Configurer la signature DKIM sur ESA

Table des matières

Introduction

Ce document décrit comment configurer la signature DKIM (DomainKeys Identified Mail) sur un appareil de sécurité de la messagerie (ESA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès ESA (Email Security Appliance).
- Accès de modification DNS pour ajouter/supprimer des enregistrements TXT.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Vérifiez que la signature DKIM est désactivée

Vous devez vous assurer que la signature DKIM est désactivée dans toutes les stratégies de flux

de messagerie. Cela vous permet de configurer la signature DKIM sans aucun impact sur le flux de messages :

1. Navigation vers Politiques de messagerie > Politiques de flux de messagerie.
2. Accédez à chaque stratégie de flux de messagerie et assurez-vous que la clé de domaine/signature DKIM est désactivée.

Créer une clé de signature DKIM

Vous devez créer une nouvelle clé de signature DKIM sur l'ESA :

1. Accédez à Politiques de messagerie > Clés de signature et sélectionnez Ajouter une clé...
2. Nommez la clé DKIM et générez une nouvelle clé privée ou collez-la dans une clé actuelle.

> Remarque : dans la plupart des cas, il est recommandé de choisir une taille de clé privée de 2 048 bits.

3. Validez les modifications.

Générer un nouveau profil de signature DKIM et publier l'enregistrement DNS dans DNS

Ensuite, vous devez créer un nouveau profil de signature DKIM, générer un enregistrement DNS DKIM à partir de ce profil de signature DKIM et publier cet enregistrement dans DNS :

1. Naviguez jusqu'à Politiques de messagerie > Profils de signature et cliquez sur Ajouter un profil.
    1. Attribuez un nom descriptif au profil dans le champ Nom du profil.
    2. Entrez votre domaine dans le champ Domain Name.
    3. Saisissez une nouvelle chaîne de sélection dans le champ Sélecteur.

    > Remarque : le sélecteur est une chaîne arbitraire utilisée pour autoriser plusieurs enregistrements DNS DKIM pour un domaine donné.

    4. Sélectionnez la clé de signature DKIM créée dans la section précédente dans le champ Clé de signature.
    5. Cliquez sur Submit.
2. À partir d'ici, cliquez sur Generate dans la colonne DNS Text Record pour le profil de signature que vous venez de créer et copiez l'enregistrement DNS qui est généré. Il doit ressembler à ce qui suit :

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

3. Validez les modifications.
4. Envoyez l'enregistrement DNS TXT DKIM à DNS à l'étape 2.

5. Attendez que l'enregistrement DNS TXT DKIM ait été entièrement propagé.
6. Accédez à Politiques de messagerie > Profils de signature.
7. Dans la colonne Test Profile, cliquez sur Test pour le nouveau profil de signature DKIM. Si le test est réussi, poursuivez avec ce guide. Si ce n'est pas le cas, vérifiez que l'enregistrement DNS TXT DKIM a été entièrement propagé.

Activer la connexion DKIM

Maintenant que l'ESA est configuré pour signer les messages DKIM, nous pouvons activer la signature DKIM :

1. Accédez à Politiques de messagerie > Politiques de flux de messagerie.
2. Accédez à chaque stratégie de flux de messagerie qui a le comportement de connexion de relais et activez la signature de clé de domaine/DKIM à On.

Remarque : par défaut, la seule stratégie de flux de messages avec un comportement de connexion de relais est la stratégie de flux de messages appelée Relayed. Vous devez vous assurer que seuls les messages de signature DKIM sont sortants.

---

3. Validez les modifications.

Tester le flux de messages pour confirmer les réussites DKIM

À ce stade, le DKIM est configuré. Cependant, vous devez tester la signature DKIM pour vous assurer qu'elle signe les messages sortants comme prévu et qu'elle réussit la vérification DKIM :

1. Envoyez un message via l'ESA et assurez-vous qu'il obtient la signature DKIM par l'ESA et la vérification DKIM par un autre hôte.
2. Une fois le message reçu à l'autre extrémité, vérifiez les en-têtes du message pour l'en-tête Authentication-Results. Recherchez la section DKIM de l'en-tête pour vérifier si elle a réussi ou non la vérification DKIM. L'en-tête doit ressembler à l'exemple suivant :
   <#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. Recherchez l'en-tête « DKIM-Signature » et vérifiez que le sélecteur et le domaine corrects sont utilisés :

   <#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
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucun moyen spécifique de dépanner cette configuration.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.