為安全電子郵件網關配置TLSv1.3

目錄

簡介

本文檔介紹用於思科安全郵件網關(SEG)的TLS v1.3協定的配置。

必要條件

需要有關SEG設定和配置的一般知識。

採用元件

- 本文中的資訊係根據以下軟體和硬體版本：
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1及更高版本。
- SEG SSL Configuration Settings。

"本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解所有命令的潛在影響。」

概觀

SEG整合了TLS v1.3協定，用於為SMTP和HTTPS相關服務、傳統UI、NGUI和Rest API加密通訊。

TLS v1.3協定具有更高的通訊安全性和更快的協商速度，因為業界正在努力將其作為標準。

SEG使用SSL的SEG WebUI或CLI中的現有SSL Configuration方法，並突出顯示了幾個重要設定。

- 配置允許的協定時提供預防建議。
- 密碼是無法操作的。
- 可以為GUI HTTPS、入站郵件和出站郵件配置TLS v1.3。
- TLS v1.0到TLS v1.3之間的TLS協定覈取方塊選擇選項使用本文中更詳細介紹的模式。

設定

SEG在AsycOS 15.5中整合了用於HTTPS和SMTP的TLS v1.3協定。建議您在選擇協定設定時小心謹慎，以防止HTTPS和電子郵件傳送/接收失敗。

Cisco SEG的早期版本在高端支援TLS v1.2，在撰寫本文時支援TLS v1.2的其他電子郵件提供商也支援TLS O365。

TLS v1.3協定的Cisco SEG實施支援3個預設密碼，這些密碼不能像其他協定允許的那樣在SEG密碼配置設定中更改或排除。

現有的SEG SSL配置設定仍允許將TLS v1.0、v1.1、v1.2操作操作操作用於密碼套件。

TLS 1.3密碼：

TLS_AES_256_GCM_SHA384

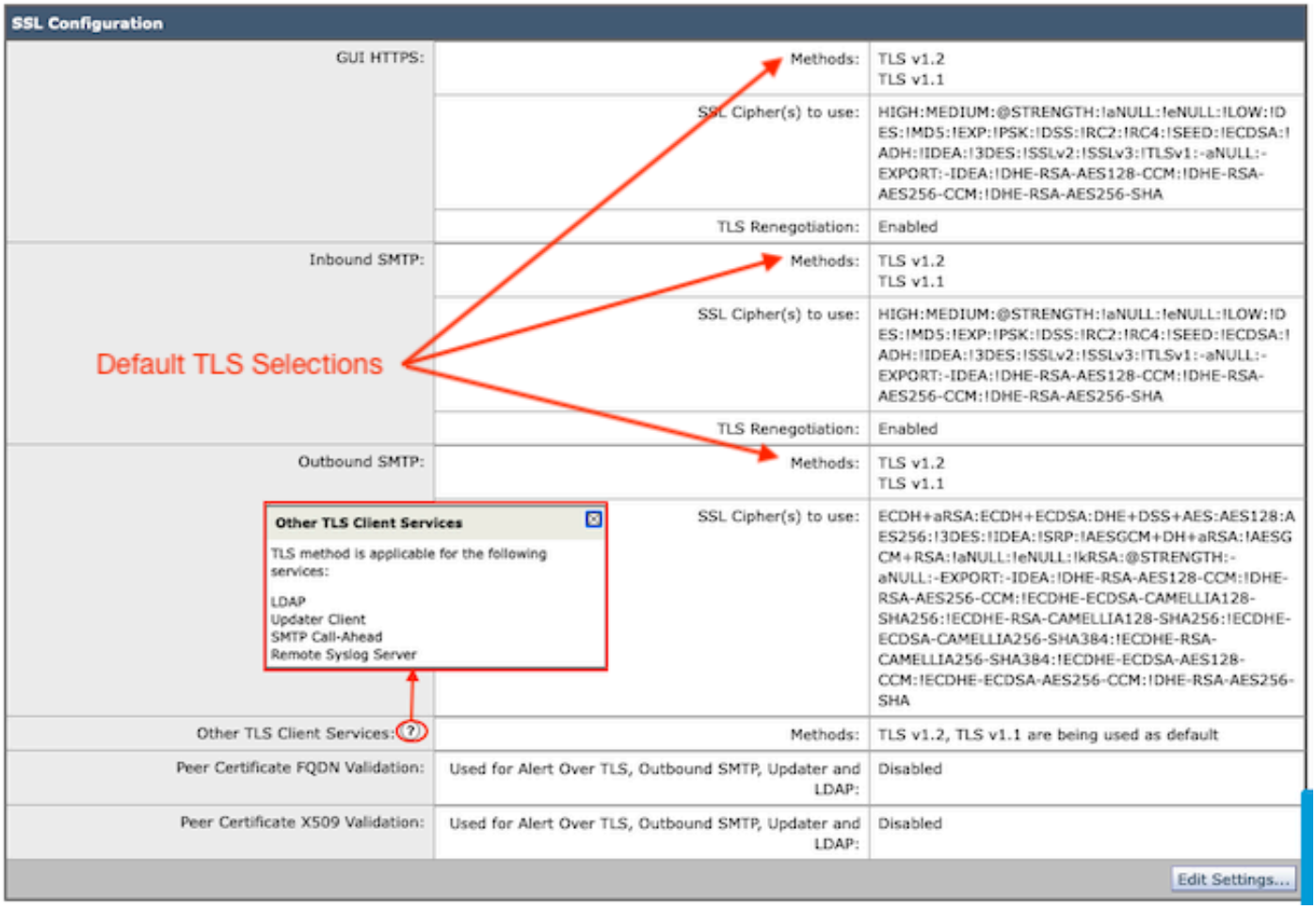
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

