Обнаружьте поддельные сообщения электронной почты на ESA и создайте исключения для отправителей, которым позволяют имитировать

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Что такое Почтовый Спуфинг?
Как обнаружить поддельную электронную почту?
Как позволить Имитировать для Определенных Отправителей?
Настройка
Создайте сообщение фильтр
Добавьте исключения спуфинга из MY_TRUSTED_SPOOF_HOSTS
Проверка
Проверьте, что Изолируются Поддельные сообщения
Проверьте, что отправляются Сообщения об исключениях спуфинга
Дополнительные сведения

Введение

Этот документ описывает, как управлять спуфингом электронной почты на Cisco Email Security Appliance (ESA) и как создать исключения для пользователей, разрешенных послать имитировавшие электронные письма.

Предварительные условия

Требования

Ваш ESA должен обрабатывать и входящие почты и исходящие письма, и должен использовать стандартную конфигурацию RELAYLIST для установки флага сообщений как выхода.

Используемые компоненты

Сведения в этом документе основываются на ESA с любой версией AsyncOS. Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Используемые отдельные компоненты включают:

- Словарь: используемый для хранения всех внутренних доменов.
- Фильтр сообщения: используемый для обработки логики обнаружения поддельной электронной почты и вставки заголовка, на который могут действовать фильтры контента.
- Карантин политики: используемый для хранения duplicartes поддельных электронных почт временно. Полагайте, что добавление IP-адреса освобожденных сообщений к MY_TRUSTED_SPOOF_HOSTS предотвращает будущие сообщения от этого отправителя от ввода карантина политики.
- MY_TRUSTED_SPOOF_HOSTS: список для ссылки на ваши доверяемые IP-адреса передачи. Добавление IP-адреса отправителя к этому списку пропустит карантин и позволит отправителю имитировать. Мы размещаем отправителей, которым доверяют, в вашу группу отправителя MY_TRUSTED_SPOOF_HOSTS так, чтобы не были изолированы поддельные сообщения от этих отправителей.
- RELAYLIST: список для аутентификации IP-адресов, которым позволяют передать, или послать исходящее электронное письмо. Если электронная почта отправляется через эту группу отправителя, предположение - то, что сообщение не является поддельным сообщением.

  Примечание: Если или группу отправителя называют чем-то другим, чем MY_TRUSTED_SPOOF_HOSTS или RELAYLIST, необходимо будет модифицировать фильтр с соответствующим именем группы отправителя. Кроме того, если у вас есть множественные слушатели, у вас может также быть несколько MY_TRUSTED_SPOOF_HOSTS.

Общие сведения

Спуфинг включен по умолчанию на ESA Cisco. Существуют несколько, допустимые причины для разрешения других доменов передать от Вашего имени. Один общий пример, Администратор ESA может хотеть к управлению поддельными электронными почтами путем изоляции имитировавших сообщений, прежде чем они будут отправлены.

Для принятия определенных мер, таких как карантин на поддельной электронной почте необходимо сначала обнаружить имитировавшую электронную почту.

Что такое Почтовый Спуфинг?

Почтовый спуфинг является подделкой почтового заголовка так, чтобы сообщение, казалось, произошло от кого-то или где-нибудь кроме настоящего источника. Почтовый спуфинг является тактикой, используемой в фишинге и кампаниях спама, потому что люди, более вероятно, откроют электронную почту, когда они будут думать, что это было передано легитимным источником.

Как обнаружить поддельную электронную почту?

Вы захотите фильтровать любые сообщения, которые имеют отправителя конверта (Почта -

От) и "дружественный от" (От) заголовка, которые содержат один из ваших собственных входящих доменов в адресе электронной почты.

Как позволить Имитировать для Определенных Отправителей?

При реализации фильтра сообщения, предоставленного в этой статье, имитировавшие сообщения помечены с заголовком, и фильтр контента используется для принятия мер на заголовке. Для добавления исключения просто добавьте IP отправителя к MY_TRUSTED_SPOOF_HOSTS.

