ESA の電子メール暗号化の設定例

目次

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）で電子メール暗号化をセットアップする方法について説明します。

前提条件

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Model: すべての C シリーズおよび X シリーズ
- エンベロープ暗号化（PostX）機能がインストール済み

設定

ESA で電子メール暗号化を有効にする

GUI から次の手順を実行します。

1. [Security Services] の下で、[Cisco IronPort Email Encryption] > [Enable Email Encryption] を選択して [Edit Settings] をクリックします。

2. 新しい暗号化プロファイルを作成するために [Add Encryption Profile] をクリックします。

3. [Key Service Type] として [Cisco Registered Envelope Service] または [Cisco IronPort Encryption Appliance]（暗号化アプライアンスを購入した場合）を選択します。

4. [Submit] をクリックし、変更を確定します。

5. 暗号化プロファイルが作成された後、オプションで、それを Cisco Registered Envelope Service（CRES）サーバにプロビジョニングできます。 新しいプロファイルの横に [Provision] ボタンが表示されます。 [**Provision**] をクリックします。

送信コンテンツ フィルタの作成

暗号化プロファイルを実装するための送信コンテンツ フィルタを作成するには、GUI から次の手順を行います。 以下の例では、送信メッセージの件名ヘッダーに「Secure:」という文字列が含まれる場合に、フィルタによって暗号化が トリガーされます。

1. [Mail Policies] の下で、[Outgoing Content Filters] を選択して [Add Filter] をクリックします。

2. 新しいフィルタを追加し、件名ヘッダーの条件を subject == "Secure: "、アクションを「Encrypt and Deliver Now (Final Action)」に設定します。 [Submit] をクリックします。

3. [Mail Policies] の下で [Outgoing Mail Policies] を選択し、デフォルト メール ポリシーまたは適切なメール ポリシーでこの新しいフィルタを有効にします。

4. 変更を確定します。

確認

ここでは、暗号化が機能していることを検証する方法について説明します。

1. 検証するには、件名に「**Secure:**」を使って新しいメールを生成し、 Web アカウント（Hotmail、Yahoo、Gmail）に電子メールを送信して、暗号化されるかどうか判別します。

2. 次の項の説明に従ってメール ログを調べることで、送信コンテンツ フィルタによりメッセージが暗号化されることを確認します。

Mail_logs での暗号化フィルタ処理の検証

これらの mail_log エントリは、Encrypt_Message という暗号化フィルタにメッセージが一致したことを示します。

```
Wed Oct 22 17:06:46 2008 Info: MID 116 was generated based on MID 115 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:07:22 2008 Info: MID 118 was generated based on MID 117 by encrypt
filter 'Encrypt_Message'
Wed Oct 22 17:31:21 2008 Info: MID 120 was generated based on MID 119 by encrypt
filter ''Encrypt_Message
```

この項で示すようにログから情報を集めるために **grep** または **findevent** コマンドを使用する方法については、「ESA メッセージ破棄の判別」の説明を参照してください。

トラブルシューティング

暗号化フィルタがトリガーされない場合、テスト メッセージで使われるメール ポリシーのメール ログを調べてください。 このメール ポリシーでフィルタが有効になっていること、および [Skip Remaining Content Filters] アクションを含む先行フィルタがこのポリシーに存在しないことを確認します。

コンテンツ フィルタを介して暗号化をトリガーするために、メッセージ トラッキング内のメッセージで正しい文字列または指定された件名タギングが使われていることを確認します。