セキュアEメールゲートウェイのTLSv1.3の設定

内容

はじめに

このドキュメントでは、Cisco Secure Email Gateway(SEG)のTLS v1.3プロトコルの設定について説明します。

前提条件

SEGの設定と設定に関する一般的な知識が必要です。

使用するコンポーネント

- このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
  - Cisco Secure Email Gateway(SEG)AsyncOS 15.5.1以降。
- SEG SSLの設定値。

"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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください」

概要

SEGはTLS v1.3プロトコルを統合し、SMTPおよびHTTPS関連サービス（Classic UI、NGUI、およびRest API）の通信を暗号化します。

TLS v1.3プロトコルは、業界が標準として機能しているため、より安全な通信とより高速なネゴシエーションを誇っています。

SEGでは、SSLのSEG WebUIまたはCLI内の既存のSSL設定方式を使用しますが、いくつかの重

要な設定が強調表示されます。

- 許可されたプロトコルを設定する際の注意事項。
- 暗号は操作できません。
- TLS v1.3は、GUI HTTPS、受信メール、および送信メール用に設定できます。
- TLS v1.0からTLS v1.3の間のTLSプロトコルのチェックボックス選択オプションでは、この記事で詳しく説明されているパターンを使用します。

設定

SEGはAsycOS 15.5内のHTTPSおよびSMTP用のTLS v1.3プロトコルを統合します。プロトコル設定を選択する際は、HTTPSおよび電子メールの配信/受信の失敗を防ぐために注意が必要です。

Cisco SEGの以前のリリースでは、ハイエンドでTLS v1.2をサポートしており、記事の作成時点でTLS v1.2をサポートしているMS O365などの他の電子メールプロバイダーもサポートしています。

TLS v1.3プロトコルのCisco SEG実装は、3つのデフォルト暗号をサポートします。これらのデフォルト暗号は、他のプロトコルで許可されるSEG暗号設定内では変更または除外できません。

