バウンス確認および宛先制御のための最良の方法 ガイド

目次

[はじめに](#)
[バウンス確認](#)
[ESA の設定](#)
[宛先管理テーブルの使用](#)
[宛先管理テーブルに新しいドメインを追加する方法](#)
[展開します指定 Entities（デンマーク人）の SMTP DNS ベース 認証を](#)
[ESA の設定](#)

概要

自由な大量メール配信は受信者のドメインを圧倒できます。 AsyncOS は E メール セキュリティ サービスがまたは各宛先 ドメインに送信 するメッセージ数開く接続の数の定義によってメッセージ デリバリーの完全な制御を与えます。

この資料では、カバーします:

1. バウンス確認のバウンス不正侵入から組織を保護するために設定
2. よい隣接ポリシーを練習する宛先管理テーブルの使用
3. 提供するために指定 Entities（デンマーク人）の SMTP DNS ベース 認証を展開してメッセージの配信を保護して下さい

確認を跳ねて下さい

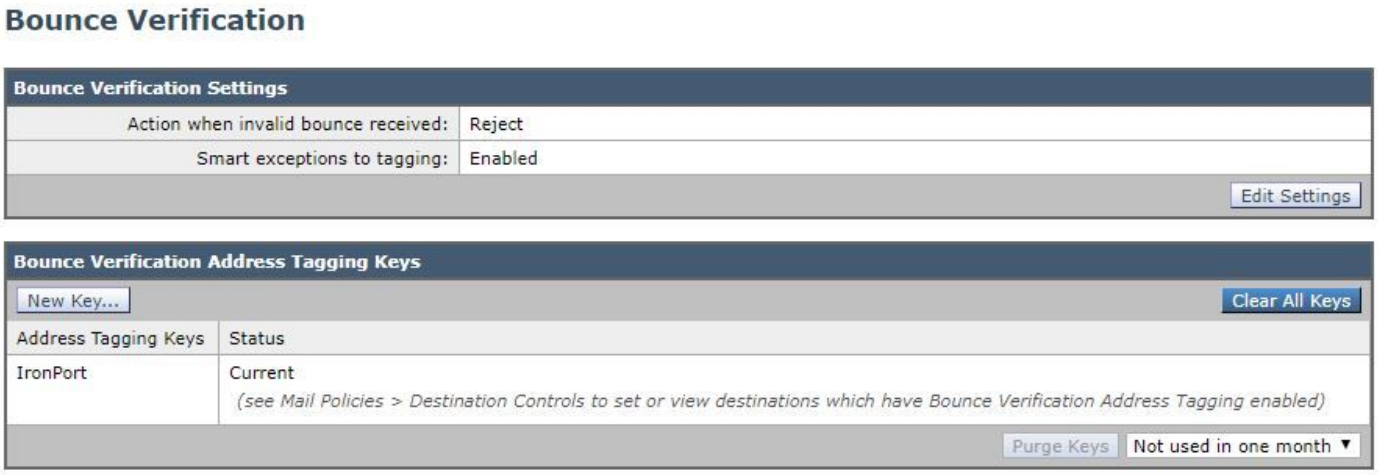
バウンス確認を有効に することは後方散乱/バウンス不正侵入を戦う非常によい方法です。 バウンス確認の後ろの概念は簡単です。 最初に、ESA を去るメッセージの上でマークして下さい。 これが環境に起きたメッセージのバウンスであることを値上げがあればあらゆるバウンス メッセージのその値上げ探されて、意味します。 値上げが抜けている場合、バウンスは詐欺的で、拒否されるか、または廃棄することができます。

たとえば、MAIL FROM: joe@example.com は MAIL FROM: prvs=joe=123ABCDEFG@example.com に書き換えられます。 エンベロープ 送信側に ESA アプライアンスによって送信 されると同時に追加される例の 123…ストリングはバウンス確認 タグです。 メッセージが跳ねる場合、ESA にそれは正当 な跳ねられたメッセージであることを知らせる跳ねられたメッセージのエンベロープ受信者のアドレスはバウンス確認 タグが含まれています。

