ESA DHAP功能啟用

目錄

簡介

本檔案介紹如何在思科電子郵件安全裝置(ESA)上啟用目錄收集攻擊預防(DHAP)功能，以防止目錄收集攻擊(DHA)。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ESA
- AsyncOS

採用元件

本文檔中的資訊基於AsyncOS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。

背景資訊

DHA是垃圾郵件製造者用來查詢有效電子郵件地址的一種技術。有兩種主要技術可用於生成DHA目標的地址：

- 垃圾郵件傳送者會建立字母和數字的所有可能組合的清單，然後附加域名。

- 垃圾郵件製造者使用標準的字典攻擊，並建立一個包含常用名字、姓氏和首字母的清單。

DHAP是思科內容安全裝置上受支援的功能，可以在使用輕型目錄訪問協定(LDAP)接受驗證時啟用。DHAP功能跟蹤來自給定發件人的無效收件人地址的數量。

一旦發件人超過管理員定義的閾值，該發件人將被視為不受信任，來自該發件人的郵件將被阻止，且不生成網路設計要求(NDR)或錯誤代碼。您可以根據發件人的信譽配置閾值。例如，不可信或可疑的發件人可以具有低DHAP閾值，而可信或可信的發件人可以具有高DHAP閾值。

啟用DHAP

要啟用DHAP功能，請從內容安全裝置GUI導航到**郵件策略 > 主機訪問表(HAT)**，然後選擇**郵件流策略**。從**Policy Name**（策略名稱）列中選擇要**編輯的**策略。

HAT具有四個基本訪問規則，用於根據來自遠端主機的連線執行操作：

- **接受:**連線被接受，電子郵件接受進一步受到監聽程式設定的限制。這包括收件人訪問表（用於公共偵聽程式）。
- **拒絕**:連線最初被接受，但嘗試連線的客戶端收到4XX或5XX問候語。不接受任何電子郵件。
- **TCPREFUSE**:在TCP級別拒絕連線。
- **中繼**:連線被接受。允許接收任何收件人，並且不受收件人訪問表的限制。域金鑰簽名僅適用於中繼郵件流策略。

在選定策略的**郵件流限制**部分中，通過設定最大值查詢並設定**Directory Harvest Attack Prevention(DHAP)**配置。每小時的收件人無效。您還可以選擇自定義Max。每小時無效收件人代碼和最大值。如果需要，每小時的收件人文本無效。

您必須重複此部分，才能為其他策略配置DHAP。

確保在GUI中提交和提交所有更改。

> **附註**：對於遠端主機設定中每小時無效收件人的最大數**量，思科建議您使用介於5和10之間的**最大值。

> **附註**：有關詳細資訊，請參閱思科支援門戶上的**AsyncOS使用手冊**。

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）。