既存のSEG SSL設定では、引き続きTLS v1.0、v1.1、v1.2の操作を暗号スイートに対して実行できます。

TLS 1.3暗号：

TLS_AES_256_GCM_SHA384

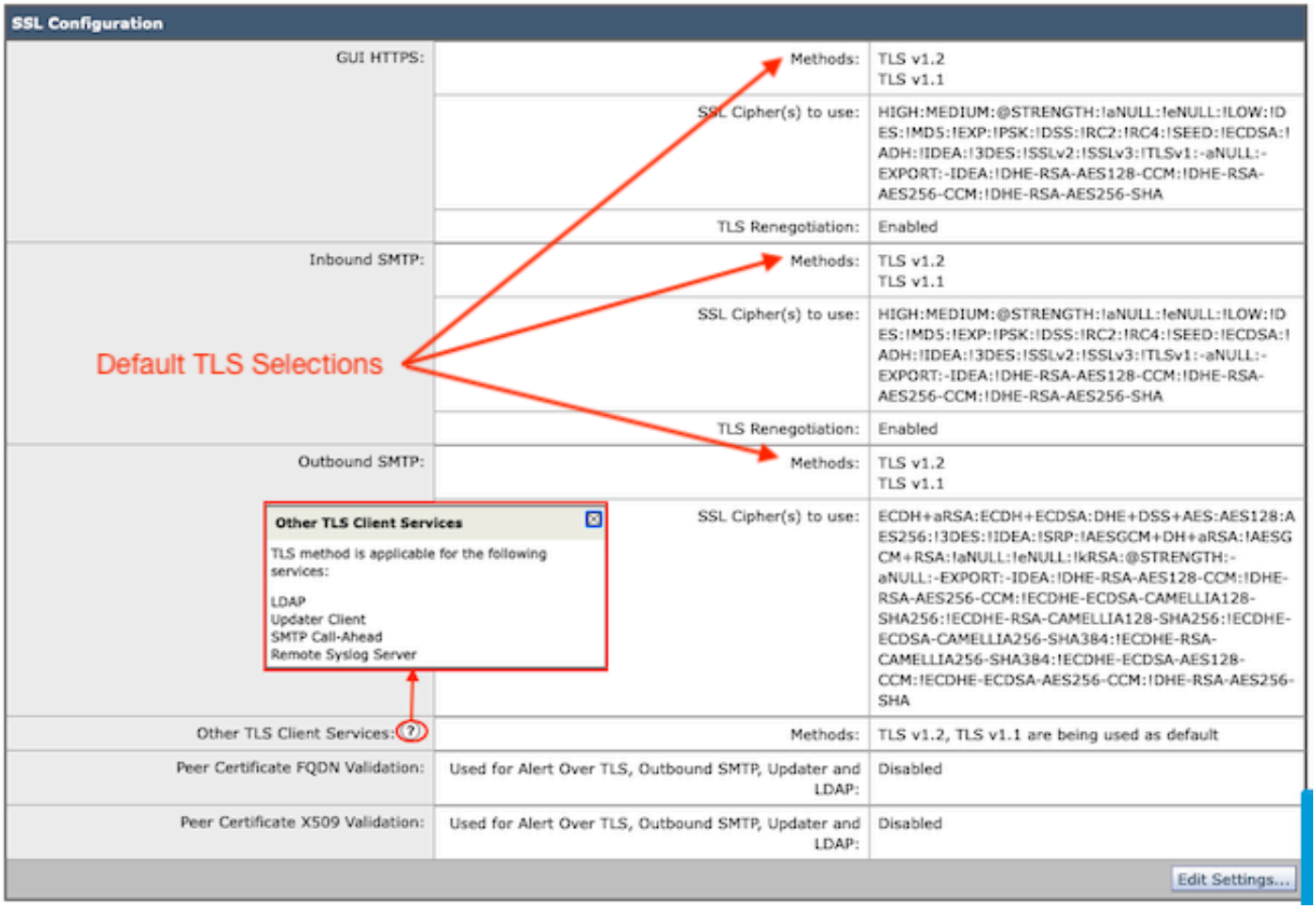
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUIからの設定