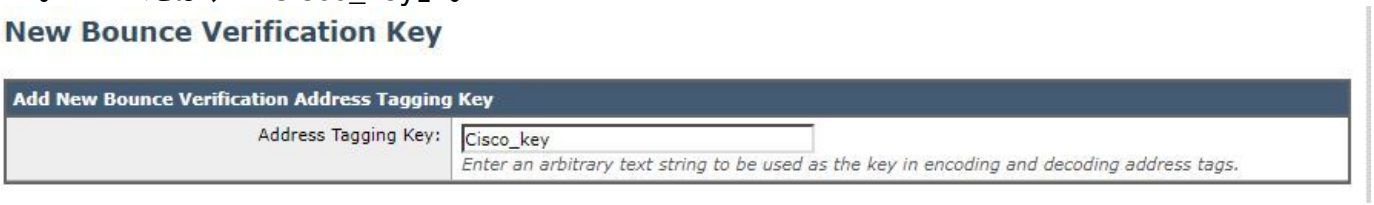
デフォルトではシステム全体でバウンス検証タギングを有効または無効にできます。 特定のドメインに対してバウンス検証タギングを有効または無効にすることもできます。 ほとんどの配備では、それはすべてのドメインのためにデフォルトで有効に なります。

ESA の設定

- **ポリシー > 跳ね上がり確認を郵送し**、『New Key』 をクリック する ナビゲート



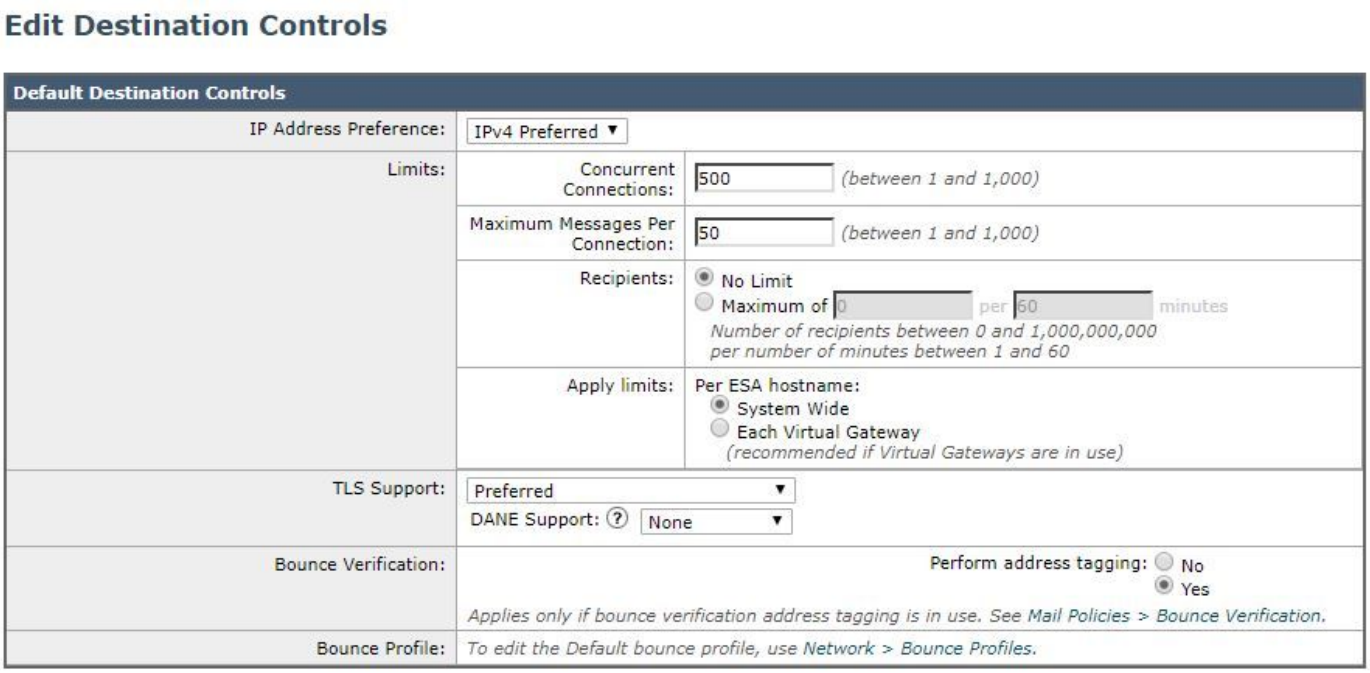
- キーとして使用されるべきエンコードで任意のテキストをデコード アドレス タグ入力すれば。 たとえば、「Cisco_key」。



