Содержание

Введение

Этот документ описывает, как отрицательные условия фильтра контента работают для сообщений электронной почты , которые содержат множественные прикрепления на Cisco Email Security Appliance (ESA).

Проблема

Вы используете фильтр контента, который позволяет определенные типы вложений электронной почты, в то время как другие типы прикреплений должны быть отмечены для карантина. Когда сообщение электронной почты поступает, который имеет множественные прикрепления, то, которое должно быть позволено и другой, который должен быть отмечен для карантина, фильтр определяет полное сообщение, как *позволено*.

Вот фильтр контента, который используется:

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

Это условие и действие функционируют, как предназначено, если сообщение электронной почты имеет одиночное прикрепление, но это не функционирует должным образом для сообщений, которые содержат множественные, другие прикрепления.

Пример сценария

Это типы прикреплений, которые позволены:

- rar
- PDF
- jpg

Все другие прикрепления должны быть переданы карантину, как задано условием фильтра и действием.

Условие фильтра

Вот условие фильтра, которое используется:

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

Действие фильтрации

Вот действие фильтрации, которое используется:

quarantine
Ожидание, как правило, состоит в том что, если сообщение электронной почты содержит прикрепление PDF и прикрепление текста, то оно должно быть изолировано из-за прикрепления текста, потому что это не находится в списке позволенных прикреплений. Однако этот фильтр контента не функционирует, как предназначено, потому что он совпадает с прикреплением PDF в сообщении и непосредственно разрешает его, даже при том, что он имеет прикрепление текста.

Решение

Не возможно изолировать электронную почту с прикреплением текста по этим причинам:

- Прикрепляемые условия для всех прикреплений, которые включены в сообщение.
- Отрицание! = сравнение проверяет, совпадает ли какое-либо из прикреплений.

Как описано, если какое-либо из прикреплений позволено, такой как тогда, когда они совпадают! =, тогда полное сообщение рассматривается, как *позволено*. Нет никакого пути вокруг этого; это - просто способ, которым работают эти условия.

Единственное другое решение состоит в том, чтобы инвертировать логику и заблокировать определенные прикрепления, не только любое прикрепление, которое не добавлено в белый список.