Configurer le filtre entrant en fonction de la vérification DKIM dans ESA

Introduction

Ce document décrit comment configurer le dispositif de sécurité de la messagerie électronique (ESA) afin d'entreprendre toute action sur la vérification des clés de domaine identifiées par e-mail (DKIM) via un filtre de contenu ou une configuration de filtre de messages entrants.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ESA
- Connaissance de base de la configuration du filtre de contenu
- Connaissance de base de la configuration des filtres de messages
- Centralisation des connaissances de configuration de la quarantaine des stratégies, des virus et des attaques

Components Used

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.

Configuration

Étape 1. Configurer la vérification DKIM

Assurez-vous que la vérification DKIM est activée. Accédez à **Politiques de messagerie > Politiques de flux de messagerie**.

Afin de configurer la vérification DKIM sur l'ESA est similaire à la vérification SPF. Dans les **paramètres** de **stratégie par défaut** des stratégies de flux de messagerie, activez simplement la vérification DKIM **activée**.

Étape 2. Vérifier l'action finale

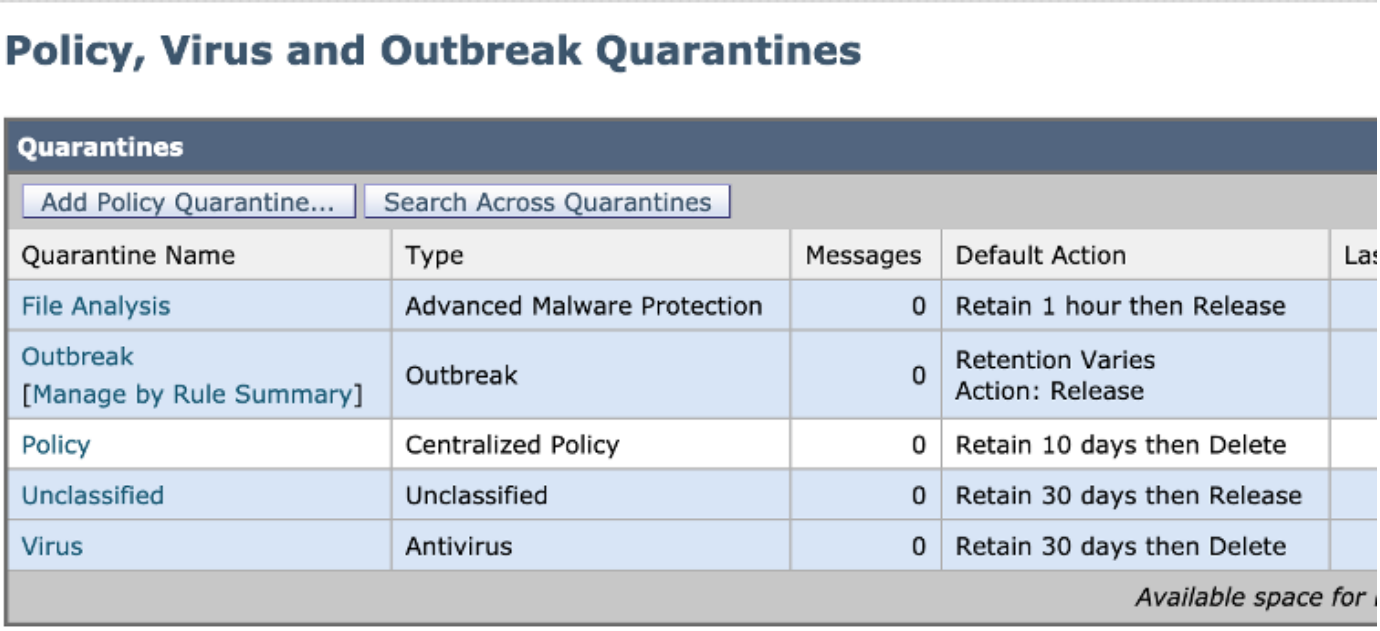
Tout d'abord, identifiez les mesures à prendre conformément à la vérification DKIM. Ex : , ajoutez une balise ou une quarantaine. Si l'action finale consiste à mettre le courrier en quarantaine, vérifiez les quarantaines configurées.

