退回驗證和目的地控制最佳實踐指南

目錄

簡介

不受控制的高流量電子郵件傳輸可能會淹沒收件人域。AsyncOS通過定義電子郵件安全服務將開啟的連線數或將傳送到每個目標域的郵件數，為您提供對郵件傳送的完全控制。

在本文檔中，我們將介紹：

1. 設定退回驗證以保護您的組織免受退回攻擊
2. 使用目標控制表實施好鄰居策略
3. 部署基於SMTP DNS的命名實體身份驗證(DANE)，以提供安全郵件傳送

退回驗證

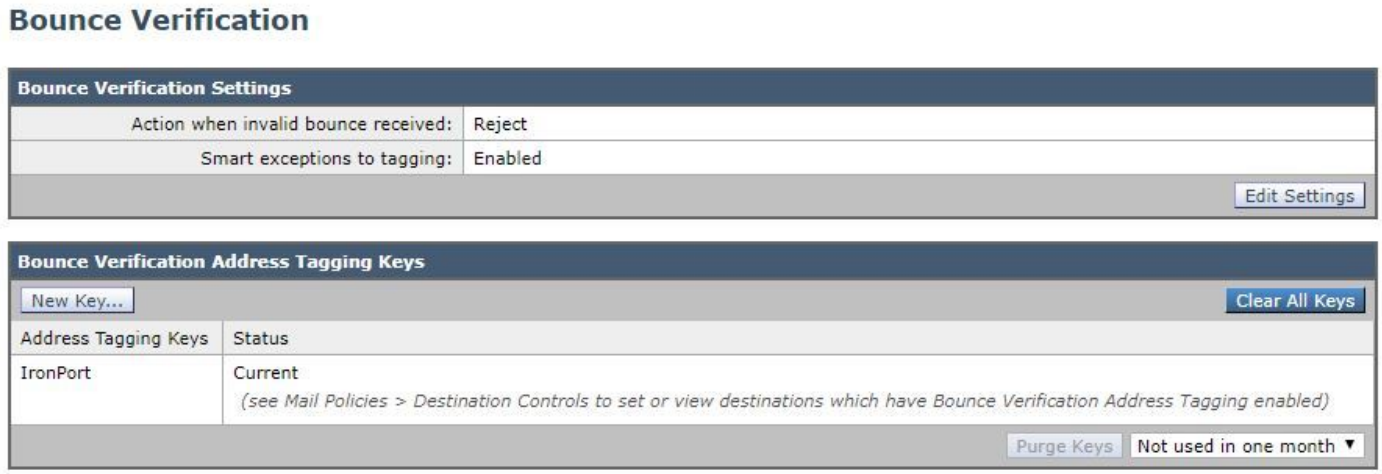
啟用退回驗證是抵禦反向散射/退回攻擊的好方法。 退回驗證的概念很簡單。首先，標籤離開您網站的 歐空局。查詢任何退回郵件上的標籤，如果標籤存在，則表示 這是源自您環境中的郵件的退回。如果缺少標註， 退回是欺詐性的，可以拒絕或刪除。

例如，MAIL FROM: joe@example.com 成為郵件發件人：prvs=joe=123ABCDEFG@example.com.示例中的123...字串是退回 在ESA裝置傳送時新增到信封發件人的驗證標籤。如果 郵件退回後，退回郵件中的信封收件人地址將包括 退回驗證標籤，它使ESA知道該標籤是合法退回的 消息。

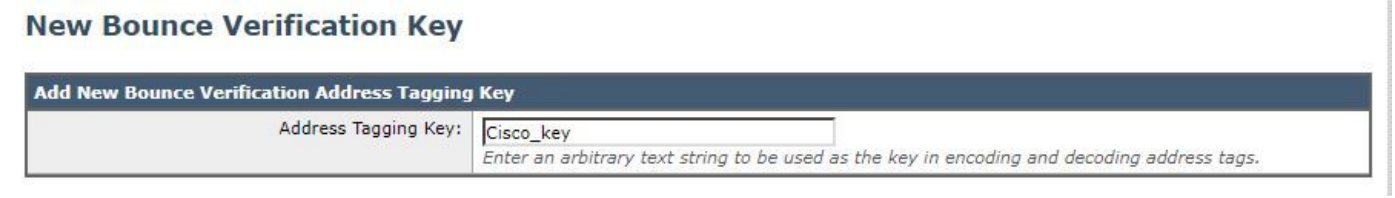
您可以預設啟用或禁用系統範圍內的退回驗證標籤。您可以 還要為特定域啟用或禁用退回驗證標籤。在大多數情況下 部署，預設情況下對所有域啟用。

