ESA電子郵件加密配置示例

目錄

簡介

本文檔介紹如何在郵件安全裝置(ESA)上設定郵件加密。

必要條件

本文中的資訊係根據以下軟體和硬體版本：

- 型號：所有C系列和X系列
- 已安裝信封加密(PostX)功能

設定

在ESA上啟用電子郵件加密

在GUI上完成以下步驟：

1. 在「安全服務」下，選擇**Cisco IronPort郵件加密>啟用郵件加密**，然後按一下**「編輯設定」**。
2. 按一下**Add Encryption Profile**以建立新的加密配置檔案。
3. 選擇**Cisco Registered Envelope Service**或**Cisco IronPort Encryption Appliance**（如果購買了加密裝置）作為金鑰服務型別。
4. 按一下**Submit and Commit Changes**。
5. 建立加密配置檔案後，您可以選擇將其調配到思科註冊信封服務(CRES)伺服器。新配置檔案

旁邊應顯示Provision按鈕。按一下「**Provision**」。

建立傳出內容過濾器

從GUI完成這些步驟，以便建立傳出內容過濾器來實施加密配置檔案。 在以下示例中，過濾器將觸發對主題標頭中包含字串「Secure：」的任何傳出消息的加密：

1. 在Mail Policies下，選擇Outgoing Content Filters，然後點選**Add Filter**。
2. 新增一個條件為主題標頭為「Secure：」（安全：）和Encrypt and Deliver Now(Final Action)操作的主題過濾==。 按一下「**Submit**」。
3. 在Mail Policies下，選擇Outgoing Mail Policies，並在預設郵件策略或相應的郵件策略中啟用此新篩選器。
4. 提交更改。

驗證

本節介紹如何驗證加密是否有效。

1. 若要驗證，請使用**Secure**：生成新**郵件**並將電子郵件傳送到Web帳戶(Hotmail、Yahoo、Gmail)以確定其是否已加密。
2. 按照下一節中的說明檢查郵件日誌，以確保郵件通過傳出內容過濾器加密。

驗證Mail_logs中的加密過濾器處理

這些mail_log條目顯示郵件與名為Encrypt_Message的加密過濾器匹配。

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
filter ''Encrypt_Message
```

有關如何使用**grep**或**findevent**命令從日誌收集資訊的說明，請參閱ESA消息處置確定，如本節所示。

疑難排解

如果加密過濾器未觸發，請檢查郵件日誌中測試郵件使用的郵件策略。確保在此郵件策略中啟用了過濾器，並且沒有在此策略中啟用之前的**跳過剩餘內容過濾器**操作的過濾器。

確保郵件跟蹤中的郵件使用正確的字串或指定的主題標籤，以便通過內容過濾器觸發加密。