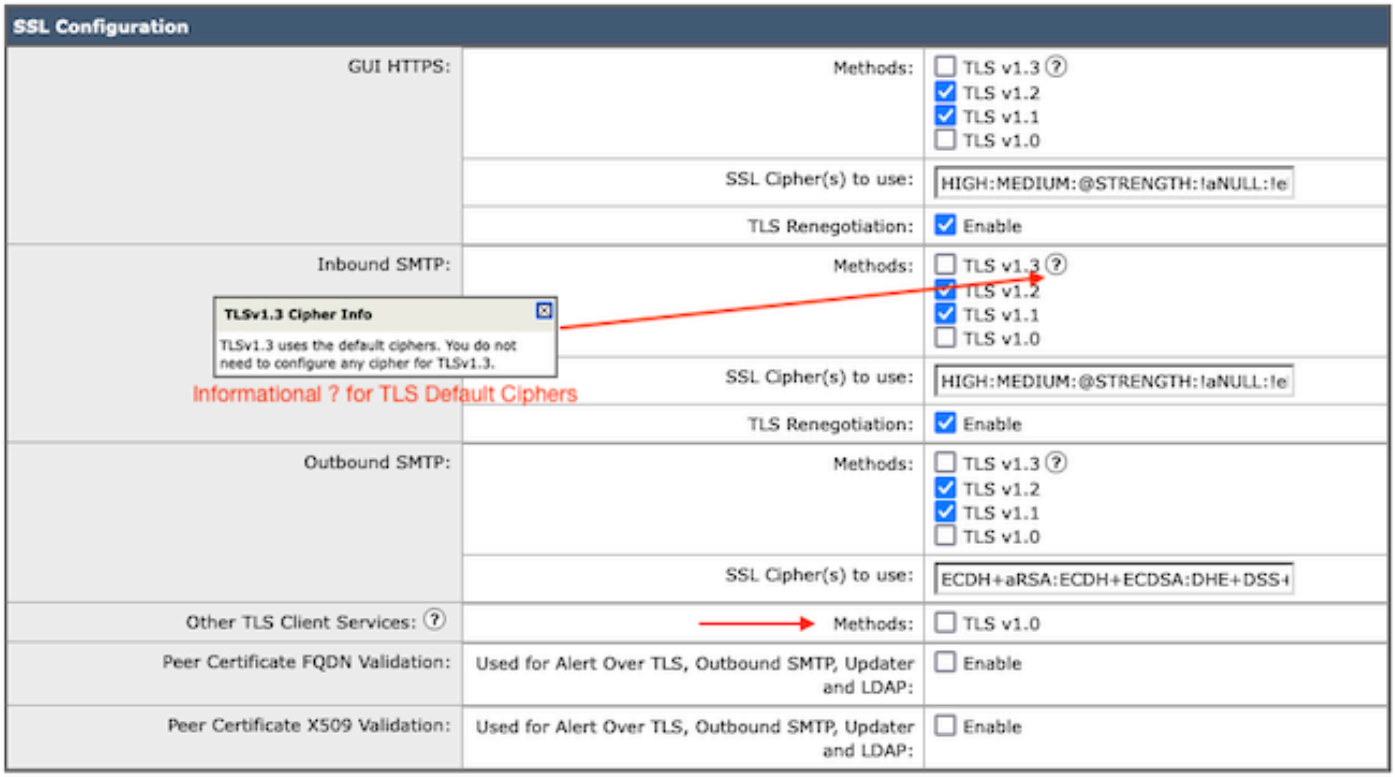
>システム管理> SSL設定に移動します

- 15.5 AsyncOSへのアップグレード後にデフォルトで選択されるTLSプロトコルには、TLS v1.1とTLS v1.2のみが含まれます。
- [その他のTLSクライアントサービス]の設定では、TLS v1.1とTLS v1.2を使用し、オプションで[TLS v1.0のみを使用]を選択します。



「設定の編集」を選択して、構成オプションを表示します。

- TLS v1.1とTLS v1.2は、他のプロトコルを選択するためにアクティブなボックスでチェックされます。
- 各TLS v1.3の横にある？は、スタティック暗号オプションの繰り返しです。
- 「その他のTLSクライアントサービス：」には、選択した場合にのみTLS v1.0を使用するオプションが表示されます。



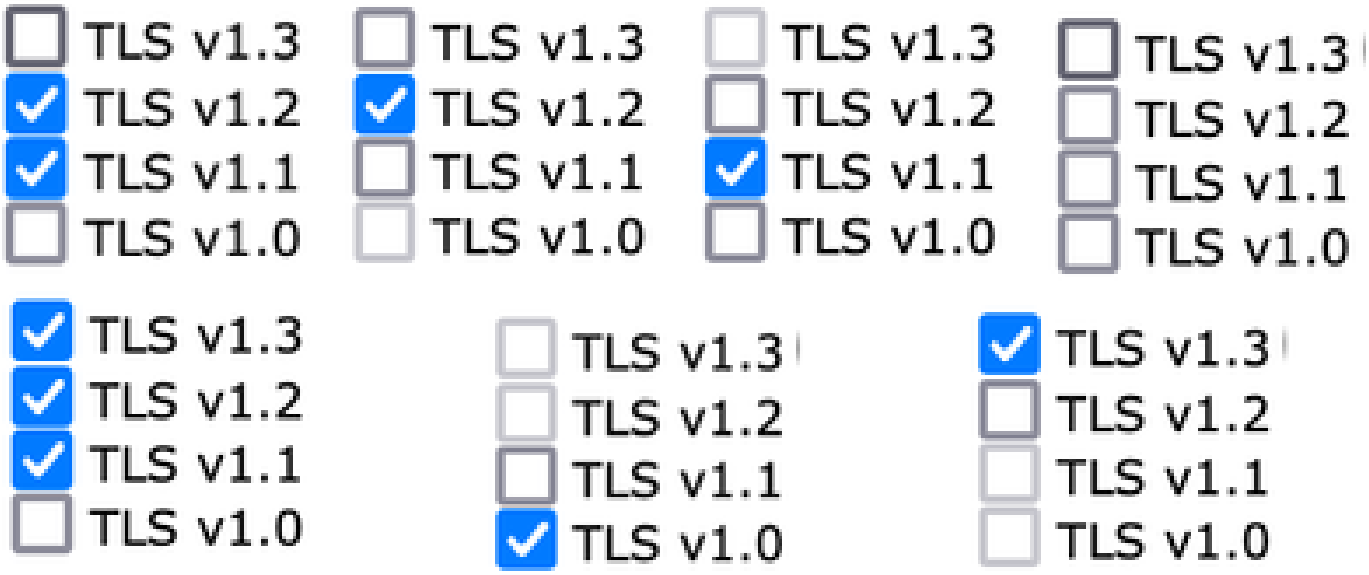
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