- Si vous n'utilisez pas la gestion centralisée :

Accédez à **ESA > Monitor> Quarantaines des stratégies, des virus et des attaques**.

- Si vous avez configuré la gestion centralisée (SMA) :

Accédez à **SMA >E-mail > Quarantaine de messages >Quarantaines de stratégies, de virus et d'attaques**, comme illustré dans l'image :

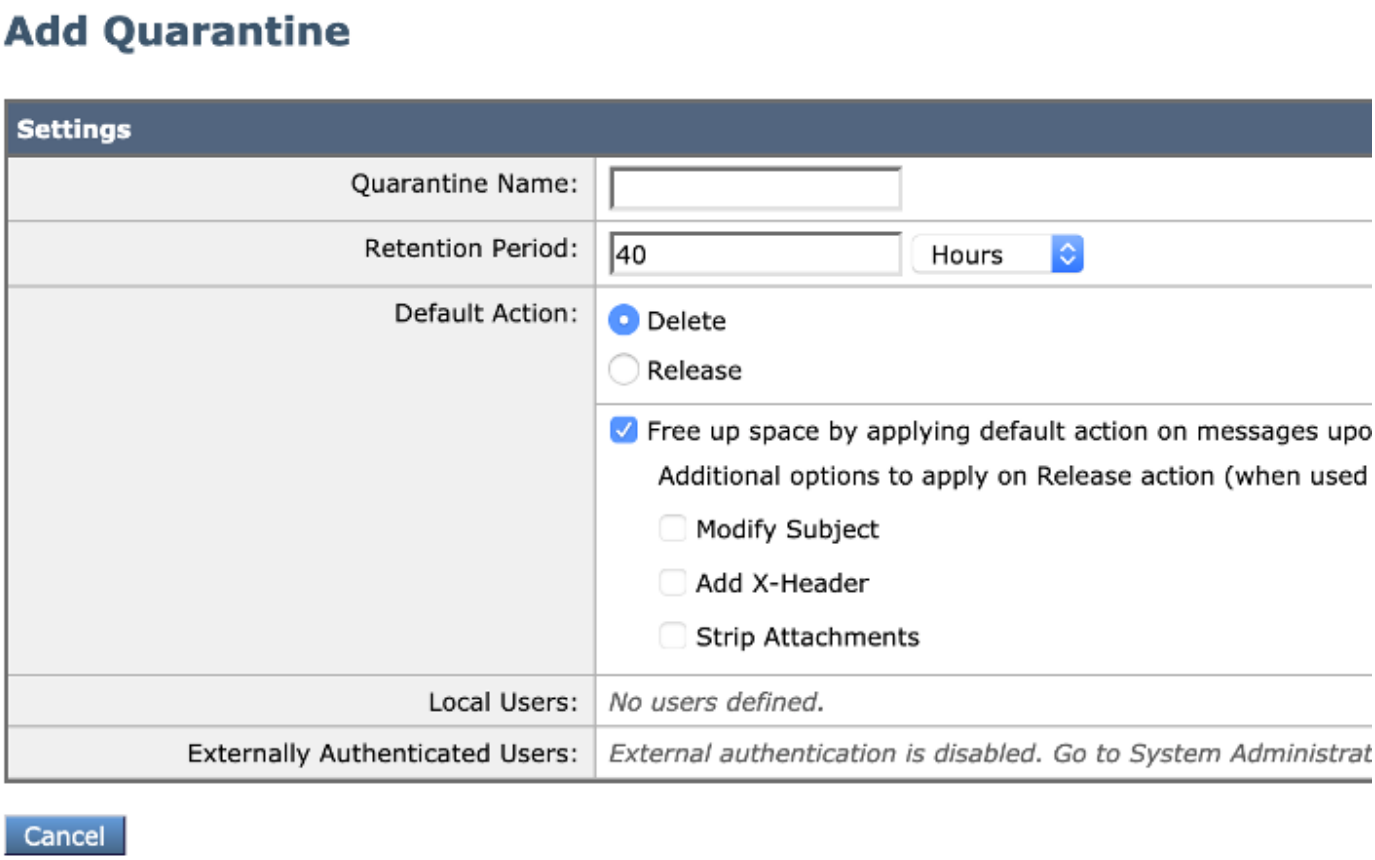


S'il n'y a pas de quarantaine spécifique pour les services **DKIM**/Domain Message Authentication, Reporting & Conformance (DMARC)/Sender Policy Framework (SPF). Il est recommandé d'en créer un.

Lors de la mise en quarantaine des stratégies, des virus et des attaques, sélectionnez **Ajouter une quarantaine de stratégie** :

