在ESA上配置DKIM簽名

目錄

簡介

本文描述如何在電子郵件安全裝置(ESA)上配置DomainKeys Identified Mail(DKIM)簽名。

必要條件

需求

思科建議您瞭解以下主題：

- 電子郵件安全裝置(ESA)訪問。
- 新增/刪除TXT記錄的DNS編輯訪問許可權。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

確保DKIM簽名已關閉

您需要確保在所有郵件流策略中關閉DKIM簽名。這樣可讓您配置DKIM簽名，而不會影響郵件流：

1. 導航到Mail Policies > Mail Flow Policies。
2. 導航到每個郵件流策略，並確保域金鑰/DKIM簽名設定為關閉。

建立DKIM簽名金鑰

您需要在ESA上建立新的DKIM簽名金鑰：

1. 導航到郵件策略>簽名金鑰，然後選擇新增金鑰.....
2. 為DKIM密鑰命名，並生成新的私鑰或貼上到當前金鑰中。

> 註：在大多數情況下，建議您選擇2048位私鑰大小。

3. 提交更改。

生成新的DKIM簽名配置檔案並將DNS記錄發佈到DNS

接下來，您需要建立新的DKIM簽名配置檔案，從該DKIM簽名配置檔案生成DKIM DNS記錄並將該記錄發佈到DNS:

1. 導航到Mail Policies > Signing Profiles，然後點選Add Profile。
    1. 在Profile Name欄位中為配置檔案指定描述性名稱。
    2. 在Domain Name欄位中輸入您的域。
    3. 在Selector欄位中輸入新的選擇器字串。

    > 注意：選擇器是一個任意字串，用於允許給定域的多個DKIM DNS記錄。

    4. 在Signing Key欄位中選擇在上一部分中建立的DKIM簽名金鑰。
    5. 按一下「Submit」。
2. 在此處，針對您剛剛建立的簽名配置檔案，按一下DNS文本記錄列中的生成，然後複製生成的DNS記錄。其外觀必須類似於以下內容：

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

3. 提交更改。
4. 將步驟2中的DKIM DNS TXT記錄提交到DNS。
5. 等待，直到DKIM DNS TXT記錄已完全傳播。
6. 轉到郵件策略>簽名配置檔案。
7. 在Test Profile列下，按一下新DKIM簽名配置檔案的Test。如果測試成功，請繼續本指南。如果不是，請確認DKIM DNS TXT記錄已完全傳播。

啟用DKIM簽名

現在，ESA已配置為DKIM簽名郵件，我們可以啟用DKIM簽名：

1. 導航到Mail Policies > Mail Flow Policies。
2. 轉到具有中繼的連線行為的每個郵件流策略，並將域金鑰/DKIM Signing設定為On。

> 注意：預設情況下，唯一具有Connection BehaviorRelay的郵件流策略是名為Relayed的

郵件流策略。您需要確保只有DKIM簽名郵件是出站郵件。

3. 提交更改。

測試郵件流以確認DKIM通過

此時，DKIM已配置。但是，您需要測試DKIM簽名，以確保它按預期對出站郵件進行簽名，並且通過DKIM驗證：

1. 通過ESA傳送消息，並確保其獲得ESA簽名的DKIM以及另一台主機驗證的DKIM。
2. 在另一端收到消息後，檢查消息的報頭中是否存在報頭Authentication-Results。查詢標頭的DKIM部分以確認它是否通過DKIM驗證。標頭必須類似於以下示例：
   <#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. 查詢標頭「DKIM-Signature」，並確認使用了正確的選擇器和域：

   <#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
   ```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前沒有針對此組態進行疑難排解的特定方法。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。