TLS暗号化を使用したCRESセキュア暗号化サービスのメッセージ応答の設定

内容

はじめに

このドキュメントでは、セキュアエンベロープの添付ファイルの代わりにCRES着信セキュア応答のTLS暗号化を設定するアクションについて説明します。

Cisco RES:TLSを使用して暗号化されていないRES応答を保護する方法

デフォルトでは、セキュリティ保護された電子メールへの返信はCisco RESによって暗号化され、メールゲートウェイに送信されます。その後、エンドユーザがCisco RESクレデンシャルで開けるように暗号化されたメールサーバにパススルーします。

Cisco RESのセキュアメッセージ応答を開くときにユーザ認証が不要になるように、Cisco RESは「暗号化されていない」形式で、Transport Layer Security(TLS)をサポートするメールゲートウェイに配信します。 ほとんどの場合、メールゲートウェイはCisco Eメールセキュリティアプライアンス(ESA)であり、この記事が適用されます。

ただし、外部スパムフィルタなど、ESAの前に別のメールゲートウェイがある場合は、ESAで証明書/TLS/メールフロー設定を行う必要はありません。この場合、このドキュメントの「ソリューション」セクションのステップ1 ~ 3は省略できます。この環境で暗号化されていない応答が動作するには、TLSをサポートする必要があるアプライアンスが外部スパムフィルタ（メールゲートウェイ）になります。TLSがサポートされている場合は、Cisco RESに確認してもらい、セキュリティで保護された電子メールに対する「暗号化されていない」応答を設定できます。

送信者ポリシーフレームワーク

Sender Policy Framework(SPF)検証エラーを回避するには、SPFレコードに次の値を追加します。

Cisco Registered Envelope Service(CRES)のSPFレコード値が、このテーブルのIP/ホスト名「Hostnames and IP Addresses」と一致しています。

シスコが提供するSPFメカニズムを使用した出力は次のとおりです。

<#root>

```
~ dig txt

res.cisco.com

 +short
"v=spf1

mx:res.cisco.com


exists:%{i}.spf.res.cisco.com

 -all"
```

既存のSPFレコードに次のメカニズムを追加します。

<#root>

```
include:res.cisco.com
```

新しいres.cisco.comメカニズムを含むFAKE/test SPFレコードの例：

<#root>

```
"v=spf1 mx:sampleorg1.com ip4:1.2.3.4

include:res.cisco.com

 -all"
```

SPFレコードにCisco RESを追加する場所と方法は、ネットワークトポロジ内でのドメインネームシステム(DNS)の実装方法によって異なります。詳細については、DNS管理者に問い合わせてください。

DNSがCisco RESを含めるように設定されていない場合、セキュアな作成およびセキュアな応答が生成され、ホストされたキーサーバを介して配信されると、発信IPアドレスが受信者の末尾にリストされたIPアドレスと一致しないため、SPF検証が失敗します。

ホスト名とIPアドレス

ホスト名	IP アドレス	レコード タイプ
res.cisco.com	184.94.241.74	A
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	A
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX

注：ホスト名とIPアドレスは、サービス/ネットワークメンテナンスまたはサービス/ネットワークの拡張に基づいて変更されることがあります。すべてのホスト名とIPアドレスをサービスに使用するとは限らない。ここでは参考のために説明します。

解決方法

- ESAで署名付き証明書と中間証明書を取得してインストールします。

> 注：アプライアンスに付属のデモ証明書によってCRES検証プロセスが失敗するため、署名機関から中間証明書を取得する必要があります。

- 新しいメールフローポリシーを作成します。
  a. GUIで、を選択しMail Policies > Mail Flow Policies > Add Policyます。

    - 名前を入力し、「セキュリティ機能： TLS」以外はすべてデフォルトのままにします。これを**Required**に設定します。

- 新しい送信者グループを作成します。

  a. GUIで、を選択しMail Policies > HAT Overview > Add Sender Groupます。

    - 名前を入力し、注文番号を#1に設定します。オプションのコメントを入力することもできます。ステップ2で作成したメールフローポリシーを選択します。他はすべて空白のままにします。

    - andをクリックSubmit しますAdd Senders。

- Senderフィールドに、次のIP範囲とホスト名を入力します。

```
.res.cisco.com
.cres.iphmx.com
208.90.57.0/26 (current CRES IP network range)
204.15.81.0/26 (old CRES IP network range)
```

-

変更を送信し、保存します。

- ESAがCisco RESサーバからTLS暗号化をネゴシエートする準備ができていると確信できたら、CRES管理ポータル内の手順を実行します。[ドメインがCisco RESでTLSをサポートしているかどうかをテストするにはどうすればよいですか。]

関連情報

- Cisco RES：キーサーバのIPアドレスとホスト名
- Cisco E メール セキュリティ アプライアンス：エンドユーザ ガイド
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。