ESA でバウンス（NDR）ストームが発生

内容

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)でバウンスストームが発生する問題とその解決策について説明します。

背景説明

バウンスストームは、ジョーの仕事や電子メールスパムの後方散乱の副作用です。

ジョー・ジョブ

joeジョブは、スプーフィングされた送信者データを使用するスパム攻撃であり、見かけの送信者の評判を悪化させ、受信者に見かけの送信者に対するアクションを実行するよう促すことを目的としています。

後方散乱

バックスキャッタは、スパム、ウイルス、およびワームの副作用で、スパムやその他のメールを受信した電子メールサーバがバウンスメッセージを送信します。これは、元のメッセージエンベロープ送信者が、被害者の電子メールアドレスを含むように偽造されているためです。これらのメッセージは受信者によって要請されず、互いに実質的に類似し、大量に配信されるため、未承諾のバルクメールまたはスパムとして認定されます。したがって、電子メールのバックスキャッタ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(DNS)ブラックリスト(DNSBL)にリストされ、インターネットサービスプロバイダーのサービス規約に違反する可能性があります。

問題

ESAに大量のメッセージが挿入されるバウンスストームが発生します。このような攻撃中に、着信接続カウントが急増します。アプライアンスがワークキューバックアップを作成する場合があります。アプライアンスがこのような攻撃を受けているかどうかを確認するには、メールログでメールの送信元アドレスをgrepします。バウンス(Non-Delivery Reports - NDR)には空のエンベロープメールの送信元アドレスが設定されます。

```
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: <>
```

バウンスストームの影響を受けるアプライアンスでは、エンベロープメールの大部分がFrom addressが'<>'になります。

解決方法

バウンスストームを管理するためのオプションが多数あります。

バウンス検証

これらの誤った方向のバウンス攻撃に対処するために、AsyncOSにはシスコバウンス検証が含まれています。 この機能を有効にすると、ESA経由で送信されたメッセージのエンベロープ送信者アドレスにタグが付けられます。次に、ESAが受信したすべてのバウンスメッセージのエンベロープ受信者が、このタグの存在を確認します。正当なバウンスメッセージが受信されると、エンベロープ送信者アドレスに追加されたタグが削除され、バウンスが受信者に配信されます。タグを含まないバウンスメッセージは別々に処理できます。

AsyncOSは、バウンスをヌルメールの送信元アドレス(<>)を持つメールと見なします。 mailer-daemon@example.comやpostmaster@example.comなどのアドレスからのメッセージは、システムによるバウンスとは見なされず、バウンス検証の対象になりません。

バウンス検証アドレスのタギングキーの設定

[バウンス検証アドレスのタギングキー(Bounce Verification Address Tagging Keys)]リストには、現在のキーと、過去に使用したパージされていないキーが表示されます。新しいキーを追加するには、次の手順を実行します。

1. の **メールポリシー** > **バウンス検証** ページで、[新しいキー]をクリックします。
2. テキスト文字列を入力し、 **Submit**.
3. 変更を保存します。

キーの消去

プルダウンメニューからパージのルールを選択し、[パージ(Purge)]をクリックすると、古いアドレスのタギングキーをパージできます。

シスコバウンス検証設定の設定

バウンス検証設定は、無効なバウンスを受信したときに実行するアクションを決定します。

- 選択 **メールポリシー** > **バウンス検証**.
- クリック **設定の編集**.
- 無効なバウンスを拒否するか、メッセージにカスタムヘッダーを追加するかを選択します。ヘッダーを追加する場合は、ヘッダー名と値を入力します。
- オプションで、スマート例外を有効にします。この設定を使用すると、内部メールサーバによって生成された受信メールメッセージおよびバウンスメッセージを、受信メールと送信メールの両方に単一のリスナーを使用した場合でも、自動的にバウンス検証処理から除外できます。
- 変更を送信し、確定します。

CLIによるシスコバウンス検証の設定

バウンス検証を設定するには、CLIで**bvconfig**および**destconfig**コマンドを使用できます。これらのコマンドについては、『Cisco AsyncOS CLIリファレンスガイド』を参照してください。

Cisco Bounce Verificationおよびクラスタ設定

バウンス検証は、両方のシスコアプライアンスが同じ「バウンスキー」を使用している限り、クラスタ構成で動作します。 同じキーを使用する場合、どちらのシステムも正当なバウンスバックを受け入れられるはずです。変更されたヘッダータグ/キーは、各シスコアプライアンスに固有のものではありません。

メールフィルタ

受信用と配信用に別々のアプライアンスを使用しているためにバウンス検証を使用できない場合は、メッセージフィルタを設定して、空のメールの送信元アドレスを持つメッセージをブロックできます。

メールブロック

これらのバウンスメッセージにはエンベロープ受信者のアドレスが存在する可能性が高いため、Lightweight Directory Access Protocol(LDAP)受信者の検証を使用して無効なアドレスをブロックすることで、これらのメッセージの影響を軽減できます。