セキュアな電子メールゲートウェイアウトバウンドMTA-STSの設定

内容

はじめに

このドキュメントでは、Secure Email Gateway(SEG)アウトバウンドメール転送エージェント – 厳密なトランスポートセキュリティ(MTA-STS)を設定する手順について説明します。

前提条件

要件

Cisco Secure Email Gateway(SEG)の一般設定および設定に関する一般的な知識。

使用するコンポーネント

この設定には次が必要です。

- Cisco Secure Email Gateway(SEG)AsyncOS 16.0以降
- 宛先制御プロファイル。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

Mail Transfer Agent - Strict Transport Security(MTA-STS)は、追加のセキュア保護レイヤでセキュアTLS接続の使用を強制するプロトコルです。MTA-STSは、暗号化された安全なチャネル経由で電子メールが送信されるようにすることで、中間者攻撃や傍受を防止します。

SEG AsyncOS 16以降では、MTA-STSが設定された受信ドメインへの発信MTA-STSメッセージ配信を実行できます。

有効にすると、SEGは宛先制御プロファイルでMTA-STS設定を確認します。SEGはMTA-STSプロセスを開始して、定義済みのレコードとポリシーを取得、検証、および適用し、受信側MTAへの接続がTLSv1.2以降で安全であることを確認します。

受信ドメインの所有者は、DNSレコードとMTA-STSポリシーを作成、公開、および維持する責任があります。

MTA-STSがSEGで機能する仕組み

- 受信側ドメインは、MTA-STSポリシーおよびMTA-STS DNSテキストレコードを維持します。
- 送信側ドメインMTAは、宛先ドメインMTA-STSポリシーを解決して処理できるMTA-STSである必要があります。

受信電子メールドメインの所有者は、次に示すように、DNS経由でMTA-STSテキストレコードを公開します。

- txtレコードにより、SEGがトリガーされ、HTTPS対応のWebサーバでホストされているMTA-STSポリシーがチェックされます。
- ポリシーは、ドメインとの通信に関するパラメータを指定します。
  - 受信するMTA-STS MXホストが含まれます。
  - モードは、テストモードまたは強制モードとして定義されます
  - TLSv1.2以降が必要です。

- MTA-STSは、ポリシー検出にDNS TXTレコードを使用します。HTTPSホストからMTA-STSポリシーを取得します。
- 新しいポリシーまたは更新されたポリシーをポリシーホストから取得するために開始されるTLSハンドシェイク中、HTTPSサーバは「MTA-STS」DNS-IDの有効なX.509証明書を提示する必要があります。

電子メールドメインの送信の側面：

- SEG（送信側MTA）がMTA-STSドメインに電子メールを送信すると、まず受信者ドメインのMTA-STSポリシーをチェックします。
- ポリシーが強制モードで設定されている場合、送信側の電子メールサーバは、受信側の電子メールサーバ（受信側MTA）へのセキュアで暗号化された接続の確立を試みます。 セキュアな接続を確立できない場合（TLS証明書が無効な場合や、接続がセキュアでないプロトコルにダウングレードされている場合など）、電子メールの配信は失敗し、送信者に障害が通知されます。

RFC8461

設定

セットアップ中に事前処置を行うことを推奨します。

1. SEG宛先制御プロファイルを設定する前に、宛先ドメインに適切に設定されたMTA-STS DNSレコードおよびポリシーレコードがあることを確認します。

- これは、MTA-STSチェッカーWebページにアクセスすることで最も効率的に実行されます。
  - Google検索「MTA-STSドメインの確認」
  - 検索結果から検証Webサイトを選択します。
  - 宛先ドメインを入力します。
- 検証チェックが完了した後にのみ、ドメインを設定します。

