Secure Email Gateway Outbound MTA-STS 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

개요

- MTA-STS가 SEG를 위해 작동하는 방식

구성

- WebUI 컨피그레이션
- CLI 컨피그레이션

다음을 확인합니다.

문제 해결

관련 정보

소개

이 문서에서는 SEG(Secure Email Gateway) 아웃바운드 메일 전송 에이전트 - MTA-STS(Strict Transport Security)를 구성하는 단계를 설명합니다.

사전 요구 사항

요구 사항

Cisco SEG(Secure Email Gateway) 일반 설정 및 구성에 대한 일반적인 지식

사용되는 구성 요소

이 설정에는 다음이 필요합니다.

- Cisco SEG(Secure Email Gateway) AsyncOS 16.0 이상
- 대상 제어 프로파일.

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.

개요

MTA-STS(Mail Transfer Agent - Strict Transport Security)는 보안 보호 레이어가 추가된 보안 TLS 연결을 사용하도록 시행하는 프로토콜입니다. MTA-STS는 이메일이 암호화된 보안 채널을 통해 전

송되도록 보장하여 중간자(man-in-the-middle) 공격과 도청을 방지합니다.

SEG AsyncOS 16 이상은 수신 도메인을 구성한 MTA-STS에 아웃바운드 MTA-STS 메시지 전달을 수행할 수 있습니다.

활성화된 경우 SEG는 대상 제어 프로필에서 MTA-STS 설정을 확인합니다. SEG는 MTA-STS 프로세스를 시작하여 정의된 레코드와 정책을 가져오고 검증하고 적용하며, 수신 MTA에 대한 연결이 TLSv1.2 이상을 통해 안전한지 확인합니다.

수신 도메인 소유자는 DNS 레코드 및 MTA-STS 정책의 생성, 게시 및 유지 관리를 담당합니다.

MTA-STS가 SEG를 위해 작동하는 방식

- 수신 도메인은 MTA-STS 정책 및 MTA-STS DNS 텍스트 레코드를 유지 관리합니다.
- 전송 도메인 MTA는 목적지 도메인 MTA-STS 정책을 확인하고 작동할 수 있는 MTA-STS여야 합니다.

수신 이메일 도메인 소유자는 DNS를 통해 MTA-STS 텍스트 레코드를 게시합니다(여기에 설명).

- txt 레코드는 HTTPS 지원 웹 서버에서 호스팅되는 MTA-STS 정책을 확인하기 위해 SEG를 트리거합니다.
- 정책은 도메인과 통신하기 위한 매개변수를 지정합니다.
    - 수신할 MTA-STS MX 호스트를 포함합니다.
    - 모드는 테스트 모드 또는 적용 모드로 정의됩니다.
    - TLSv1.2 이상이 필요합니다.

- MTA-STS는 정책 검색을 위해 DNS TXT 레코드를 사용합니다. HTTPS 호스트에서 MTA-STS 정책을 가져옵니다.
- 정책 호스트에서 새 정책 또는 업데이트된 정책을 가져오기 위해 시작된 TLS 핸드셰이크 중에 HTTPS 서버는 "MTA-STS" DNS-ID에 대해 유효한 X.509 인증서를 제공해야 합니다.

이메일 도메인 전송 측면:

- SEG(MTA 전송)가 MTA-STS 도메인으로 이메일을 전송할 때 먼저 수신자 도메인 MTA-STS 정책을 확인합니다.
- 정책이 Enforce Mode(시행 모드)로 구성된 경우 전송 이메일 서버는 수신 이메일 서버(수신 MTA)에 대한 암호화된 보안 연결을 설정하려고 시도합니다. 보안 연결을 설정할 수 없는 경우(예: TLS 인증서가 유효하지 않거나 연결이 안전하지 않은 프로토콜로 다운그레이드된 경우), 이메일은 전달에 실패하고 발신자에게는 실패에 대한 알림이 전송됩니다.

RFC8461

구성

설정 과정에서 예비 작업이 권장됩니다.

