ESAおよびCESでのTransport Layer Security(TLS)バージョン1.0の設定

内容

はじめに

このドキュメントでは、Cisco Eメールセキュリティアプライアンス(ESA)とCiscoクラウドEメールセキュリティ(CES)の割り当てでTransport Layer Security(TLSv)バージョン1.0(TLSv1.0)を有効にする方法について説明します。

Cisco ESAおよびCESでTLSv1.0を有効にするにはどうすればよいですか。

注：プロビジョニングされたCisco CES割り当ては、TLSv1.0プロトコルに対する脆弱性の影響により、セキュリティ要件に従ってデフォルトでTLSv1.0が無効になっています。これには、SSLv3共有暗号スイートのすべての使用を削除する暗号文字列が含まれます。

注意:SSL/TLSの方式と暗号は、会社の特定のセキュリティポリシーと設定に基づいて設定されます。 暗号に関するサードパーティの情報については、推奨されるサーバ設定と詳細情報が記載された Mozilla のドキュメント「Security/Server Side TLS」を参照してください。

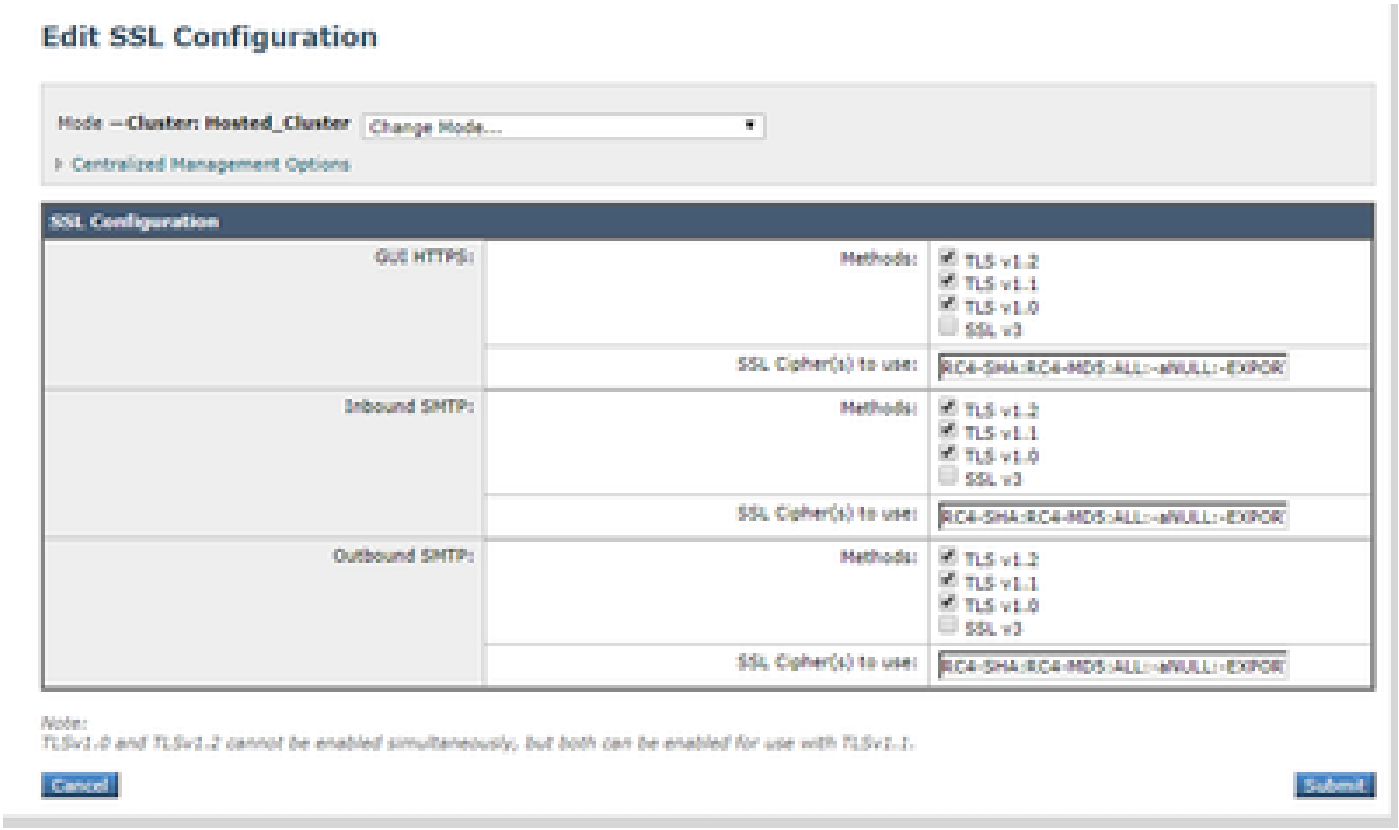
Cisco ESAまたはCESでTLSv1.0を有効にするには、グラフィカルユーザインターフェイス(GUI)またはコマンドラインインターフェイス(CLI)を使用します。

