# Filtres de contenu ESA pour des messages électroniques avec de plusieurs connexions

## Contenu



## Introduction

Ce document décrit comment les conditions satisfaits négatifs de filtre fonctionnent pour les messages électroniques qui contiennent de plusieurs connexions sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

## Problème

Vous utilisez un filtre satisfait qui permet certains types de pièces jointes à un courriel, alors que d'autres types de connexions devraient être marqués pour la quarantaine. Quand un message électronique arrive qui a de plusieurs connexions, on qui devrait être permis et des autres qui devrait être marqué pour la quarantaine, le filtre identifie le message entier comme *laissé*.

Voici le filtre satisfait qui est utilisé :

```
if attachment filename != (list of attachments), then quarantine
```

Ces fonctions de condition et d'action comme prévues si le message électronique a une connexion simple, mais lui ne fonctionne pas correctement pour les messages qui contiennent de plusieurs, différentes connexions.

### Exemple de scénario

Ce sont les types de connexions qui sont permises :

- RAR
- pdf
- jpg

Toutes autres connexions devraient être envoyées pour mettre en quarantaine, comme spécifié

par l'état et l'action de filtre.

### État de filtre

Voici l'état de filtre qui est utilisé :

```
if attachment filename != (rar|pdf|jpg)
```

### Action de filtre

Voici l'action de filtre qui est utilisée :

**quarantine**
L'attente est typiquement que si le message électronique contient une connexion **pdf** et une connexion de **txt**, alors il devrait être dû mis en quarantaine à la connexion de **txt** parce qu'il n'est pas dans la liste de connexions permises. Cependant, ce filtre satisfait ne fonctionne pas comme prévu parce qu'il apparie la connexion **pdf** dans le message et la permet directement, quoiqu'il ait une connexion de **txt**.

## Solution

Il n'est pas possible de mettre en quarantaine l'email avec la connexion de **txt** pour ces raisons :

- Les conditions de connexion sont pour **toutes les** connexions qui sont incluses dans un message.
- Le négatif **! = la** comparaison vérifie si les connexions **l'unes des** s'assortissent.

Comme décrit, si on permet des connexions **l'unes des**, comme quand elles apparient **! =**, alors le message entier est traité comme *laissé*. Il n'y a aucune manière autour de ceci ; c'est simplement la manière dont ces conditions fonctionnent.

Le seul l'autre solution est d'inverser la logique et de bloquer les connexions spécifiques, pas simplement n'importe quelle connexion qui blanc-n'est pas répertoriée.