Ici, vous pouvez configurer :

- Nom de la quarantaine : par exemple, **DkimQuarantine**
- Période de rétention : C'est à vous de décider et cela dépend des besoins de votre organisation et de l'action par défaut. Après la période de rétention de l'e-mail sera supprimé ou libéré et remis, selon votre sélection, comme indiqué sur l'image :



Étape 3. Filtre entrant pour ESA

a. Créez un filtre de contenu entrant pour ESA :

Accédez à **ESA > Politiques de messagerie > Filtres de contenu entrant > Ajouter un filtre**.

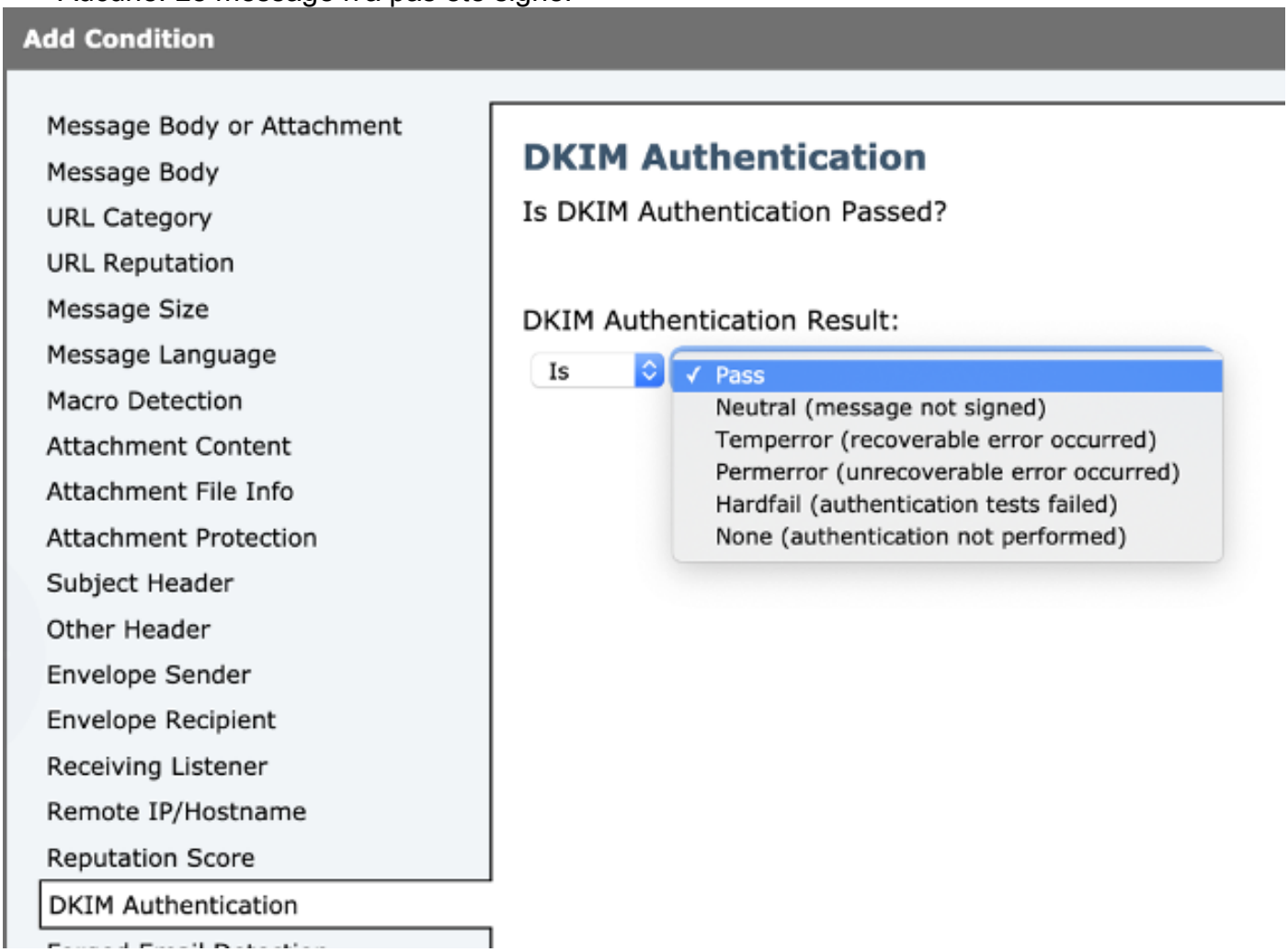
- Première section : Vous pouvez configurer le **nom**, la **description** et **l'ordre** du filtre :

