瞭解與郵件流策略和目標控制相關的引數

目錄

簡介

本檔案介紹電子郵件安全設備(ESA)有關如何限制/限制傳送者和交付的幾個組態方面。文章中將介紹的功能是「郵件流策略」和「目標控制」。

必要條件

需求

思科建議您瞭解以下主題：

- 基本瞭解郵件流策略和目標控制
- 熟悉ESA配置中這些功能的用法

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

郵件流策略和目標控制的優勢

這兩個功能都有一個非常重要的功能，那就是速率限制/調節。此方面可幫助管理員控制哪些流量應自由流動，哪些流量應允許有限制。

郵件流策略

這些策略適用於ESA的發件人組，並根據這些策略執行電子郵件流量調制。

郵件流策略始終應用於傳入到ESA的流量，無論該電子郵件是入站或出站郵件。

郵件流策略在後端使用該策略的所選連線行為工作。ESA中提供的不同連線行為包括：

1. 接受
2. 拒絕
3. 中繼
4. TCP拒絕
5. 繼續

接受:連線被接受，電子郵件接受則進一步受到監聽程式設定的限制，包括收件人訪問表（針對公共監聽程式）。 此連線行為將電子郵件視為入站電子郵件

拒絕：嘗試連線的客戶端獲得4XX或5XX SMTP狀態代碼。不接受任何電子郵件。這主要用於黑名單發件人

中繼：已接受連線。允許接收任何收件人，並且不受收件人訪問表的限制。這將電子郵件視為出站郵件

TCP拒絕：在TCP級別拒絕連線。

繼續：忽略HAT中的對映，並繼續處理HAT。如果傳入連線與非CONTINUE的後續條目匹配，則改用該條目。CONTINUE規則用於便於在GUI中編輯HAT。

郵件流策略的元件

最大每個連線的消息：通過遠端主機的每個連線可由此監聽程式傳送的最大消息數。每個ICID描述一個連線

最大每封郵件的收件人：使用此郵件流策略處理的來自此主機的每封郵件的最大收件人數

最大郵件大小：標籤到郵件流策略的此偵聽程式將接受的郵件的最大大小。最小的可能最大郵件大小為1 KB。

最大來自單個IP的併發連線：允許從單個IP地址連線到此監聽程式的最大併發連線數。

自定義SMTP橫幅代碼：與此監聽程式建立連線時返回的SMTP代碼。

自定義SMTP標語文本：與此監聽程式建立連線時返回的SMTP標語文本。可以在該欄位中使用一些變數。

覆蓋SMTP標語主機名：預設情況下，向遠端主機顯示SMTP標語時，裝置將包含與監聽程式的介面

關聯的主機名（例如，220-hostname ESMTP）。 您可以選擇在此處輸入其他主機名來覆蓋此標語。此外，還可以將hostname欄位留空，以選擇*not* 在標語中顯示主機名。

郵件流限制

最大每小時收件人數：此偵聽程式每小時從遠端主機接收的最大收件人數。全域性跟蹤每個發件人IP地址的收件人數。每個監聽程式跟蹤其自己的速率限制閾值，但是，由於所有監聽程式都針對單個計數器進行驗證，因此如果同一個IP地址（傳送方）連線到多個監聽程式，則更有可能超過速率限制。可以在該欄位中使用一些變數。

最大每小時收件者代碼：當主機超過為此偵聽程式定義的每小時最大收件人數量時返回的SMTP代碼。

最大每小時收件人數文本：當主機超過為此監聽程式定義的每小時最大收件人數時返回的SMTP標語文本。

信封發件人的速率限制

最大每個時間間隔的收件人：指定時間段內此偵聽程式將從唯一信封發件人接收的最大收件人數（基於發件人地址）。將全域性跟蹤收件人數。每個偵聽程式跟蹤其自身的速率限制閾值；但是，由於所有偵聽器都根據單個計數器進行驗證，因此，如果多個偵聽器接收來自同一郵件發件人地址的郵件，則更有可能超過速率限制。