ESA配置

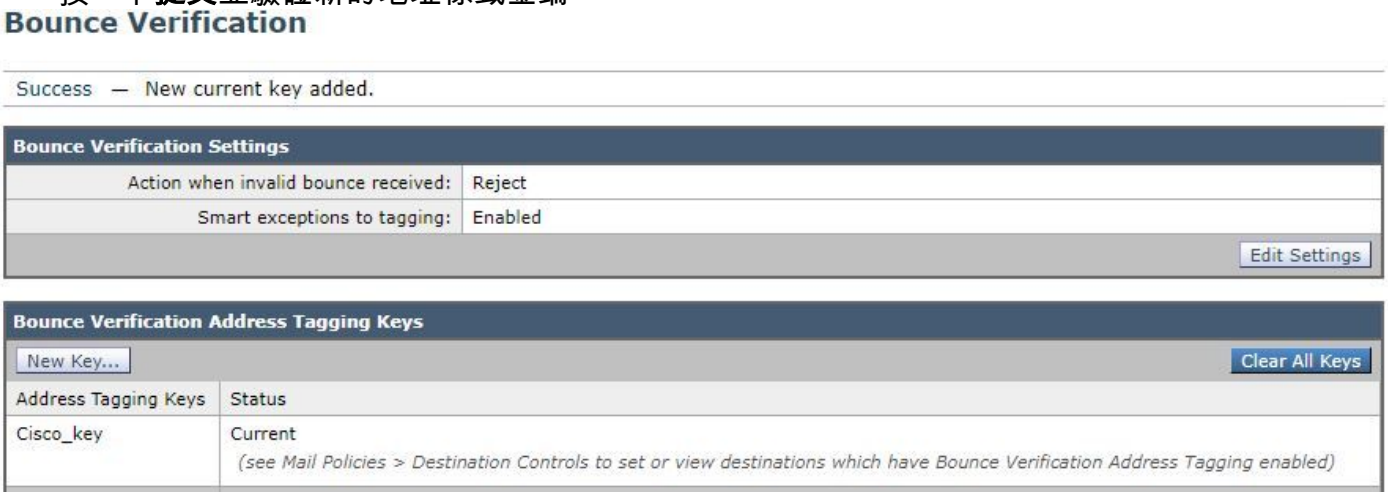
- 導航到**Mail Policies > Bounce Verification**，然後點擊**New Key**