- Deuxième section : Ajouter une condition. Vous pouvez ajouter plusieurs conditions et configurer plus de filtres de contenu afin d'effectuer une action sur la vérification DKIM :

Authentification-Résultats attendus et signification :

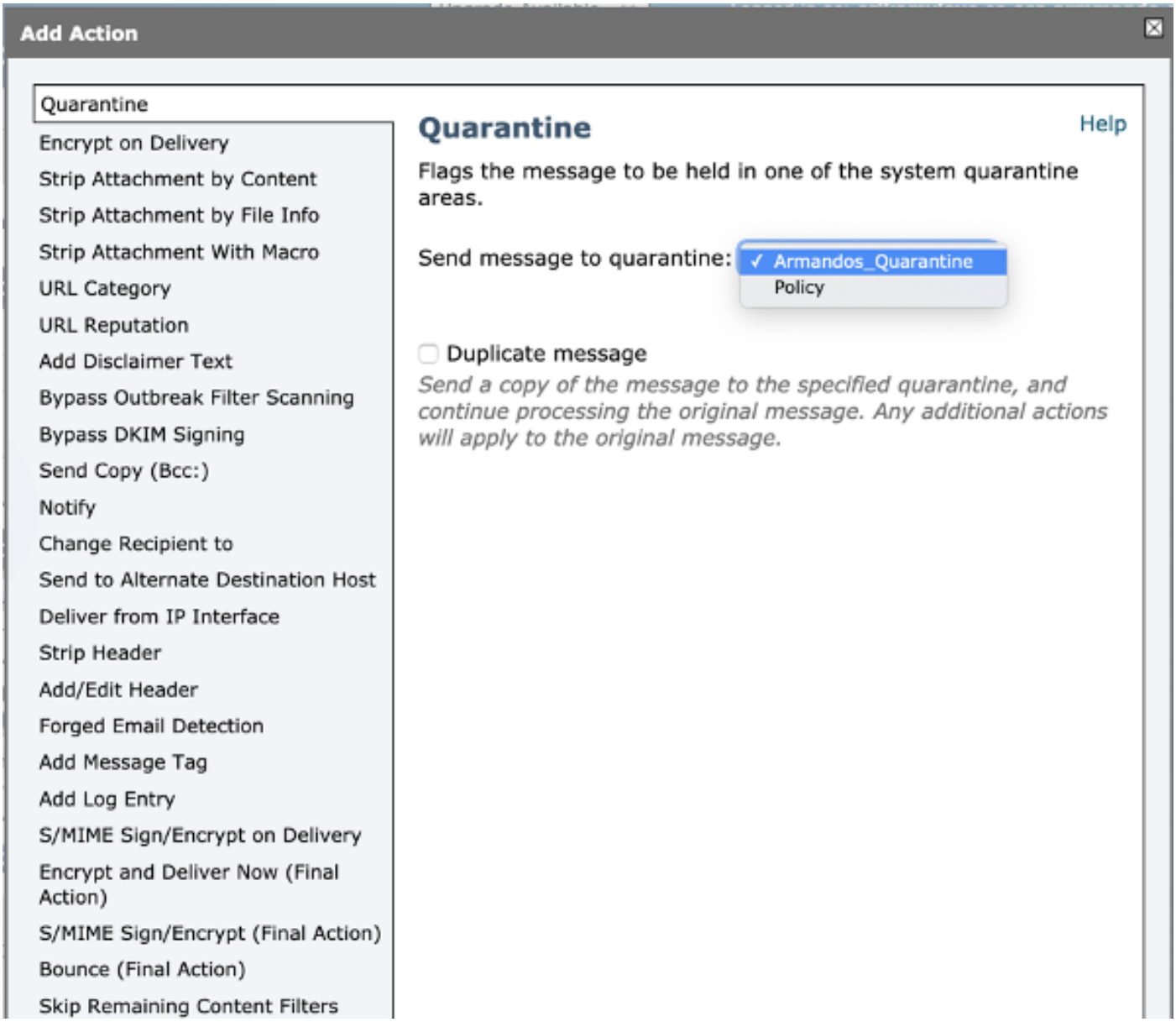
- Passe : Le message a réussi les tests d'authentification.

- Neutre : L'authentification n'a pas été effectuée.
