

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=123ABCDEFGH@example.com に書き換えられます。エンベロープ 送信側に ESA アプリケーションによって送信 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

Bounce Verification

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
Edit Settings	

Bounce Verification Address Tagging Keys	
New Key... Clear All Keys	
Address Tagging Keys	Status
IronPort	Current <small>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>
Purge Keys Not used in one month ▼	

- ・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」。

New Bounce Verification Key

Add New Bounce Verification Address Tagging Key	
Address Tagging Key:	<input type="text" value="Cisco_key"/> <small>Enter an arbitrary text string to be used as the key in encoding and decoding address tags.</small>

- ・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

Bounce Verification

Success — New current key added.

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
Edit Settings	

Bounce Verification Address Tagging Keys	
New Key... Clear All Keys	
Address Tagging Keys	Status
Cisco_key	Current <small>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>

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

Edit Destination Controls

Default Destination Controls	
IP Address Preference:	IPv4 Preferred ▼
Limits:	Concurrent Connections: <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> No Limit <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <small>Number of recipients between 0 and 1,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Preferred ▼ DANE Support: <input type="text" value="None"/> ▼
Bounce Verification:	Perform address tagging: <input type="radio"/> No <input checked="" type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	To edit the Default bounce profile, use Network > Bounce Profiles.

- 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。

Destination Control Table							
Add Destination...						Import Table	
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	Delete
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	On	Default	

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.com IP 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: デフォルトして下さい (はい)

Add Destination Controls

Destination Controls	
Destination:	<input type="text" value="gmail.com"/>
IP Address Preference:	<input type="text" value="Default (IPv4 Preferred)"/>
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)
	Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="180"/> per <input type="text" value="1"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	<input type="text" value="Default (Preferred)"/>
	DANE Support: <input type="text" value="Default (None)"/>
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	<input type="text" value="Default"/>
	<small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

- ・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:

Destination Controls

Success — Destination Controls entry "gmail.com" was updated.

Destination Control Table							Items per page 20
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
gmail.com	Default	20 concurrent connections, 5 messages per connection, 180 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	On	Default	

* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

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て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.com` TLS サポート: Preferred
デンマーク人サポート: 日和見主義

Add Destination Controls

Destination Controls	
Destination:	<input type="text" value="dane_protected.com"/>
IP Address Preference:	<input type="text" value="Default (IPv4 Preferred)"/>
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	<input type="text" value="Preferred"/> DANE Support: <input type="text" value="Opportunistic"/>
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	<input type="text" value="Default"/> <small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

- 変更を『SUBMIT』をクリックし、保存して下さい。