為ESA偵聽器上的入站連線加密配置TLS

目錄

簡介

本文檔介紹如何在郵件安全裝置(ESA)上的監聽程式上啟用傳輸層安全(TLS)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於任何AsyncOS版本的ESA。

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。

背景資訊

您必須為任何需要加密入站連線的偵聽程式啟用TLS。您可能要在面向Internet（公共偵聽程式）的偵聽程式上啟用TLS，但不是為內部系統的偵聽程式（專用偵聽程式）啟用TLS。 或者，您可能希望為所有監聽器啟用加密。預設情況下，無論是私有監聽器還是公共監聽器都不允許TLS連線。必

須在偵聽程式的主機訪問表(HAT)中啟用TLS，才能為入站（接收）或出站（傳送）電子郵件啟用TLS。此外，專用偵聽程式和公共偵聽程式的郵件流策略設定預設情況下已關閉TLS。

設定

您可以在監聽程式上為TLS指定三種不同的設定：

設定	含義
否	傳入連線不允許TLS。與監聽程式的連線不需要加密的簡單郵件傳輸協定(SMTP)會話。這是您在裝置
偏好	允許從郵件傳輸代理(MTA)傳入連線到偵聽程式TLS。
必需	從MTA到監聽程式的傳入連線允許TLS，並且在收到STARTTLS命令之前，ESA會以錯誤消息來響應

通過GUI在監聽程式的HAT郵件流策略上啟用TLS

請完成以下步驟：

1. 在「郵件流策略」頁中，選擇要修改其策略的監聽程式，然後按一下要編輯的策略名稱的連結。（也可以編輯預設策略引數。）此時將顯示「編輯郵件流策略」頁。
2. 在「加密和驗證」部分的「使用TLS：」欄位中，選擇監聽程式所需的TLS級別。
3. 按一下「Submit」。
4. 按一下Commit Changes，新增可選註釋（如有必要），然後按一下Commit Changes以儲存更改。

附註：建立監聽程式時，可以將TLS連線的特定證書分配給各個公共監聽程式。

通過CLI對偵聽程式的HAT郵件流策略啟用TLS

1. 使用listenerconfig > edit命令以選擇要配置的監聽程式。
2. 使用hostaccess > default命令可編輯監聽程式的預設HAT設定。
3. 輸入以下選項之一，以便在系統提示時更改TLS設定：

```
Do you want to allow encrypted TLS connections?

   1. No
   2. Preferred
   3. Required
 [1]>3

You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```

請注意，此示例要求您使用certconfig命令以確儲存在可與監聽程式一起使用的有效證書。如果您尚未建立任何證書，監聽程式將使用裝置上預安裝的演示證書。您可以使用演示證書啟用TLS以進行測試，但該證書並不安全，建議不要將其用於常規用途。使用listenerconfig > edit > certificate命令將證書分配給監聽程式。配置TLS後，設定將反映在CLI中監聽程式的摘要中：

```
Name: Inboundmail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
```

```
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: Required
```

4. 輸入**commit**命令以啟用更改。

驗證

使用本節內容，確認您的組態是否正常運作。

- 使用文本郵件日誌檔案並檢視以下文檔：確定ESA是否在使用TLS進行傳送或接收
- 使用郵件跟蹤：GUI:監控>郵件跟蹤
- 使用報告：GUI:「監控」>「TLS連線」
- 使用第三方網站，例如checktls.com

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

您可以指定當消息傳送到需要TLS連線的域時，如果TLS協商失敗，ESA是否傳送警報。警報消息包含失敗的TLS協商的目標域的名稱。ESA將警報消息傳送到設定為接收系統警報型別的警告嚴重性級別警報的所有收件人。您可通過GUI中的System Administration > Alerts頁面(或通過CLI中的**alertconfig**命令)管理警報收件人。

相關資訊

- AsyncOS for Email最終使用手冊
- 技術支援與文件 - Cisco Systems