發件人速率限制錯誤代碼：當信封超過為此偵聽程式定義的時間間隔的最大收件人數時返回的SMTP代碼。

發件人速率限制錯誤文本：當信封發件人超過為此偵聽程式定義的時間間隔的最大收件人數時返回的SMTP標語文本。

例外： 如果您希望某些信封發件人不受定義的速率限制，請選擇包含信封發件人的地址清單。

地址清單是從「郵件策略」(Mail Policies)的「地址清單」(Address List)中定義的（完整電子郵件地址、域、IP地址可用於免除）

使用SenderBase進行流量控制：為此偵聽程式啟用SenderBase信譽服務的「查詢」。

按IP地址相似性分組：用於在管理大型CIDR塊中偵聽程式的主機訪問表(HAT)中的條目時，根據每個IP地址跟蹤和速率限制傳入郵件。您可以定義一個有效位範圍（從0到32），通過該範圍對類似的IP地址進行分組，以實現速率限制，同時仍保留該範圍內每個IP地址的單獨計數器。

附註：要求禁用「使用SenderBase」。

目錄收集攻擊預防(DHAP)

最大每小時無效收件人數：此偵聽程式每小時將從遠端主機接收的最大無效收件人數。此閾值表示RAT拒絕和SMTP Call-Ahead伺服器拒絕的總數，以及被丟棄在SMTP會話中或退回到工作隊列中的無效LDAP收件人的郵件總數（在相關偵聽程式的LDAP接受設定中配置）。

在SMTP會話中達到DHAP閾值時丟棄連線：

如果達到無效收件人的閾值，裝置將丟棄與主機的連線。

最大每小時無效收件人代碼：指定刪除連線時使用的代碼。預設代碼為550。

最大每小時無效收件人文本：指定要用於已刪除連線的文本。預設文本為「無效收件人太多」。

安全性功能

垃圾郵件/AMP/病毒/發件人域信譽驗證/爆發過濾器/高級網路釣魚防護/灰色郵件/內容和郵件過濾器：可從此處啟用或禁用安全引擎/掃描和過濾器相關掃描

加密和身份驗證：我們可以為此偵聽程式在SMTP會話中修改設定為Off、Prefer或Require Transport Layer Security(TLS)。

「驗證客戶端證書」(Verify Client Certificate)選項指導郵件安全裝置在客戶端證書有效時與使用者的郵件應用程式建立TLS連線。

對於「首選TLS」，如果使用者沒有證書，則裝置仍允許非TLS連線，但如果使用者具有無效證書，則拒絕連線。

對於「需要TLS」設定，選擇此選項需要使用者具有有效的證書，以便裝置允許連線。

SMTP身份驗證：允許、禁止或要求從連線到偵聽程式的遠端主機進行SMTP身份驗證

如果同時啟用TLS和SMTP身份驗證：需要TLS提供SMTP身份驗證

域金鑰/DKIM簽名：在此偵聽器上啟用域金鑰或DKIM簽名

DKIM驗證：啟用DKIM驗證。

S/MIME解密/驗證：啟用S/MIME解密或驗證。

處理後的簽名：選擇在S/MIME驗證後是否從郵件保留或刪除數位簽章。

S/MIME公鑰收集：啟用S/MIME公鑰收集。

驗證失敗時的收集證書：選擇在傳入簽名消息的驗證失敗時是否獲取公鑰。

儲存更新的證書：選擇是否獲取更新的公鑰

SPF/SIDF驗證： 在此偵聽程式上啟用SPF/SIDF簽名。

合規級別：設定SPF/SIDF一致性級別。您可以選擇SPF、SIDF或SIDF相容

如果使用「Resent-Sender：」或「Resent-From：」，請降級PRA驗證結果：如果選擇與SIDF相容的一致性級別，請配置是否將PRA身份驗證的通過結果降級為「無」（如果有Resent-Sender）：或Resent-From:郵件中存在標頭