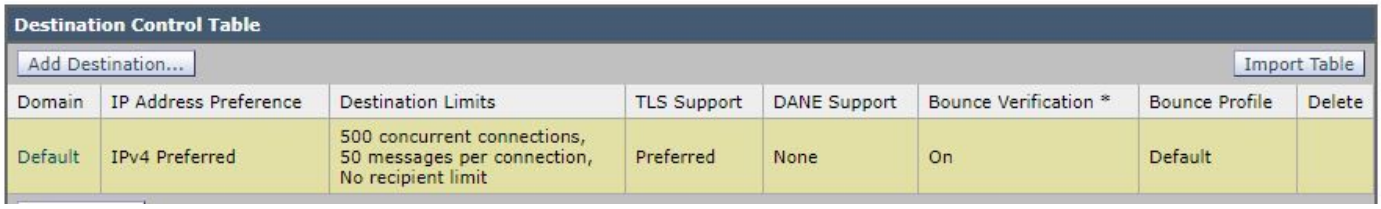
- キーをタグ付けする新しいアドレスを『SUBMIT』 をクリック し、確認して下さい

この場合、「デフォルト」ドメインのバウンス確認を有効に しよう:

- **ポリシー > 宛先制御を郵送し**、**デフォルトを**クリックするためにナビゲート して下さい。
- **バウンス確認を**設定して下さい: **アドレス タグ付けを行って下さい: はい**



- **変更を**『SUBMIT』 をクリック し、**保存して下さい。** バウンス確認がデフォルト ドメイン のため今であることに注目して下さい。



宛先管理テーブルの使用

自由なメール配信は受信者のドメインを圧倒できます。 ESA はアプライアンスが開くまたはアプライアンスが各宛先 ドメインに送るメッセージ数接続の数の定義によってメッセージ デリバリーの完全な制御を与えます。 宛先管理テーブルは接続およびメッセージ レートに ESA がリモート宛先に渡しているとき設定を提供したものです。 それはまたこれらの宛先に TLS の使用を試みるか、または実施するために設定を提供します。 ESA は宛先管理テーブルのためのデフォルト設定で設定されます。