1. SEG 대상 제어 프로필을 구성하기 전에 대상 도메인에 MTA-STS DNS 레코드 및 정책 레코드가 올바르게 구성되어 있는지 확인합니다.

- 이는 MTA-STS 검사기 웹 페이지에 액세스하여 가장 효율적으로 수행할 수 있습니다.
  - Google 검색 "MTA-STS 도메인 확인"
  - 검색 결과에서 확인 웹 사이트를 선택합니다.
  - 대상 도메인을 입력합니다.
- 확인 검사가 완료되면 도메인만 구성합니다.

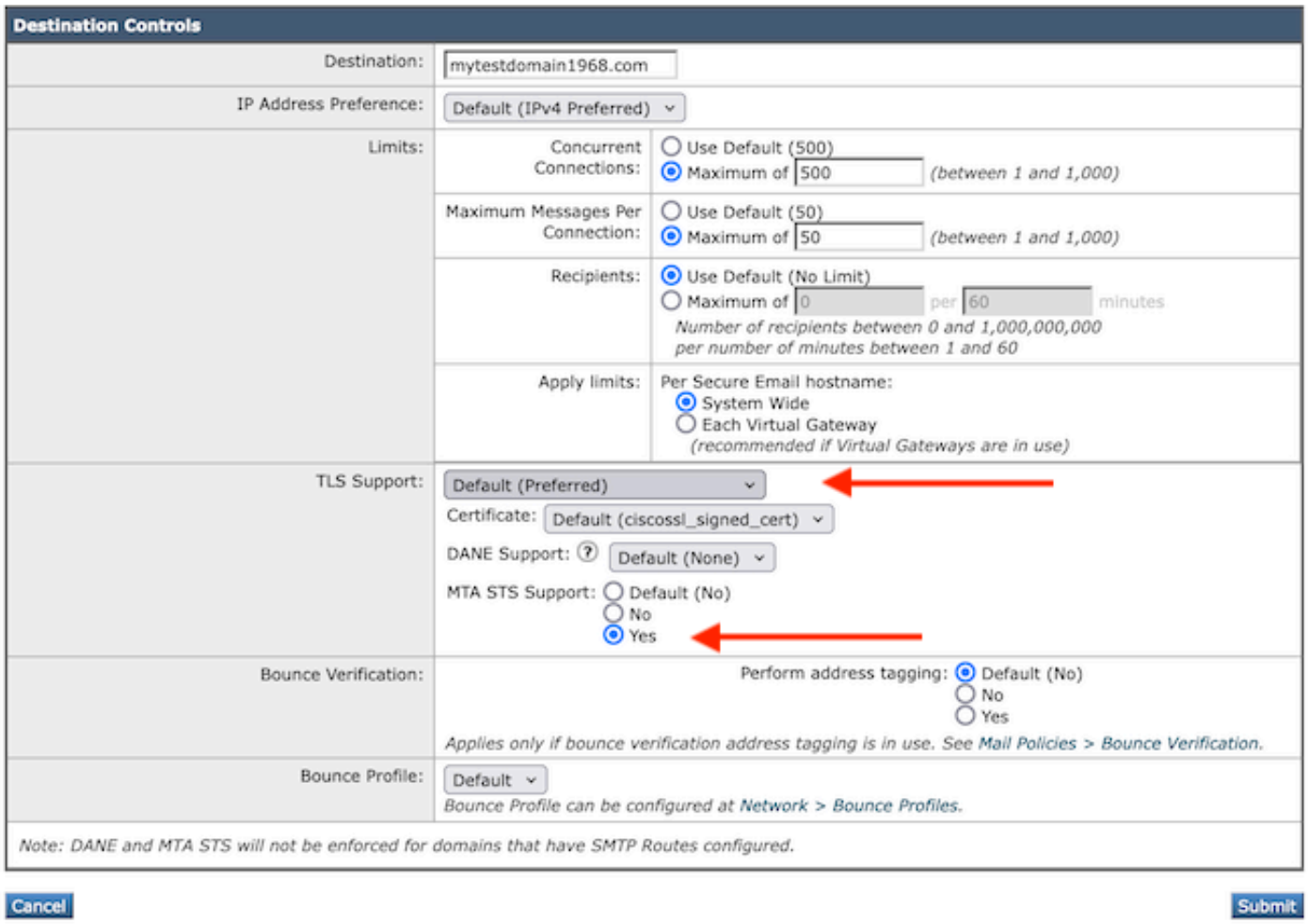
2 . 대상 컨트롤 기본 정책에서 MTA-STS를 사용하지 마십시오.

