

Содержание

[Введение](#)

[Обзор действия фильтрации сообщения](#)

[Описания действия фильтрации сообщения](#)

Введение

Этот документ описывает различия между drop-attachments-by-name, - типом, - тип файла, и действиями фильтрации сообщения-mimetype на Cisco Email Security Appliance (ESA).

Обзор действия фильтрации сообщения

Сообщения, которые передаются с помощью MIME, могут иметь метки, назначенные на различные части тела, которые часто называют прикреплениями. Эти метки могут (и делать) конфликт друг с другом в информации, которую они предоставляют. Кроме того, часть тела могла бы иметь свои собственные характеристики. Например, пользователь мог бы взять Изображение в формате JPEG, подключить его к сообщению электронной почты, дать ему тип MIME **текста/HTML** и отметить его именем файла MIME **января mp3**. Все эти метки конфликтуют с действительностью того, каково прикрепление.

Например, рассмотрите этот заголовок сообщения:

В этом случае имена файлов MIME и типы MIME все последовательны, и могли бы, или не мог бы совпасть с фактическим форматом части тела (прикрепление). Однако в этом заголовке, существуют несоответствия:

Для правильно построенных сообщений проведение довольно легко. Но в случае кого-то или преднамеренно или непреднамеренно пытающийся обойти политику, требуется дополнительная гибкость.

Менеджеры сети часто хотят отбросить прикрепления определенного типа, такие как все файлы MP3. Однако реализация этой политики означает, что необходимо решить, какая из меток вы хотите обратить внимание на (если любой из них). AsyncOS дает вам гибкость для рассмотрения типа MIME (такого как *текст/HTML*), имя файла MIME (такое как *январь mp3*), и к фактически *берет отпечатки пальцев* у прикрепления, чтобы попытаться определить, каков истинный формат. При проведении политики с помощью фильтров сообщения или фильтров контента, вы могли бы хотеть использовать один или больше этих меток.

Описания действия фильтрации сообщения

Вот описания действия фильтрации сообщения:

- **drop-attachments-by-name** - Проверяет имена файлов каждого прикрепления в

сообщении, чтобы видеть, совпадает ли оно с данным регулярным выражением. Имя файла взято от заголовков MIME. Это сравнение учитывает регистр. Если одно из прикреплений сообщения совпадает с именем файла, это правило возвращает **true**. Если прикрепление будет архивом, то IronPort устройство Серии С получит имена файлов из архива и применит правила **scanconfig** (по умолчанию, типы MIME видео /*, аудио /* и отобразит /* не просмотрены, и ничто, чего более чем 5 МБ просмотрены), соответственно.

- **drop-attachments-by-type** - Отбрасывает все прикрепления на сообщениях, которые имеют тип MIME, определенный или данным типом MIME или расширением файла. Прикрепления архивного файла (zip, tar) будут отброшены, если они будут содержать файл, который совпадает.
- **drop-attachments-by-filetype** - Исследует прикрепления на основе отпечатка пальца файла, и не только расширение имени файла с тремя буквами. Это подобно команде файла UNIX. В дополнение к типам отдельного файла, которые могут быть заданы, Сжатые выражения группы, Документ, Исполняемый файл, Образ и Среды включают все типы файла общего типа. Например, *Исполнимая* группа включает .exe, .java .msi .pif, .dll, .scr, and.com файлы. См. Руководство пользователя AsyncOS для полного списка типов файла, которые могут быть заданы.
- **drop-attachments-by-mimetype** - Отбрасывает все прикрепления на сообщениях, которые имеют данный тип MIME. Это действие не пытается установить тип MIME расширением файла, таким образом, это также не исследует содержание архивов.