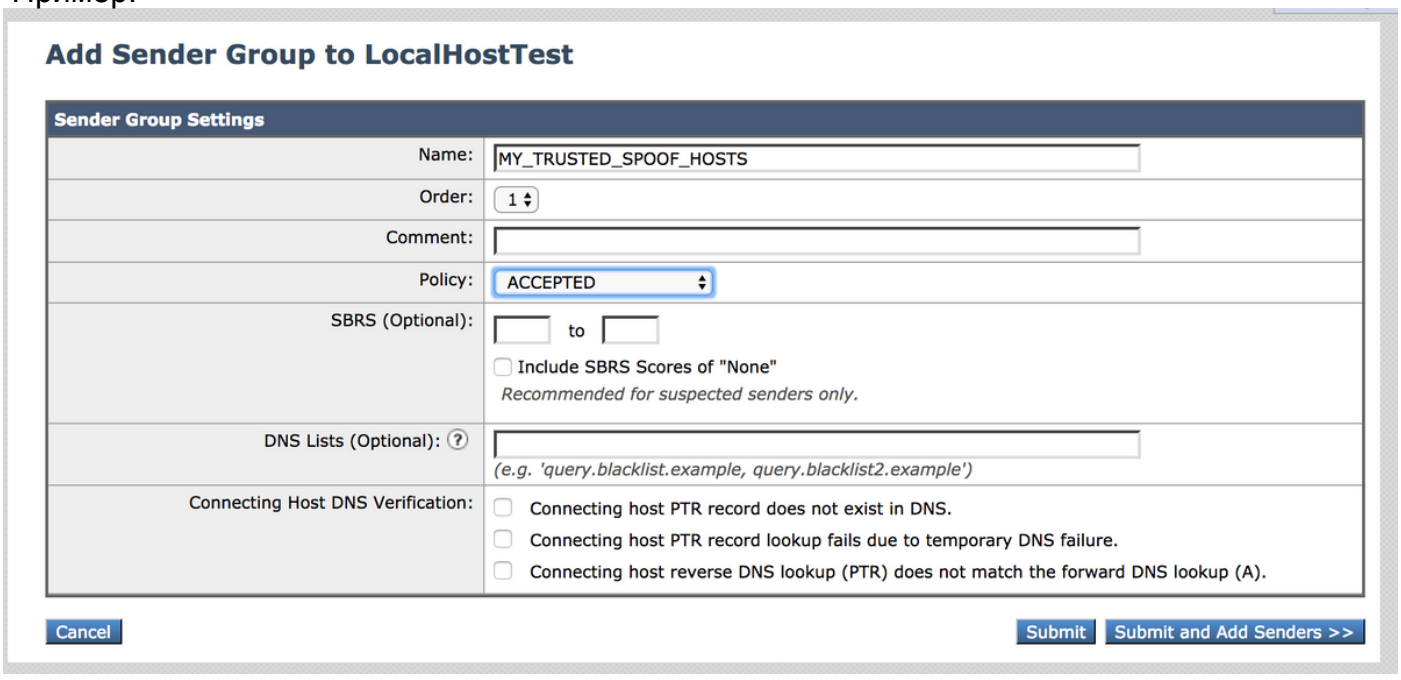
Настройка

Создайте Sendergroup

Создайте словарь для всех доменов, для которых вы хотите отключить спуфинг на ESA:

1. От GUI ESA перейдите для **Отправки по почте Политики> Обзор HAT**
2. Нажмите Add.
3. В Поле "name" задают **MY_TRUSTED_SPOOF_HOSTS**
4. В "Order" поле задают **1**
5. Для поля "Policy" задайте **ACCEPTED**
6. Нажмите **Submit** для сохранения изменений.
7. Наконец, нажмите **Commit Changes** для сохранения конфигурации

Пример:



