阻止在ESA和SMA上協商空密碼或匿名密碼

目錄

簡介

本文說明如何更改思科電子郵件安全裝置(ESA)和思科安全管理裝置(SMA)密碼設定，以防止協商空或匿名密碼。本文檔適用於基於硬體的裝置和基於虛擬的裝置。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ESA
- Cisco SMA

採用元件

本文檔中的資訊基於Cisco ESA和Cisco SMA的所有版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

防止協商空密碼或匿名密碼

本節介紹如何在運行AsyncOS for Email Security 9.1版及更高版本的Cisco ESA上阻止協商空或匿名密碼，以及在Cisco SMA上阻止協商。

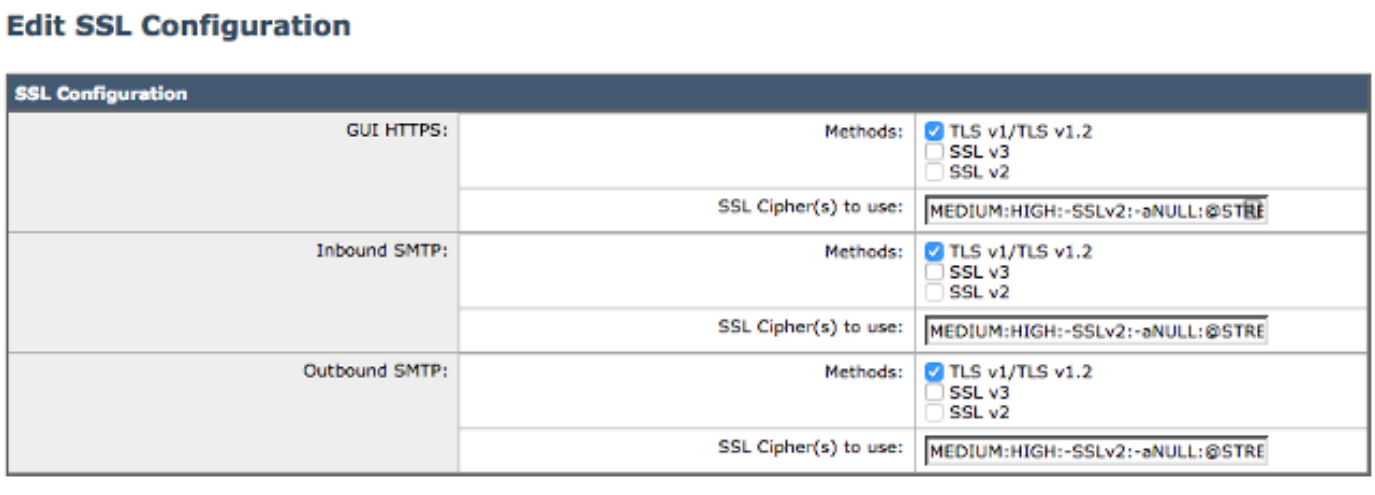
運行AsyncOS for Email Security 9.5版或更高版本的ESA

隨著AsyncOS for Email Security版本9.5的推出，現在支援TLS v1.2。上一節中描述的命令仍然有效；但是，輸出中將會顯示TLS v1.2的更新。

以下是CLI的輸出示例：

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

若要從GUI中訪問這些設定，請導航到**系統管理> SSL配置>編輯設定……**:



提示：有關完整資訊，請參閱9.5版或更高版本相應的ESA最終使用手冊。

運行AsyncOS for Email Security版本9.1或更高版本的ESA

您可以使用**sslconfig** 指令修改ESA上使用的密碼。為了防止ESA協商空或匿名密碼，請在ESA CLI中輸入 **sslconfig**命令並應用以下設定：