TLSプロトコルの選択オプションには、TLS v1.0、TLS v1.1、TLS v1.2、TLS v1.3があります。

- AsyncOS 15.5へのアップグレード後は、TLS v1.1およびTLS v1.2プロトコルのみがデフォルトで選択されます。

注:TLS1.0は非推奨であるため、デフォルトでは無効になっています。所有者が有効にすることを選択した場合、TLS v1.0は引き続き使用できます。

- チェックボックスのオプションは、互換性のないオプションで使用可能なプロトコルを示す太字のボックスとグレー表示のボックスで点灯します。
- 図のオプションの例は、チェックボックスのオプションを示しています。



選択したTLSプロトコルのコミット後のサンプルビュー。

SSL Configuration

GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services:	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled

Edit Settings...

注:GUIのHTTPS TLSプロトコルを変更すると、httpsサービスのリセットにより、WebUIで短い接続解除が発生します。

CLI による設定：

SEGは、次の3つのサービスでTLS v1.3を許可します。

- GUIによるHTTPS
- 受信SMTP
- 送信SMTP

> sslconfigコマンドを実行して、GUI HTTPS、着信SMTP、発信SMTPに対して現在設定されているプロトコルと暗号を出力します。

- GUI HTTPS方式：tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 着信SMTP方式：tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 発信SMTP方式：tlsv1_1tlsv1_2tlsv1_3

実行する操作を選択します。

- GUI:GUIのHTTPS ssl設定を編集します。
- INBOUND：着信SMTP ssl設定を編集します。
- OUTBOUND：発信SMTP ssl設定を編集します。

[]>インバウンド

使用する受信SMTP SSL方式を入力します。

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

注:SEG選択プロセスには、2などの単一のメニュー番号、1 ~ 4などのメニュー番号の範囲、またはカンマ1、2、3で区切られたメニュー番号を含めることができます。