從WebUI配置

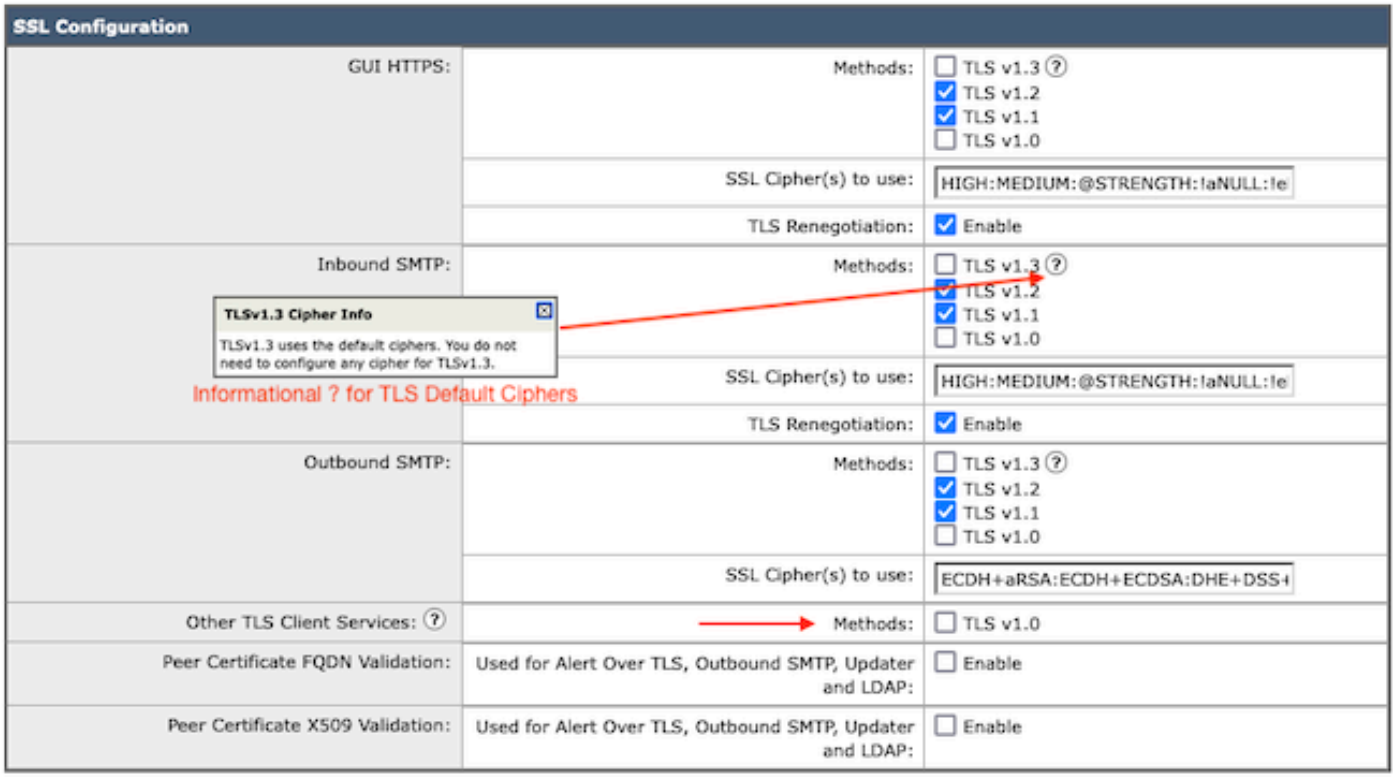
導航至>系統管理> SSL配置

- 升級到15.5 AsyncOS後的預設TLS協定選擇僅包括TLS v1.1和TLS v1.2。
- 「其他TLS客戶端服務」的設定使用TLS v1.1和TLS v1.2以及選擇，僅使用TLS v1.0的選項。



