CRES FAQ： TLS を使用して非暗号化 CRES 返信を保護する方法

目次

概要

この資料に Cisco E メール セキュリティ アプライアンス（ESA）と共同して Cisco Registered Envelope Service （CRES）、ユーザがそれらを復号化する必要はないことを可能にするからの応答を保護するのに Transport Layer Security （TLS）を使用する方法を記述されています。

TLS を使用して非暗号化 CRES 返信を保護する方法

デフォルトで、セキュア メールへの応答は CRES によって暗号化され、メールゲートウェイに送られます。 それらそして CRES 資格情報と開くためにエンドユーザ用の暗号化されるメールサーバへのパススルー。

ユーザ向けの必要を避けるために CRES は TLS をサポートするメールゲートウェイに「非暗号化」形式でセキュア応答を開発するために CRES と認証する渡します。 ほとんどの場合メールゲートウェイは ESA であり、この技術情報は適用します。

ただし外部スパム フィルタのような ESA の前に坐るもう一つのメールゲートウェイがあれば、そこに certificate/TLS/mail フロー設定のための必要が ESA のありません。 この場合、この資料の Solution セクションのステップ 1 に 3 をスキップできます。 この環境ではたらく非暗号化応答に関しては外部スパム フィルタ（メールゲートウェイ）は TLS をサポートする必要があるアプライアンスです。 それらが TLS をサポートする場合、CRES をこれを確認し、メールを保護するために「非暗号化」応答のために設定されて得てもらうことができます。

送信側 政策の枠組

送信側 政策の枠組（SPF）確認失敗を防ぐために、mx を追加して下さい: SPF レコードへの res.cisco.com、mxnat1.res.cisco.com および mxnat3.res.cisco.com。

SPF レコードに CRES を追加するかどこで、どのようにドメイン ネーム システム（DNS）がネットワーク トポロジで設定されるかによって決まります。 詳細については DNS 管理者に連絡して下さい。

CRES を含むために DNS が設定されない場合セキュア場合の応答を生成されます構成し、保護すればホストされたキー サーバを通って渡されて、発信 IP アドレスは SPF 確認失敗に終って受信者でリストされた IP アドレスを終了します、一致する。

ホスト名および IP アドレス

[hostname]	IP アドレス	レコード タイプ
res.cisco.com	184.94.241.74	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
---- ---- ----	---- ---- ----	---- ---- ----
mxnat1.res.cisco.com	208.90.57.32	A
mxnat3.res.cisco.com	184.94.241.96	A

ホスト名および IP アドレスはサービス/ネットワークメンテナンスに基づいて変更に応じてあり、保守しましたり/ネットワーク拡大。

解決策

1. ESA で署名入り認証および中間物証明書を得、インストールして下さい。 **注:** それはアプライアンスに失敗するために引き起こす CRES 確認プロセスを来るデモ 証明書として重要得ます署名 権限からの中間証明書をです。
2. 新しいメール フロー ポリシーを作成して下さい: GUI から、選択して下さい **Mail ポリシー > Mail フロー ポリシー > Add ポリシーを...**名前を入力し、デフォルトで*セキュリティ機能*を除いてすべてを残して下さい*: TLS.* **必須**にこれを設定 して下さい。
3. 新しい送信側 グループを作成して下さい: GUI から、選択して下さい **Mail ポリシー > 帽子概要 > Add 送信側 グループを...**#1 に名前および一定注文番号を入力して下さい。 またコメントを入力することができます。 ステップ 2.許可で他のすべてをブランク作成したメール フロー ポリシーを選択して下さい。**送信側を >>** 『SUBMIT』 をクリック し、**追加して下さい**。
4. 送信側 フィールドでは、これらの IP 範囲およびホスト名を入力して下さい:
   ```
   .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)
   ```
5. 変更を送信し、保存します。
6. 確信していた後 ESA は CRES サーバからの TLS のドメインが CRES の TLS をサポートする場合 I テストがどのようにのか、従いますステップに準備をされますか。 CRES サーバを TLS を使用し始めるように要求するため。

関連情報

- ESA に関する FAQ： CRES キー サーバの IP とホスト名
- Cisco 電子メール 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