在Cisco ESA和CES上配置傳輸層安全版本1.0

目錄

簡介

本文檔介紹如何在思科郵件安全裝置(ESA)和思科雲郵件安全(CES)分配上啟用傳輸層安全1.0版(TLSv1.0)。

如何在Cisco ESA和CES上啟用TLSv1.0?

> **附註**：由於漏洞對TLSv1.0協定的影響，Cisco CES分配根據安全要求預設禁用TLSv1.0。其中包括用於刪除SSLv3共用密碼套件所有用法的密碼字串。

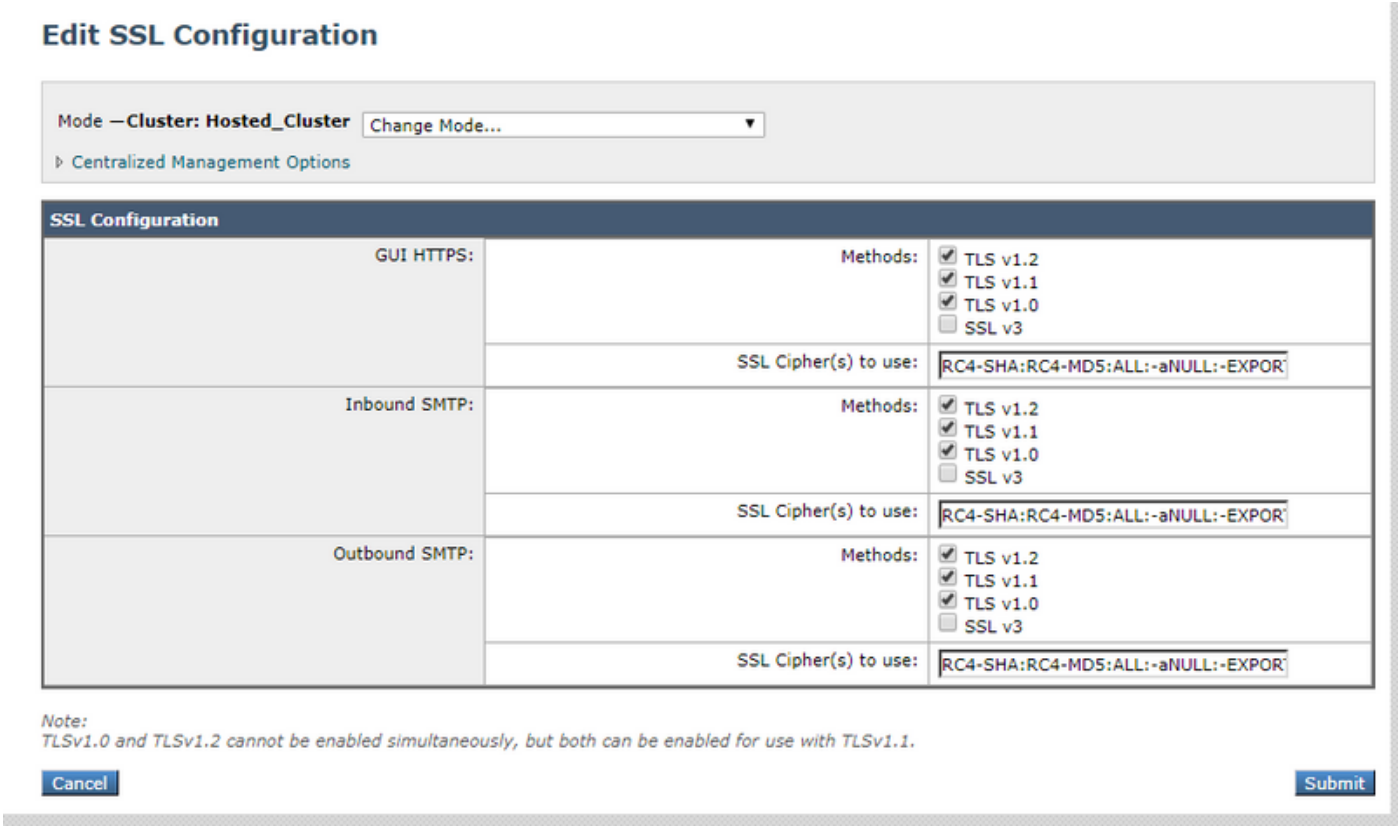
> **注意**：SSL/TLS方法和密碼是根據貴公司的特定安全策略和首選項設定的。有關密碼的第三方資訊，請參閱安全/伺服器端TLS Mozilla文檔，以瞭解建議的伺服器配置和詳細資訊。

為了在Cisco ESA或CES上啟用TLSv1.0，您可以通過圖形使用者介面(GUI)或命令列介面(CLI)來啟用。

> **附註**：要在CLI上訪問您的CES，請檢視：**訪問您的Cloud Email Security(CES)解決方案的命令列介面(CLI)**

圖形使用者介面

1. 登入到GUI。
2. 導覽至**System Administration > SSL Configuration**。
3. 選擇**編輯設定**。
4. 選中**TLSv1.0**框。必須注意的是，TLSv1.2不能與TLSv1.0結合啟用，除非還啟用了橋接協定TLSv1.1，如下圖所示：



命令列介面

1. 執行命令**sslconfig**。
2. 運行命令**GUI**或**INBOUND**或**OUTBOUND**（具體取決於要為以下專案啟用TLSv1.0）：

```
(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]>
```

密碼

ESA和CES分配可以使用嚴格的密碼套件進行配置，在啟用TLSv1.0協定時，確保SSLv3密碼不被阻止非常重要。無法允許SSLv3密碼套件會導致TLS協商失敗或突發TLS連線關閉。

密碼字串示例：

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA
```

此密碼字串阻止ESA/CES允許在SSLv3密碼上協商，如**!SSLv3:**所示，這意味著當在握手中請求協定時，SSL握手會失敗，因為沒有可用於協商的共用密碼。

為了確保使用TLSv1.0的示例密碼字串函式，需要修改它以刪除被替換的密碼字串中出現的**!SSLv3:!TLSv1:**:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:-aNULL:-EXPORT:-IDEA
```

> **附註**：您可以使用**VERIFY**命令在ESA/CES CLI上驗證在SSL握手上共用的密碼套件。

在mail_logs/Message Tracking中記錄的可能錯誤，但不限於：

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL
routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure')
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL
routines:SSL23_GET_SERVER_HELLO:unsupported protocol')
```

相關資訊

- 更改在ESA上與SSL/TLS一起使用的方法和密碼
- SSL密碼強度詳細資訊
- ESA上的TLS綜合設定指南
- 技術支援與文件 - Cisco Systems