- MTA-STS를 활용하도록 구성된 각 대상 제어 프로파일은 SEG에 작은 부담을 더합니다. 기본 대상 제어 정책에 MTA-STS가 구성된 경우 도메인을 확인하지 않고 SEG 서비스에 영향을 줄 수 있습니다.

WebUI 컨피그레이션

- Mail Policies(메일 정책) > Destination Controls(대상 제어) 페이지로 이동합니다.
- Add Destination Controls(대상 제어 추가)를 선택하거나 기존 대상 제어 프로필을 수정합니다 .
  - TLS Support(TLS 지원) 설정은 다양한 TLS 지원 옵션을 수용하는 None(없음)을 제외한 모든 설정을 허용합니다.
  - 하위 메뉴 DANE 지원 옵션에는 Mandatory(필수), Opportunistic(기회적) 또는 None(없음)이 포함됩니다.
  - MTA-STS 지원 설정 = 예
- Submit(제출)을 선택한 다음 Commit(커밋)을 선택하여 변경 사항을 적용합니다.

참고: 수신 MTA가 Gsuite 또는 O365와 같은 호스팅 환경에 있는 경우 Destination Controls TLS to TLS Required-Verify Hosted Domains를 구성합니다.



대상 제어 프로필

상호 운용성 주의 사항:

DANE 지원은 MTA STS보다 우선하며 다음과 같은 작업에 영향을 줄 수 있습니다.

- DANE이 성공하면 MTA-STS를 건너뛰고 메일을 전달합니다.
- DANE 필수 항목이 실패하면 메일이 배달되지 않습니다.
- DANE Opportunistic이 실패하고 컨피그레이션 오류로 인해 MTA-STS를 건너뛰면 SEG는 구성된 TLS 설정을 사용하여 전달을 시도합니다.
- SMTP 경로가 도메인에 대해 구성된 경우 MTA-STS가 적용되지 않습니다.

CLI 컨피그레이션

- destconfig
  - 새로 만들기/편집
    - TLS 옵션 메뉴 항목이 표시될 때까지 기본 선택 항목을 입력합니다.
    - TLS용 옵션 2-6은 MTA-STS를 지원합니다.

이 도메인에 대해 특정 TLS 설정을 적용하시겠습니까? [N]> y

TLS 지원을 사용하시겠습니까?
1. 아니요
2. 기본 설정

3. 필수
4. 기본 설정 - 확인
5. 필수 - 확인
6. 필수 - 호스팅된 도메인 확인
[2]>2

TLS를 활성화하도록 선택했습니다. 구성된 유효한 인증서가 있는지 확인하려면 certconfig 명령을 사용하십시오.
DANE 지원을 구성하시겠습니까? [N]>

MTA STS 지원을 구성하시겠습니까? [N]> y

MTA STS 지원을 사용하시겠습니까?
1. 끄기
2. 켜짐
[1]> 2

SMTP 경로가 구성된 도메인에는 MTA STS가 적용되지 않습니다.

1. 나머지 옵션을 완료하여 특정 대상 제어 프로필을 완료합니다.
2. Submit(제출) > Commit(커밋)을 사용하여 변경 사항을 적용합니다.

다음을 확인합니다.

정보 수준 mail_logs:

```
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(mta-test.domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

디버그 수준 mail_logs:

```
Thu Sep 26 15:23:39 2024 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
Thu Sep 26 15:23:39 2024 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131794459543073830L, 0, 'insec
Thu Sep 26 15:23:39 2024 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
Thu Sep 26 15:23:39 2024 Debug: Valid cache entry found for the domain (domain.com).Thu Sep 26 15:23:39
Thu Sep 26 15:23:39 2024 Debug: DNS query: QIP (domain.com,'MX','10.10.5.61',15)
Thu Sep 26 15:23:39 2024 Info: Applying MTA-STS policy for the domain (domain.com)
Thu Sep 26 15:23:40 2024 Info: New SMTP DCID 834833 interface 10.1.1.2 address 10.1.1.3 port 25
Thu Sep 26 15:23:41 2024 Debug: DNS query: Q(domain.com, 'MX')
Thu Sep 26 15:23:41 2024 Info: DCID 834833 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384 s
Thu Sep 26 15:23:41 2024 Info: MTA-STS policy for the domain (domain.com) Successful.
Thu Sep 26 15:23:41 2024 Info: Delivery start DCID 834833 MID 5444 to RID [0]
```