- 輸入任意文本，用作編碼和解碼地址標籤的金鑰。例如，"Cisco_key"。

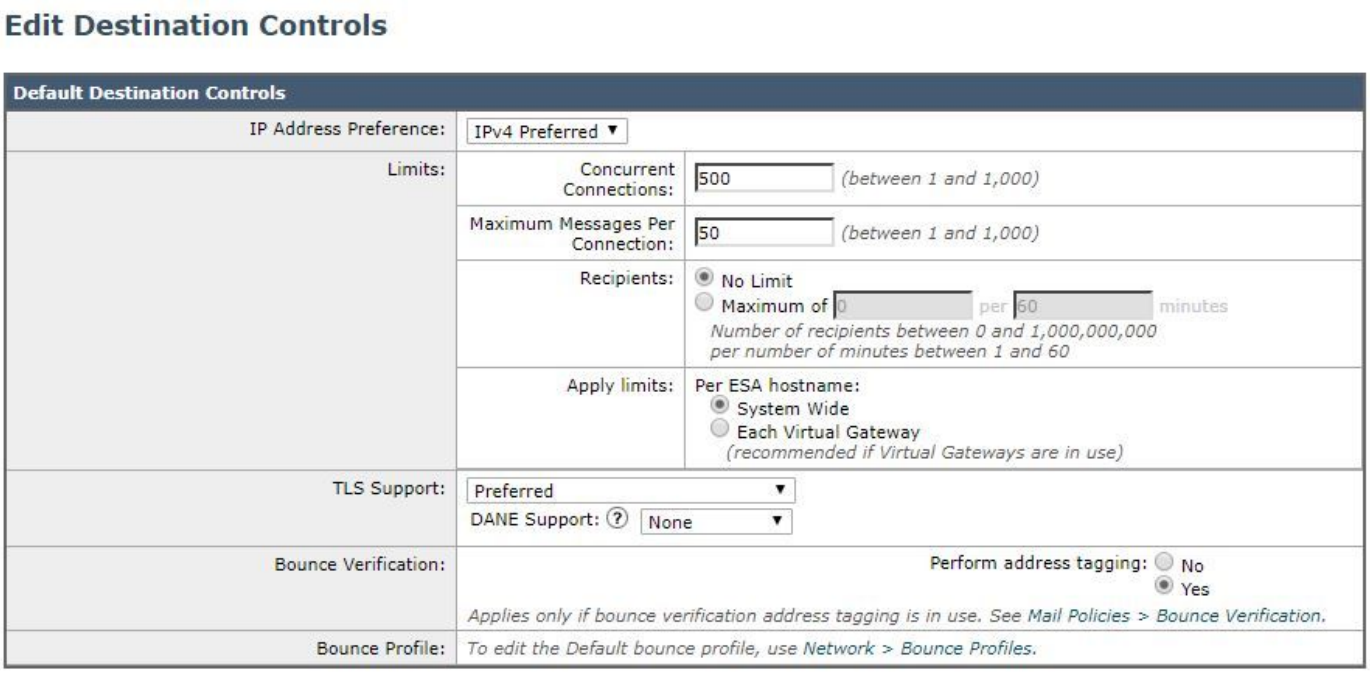


- 按一下**提交**並驗證新的地址標籤金鑰

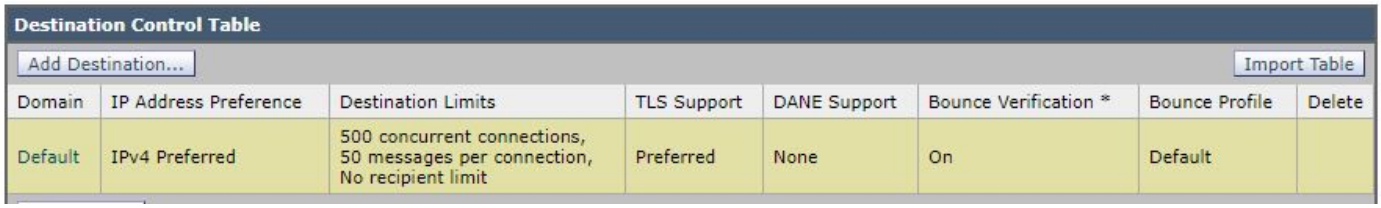


現在，讓我們為我們的「預設」域啟用退回驗證：

- 導航到**Mail Policies > Destination Controls**，然後點選**Default**。
- 配置**退回驗證：執行地址標籤：是**



- 按一下**Submit**和**Commit changes**。請注意，預設域的退回驗證現在已開啟。



使用目標控制表

不受控制的電子郵件傳輸可能會淹沒收件人域。ESA使您能夠完全控制 通過定義裝置將開啟的連線數或連線數 裝置將傳送到每個目標域的郵件。 目標控制表提供當ESA為 傳送到遠端目標。它還提供了用於嘗試或強制對這些目標使用TLS的設定。ESA配置了目標控制表的預設配置。

