Содержание

Введение

Этот документ описывает, как просмотреть почтовые журналы для определения расположения сообщения, освобожденного от карантина на Cisco Email Security Appliance (ESA) или Устройство менеджмента Cisco Security (SMA).

Когда сообщение освобождено от карантина, где это зарегистрировано?

На ESA при выпуске сообщения от Карантина спама IronPort (ISQ), карантина Политики, или о другом пользовательском карантине, том действии и привязанном событии сообщают в текстовых Журналах Почты IronPort (mail_logs) файл. Запись журнала связана с исходным MID.

Лучший способ приблизиться к разыскиванию этого состоит в том, чтобы добраться или *От*, *До*, или *Предмет* исходного сообщения, которое было изолировано. Затем, ищите его в журнале, чтобы видеть, было ли это освобождено от карантина, и затем посмотрите, принял ли конечный почтовый сервер его или возвратился его.

Пример, ища почтовые журналы отправителя "spam@test.com":

Вы захотите обратить внимание на идентификатор сообщения (MID) и идентификатор соединения доставки (DCID).

Мы видим , что этот определенный MID передавался карантину спама от полного mail_logs или отслеживанию сообщений:

После того, как освобожденный, ниже пример того, что искать в сообщении, которое освобождено от ISQ:

В данном примере освобождено сообщение, и интерфейс (192.168.0.199) является слушателем на ESA, соединяясь с (192.168.0.200) как заключительный почтовый сервер конца доставки.

При рассмотрении Карантинных Журналов Спама (euq_logs) действие выпуска показывает придерживающееся:

Точно так же, если бы исходное сообщение изолировало к карантину Политики, и затем

было освобождено, вы видели бы подобный данному примеру:

От карантина Политики сообщение освобождено от карантина Политики, и интерфейс (192.168.0.199) является слушателем на ESA, соединяясь с (192.168.0.200) как заключительный почтовый сервер конца доставки.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Что такое Идентификатор сообщения (MID), Инжекционный Идентификатор соединения (ICID) или Идентификатор соединения Доставки (DCID)?
- Cisco Systems – техническая поддержка и документация