICA G2
            Certificate 2 of 3 in chain: Cert VALIDATED: ok
            Not Valid Before: Dec 17 14:25:10 2013 GMT
            Not Valid After: Dec 17 14:25:10 2023 GMT
            subject= /C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID SSL ICA G2
            issuer= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
            Certificate 3 of 3 in chain: Cert VALIDATED: ok
            Not Valid Before: Nov 24 18:27:00 2006 GMT
            Not Valid After: Nov 24 18:23:33 2031 GMT
            subject= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
            issuer= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
[000.831] -->EHLO www6.CheckTLS.com
[000.874]<-- 250-rcdn-inbound-c.cisco.com
            250-8BITMIME
            250 SIZE 33554432
[000.874]   TLS successfully started on this server
[000.874] -->MAIL FROM:<test@checktls.com>
[000.915]<-- 250 sender <test@checktls.com> ok
[000.915]   Sender is OK
[000.916] -->QUIT
[000.957]<-- 221 rcdn-inbound-c.cisco.com
```

TLS-Verify Failure에 대한 CheckTLS.com 출력의 예

TestReceiver

CheckTLS Confidence Factor for "i[redacted]": 90

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
[redacted]	5	OK (121ms)	OK (683ms)	OK (407ms)	OK (236ms)	FAIL	OK (2,122ms)	OK (122ms)	OK (122ms)
[redacted]	5	OK (125ms)	OK (715ms)	OK (130ms)	OK (125ms)	FAIL	OK (1,608ms)	OK (125ms)	OK (127ms)
Average		100%	100%	100%	100%	0%	100%	100%	100%

인증서 호스트 이름이 확인되지 않음(mailC.example.com != gvsvipa006.example.com)
해결

> **참고:** 자체 서명 인증서가 사용 중인 경우 "Cert OK(인증서 확인)" 열의 예상 결과는 "FAIL(실패)"입니다.

CA 서명 인증서가 사용 중이고 TLS-verify가 계속 실패하면 다음 항목이 일치하는지 확인합니다.

- 인증서 일반 이름입니다.
- 호스트 이름(GUI > Network > Interface).
- MX 레코드 호스트 이름: TestReceiver 테이블의 MX Server 열입니다.

CA 서명 인증서가 설치되어 있고 오류가 표시되는 경우 다음 섹션을 계속 진행하여 문제를 해결하는 방법에 대한 자세한 내용을 확인하십시오.

문제 해결

이 섹션에서는 ESA에서 기본 TLS 문제를 해결하는 방법에 대해 설명합니다.

중간 인증서

특히 새 인증서 생성 대신 현재 인증서가 업데이트될 경우 중복 중간 인증서를 찾습니다. 중간 인증서가 변경되었거나 잘못 체인으로 연결되었으며 인증서가 여러 중간 인증서를 업로드했을 수 있습니다. 이로 인해 인증서 체인 및 확인 문제가 발생할 수 있습니다.

필수 TLS 연결 실패에 대한 알림 활성화

TLS 연결이 필요한 도메인에 메시지가 전달될 때 TLS 협상이 실패할 경우 알림을 전송하도록 ESA를 구성할 수 있습니다. 경고 메시지에는 실패한 TLS 협상에 대한 대상 도메인의 이름이 포함되어 있습니다. ESA는 *시스템* 경고 유형에 대한 경고 심각도 레벨 경고를 수신하도록 설정된 모든 수신자에게 경고 메시지를 전송합니다.

> **참고**: 이 설정은 전역 설정이므로 도메인별로 설정할 수 없습니다.

TLS 연결 알림을 활성화하려면 다음 단계를 완료하십시오.

1. Mail Policies(**메일 정책) > Destination Controls(대상 제어)로 이동합니다**.
2. Edit **Global Settings를 클릭합니다**.
3. Send alert when **a required TLS connection fails(필수 TLS 연결 실패 시 알림 전송) 확인란**을 선택합니다.

   팁: destconfig **> setup** CLI 명령을 사용하여 이 **설정을** 구성할 수도 있습니다.

ESA는 도메인에 TLS가 필요하지만 어플라이언스 메일 로그에서는 사용할 수 없는 인스턴스도 기록합니다. 이 문제는 다음 조건 중 하나가 충족될 때 발생합니다.

- 원격 MTA는 ESMTP를 지원하지 않습니다(예: ESA의 EHLO *명령*을 이해하지 못함).
- 원격 MTA는 ESMTP를 지원하지만 STARTTLS *명령*이 EHLO 응답에 광고된 확장 목록에 *있지* 않습니다.
- 원격 MTA에서 STARTTLS *확장*을 광고했지만 ESA에서 STARTTLS 명령을 보낼 때 오류가 *발생하면서* 응답했습니다.

메일 로그에서 성공한 TLS 통신 세션 찾기

TLS 연결은 필터 작업, 안티바이러스 및 안티스팸 판정, 전달 시도 등 메시지와 관련된 다른 중요한 작업과 함께 메일 로그에 기록됩니다. 성공적인 TLS 연결이 있으면 메일 로그에 결과 *TLS 성공* 항목이 있습니다. 마찬가지로 실패한 TLS 연결은 TLS *실패* 항목을 생성합니다. 메시지에 로그 파일에 연결된 TLS 항목이 없는 경우 해당 메시지는 TLS 연결을 통해 전달되지 않았습니다.

팁: 메일 로그를 이해하려면 ESA Message Disposition Determination Cisco 문서를 참조하십시오.

다음은 원격 호스트(수신)에서 성공한 TLS 연결의 예입니다.

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

다음은 원격 호스트(수신)에서 실패한 TLS 연결의 예입니다.

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
```

```
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

다음은 원격 호스트에 대한 성공적인 TLS 연결의 예입니다(전달).

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

다음은 원격 호스트에 대한 실패한 TLS 연결(전달)의 예입니다.

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- Cisco Content Security Management Appliance - 최종 사용자 가이드
- 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.