# Содержание



# Вопрос

Как я перехватываю и блокирую встроенные гиперссылки, которые имеют исполняемые файлы?

# Ответ

Можно использовать фильтр сообщения для сканирования тела и любых прикреплений HTML. Обычно, эти электронные почты прибывают на пути электронные почты HTML. Для механизма сканирования для обнаружения его необходимо использовать тело - содержит условие. Если вы только обрабатываете исходящую почту, то можно использовать 'only-body-contains' условие.

Фильтр следующего сообщения будет искать любую гиперссылку длины, которая заканчивается исполняемым файлом. Как только условие соблюдают, два действия активируют. Первое действие должно будет уведомить локального администратора путем отправки электронного письма admin@example.com.

Вторым будет заключительное действие отбрасывания электронной почты. Электронная почта не должна быть отбрасыванием, но вместо этого может быть изолирована. Удаление действия ниже '`отбрасывания ()`'; может быть заменен действием '`карантина ('Политика')`';.

Карантин должен быть определен, иначе механизм фильтра не позволит фильтр. Можно или использовать карантин политики по умолчанию или создать собственный карантин (см. карантин в руководстве, чтобы создать или удалить карантин).

Можно также использовать эту версию, которая удалила плохие URL из тела и заменила их URL REMOVED.

Для подробных инструкций о том, как ввести фильтр сообщения, рассмотрите , Как я добавляю новый фильтр сообщения к своему Устройству Cisco IronPort?

См. РУКОВОДСТВО ОПЫТНОГО ПОЛЬЗОВАТЕЛЯ CISCO ESA ASYNCOS для Безопасности электронной почты Устройства разделяют вызванную Принудительную политику для рассмотрения фильтров сообщения.