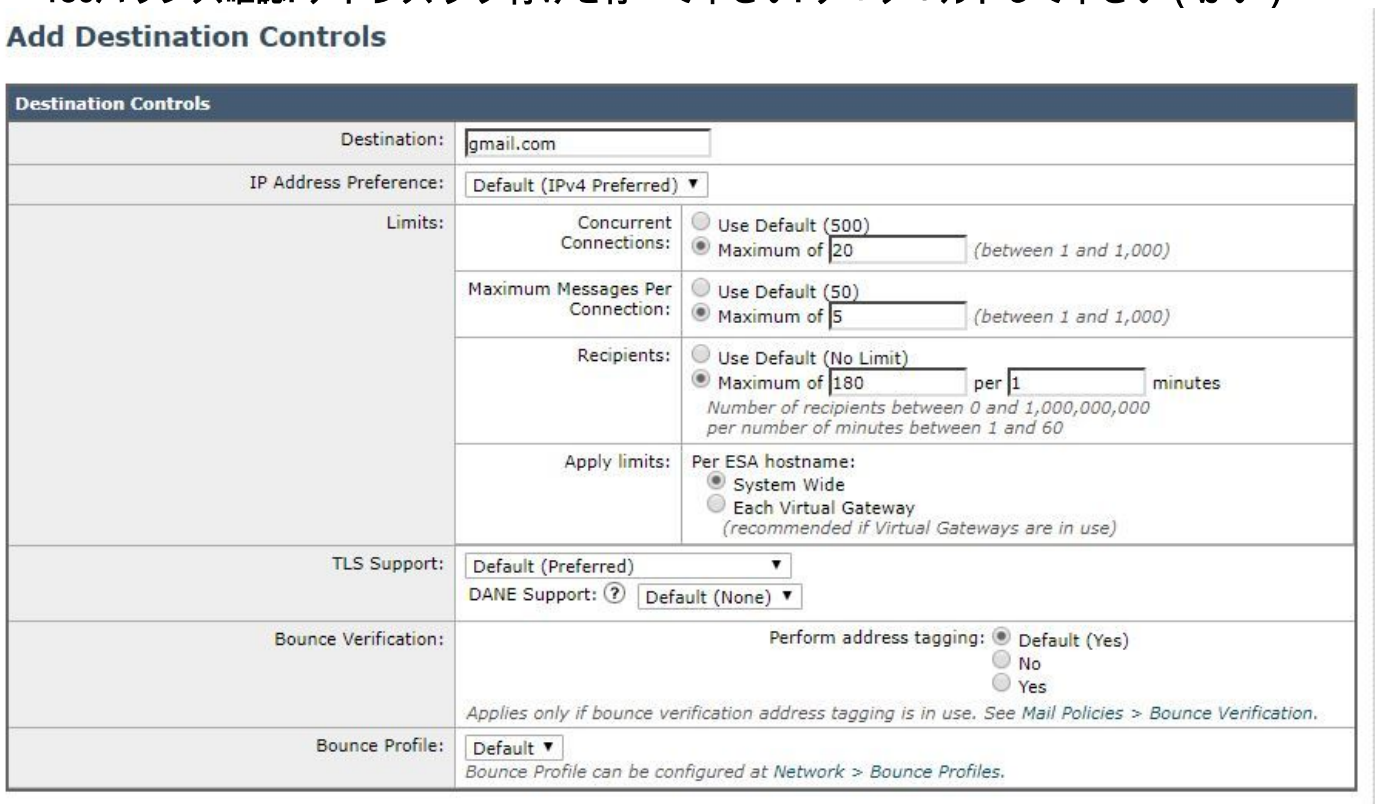
この資料でカバーする何をどのようにデフォルトが範囲の宛先の制御を管理し、設定できるかです。 たとえば言うメッセージが続く必要があるか、または受信者のメールボックスはストレージ制限を余りにすぐに送信 して いることを Gmail ユーザがまたは支持する SMTP 4XX 応答コードを送信 することを危険にさらし、ことを超過しましたことを、Google に受信一組の受信がが支配しますあります。 下記の Gmail 受信者に送られたメッセージの量を制限する宛先管理テーブルに Gmail ドメインを追加します。

宛先管理テーブルに新しいドメインを追加する方法

述べられるように、Google に Gmail に送信 する 送信側用の制限があります。 制限を受け取ることは Gmail 送信側ここに制限によって送達される- https://support.google.com/a/answer/1366776?hl=en を検知 することによって確認することができます