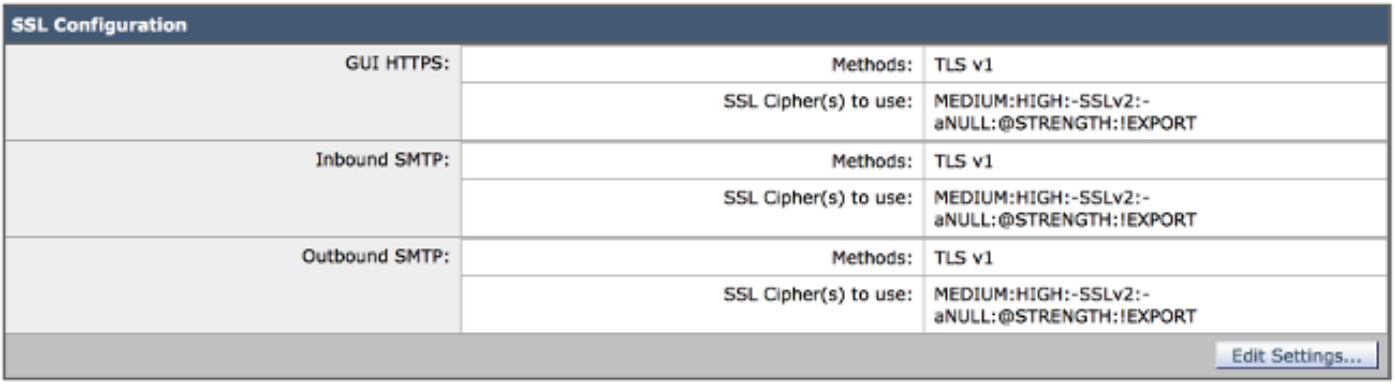
- 入站簡單郵件傳輸協定(SMTP)方法：**sslv3tlsv1**
- 入站SMTP密碼：**中：高：-SSLv2: — 空：@STRENGTH**
- 出站SMTP方法：**sslv3tlsv1**
- 出站SMTP密碼：**中：高：-SSLv2: — 空：@STRENGTH**

以下是傳入密碼的組態範例：

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

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.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

附註：根據每個密碼的需要設定GUI、INBOUND和OUTBOUND。

自AsyncOS for Email Security 8.5版起，還可以通過GUI使用**sslconfig**命令。若要從GUI中訪問這些設定，請導航到**系統管理> SSL配置>編輯設定**:



> **提示：**安全套接字層協定(SSL)3.0版(RFC-6101)是一種過時和不安全的協定。SSLv3 CVE-2014-3566(稱為*在降級傳統加密(POODLE)攻擊時填充Oracle*)中存在漏洞，思科錯誤ID CSCur27131會對其進行跟蹤。思科建議在更改密碼時禁用SSLv3，僅使用傳輸層安全(TLS)，然後選擇*選項3*(TLS v1)。 如需完整的詳細資訊，請參閱Cisco錯誤ID CSCur27131。

運行AsycnOS for Content Security Management 9.6或更高版本的SMA

與ESA類似，在CLI上運行**sslconfig**命令。

運行AsyncOS for Content Security Management 9.5或更高版本的SMA

sslconfig命令不可用於舊版本的SMA。

> **附註**：舊版本的AsyncOS for SMA僅支援TLS v1。 請升級到SMA上的9.6或更高版本，以便進行最新的SSL管理。

您必須從SMA CLI完成以下步驟才能修改SSL密碼：

1. 將SMA配置檔案儲存到本地電腦。
2. 開啟XML檔案。
3. 在XML中*搜尋<ssl>*一節：

```
<ssl>
   <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
   <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
   <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
   <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
   <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
   <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
 </ssl>
```

4. 根據需要修改密碼並儲存XML:

```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
```

```
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```

5. 將新配置檔案載入到SMA上。

6. **提交**並**提交**所有更改。

相關資訊

- Cisco ESA — 發行說明
- Cisco ESA — 使用手冊
- Cisco SMA — 發行說明
- Cisco SMA — 使用手冊
- 技術支援與文件 - Cisco Systems