

ESA に関する FAQ : ESA でのバウンス検証の設定方法

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[バウンス検証の概要](#)

[ESA でのバウンス検証の設定方法](#)

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス上にバウンス検証を設定する方法を説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco ESA
- AsyncOS

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco ESA、すべての AsyncOS バージョン

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

このセクションでは、ESA でのタギングおよびバウンス検証の概要を説明します。

バウンス検証の概要

バウンス検証を有効にした状態で電子メールを送信すると、ESA がメッセージ内のエンベロープ送信者アドレスを書き換えます。たとえば、**MAIL FROM: joe@example.com** は **MAIL FROM: prvs=joe=123ABCDEFGF@example.com** に書き換えられます。この例の 123... という文字列が、アプライアンスによって電子メールが送信されるときに [Envelope Sender] に追加されたバウンス検証タグです。メッセージがバウンスする場合、通常は、バウンスのエンベロープ受信者アドレスにバウンス検証タグが追加されます。

注: 詳細については、『**Advanced User Guide**』の「**Configuring Bounce Verification Address Tagging Keys**」セクションを参照してください。

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。通常は、デフォルトで有効にしておき、除外する具体的なドメインを [Destination Controls] テーブルに列挙するという方法をとります。

コンテンツ セキュリティ アプライアンスが、すでにタグ付きアドレスが含まれるバウンスメッセージを緩衝地帯 (DMZ) 内の別のコンテンツ セキュリティ アプライアンスに配信する場合、AsyncOS は別のタグを追加しません。

注意: バウンス検証を有効にした場合、[Envelope Sender] がブランクの状態でメールが送信されると、正当なメールでもアプライアンスによって拒否される可能性があります。

ESA でのバウンス検証の設定方法

ESA でバウンス検証を設定するには、次の手順に従います。

1. [Mail Policies] > [Bounce Verification] に移動し、ランダムに選択した数字と文字 (例 : 4r5t6y7u) からなるタギング キーを手動で入力します。

2. バウンス検証設定を編集します。

[Mail Policies] > [Destination Controls] に移動し、バウンス検証を有効にします。

[Domain] フィールドで [Default] を選択します (または、カスタム宛先を選択します)。

[Default] ウィンドウが開き、[Bounce Verification] セクションが表示されたら、[Yes] をクリックします。

3. タグなし (誤った) バウンスがブロックされることを確認します。

[Mail Policies] > [Mail Flow Policies] に移動します。

適切なポリシーを選択し、[Security Features] セクションを見つけます。

[Evaluate Untagged Bounces] の値が [No] に設定されていることを確認します。AsyncOS の以前のバージョンでは、[Evaluate Untagged Bounces] の値が [No] に設定されているはずで
す。