CLI sslconfigの後続のプロンプトでは、「enter」キーを押すか、必要に応じて設定を変更して、既存の値を受け入れます。

コマンド> commit >>必要に応じてオプションのコメントを入力>> Enterキーを押して変更を完了します。

確認

このセクションでは、TLSプロトコルのバージョンの不一致や構文エラーが原因で発生する可能性のある基本的なテストシナリオとエラーについて説明します。

宛先がサポートされていないTLS v1.3が原因で拒否を生成するSEG発信SMTPネゴシエーションのサンプルログエントリ：

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

正常にネゴシエートされたTLS v1.3を受信する送信側SEGのサンプルログエントリ：

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

TLS v1.3が有効になっていない受信SEGのサンプルログエントリ。

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

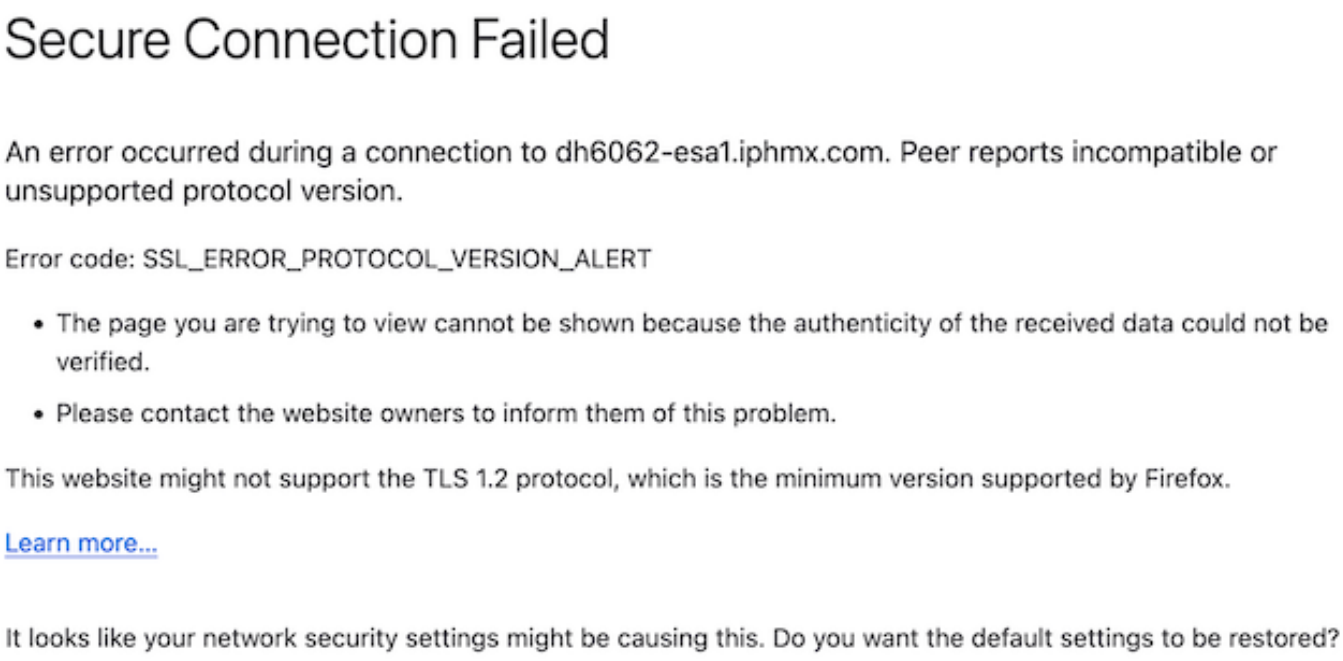
SEGでサポートされるTLS v1.3の受信

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

ブラウザの機能を確認するには、TLSv1.3で設定されたSEG WebUIまたはNGUIへのWebブラウザセッションを開きます。

 注：テストしたすべてのWebブラウザは、TLS v1.3を受け入れるように設定済みです。

- テスト：Firefoxでブラウザ設定を構成し、TLS v1.3サポートを無効にすると、アプライアンスのClassicUIとNGUIの両方でエラーが生成されます。
- Firefoxを使用したクラシックUIで、テストとしてTLS v1.3を除外するように設定されている。
- NGUIは、URL内のポート番号4431（デフォルト）を例外として、同じエラーを受信します。



- 通信を確保するには、TLSv1.3が含まれるようにブラウザの設定を確認します。(このサンプルはFirefoxのもので、番号1 ~ 4を使用します

関連情報

- Cisco Secure Email Gateway – セットアップガイド
- サポートガイドへのCisco Secure Email Gateway起動ページ
- Cisco Secure Email Gateway – リリースノート

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。