ESA はバウンス（NDR）嵐を経験します

目次

概要

この資料は E メール セキュリティ アプライアンス（ESA）がバウンス嵐を経験し、問題にソリューションを提供するところで直面する問題を記述したものです。

背景説明

バウンス嵐は電子メール スパムのジョー ジョブまたは後方散乱の副次的影響です。

ジョー ジョブ

スプーフィングされた送信側 データを使用し、明白な送信側の評判を変色させることをおよび/または受信者を明白な送信側に対して処置をとるために誘導することを向けるジョー ジョブはスパム 攻撃です。

後方散乱

後方散乱が電子メール スパム、ウイルスおよびワームの副次的影響善意の当事者にスパムおよび他のメール送信バウンス メッセージを受け取る電子メールサーバである。 これは対象の eメールアドレスが含まれているために元のメッセージ エンベロープ 送信側は造られるので発生します。これらのメッセージが受信者によって懇請されなかったし、互いに大幅に類似したで、バルク数量で渡されるので、ように非要請バルク電子メールかスパム修飾します。 そのように、電子メール後方散乱を生成するシステムはさまざまなドメイン ネーム システム ブラックリスト（DNSBLs）でリストされるようになり、インターネットサービスプロバイダー年期に違反してある場合もあります。

問題

ESA は ESA にインジェクトされるメッセージの大洪水があるバウンス嵐を経験します。 そのような攻撃の間の着信接続数スパイク。 アプライアンスは workqueue バックアップを開発するかもしれません。 アプライアンスがそのような攻撃に応じてあるかどうか確認するため、メールがアドレス**から**のメールのために記録 するグレップ。 バウンス（未配達レポート- NDRs に）アドレス**から**の空エンベロープ メールがあります。

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

バウンス嵐に応じてあるアプライアンスに「<>」のアドレス**から**のエンベロープ メールのメッセージの大半があります。

解決策

バウンス嵐を管理するいくつかのオプションがあります。

バウンス確認

これらの誤った方向に導かれたバウンス不正侵入を戦うために、AsyncOS は Cisco バウンス確認が含まれています。 有効に されたとき、この機能は ESA によって送信 される メッセージのためのエンベロープ 送信側 アドレスをタグ付けします。 ESA によって受け取ったこのタグの存在があるようにあらゆるバウンス メッセージのためのエンベロープ受信者はそれから確認されます。 正当 なバウンス メッセージが受け取られるとき、タグ アドレスが取除かれるおよびバウンスは受信者に提供されますエンベロープ 送信側に追加された。 タグが含まれていないバウンス メッセージは別々に処理することができます。

AsyncOS はバウンスをようにアドレス（<>）**から**ヌル メールのメール考慮します。 mailer-daemon@example.com または postmaster@example.com のようなアドレスからあるメッセージはシステムによってバウンスとはみなされないし、バウンス確認に応じてありません。

キーをタグ付けするバウンス確認 アドレスを設定して下さい

キー リストをタグ付けするバウンス確認 アドレスは unpurged 電流 キーおよびあらゆる以前使用したキー入力することを示します。 New 鍵を追加するために、これらのステップを完了して下さい:

1. **メール ポリシー > 跳ね上がり確認** ページで、『New Key』 をクリック して下さい。
2. 文字列を入力し、『SUBMIT』 をクリック して下さい。
3. 変更を保存します。

キーの削除

プルダウン メニューからの削除にルールを選択し、『Purge』 をクリック すればキーをタグ付けする古いアドレスを削除できます。

Cisco バウンス確認設定を設定して下さい

バウンス確認設定は無効 なバウンスが受け取られるとき奪取 するかどの操作判別します。

- **メール ポリシー > バウンス確認を**選択して下さい。
- Edit Settings をクリックします。
- 無効 なバウンスを拒否するか、またはメッセージにカスタム ヘッダーを付加するためにかどうか選択して下さい。 ヘッダを付加したいと思う場合ヘッダー名および値を入力して下さい。
- 任意で、スマートな例外を有効に して下さい。 この設定は (単一リスナーが両方のために着信 および 発信メール使用される時でさえ) 自動的にバウンス確認処理から免除されるべき内部メールサーバによって生成される着信メール メッセージおよびバウンス メッセージを可能にします。
- 変更を送信し、確定します。

CLI で Cisco バウンス確認を設定して下さい

CLI でバウンス確認を設定するために **bvconfig** および **destconfig** コマンドを使用できます。 これらのコマンドは Cisco AsyncOS CLI レファレンスガイドで説明されています。

Cisco バウンス確認およびクラスタ設定

バウンス確認はクラスタ設定で Cisco アプライアンスが両方とも同じ「バウンス キーを」。使用する限りはたらきます 同じキーを使用するとき、どちらかのシステムは正当 な bounceback を受け入れられますはずです。 修正されたヘッダ タグ/キーは Cisco 各アプライアンスに特定ではないです。

メール フィルタ

受信および配信のために別々のアプライアンスを使用するのでバウンス確認を使用できなければ、アドレス**からの**空メールがあるメッセージをブロックするためにメッセージ フィルターを設定できます。

メール ブロック

これらのバウンス メッセージに多分非存在エンベロープ受信者のアドレスがあるので下部のを助ける、メッセージ交換 Lightweight Directory Access Protocol （LDAP）受信者の検証によって無効アドレスそのようなメッセージの影響ことができます。