選取「編輯設定」以顯示組態選項。

- TLS v1.1和TLS v1.2已選中，並且選中了活動框以選擇其他協定。
- 每個TLS v1.3旁邊的？是靜態Cipher選項的重複。
- 「其他TLS使用者端服務：」現在會顯示僅在選取時才使用TLS v1.0的選項。



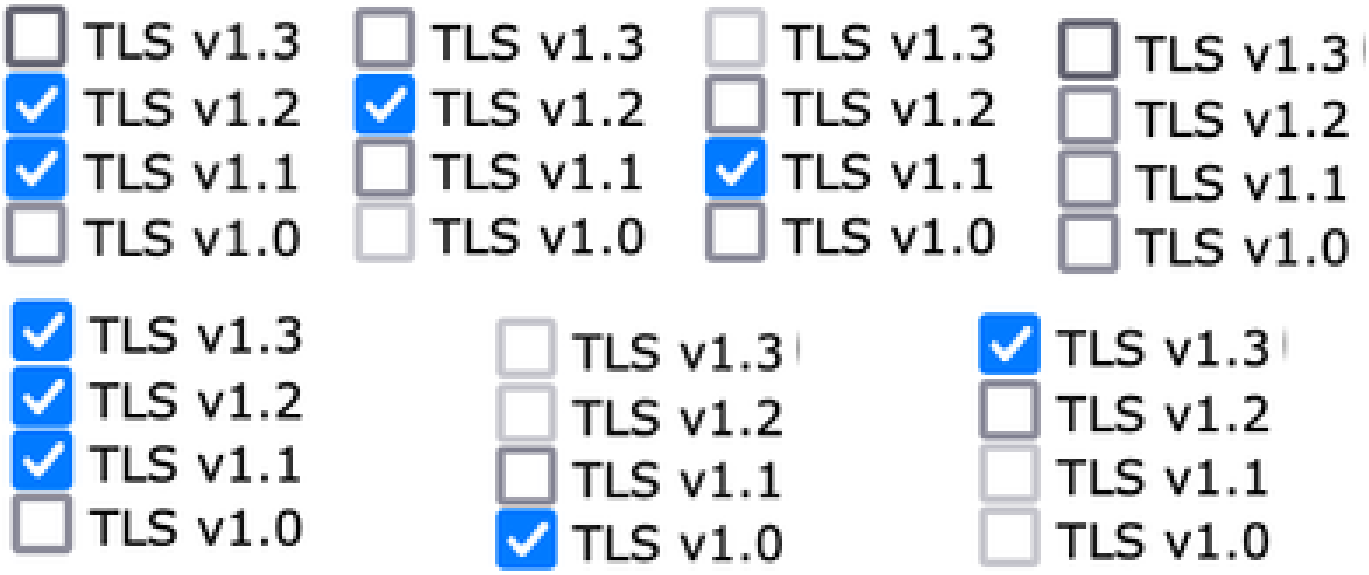
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