- Température : Une erreur récupérable s'est produite.
- Erreur : Une erreur irrécupérable s'est produite.
- Hardfail : Les tests d'authentification ont échoué.
- Aucune. Le message n'a pas été signé.



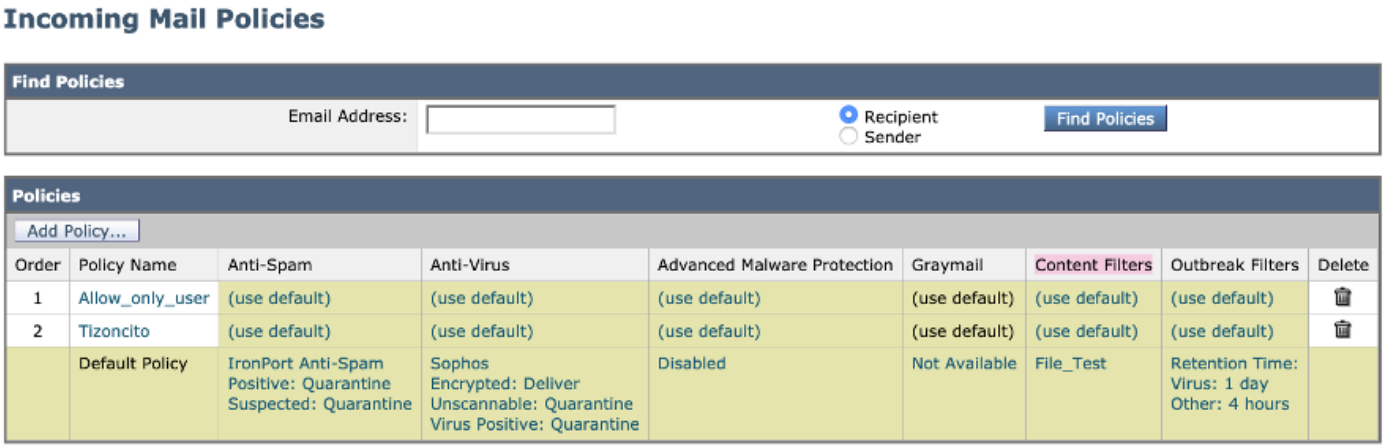
Note: Exigences de vérification DKIM : L'expéditeur doit signer le message avant de pouvoir le vérifier. Une clé publique doit être disponible dans le DNS pour vérification dans le domaine émetteur.