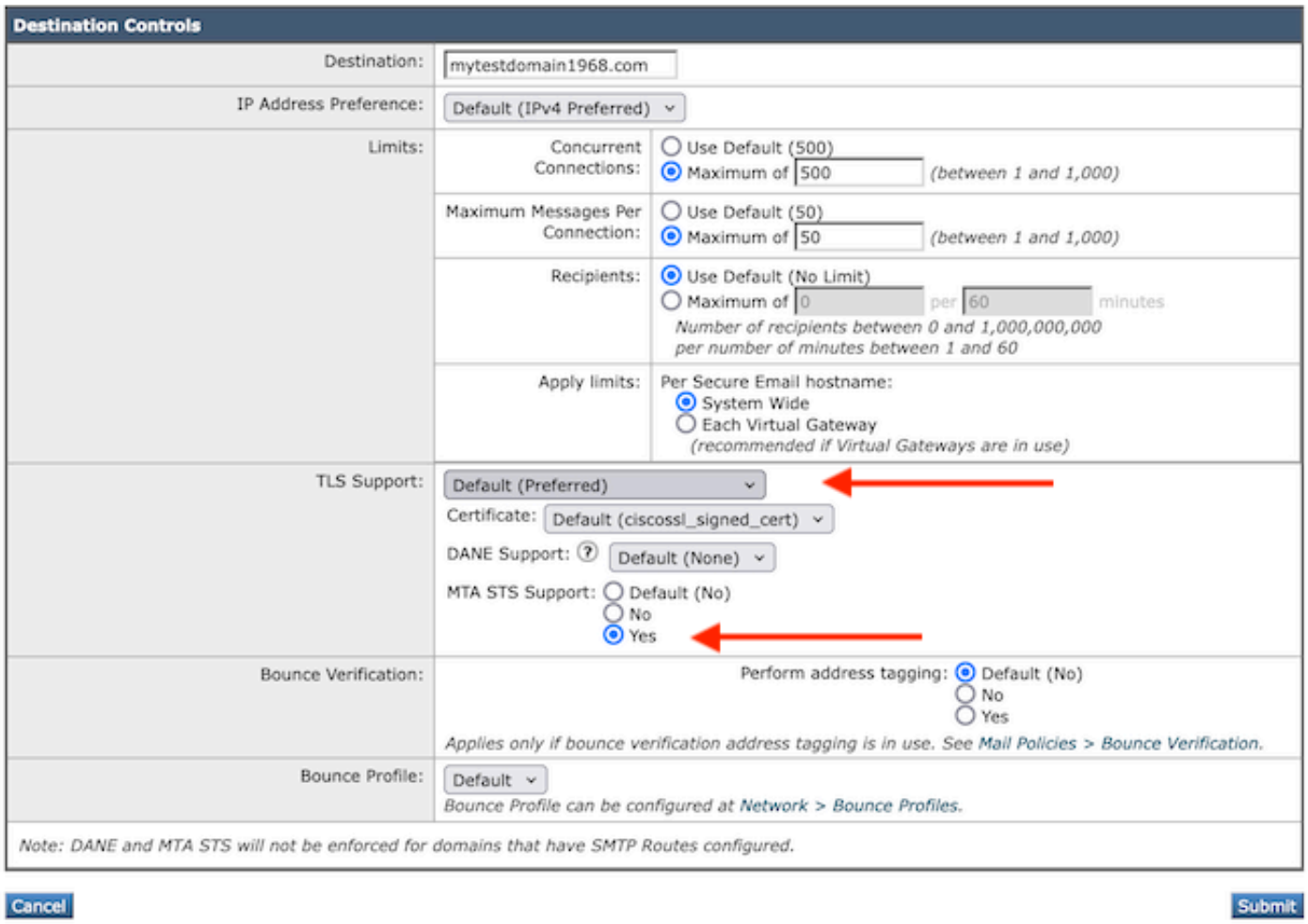
2. 宛先制御のデフォルトポリシーには、MTA-STSを使用しないでください。

- MTA-STSを使用するように設定された各宛先制御プロファイルは、SEGにわずかな負荷を追加します。デフォルトの宛先制御ポリシーにMTA-STSが設定されており、ドメインを確認しない場合、SEGサービスに影響を与える可能性があります。

WebUIの設定

- Mail Policies > Destination Controls Pageの順に移動します。
- Add Destination Controlsを選択するか、既存のDestination Control Profileを編集します。
  - TLS Support設定では、Noneを除くすべての設定が許可され、さまざまなTLSサポートオプションに対応します。
  - サブメニューのDANE Support Optionsには、Mandatory、Opportunistic、またはNoneがあります。
  - MTA-STS Support設定= Yes
- Submitを選択してから、Commitを選択して変更を適用します。

注：受信側MTAがGsuiteやO365などのホストされた環境にある場合は、宛先制御TLSをTLS Required-Verify Hosted Domainsに設定します。



宛先制御プロファイル

相互運用性に関する注意：

DANEサポートはMTA STSよりも優先され、実行されるアクションに影響を与える可能性があります。

- DANEが成功すると、MTA-STSがスキップされ、メールが配信されます。
- DANEの必須が失敗した場合、メールは配信されません。
- DANE Opportunisticが失敗し、設定エラーのためにMTA-STSがスキップされた場合、SEGは設定されたTLS設定を使用して配信を試みます。
- SMTPルートがドメインに設定されている場合、MTA-STSは適用されません。