TLS協定選擇選項包括TLS v1.0、TLS v1.1、TLS v1.2、TLS v1.3。

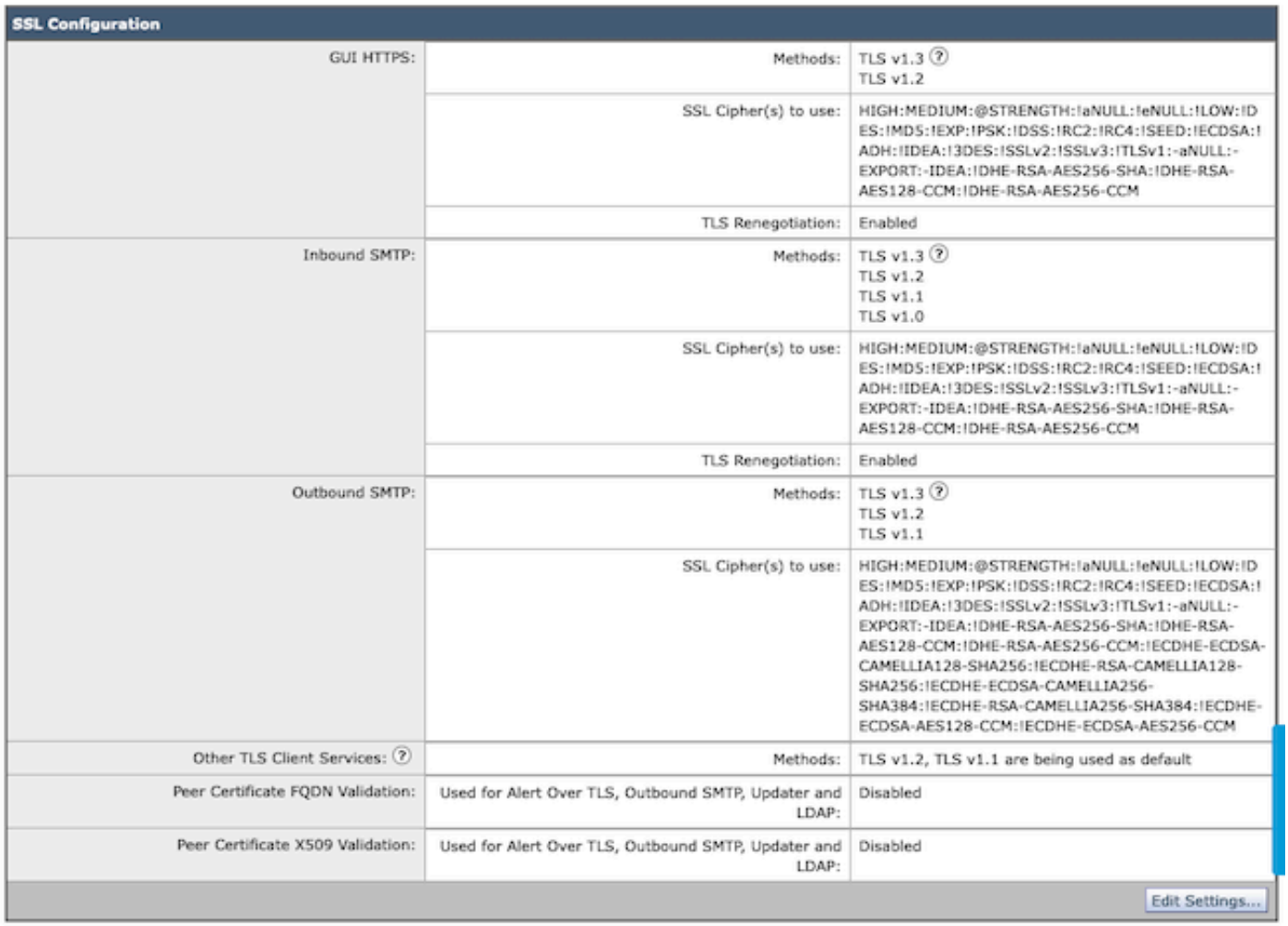
- 升級到AsyncOS 15.5後，預設情況下僅選擇TLS v1.1和TLS v1.2協定。

注意：TLS1.0已停用，因此預設為停用。如果所有者選擇啟用TLS v1.0，則它仍然可用。

- 核取方塊選項會亮起，顯示可用通訊協定的粗體方塊，不相容選項的灰顯方塊會亮起。
- 影像中的範例選項說明了核取方塊選項。



提交後選定TLS協定的示例檢視。



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...

注意：修改GUI HTTPS TLS協定會由於https服務重置而導致WebUI短時間斷開連線。

CLI配置：

SEG允許TLS v1.3在3個服務上：

- GUI HTTPS
- 入站SMTP
- 出站SMTP

執行命令> sslconfig時，會輸出GUI HTTPS、入站SMTP、出站SMTP當前配置的協定和密碼

- GUI HTTPS方法：tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 入站SMTP方法：tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 出站SMTP方法：tlsv1_1tlsv1_2tlsv1_3

