ESAでのDKIM署名の設定

内容

はじめに

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DomainKeys Identified Mail(DKIM)署名を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Eメールセキュリティアプライアンス(ESA)アクセス
- TXTレコードを追加または削除するためのDNS編集アクセス。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

DKIM署名がオフになっていることを確認します。

すべてのメールフローポリシーでDKIM署名がオフになっていることを確認する必要があります。これにより、メールフローに影響を与えずにDKIM署名を設定できます。

1. Mail Policies > Mail Flow Policiesに移動します。
2. 各メールフローポリシーに移動し、Domain Key/DKIM SigningがOffに設定されていることを確認します。

DKIM署名キーの作成

ESAで新しいDKIM署名キーを作成する必要があります。

1. Mail Policies > Signing Keys の順に移動し、Add Key...を選択します。
2. DKIMキーに名前を付け、新しい秘密キーを生成するか、現在のキーに貼り付けます。

> 注：ほとんどの場合、2048ビットの秘密キーのサイズを選択することをお勧めします。

3. 変更を保存します。

新しいDKIM署名プロファイルを生成し、DNSレコードをDNSに発行する

次に、新しいDKIM署名プロファイルを作成し、そのDKIM署名プロファイルからDKIM DNSレコードを生成し、そのレコードをDNSに発行する必要があります。

1. Mail Policies > Signing Profilesの順に移動し、Add Profileをクリックします。
    1. Profile Nameフィールドに、プロファイルをわかりやすい名前で指定します。
    2. Domain Nameフィールドにドメインを入力します。
    3. Selectorフィールドに新しいセレクタ文字列を入力します。

    > 注：セレクタは、特定のドメインに対して複数のDKIM DNSレコードを許可するために使用される任意の文字列です。

    4. フィールドSigning Keyの前のセクションで作成したDKIM署名キーを選択します。
    5. [Submit] をクリックします。
2. ここから、作成した署名プロファイルのDNSテキストレコード列の生成をクリックし、生成されたDNSレコードをコピーします。これは次のようになります。

```
selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMa
```

3. 変更を保存します。
4. ステップ2のDKIM DNS TXTレコードをDNSに送信します。
5. DKIM DNS TXTレコードが完全に伝播されるまで待ちます。
6. Mail Policies > Signing Profilesの順に移動します。
7. Test Profile列で、新しいDKIM署名プロファイルのTestをクリックします。テストが成功し

たら、このガイドに進みます。そうでない場合は、DKIM DNS TXTレコードが完全に伝播されていることを確認します。

DKIMのサインオン

ESAがDKIM署名メッセージに設定されたので、DKIM署名をオンにします。

1. [Mail Policies] > [Mail Flow Policies] に移動します。
2. Connection BehaviorがRelayに設定されている各メールフローポリシーに移動し、Domain Key/DKIM SigningをOnにします。

注：デフォルトでは、Connection BehaviorがRelayの唯一のメールフローポリシーは、Relayedと呼ばれるメールフローポリシーです。発信メッセージがDKIM署名メッセージのみであることを確認する必要があります。

---

3. 変更を保存します。

DKIMに合格したことを確認するメールフローのテスト

この時点で、DKIMが設定されます。ただし、DKIM署名をテストして、発信メッセージに想定どおりに署名し、DKIM検証に合格していることを確認する必要があります。

1. ESAを介してメッセージを送信し、ESAによって署名されたDKIMと別のホストによって検証されたDKIMを受け取ることを確認します。
2. もう一方の端でメッセージを受信したら、メッセージのヘッダーでAuthentication-Resultsヘッダーを確認します。ヘッダーのDKIMセクションを探して、DKIM検証に合格したかどうかを確認します。ヘッダーは次の例のようになります。
   <#root>

```
Authentication-Results: mx1.domainsite; spf=SoftFail smtp.mailfrom=user1@domainsite;

dkim=pass

 header.i=none; dmarc=fail (p=none dis=none) d=domainsite
```

3. ヘッダー「DKIM-Signature」を探し、正しいセレクタとドメインが使用されていることを確認します。

   <#root>

```
DKIM-Signature: a=rsa-sha256;

d=domainsite

;

s=selector2

;
   c=simple; q=dns/txt; i=@domainsite;
   t=1117574938; x=1118006938;
   h=from:to:subject:date;
```

```
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
          VoG4ZHRNiYzR
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング方法はありません。

関連情報

- シスコのテクニカルサポートとダウンロード

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。