CLI での設定

- destconfig
  - 新規/編集
    - TLSオプションメニュー項目が表示されるまで、希望する選択肢を入力します。
    - TLSのオプション2 ~ 6はMTA-STSをサポートします。

このドメインに特定のTLS設定を適用しますか？[N]> y

TLSサポートを使用しますか？
1. いいえ

2. 推奨
3. 必須
4. 推奨 – 確認
5. 必須 – 確認
6. 必須 – ホステッドドメインの確認
[2]> 2

TLSを有効にすることを選択しました。certconfigコマンドを使用して、有効な証明書が設定されていることを確認してください。
DANEサポートを設定しますか？[N]>

MTA STSサポートを設定しますか？[N]> y

MTA STSサポートを使用しますか？
1. オフ
2. オン
[1] > 2

SMTPルートが設定されているドメインには、MTA STSは適用されません。

1. 残りのオプションを完了して、特定の宛先制御プロファイルを終了します。
2. Submit > Commitを使用して変更を適用します。

確認

情報レベル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
```

デバッグレベル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でサポートされるTLS v1.3を受信：

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

2024年9月24日（火）09:13:52 Debug: DNS query: Q(_mta-sts.domain.com, 'TXT')
2024年9月24日（火）09:13:52 Debug: DNS query: QN(_mta-sts.domain.com, 'TXT', 'recursive_nameserver0.parent')
2024年9月24日（火）09:13:52 Debug: DNS query: QIP (_mta-sts.domain.com,'TXT','10.10.5.61',15)
2024年9月24日（火）09:13:52 Debug: DNS encache (_mta-sts.domain.com, TXT, [(131366525701580508L, 0, 'insecure', ('v=STSv1; id=12345678598Z;',))])
2024年9月24日（火）09:13:52 Info: Successfully fetched MTA-STS TXT record for domain(domain.com)
2024年9月24日（火）09:13:52 Debug: Fetch MTA-STS policy for the domain(domain.com)
2024年9月24日（火）09:13:52 Debug: Requesting MTA-STS policy fetch via proxy
9月24日（火）09:13:52 2024デバッグ：ドメインdomain.comの接続タイムアウトが原因で、STSポリシーのフェッチ要求が失敗しました。
2024年9月24日（火）09:13:52 Info: Failure encountered while fetching MTA-STS policy for the domain(domain.com)

9月19日（木） 13:04:50 2024情報：ドメインのMTA-STS TXTレコードが正常にフェッチされました(domain.com)
9月19日（木）13:04:50 2024デバッグ：ドメインのMTA-STSポリシーの取得(domain.com)
9月19日（木） 13:04:50 2024デバッグ：プロキシ経由でのMTA-STSポリシーフェッチの要求
9月19日（木） 13:04:50 2024 Debug: Request to fetch STS policy failed due to a connection timeout., for the domain domain.com
2024年9月19日（木） 13:04:50 Info: Failure encountered while fetching MTA-STS policy for the domain(domain.com)

9月19日（木） 13:04:50 2024情報：MID 5411配信キュー

トラブルシュート

1. SEGが配信に失敗し、エラー「peer cert does not match domain domain.com」が表示された場合

これは、宛先がG SuiteやM365などのホステッドサービスであることを示します。Destination Controls Profile TLS setting > TLS Required - Verify Hosted Domainsの順に変更します。

```
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. 送信側または受信側の証明書が正しく設定されていない場合、または証明書の有効期限が切れている場合、通信が失敗します。

3. SEGは、正しい宛先の中間証明書とルート証明書が認証局(CA)リストにあることを確認する必要があります。

4. SEG cliからの単純なTelnetテストによるDNS txtレコードの検証と、ポリシーWebサーバへの基本応答テスト

- cli > dig _mta-sts.domain.com txtからのDNSクエリ：

;；応答セクション：
_mta-sts.domain.comを参照してください。0 IN TXT "v=STSv1; id=12345678598Z;"

- cli > telnet mta-sts.domain.com 443から基本的なWebサーバへの到達可能性を確認するためのTelnet:
- 通常のWebブラウザを使用して、MTA-STSポリシーを表示します。
  - https://mta-sts.domain.com/.well-known/mta-sts.txt

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

関連情報

- サポートガイドへのCisco Secure Email Gatewayの起動ページ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。