Содержание

Вопрос:

Как я настраиваю ESA для пропуска защиты от спама и/или сканирования антивируса для моих доверяемых отправителей?

AsyncOS предлагает три основных программных средства, которые можно использовать для пропуска защиты от спама или проверки антивируса пользующихся наибольшим доверием отправителей. Обратите внимание на то, что ESA не советует пропускать антивирус, проверяющий в любое время, даже для ваших пользующихся наибольшим доверием отправителей, из-за потенциала для непреднамеренного заражения с вирусами. Ниже приводится обсуждение этих трех способов, которыми можно пропустить проверку защиты от спама некоторое подмножество потока сообщений.

Первое программное средство, доступное вам, является Политикой Потока Почты таблицы доступа к хосту (HAT). Использование Почтовой Политики Потока, можно определить отправителей IP-адресом (использующий или числовые IP-адреса или имена DNS PTR) счетом SenderBase, или белым списком локального DNS или черным списком. Как только вы определили отправителей, как доверяется в Sender Group в HAT, можно тогда отметить ту группу отправителя для пропуска сканирования для защиты от спама.

Например, давайте предположим, что вы хотели определить определенного делового партнера, EXAMPLE.COM, который не должен иметь защиты от спама, проверяющей их почту. Необходимо было бы узнать IP-адреса почтового сервера SCU.COM (или записи указателя DNS). В этом случае давайте предположим, что EXAMPLE.COM имеет почтовые серверы, которые будут иметь IP-адреса с записями PTR DNS "smtp1.mail.scu.com" через "smtp4.mail.scu.com". Помните в этом случае, что мы смотрим на запись PTR (иногда названный обратным DNS) для почтовых серверов; это не имеет никакого отношения к доменному имени, которое люди в SCU.COM будут использовать для исходящей почты.

Вы могли создать новую Sender Group (или использовать существующую группу отправителя, такую как WHITELIST) с Почтовой Политикой> Обзор> Add Sender Group. Давайте создадим тот по имени "NotSpammers". После отправки этой страницы вы будете возвращены к экрану Mail Policies> Overview, где у вас будет возможность добавить новую политику для этой Sender Group. При щелчке по "Add Policy" вам дадут возможность создать новую политику. В этом случае мы хотим только отвергнуть политику по умолчанию в одной области: Обнаружение Спама. Дайте политике название и установите поведение соединения быть, "Принимают", затем прокручивают вниз к разделу Обнаружения Спама и заставляют эту политику пропускать проверку спама. Утверждайте, что новая политика, и не забывает "Передавать Изменения".

Альтернативный подход должен использовать Политику Входящей почты для пропуска сканирования для защиты от спама. Различие между HAT и Политикой Входящей почты - то, что HAT совершенно основан на IP - информации на отправителе: истинный IP-адрес, IP-адрес, как отражено в DNS, счет SenderBase (который основывается на IP-адресе), или белый список DNS или запись черного списка на основе IP-адреса. Политика Входящей почты основывается на информации о конверте сообщения: к кому сообщение или от кого

сообщение. Это означает, что они восприимчивы к тому, чтобы быть введенным в заблуждение кем-то исполняющим роль отправителя сообщения. Однако, если вы хотите просто пропустить всю проверку защиты от спама входящую почту, прибывающую от людей, у которых есть адреса электронной почты, которые заканчиваются в "@example.com", вы могли сделать это также.

Для создания такой политики перейдите к Почтовой Политике>, Политика Входящей почты> Добавляет Политику. Это позволит вам добавить политику, которая определяет ряд отправителей (или получатели). Как только вы определяете Политику Входящей почты, это появится на экране обзора (Почтовая Политика> Политика Входящей почты). Можно тогда щелкнуть по столбцу "Anti-Spam" и отредактировать определенные параметры настройки для защиты от спама для этого индивидуального пользователя.

Параметры настройки Для защиты от спама для определенной политики имеют много опций, но в этом случае, мы просто хотим пропустить проверку для защиты от спама. Обратите внимание здесь на другое различие между ОСНОВАННОЙ НА НАТ политикой и Политикой Входящей почты: в то время как Политика Входящей почты имеет намного больший контроль, НАТ может только позволить вам пропустить или не пропустить сканирование для защиты от спама. Например, вы могли принять решение изолировать спам от определенных отправителей и удалить спам из других отправителей.

Третья опция для пропуска сканирования для защиты от спама находится в сообщении Фильтры. (Обратите внимание на то, что Фильтры контента не могут использоваться для этого, потому что Фильтры контента происходят после того, как сканирование для защиты от спама уже произошло). Одно из действий в сообщении Фильтры является "пропуском-spamcheck". Фильтр сообщения ниже пропустит проверку защиты от спама отправителей, у кого есть определенный IP - адрес или кто происходит из названия отдельного домена:

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')     )
   {
       skip-spamcheck();
   }
```