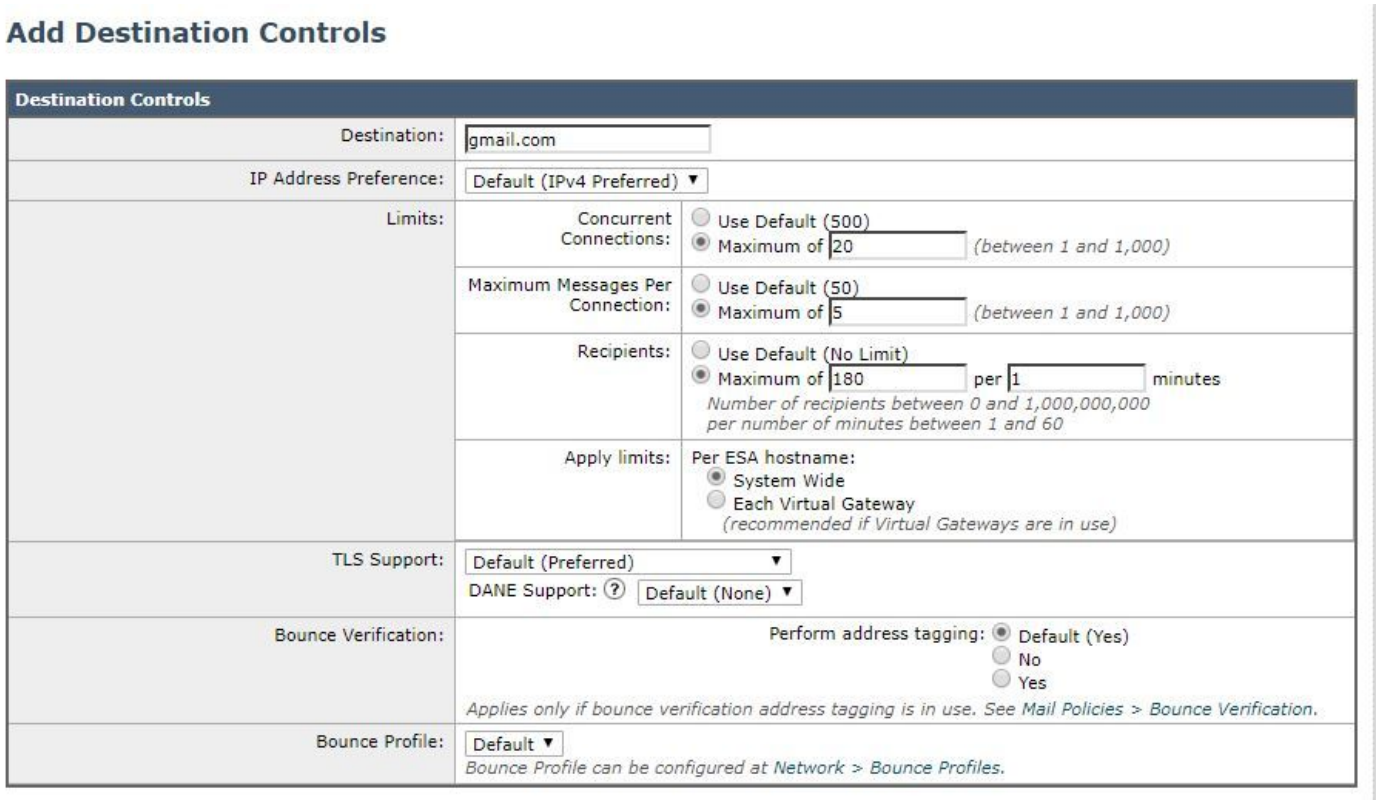
我們將介紹如何管理和配置對預設不適用的目標的控制。例如，Google有一組接收規則，Gmail使用者應遵循這些規則，否則他們可能會發回SMTP 4XX響應代碼和一條消息，告知你傳送得太快或者收件人的郵箱超過了它的儲存限制。我們將將Gmail域新增到目標控制表中，限制傳送到以下Gmail收件人的郵件量。