HELO測試：配置是否要針對HELO身份執行測試（將此項用於SPF和SIDF相容一致性級別）

DMARC驗證：在此偵聽程式上啟用DMARC驗證

使用DMARC驗證配置檔案：選擇要在此監聽程式上使用的DMARC驗證配置檔案。從Mail Policies —> DMARC —> Add Profile建立相同內容

DMARC反饋報告：允許傳送DMARC彙總反饋報告。

退回驗證

將未標籤的退回視為有效：僅在啟用退回驗證標籤時應用。預設情況下，裝置會認為未標籤的退回無效，並根據「退回驗證」設定拒絕退回或新增自定義報頭。如果您選擇將未標籤的退回視為有效，裝置將接受退回郵件。

發件人驗證

信封發件人DNS驗證：

由於不同原因，無法驗證發件人。未驗證的發件人分為以下類別：

- DNS中不存在連線主機PTR記錄。
- 由於臨時DNS故障，連線主機PTR記錄查詢失敗。
- 連線主機反向DNS查詢(PTR)與正向DNS查詢(A)不匹配。

我們可以啟用或禁用發件人驗證功能。

使用發件人驗證例外表：我們可以使用發件人驗證域例外表來允許豁免。我們只能有一個異常表，但可以啟用每個郵件流策略。

異常表可以從郵件策略 — >發件人驗證異常表 — >新增發件人驗證異常

目的地控制

此功能可控制電子郵件傳送。所有通過ESA完成處理並即將退出ESA以便進一步送達的電子郵件都可以通過「目標控制」功能進行控制。

Default Destination Controls配置檔案適用於所有交貨。為了應對特定域交付控制的需要，我們必須建立自定義的目標控制配置檔案。

目標控制配置檔案的元件

限制

同時連線數：裝置將嘗試開啟以完成傳送的遠端主機的同時連線(DCID)數。

每次連線郵件數上限：在裝置啟動新連線之前，ESA將通過連線(DCID)傳送到目標域的消息數量。

收件人：裝置將在給定時間段內傳送到給定遠端主機的收件人數。

應用限制：這些方面有助於確定如何應用我們針對每個目標和MGA主機名指定的限制。

TLS支援

這有助於確定到遠端主機的TLS連線是否設定為「無」/「首選」/「必需」

DANE支援：如果將DANE配置為「Opportational」，並且遠端主機不支援DANE，則優先使用機會TLS來加密SMTP會話。

如果將DANE配置為「Mandatory」，並且遠端主機不支援DANE，則不會建立與目標主機的連線。

如果將DANE配置為「必填」或「機會主義」，並且遠端主機支援DANE，則首選它加密SMTP會話。

附註：不會對配置了SMTP路由的域實施DANE。

退回驗證

這有助於確定是否通過退回驗證執行信封發件人地址標籤(prvs-xxxxxx-xxxx)。

可以從郵件策略 — >退回驗證 — >新增新金鑰

退回配置檔案

退回配置檔案可由裝置用於給定的遠端主機。如果存在傳送問題，它會決定在硬退回電子郵件之前將電子郵件保留在ESA的傳送隊列中的時間

退回配置檔案通過Network —> Bounce Profiles設定

全域性設定

證書：這就是我們定義在建立SSL/TLS連線時向下一躍點發起電子郵件傳遞時要使用的證書的方面。在這方面始終建議使用證書頒發機構(CA)簽名的證書。

當所需的TLS連線失敗時傳送警報：我們可以指定在將消息傳遞到需要TLS連線的域時，如果TLS協商失敗，裝置是否傳送警報。警報消息包含失敗的TLS協商的目標域的名稱。裝置會將警報消息傳送到設定為接收系統警報類型的警告嚴重性級別警報的所有收件人。

我們可以通過「系統管理」 — >「警報」管理警報收件人