排除ESA上的常見HAT/RAT錯誤

目錄

簡介

概觀

- 帽子
- 發件人組
- SenderBase信譽分數
- 已應用外部威脅源(ETF)源
- 郵件流策略
- RAT

常見實施方案

- 手動阻止發件人
- 將IP地址組/範圍新增到HAT中

疑難排解

- 發件人匹配不正確的發件人組
- 發件人組主機配置不正確
- HAT/RAT拒絕是否對「由信譽過濾阻止」有影響？
- 通過RAT表驗證拒絕
- 如何記錄被拒絕連線的其他發件人/收件人資訊？

相關資訊

簡介

本文描述用於診斷郵件安全裝置(ESA)上的主機訪問表(HAT)和收件人訪問表(RAT)常見問題的高級概述、配置指南和故障排除技術。

概觀

帽子

對於每個配置的監聽程式，必須定義一組規則來控制來自遠端主機的傳入連線。例如，您可以定義遠端主機以及它們是否可以連線到監聽程式。AsyncOS允許您定義允許哪些主機使用HAT連線到監聽程式。

HAT維護一組規則，這些規則控制來自遠端主機的監聽程式的傳入連線。每個已配置的監聽程式都有其自己的獨立HAT。可以為公共偵聽程式和專用偵聽程式配置HAT。

預設情況下，HAT被定義為根據監聽程式型別執行不同的操作：

- 公共偵聽程式：HAT設定為接受來自所有主機的電子郵件。
- 專用監聽程式：HAT配置為從指定的主機中繼電子郵件，並拒絕所有其他主機。

HAT規則由發件人組、SenderBase信譽得分(SBRS)、應用的外部威脅源以及郵件流策略組成。

發件人組

發件人組是由以下一個或多個標識的發件人清單：

- IP地址（IPv4或IPv6）
- IP範圍
- 特定主機或域名
- IP信譽服務「組織」分類
- IP信譽得分(IPRS)範圍（或缺少得分）
- DNS清單查詢響應

SenderBase信譽分數

裝置可以查詢IP信譽服務以確定IP信譽評分。IP信譽得分是根據IP信譽服務中的資訊分配給IP地址、域或組織的數字值。

已應用外部威脅源(ETF)源

ETF框架允許ESA使用通過TAXII協定通訊的STIX格式外部威脅資訊。

能夠使用外部威脅資訊可幫助組織：

- 主動應對網路威脅，如惡意軟體、勒索軟體、網路釣魚攻擊和針對性攻擊。
- 訂閱本地和第三方威脅情報源。
- 提高功效。

您需要有效的功能金鑰才能在ESA上使用ETF。有關如何獲取功能金鑰的資訊，請聯絡您的思科銷售代表和/或思科全球許可運營。

郵件流策略

郵件流策略允許您控制或限制在SMTP會話期間從發件人到偵聽程式的電子郵件流。可以通過在郵件流策略中定義以下型別的引數來控制SMTP會話：

- 連線引數（例如，每個連線的最大消息數）
- 速率限制引數（例如，每小時的最大收件人數）
- 自定義SMTP代碼和響應在SMTP會話期間進行通訊
- 啟用/禁用反垃圾郵件檢測
- 啟用/禁用防病毒保護
- 加密（例如TLS）
- 驗證與驗證（例如DMARC、DKIM和SPF）

RAT

AsyncOS對每個公共偵聽程式使用RAT來管理收件人地址的接受或拒絕。收件人地址包括：

- 域
- 電子郵件地址
- 電子郵件地址組

預設情況下，RAT拒絕所有收件人，以阻止建立開放中繼。

常見實施方案

手動阻止發件人

若要按發件人IP地址阻止特定發件人，請在阻止清單發件人組下為IP地址新增手動條目，並確保該操作設定為「拒絕」或「TCP拒絕」。 有關配置說明，請參閱在ESA上手動阻止發件人IP。

將IP地址組/範圍新增到HAT中

相鄰IP地址可以劃分為子網(例如192.0.2.0/24)、IP地址範圍（例如192.0.2.10-20）或部分IP地址（例如192.0.2）並新增到表中。要新增多個非相鄰IP地址，請遵循以下步驟：

在 GUI 上：

1. 導航到Mail Policies > HAT Overview（如有必要，選擇適當的群集級別）。
2. 選擇要修改的Sender Group，然後選擇Add Sender。
3. 在「Sender」欄位中，輸入適用的IP範圍(例如192.0.2.0/24)和可選註釋，然後選擇Submit。
4. 按一下Commit Changes儲存。

在CLI上：

1. 運行命令序列：

   <#root>

   listenerconfig >> EDIT

2. 輸入要編輯的監聽程式的名稱或編號。
3. 運行命令序列，然後輸入要編輯的發件人組編號或名稱：

   HOSTACCESS >> EDIT >> 1

4. 選擇new並輸入要新增的發件人清單（以逗號分隔）。
5. 完成後，運行commit以儲存更改。

疑難排解

發件人匹配不正確的發件人組

驗證ESA上的郵件日誌或安全管理裝置(SMA)上的郵件跟蹤，並在傳入連線ID(ICID)中檢查這些條目：

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

原因：已在發件人組上啟用連線主機DNS驗證，並且已選擇在DNS中不存在連線主機PTR記錄。

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

原因：已在發件人組上啟用連線主機DNS驗證，並且連線主機反向DNS查詢(PTR)與選擇的前向DNS查詢(A)不匹配。

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

原因：已在發件人組上啟用連線主機DNS驗證，並且由於選擇了臨時DNS故障，連線主機PTR記錄查詢失敗。

發件人組主機配置不正確

發件人組是由以下內容標識的發件人清單：

- IP地址（IPv4或IPv6）
- IP範圍
- 特定主機或域名
- IP信譽服務「組織」分類
- IP信譽得分(IPRS)範圍（或缺少得分）
- DNS清單查詢響應

Sender Group: ESA Sender Group Matching Partial Hostnames（發件人組：匹配部分主機名）下配置錯誤的地址示例。

HAT/RAT拒絕是否對「由信譽過濾阻止」有影響？

是，郵件流策略中帶有拒絕操作的發件人組拒絕的郵件將計入「Stopped by Reputation Filtering」報告計數器。

附註：此計數器可以包括HAT策略拒絕和基於SBRS的拒絕。驗證郵件日誌中的拒絕原因以區分來源。

通過RAT表驗證拒絕

以下是ESA上郵件日誌的日誌輸出示例：

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

原因：在ESA配置中的RAT下不允許特定域。

如何記錄被拒絕連線的其他發件人/收件人資訊？

預設情況下，拒絕的連線僅記錄郵件日誌中的發件人MTA IP地址，而不記錄信封發件人或信封收件人。如果故障排除需要額外的日誌記錄，可以在AsyncOS上啟用延遲的HAT拒絕。

⚠ 注意：思科建議您不要永久啟用此功能，因為它需要額外的資源。

更多詳細資訊可在此處找到：HAT延遲拒絕常見問題。

相關資訊

- Cisco Email Security Appliance - 一般使用者指南
- 思科技術支援與下載

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）。