ESA遇到反彈(NDR)風暴

目錄

簡介

本文描述您的郵件安全裝置(ESA)遇到反彈風暴時遇到的問題，並提供該問題的解決方案。

背景資訊

反彈風暴是喬伊工作的副作用或電子郵件垃圾郵件的反向傳播。

喬·喬布

joe作業是一種垃圾郵件攻擊，它使用偽裝的發件人資料，旨在破壞顯性發件人的聲譽和/或誘使收件人對該顯性發件人採取行動。

反向散射

反向散射是垃圾郵件、病毒和蠕蟲的副作用，接收垃圾郵件和其他郵件的電子郵件伺服器會向無辜方傳送退回郵件。之所以會出現這種情況，是因為原始郵件信封發件人是偽造的，以便包含受害者的電子郵件地址。由於這些消息不是由收件人請求的，彼此基本相似，並且以批次方式傳送，因此它們被定義為未經請求的大量電子郵件或垃圾郵件。因此，生成電子郵件反向散射的系統可能會被列入各種域名系統黑名單(DNSBL)中，並且違反網際網路服務提供商的服務條款。

問題

您的ESA會遇到反彈風暴，ESA中注入了大量郵件。在這樣的攻擊中，傳入的連線計數會激增。裝置可能會開發工作隊列備份。為了驗證裝置是否受到此類攻擊，請記錄郵件發件人地址的**郵件**日誌。退回郵件（非送達報告 — NDR）具有空的信封郵件來**自**地址。

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

受到退迴風暴影響的裝置將包含信封郵件發件人地址「**<>**」的大部分郵件。

解決方案

管理反彈風暴的選項有很多。

退回驗證

為了防止這些誤定向反彈攻擊，AsyncOS包括思科反彈驗證。 啟用時，此功能會標籤通過ESA傳送的郵件的信封發件人地址。然後，檢查ESA接收的任何退回郵件的信封收件人是否包含此標籤。收到合法退回郵件時，新增到信封發件人地址的標籤將被刪除，退回郵件將被傳送給收件人。可以單獨處理不包含該標籤的退回郵件。

AsyncOS將退回視為具有空郵件發件人**地址**(**<>**)的郵件。 系統不會將來自mailer-daemon@example.com或postmaster@example.com等地址的郵件視為退回郵件，因此不會進行退回驗證。

配置退回驗證地址標籤金鑰

退回驗證地址標籤金鑰清單顯示當前金鑰和過去使用過的所有未清除金鑰。若要新增新金鑰，請完成以下步驟：

1. 在 **郵件策略 > 退回驗證** 頁面上，按一下**New Key**。
2. 輸入文本字串並按一下 **提交**.
3. 提交更改。

清除金鑰

如果從下拉選單中選擇清除規則並按一下「清除」，則可以清除舊的地址標籤**鍵。**

配置思科退回驗證設定

退回驗證設定可確定在收到無效退回時要執行的操作。

- 選擇 **郵件策略 > 退回驗證**.
- 按一下 **編輯設定**.
- 選擇是拒絕無效退回還是向郵件新增自定義信頭。如果要新增報頭，請輸入報頭名稱和值。
- 或者，啟用智慧例外。此設定允許自動免除對內部郵件伺服器生成的傳入郵件和退回郵件的退回驗證處理（即使對傳入和傳出郵件使用單個偵聽程式）。

- 提交並提交更改。

使用CLI配置思科退回驗證

您可以在CLI中使用**bvconfig**和**destconfig**命令來設定退回驗證。這些命令將在Cisco AsyncOS CLI參考指南中討論。

思科退回驗證和群集配置

退回驗證可在群集配置中工作，只要兩個思科裝置使用相同的「退回金鑰」。 使用同一金鑰時，任一系統都應能夠接受合法的反饋。修改後的標頭標籤/金鑰並非特定於每個思科裝置。

郵件篩選器

如果您由於使用單獨的裝置接收和傳送而無法使用退回驗證，則可以設定郵件過濾器以阻止郵件發件人地址為**空的**郵件。

郵件阻止

由於這些退回郵件很可能具有不存在的信封收件人地址，因此您可以通過會話輕型目錄訪問協定(LDAP)收件人驗證來阻止無效地址，以幫助降低此類郵件的影響。