```
Thu Sep 26 15:23:44 2024 Info: Message finished MID 5444 done
```

SEG 지원 TLS v1.3 수신:

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

2024년 9월 24일 화요일 09:13:52 디버그: DNS 쿼리: Q(_mta-sts.domain.com, 'TXT')
2024년 9월 24일 화요일 09:13:52 디버그: DNS 쿼리: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
2024년 9월 24일 화요일 09:13:52 디버그: DNS 쿼리: QIP(_mta-sts.domain.com,'TXT','10.10.5.61',15)
2024년 9월 24일 화요일 09:13:52 디버그: DNS 캡슐화(_mta-sts.domain.com, TXT, [(131366525701580508L, 0, '비보안', ('v=STSv1; id=12345678598Z;',))])
2024년 9월 24일 화요일 09:13:52 정보: 도메인(domain.com)에 대한 MTA-STS TXT 레코드를 가져왔습니다.
2024년 9월 24일 화요일 09:13:52 디버그: 도메인에 대한 MTA-STS 정책 가져오기(domain.com)
2024년 9월 24일 화요일 09:13:52 디버그: 프록시를 통해 MTA-STS 정책 가져오기 요청
2024년 9월 24일 화요일 09:13:52 디버그: 연결 시간 초과로 인해 STS 정책 가져오기 요청이 실패했습니다. 도메인 domain.com
2024년 9월 24일 화요일 09:13:52 정보: 도메인에 대한 MTA-STS 정책을 가져오는 동안 오류가 발생했습니다(domain.com).

2024년 9월 19일 목요일 13:04:50 도메인(domain.com)에 대한 MTA-STS TXT 레코드를 가져왔습니다.
9월 19일 목요일 13:04:50 2024 디버그: 도메인에 대한 MTA-STS 정책 가져오기(domain.com)
9월 19일 목요일 13:04:50 2024 디버그: 프록시를 통해 MTA-STS 정책 가져오기 요청
9월 19일 목요일 13:04:50 2024 디버그: 연결 시간 초과로 인해 STS 정책 가져오기 요청이 실패했습니다. 도메인 domain.com
2024년 9월 19일 목요일 13:04:50 도메인에 대한 MTA-STS 정책을 가져오는 동안 오류가 발생했습니다(domain.com).

2024년 9월 19일 목요일 13:04:50 MID 5411 전달 대기 중

문제 해결

1. SEG가 "peer cert does not match domain.com(피어 인증서가 domain domain.com과 일치하지 않음)" 오류와 함께 전달되지 않는 경우

대상이 G Suite 또는 M365와 같은 호스트된 서비스임을 나타냅니다. 대상 도메인 프로필 TLS 설정 > TLS 필수 - 호스트된 도메인 확인을 변경합니다.

```
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS deferring: verify error: peer cert does not match domain
Tue Sep 24 10:02:52 2024 Info: DCID 831556 TLS was required but could not be successfully negotiated
```

2. 송신 또는 수신 인증서가 제대로 구성되지 않았거나 만료된 경우 통신이 실패합니다.

3. SEG는 인증 기관 목록에 있는 적절한 대상 중간 인증서와 루트 인증서를 확인해야 합니다.

4. SEG cli에서 DNS txt Record를 확인하는 간단한 텔넷 테스트와 정책 웹 서버에 대한 기본 응답 테스트.

- cli에서 DNS 쿼리 > dig _mta-sts.domain.com txt:

;; 응답 섹션:
_mta-sts.domain.com을 참조하십시오. 0은 TXT "v=STSv1; id=12345678598Z;"

- Telnet - cli > telnet mta-sts.domain.com 443에서 기본 웹 서버 연결성을 확인합니다.
- 일반 웹 브라우저를 사용하여 MTA-STS 정책을 봅니다.
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

```
version: STSv1
mode: enforce
mx: *.mail123.domain.com
max_age: 604800
```

관련 정보

- Cisco Secure Email Gateway 시작 페이지 - 지원 가이드

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.