向目標控制表新增新域

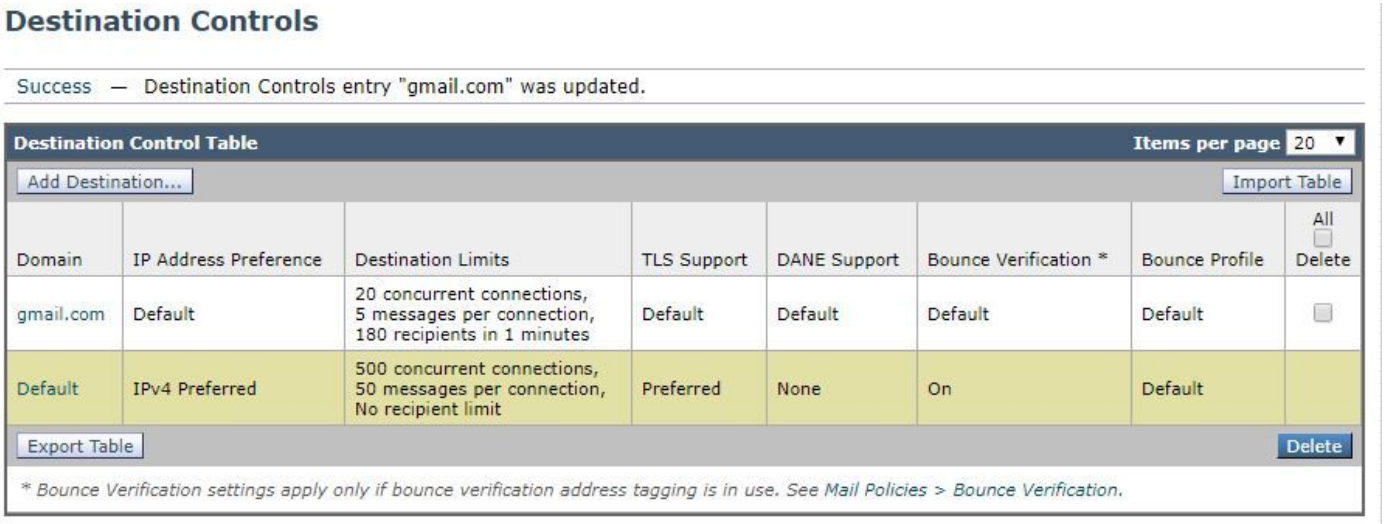
如前所述，Google對傳送者傳送至Gmail有限制。可以通過檢視此處發佈的Gmail發件人限制來驗證接收限制 — https://support.google.com/a/answer/1366776?hl=en

讓我們為Gmail設定目標域作為良好鄰居策略的示例。

- 導航到**郵件策略(Mail Policies)>目標控制(Destination Controls)**，然後點選**新增目標(Add Destination)**，然後使用以下引數建立新配置檔案： **目標:gmail.comIP地址首選項：首選IPv4同時連線數：最多20個每個連線的最大消息數：5收件人：每分鐘最多180個退回驗證：執行地址標籤：預設（是）**



• 按一下**Submit**和**Commit changes**。新增域後，我們的目標控制表看起來是這樣的。請注意以下影象中的「目標限制」和「退回驗證」更改：



部署SMTP基於DNS的命名實體身份驗證(DANE)

SMTP基於DNS的命名實體身份驗證(DANE)協定使用在DNS伺服器上配置的域名系統安全(DNSSEC)擴展和DNS資源記錄（也稱為TLSA記錄）來驗證具有DNS名稱的X.509證書。

TLSA記錄會新增到憑證中，其中包含憑證授權單位(CA)、終端實體憑證或用於RFC 6698中所述DNS名稱的信任錨點的詳細資訊。域名系統安全(DNSSEC)擴展通過解決DNS安全中的漏洞，在DNS上提供更高的安全性。使用加密金鑰和數位簽章的DNSSEC可確保查詢資料正確並連線到合法伺服器。

