CSC 6.X:電子郵件信譽配置示例

目錄

簡介

本文提供如何在思科內容安全與控制(CSC)安全服務模組(SSM)上設定電子郵件信譽的範例設定。

必要條件

需求

您需要擁有Security Plus許可證才能使用此功能。

採用元件

本檔案中的資訊是根據軟體版本6.3的思科內容安全與控制SSM。

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

Email Reputation是一項減少垃圾郵件的技術。通過啟用此功能，CSC SSM驗證郵件的發件人是否為黑名單地址。它維護一個資料庫清單，其中包含產生垃圾郵件的所有IP地址。如果發現郵件具有此清單中的發件人，則該郵件被視為垃圾郵件並被丟棄。

此電子郵件信譽技術(ERS)提供的服務級別基本上是兩種型別。這些服務主要基於源IP地址的真實性級別。

- ERS標準 — 包含已知垃圾郵件來源
- ERS Advanced — 包含已知來源和可疑來源

將IP地址新增到ERS標準資料庫時，它被稱為垃圾郵件源，很少看到您看到此清單中刪除的IP地址。ERS Standard包含始終引發垃圾郵件的IP地址清單。

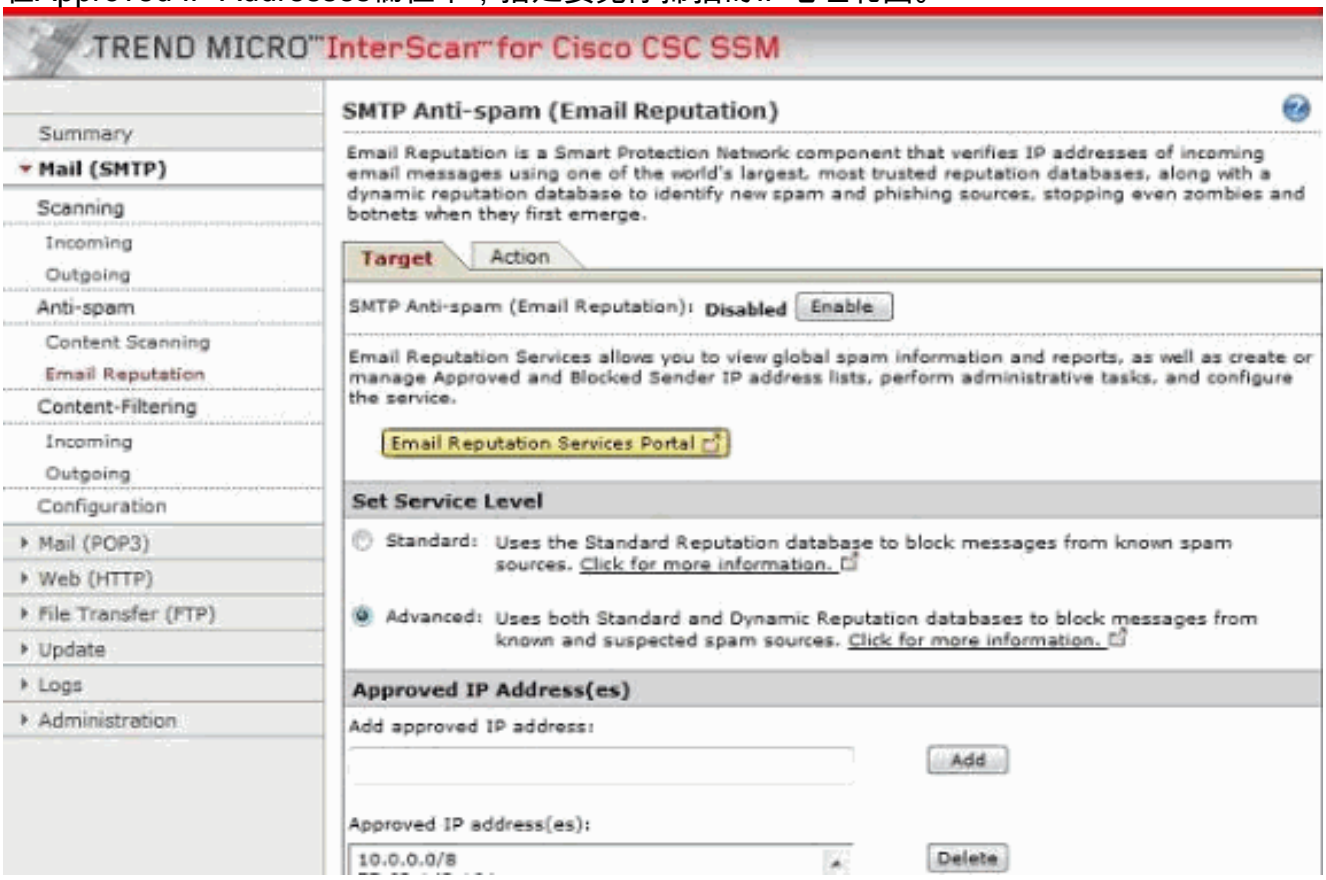
ERS Advanced包含一列IP地址，如果發現這些地址不會進一步產生垃圾郵件，則應該將其刪除。例如，當被入侵時，此資料庫中可以列出被入侵的郵件伺服器。當恢復為正常狀態時，會將其從此資料庫中刪除。