注:CLIでCESにアクセスするには、「クラウドEメールセキュリティ(CES)ソリューションのコマンドラインインターフェイス(CLI)へのアクセス」を参照してください。

グラフィカル ユーザ インターフェイス

1. GUIにログインします。
2. System Administration > SSL Configurationの順に移動します。

3. Edit Settingsを選択します。
4. TLSv1.0ボックスにチェックマークを付けます。重要な点として、TLSv1.2とTLSv1.0の組み合わせでは、ブリッジングプロトコルTLSv1.1も図のように有効にされない限り、TLSv1.2を有効にすることはできません。



コマンドライン インターフェイス

1. sslconfigコマンドを実行します。
2. TLSv1.0を有効にする項目に応じて、コマンドGUIまたはINBOUNDまたはOUTBOUNDを実行します。

```
<#root>

(Cluster Hosted_Cluster)>

sslconfig



sslconfig settings:

GUI HTTPS method: tlsv1_2


GUI HTTPS ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Inbound SMTP method: tlsv1_2
```

```
Inbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Outbound SMTP method: tlsv1_2


Outbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
- CLUSTERSET - Set how ssl settings are configured in a cluster.
- CLUSTERSHOW - Display how ssl settings are configured in a cluster.

[]> INBOUND



Enter the inbound SMTP ssl method you want to use.

1. TLS v1.0



2. TLS v1.1



3. TLS v1.2


4. SSL v2
5. SSL v3

[3]> 1-3



Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT]>
```

暗号

ESAとCESの割り当ては、厳密な暗号スイートで設定できます。TLSv1.0プロトコルを有効にする際は、SSLv3暗号がブロックされないことを確認することが重要です。SSLv3暗号スイートを許可しないと、TLSネゴシエーションが失敗したり、TLS接続が突然クローズされたりする可能性があります。

サンプル暗号文字列：

<#root>

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

!SSLv3:!TLSv1

```
:-aNULL:-EXPORT:-IDEA
```

!SSLv3:に示されているように、この暗号文字列により、ESA/CESではSSLv3暗号でのネゴシエーションが許可されなくなります。これは、ハンドシェイクでプロトコルが要求される際に、ネゴシエーションに使用できる共有暗号がないため、SSLハンドシェイクが失敗することを意味します。

TLSv1.0のサンプル暗号文字列関数を確認するには、置き換えられた暗号文字列に含まれる!SSLv3:!TLSv1:を削除するように変更する必要があります。

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

注:VERIFYコマンドを使用すると、ESA/CES CLIのSSLハンドシェイクで共有される暗号スイートを確認できます。

---

mail_logs/Message Trackingに記録される可能性のあるエラー（次のものに限定されません）

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL routines:SSL23_
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL routines:SSL23_
```

関連情報

- ESA の SSL/TLS で使用される方式と暗号の変更
- SSL 暗号強度の詳細
- ESA での TLS 向けの包括的な設定ガイド
- テクニカル サポートとドキュメント - Cisco Systems

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。