- Troisième section : Sélectionnez une action. Vous pouvez ajouter plusieurs actions telles que l'ajout d'une entrée de journal, l'envoi en quarantaine, la suppression de l'e-mail, la notification, etc. Dans ce cas, sélectionnez la quarantaine précédemment configurée, comme illustré dans l'image :



Ajouter un nouveau filtre à la stratégie de flux de courrier :

Une fois qu'un filtre a été créé. À partir du SEEE, ajoutez le filtre sur chaque stratégie de flux de courrier où vous voulez vérifier DKIM avec une action finale. Accédez à **ESA> Politiques de messagerie > Politiques de messagerie entrante**, comme l'illustre l'image :



Cliquez sur la ligne **Filtres de contenu** et **Stratégie de flux de courrier**.

Note: (utiliser la valeur par défaut) ne signifie pas qu'il est configuré en tant que paramètres de stratégie par défaut. Configurez chaque stratégie de flux de courrier avec les filtres nécessaires.

b. Créez un filtre de message pour ESA :

Tous les filtres de messages sont configurés à partir de l'interface de ligne de commande ESA. Entrez la commande **Filtres** et suivez les instructions :

```
ESA. com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> NEW
Enter filter script.  Enter '.' on its own line to end.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

Une fois le filtre créé, passez en revue la légende : **1 filtres ajoutés**.

Les conditions et les actions à configurer sont les mêmes que celles utilisées par le filtre de contenu entrant.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Filtre de contenu entrant :

- Àpartir de l'interface utilisateur Web ESA (WebUI)

a. Vérifiez si le filtre est configuré :

Accédez à **ESA > Politiques de messagerie >Filtres de contenu entrant.** Le filtre doit être configuré selon l'ordre précédemment sélectionné dans la liste affichée.

b. Vérifiez si le filtre est appliqué :

Accédez à **ESA>Politiques de messagerie >Stratégies de messagerie entrante**.

Le nom du filtre doit être affiché dans la colonne Filtres de contenu et la ligne Stratégie de flux de courrier. Si la liste est large et que vous ne pouvez pas voir le nom, cliquez sur la liste de filtres afin d'identifier les filtres appliqués à la stratégie.

Filtre de message :

```
From ESA CLI:
ESA. com> filters
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

La liste indique si le filtre est configuré et actif.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vérifier la configuration :

Vous devez vous assurer que :

- La stratégie de flux de courrier comporte dkim : sur la vérification
- Une action est configurée dans un filtre de contenu ou de message
- Dans le cas d'un filtre de contenu, vérifiez que le filtre est associé à un flux de courrier

Vérifier le suivi des messages :

Le suivi des messages nous permet d'observer :

- Résultat de la vérification DKIM, par exemple : permit
- L'entrée de journal configurée (si elle a été configurée)
- Le filtre appliqué (nom et action effectuée)

Suivi à partir de ESA :

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
```

```
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

Informations connexes

- Meilleures pratiques ESA-SPF-DKIM-DMARC
- Guide de l'utilisateur final du dispositif de sécurité de la messagerie
- DKIM RFC4871
- DKIM RFC8301
- DKIM RFC8463
- Support et documentation techniques - Cisco Systems