設定

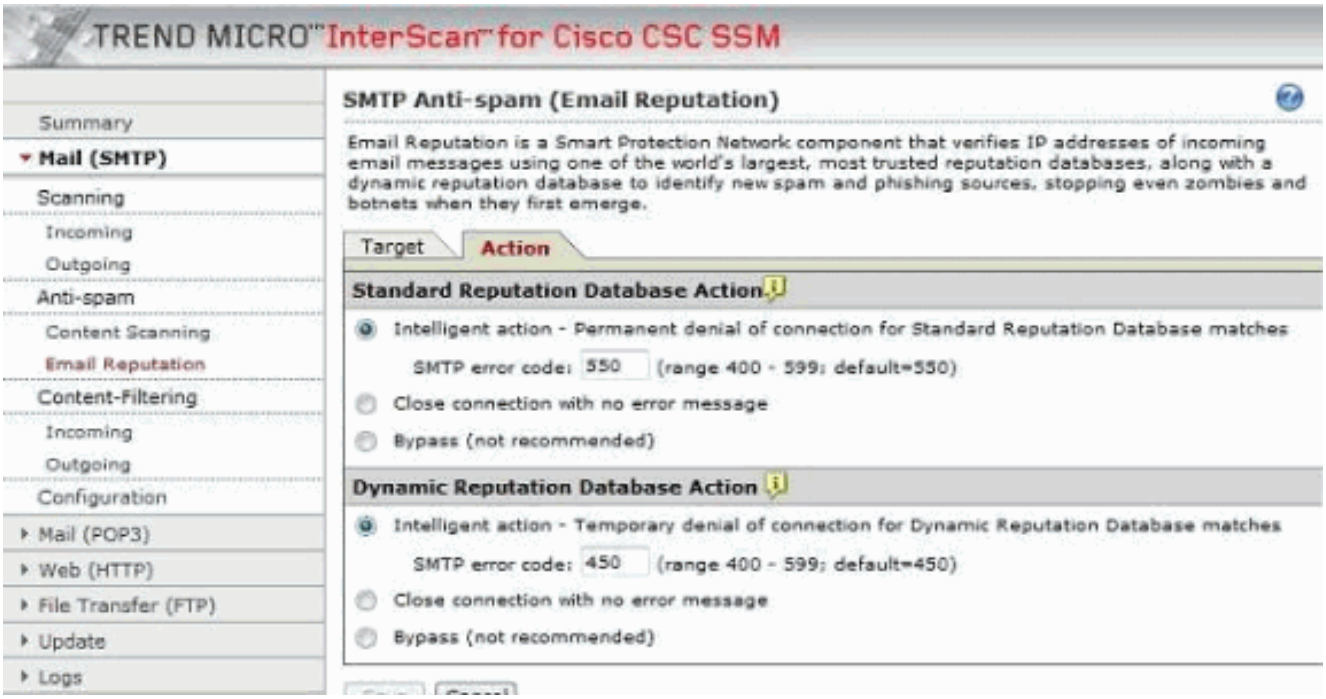
本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

1. 選擇**Mail(SMTP)> Anti-spam > Email Reputation**。將開啟一個新視窗。
2. 在「目標」頁籤中，按一下**啟用**以啟用此電子郵件信譽功能。
3. 選擇**Advanced**作為服務級別。
4. 在Approved IP Addresses欄位中，指定要免除掃描的IP地址範圍。



5. 在操作頁籤中，根據您的企業安全策略指定操作型別。可以使用以下三種操作：關閉連線並顯示錯誤消息關閉連線，無錯誤消息繞過連線



驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

無法從某些域接收電子郵件

問題：

問題在於無法從特定域接收電子郵件。CSC模組似乎正在阻止電子郵件。繞過模組時，一切正常。收到以下錯誤消息：`2012/02/06 14:33:00 GMT+00:00 NRS 174.37.94.181 RBL-Fail-QIL-NA-550 NA 0 NA NA 0 NA NA 0 NA`

解決方案：

為了解決此問題，請正確設定電子郵件信譽功能。

相關資訊

- Cisco ASA內容安全與控制(CSC)安全服務模組支援
- 技術支援與文件 - Cisco Systems