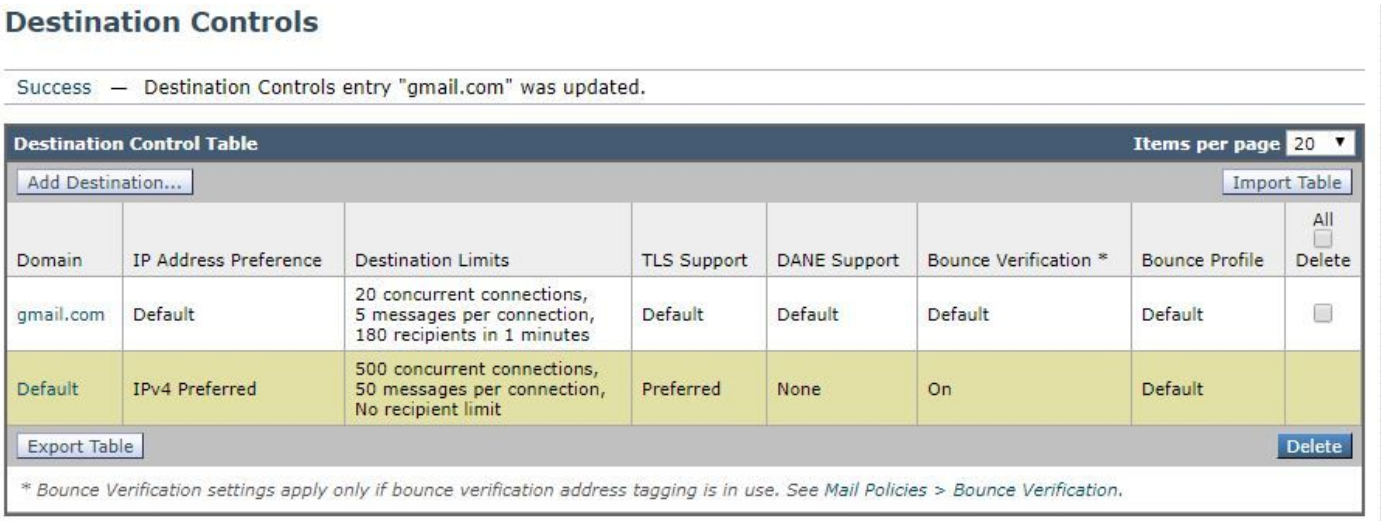
私達をよい隣接ポリシーの一例として Gmail のための宛先 ドメインを設定することを許可して下さい。

- **ポリシー > 宛先制御を郵送し、宛先を『Add』 をクリック し、次のパラメータを使用して新しいプロファイルを作成するナビゲート: Destination： gmail.comIP アドレス プリファレンス: 好まれる IPv4同時接続: 最大 20接続ごとの最大メッセージ: 5受信者: 最大 1 分ごとに 180バウンス確認: アドレス タグ付けを行って下さい: ディフォルトして下さい（ はい ）**



- **変更を**『SUBMIT』 をクリック し、**保存して下さい。** これは宛先管理テーブルがドメインの付加の後でのように見えるものにです。

注「宛先」は制限し、「バウンス確認」は下記のようにイメージで変更します:



展開します指定 Entities（デンマーク人）の SMTP DNS ベース認証を

Entities 指定（デンマーク人）プロトコルの SMTP DNS ベース 認証は DNSサーバでおよび DNS リソースレコード、別名 TLSA レコード設定されるセキュリティ（DNSSEC）拡張を使用して DNS名を用いる X.509 証明書をドメイン ネーム システム（DNS）検証します。

TLSA レコードは認証局（CA）、エンド エンティティー 認証、または RFC 6698 に説明がある DNS名のために使用される信頼アンカーについての詳細が含まれている証明書に追加されます。 ドメイン ネーム システム（DNS） セキュリティ（DNSSEC）拡張機能は DNS で DNS セキュリティの脆弱性を当たることによって追加されたセキュリティを提供します。 暗号化キーおよびデジタル署名を使用して DNSSEC はルックアップ データが正しい確認し、サーバを正当化するためにことを接続します。