選擇要執行的作業：

- GUI -編輯GUI HTTPS ssl設定。
- 入站-編輯入站SMTP ssl設定。

- 出站-編輯出站SMTP ssl設定。

[]>入站

輸入要使用的入站SMTP SSL方法。

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

[2-4]> 1-3

附註： SEG選取流程可以包含一個單一功能表編號（例如2）、一個功能表編號範圍（例如1-4），或是以逗號1、2、3分隔的功能表編號。

CLI sslconfig後續提示透過按enter鍵或修改設定接受現有值。

完成更改時使用>commit >>輸入可選註釋>>按Enter完成更改。

驗證

本節包含一些由於TLS協定版本不匹配或語法錯誤而導致的基本測試方案和錯誤。

由於目標不支援的TLS v1.3而生成拒絕的SEG傳出SMTP協商的日誌條目示例：

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

接收成功協商的TLS v1.3的傳送SEG的日誌條目示例：

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

未啟用TLS v1.3的接收SEG的日誌條目示例。

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

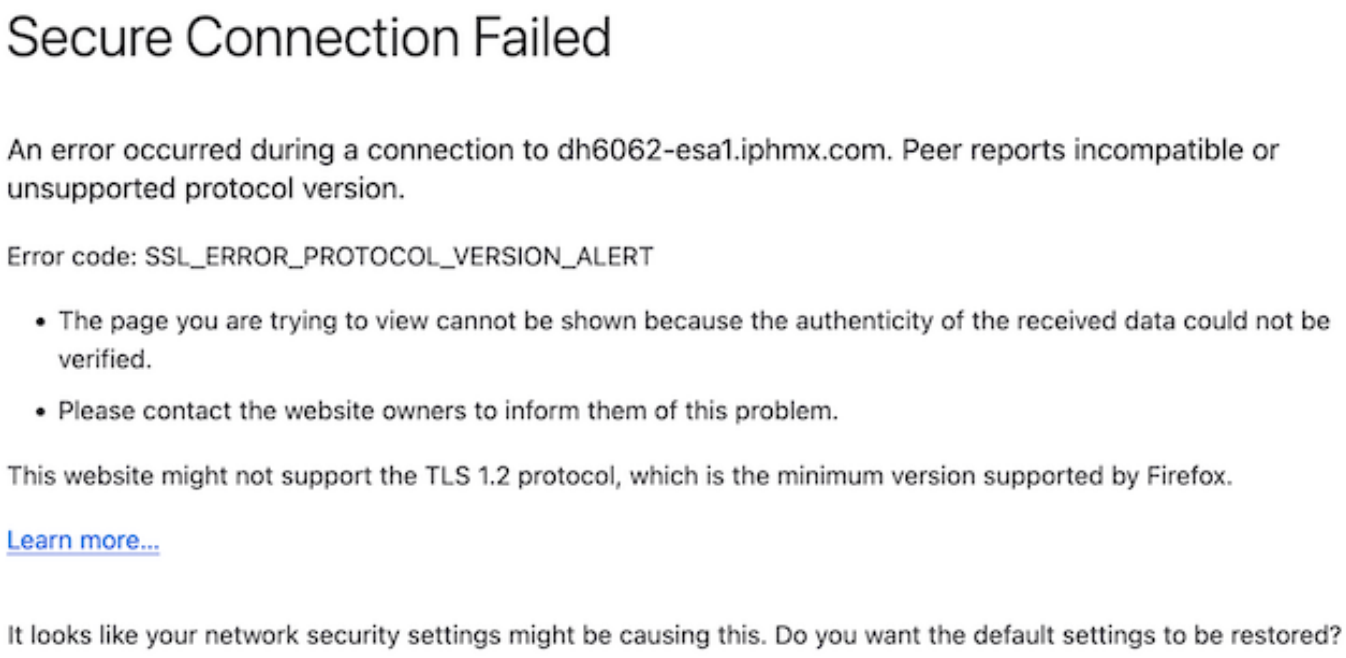
接收SEG支援的TLS v1.3

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

要驗證您的瀏覽器功能，只需打開一個到配置了TLSv1.3的SEG WebUI或NGUI的Web瀏覽器會話。

注意：我們測試的所有網路瀏覽器均已配置為接受TLS v1.3。

- 測試：在Firefox上配置瀏覽器設定停用TLS v1.3支援會在裝置的ClassicUI和NGUI上產生錯誤。
- 使用Firefox的傳統UI配置為排除TLS v1.3作為測試。
- NGUI會收到相同的錯誤，唯一的例外是URL中的埠號4431（預設）。



- 為確保通訊，請驗證瀏覽器設定，以確保包含TLSv1.3。(此示例來自Firefox，使用數字1-4

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

相關資訊

- Cisco Secure Email Gateway -安裝指南
- 用於支援指南的思科安全郵件網關啟動頁面
- Cisco Secure Email Gateway -版本說明

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。