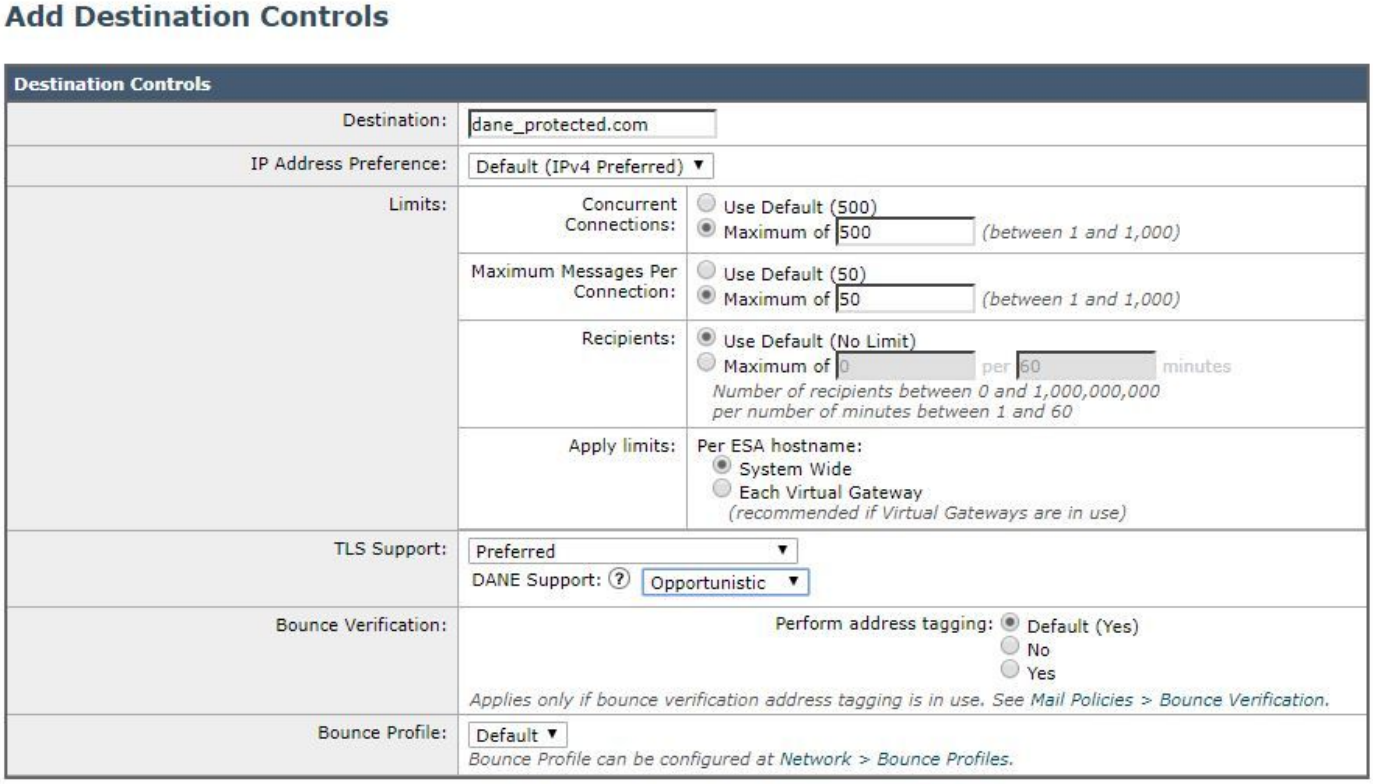
使用SMTP DANE進行傳出TLS連線的優點如下：

- 通過防止中間人(MITM)降級攻擊、竊聽和DNS快取中毒攻擊，提供安全郵件傳送。
- 提供TLS證書和DNS資訊在DNSSEC保護下的真實性。

ESA配置

在ESA上開始設定DANE之前，請確保信封發件人和TLSA資源記錄已驗證DNSSEC，且接收域受DANE保護。可以使用CLI命令**daneverify**在ESA上執行此操作。

- 導航到**郵件策略(Mail Policies)>目標控制(Destination Controls)**，然後點選**新增目標(Add Destination)**，然後使用以下引數建立新配置檔案： **目標：dane_protected.comTLS 支援：偏好DANE支援：機會主義**



- 按一下**Submit**和**Commit changes**。