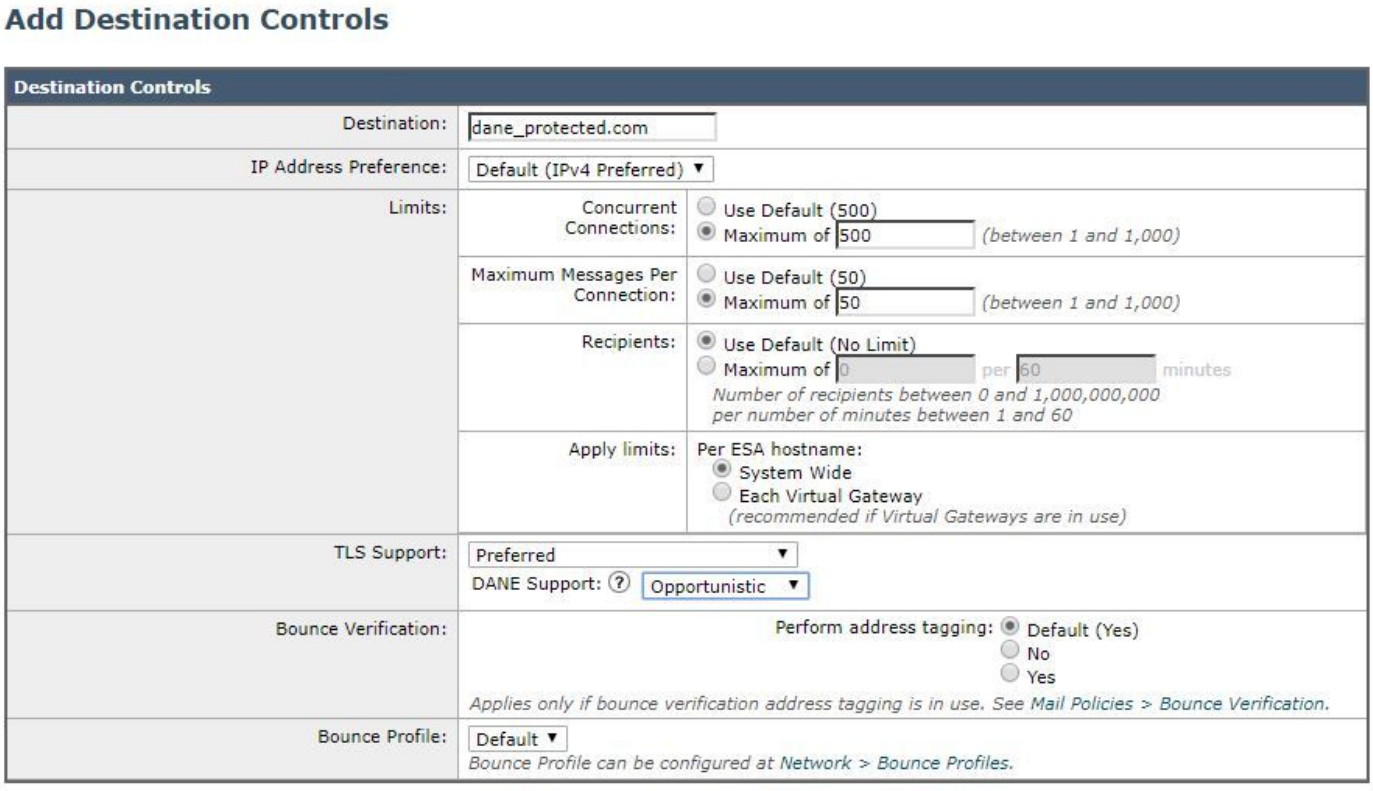
以下は発信 TLS 接続のために SMTP デンマーク人を使用することの利点です:

- マン イン ザ ミドル（MITM）ダウングレード不正侵入提供しま、および不正侵入の毒する DNS キャッシュを盗聴します防ぐことによってメッセージのセキュア配信を。
- DNSSEC によって保護されたとき TLS 証明書および DNS 情報の信頼性を提供します。

ESA の設定

ESA のデンマーク人を設定し始める前に確認されるエンベロープ 送信側および TLSA リソース レコードが DNSSEC であること、そして受信ドメインが保護されるデンマーク人であることを確認して下さい。 CLI コマンドを使用して ESA で **daneverify** これをすることができます。

- **ポリシー > 宛先制御を郵送し、宛先を『Add』 をクリック し、次のパラメータを使用して新しいプロファイルを作成するナビゲート: Destination： dane_protected.comTLS サポート: Preferredデンマーク人サポート:** 日和見主義



- **変更を**『SUBMIT』 をクリック し、**保存して下さい。**