Создайте словарь

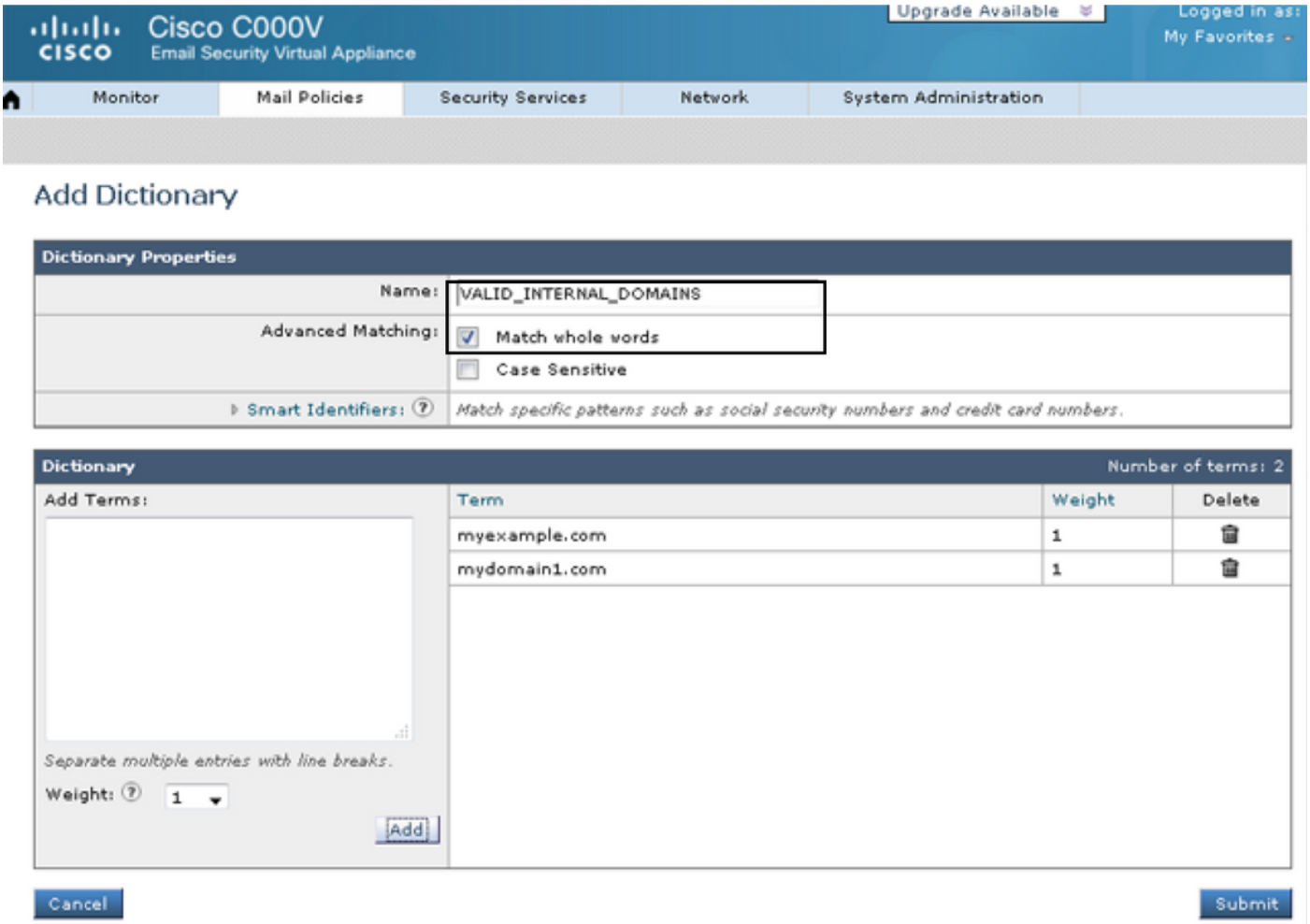
Создайте словарь для всех доменов, для которых вы хотите отключить спуфинг на ESA:

1. От GUI ESA перейдите для **Отправки по почте Политики> Словари.**
2. Нажмите Add **словарь.**
3. В Поле "name" задают 'VALID_INTERNAL_DOMAINS', например.
4. Под "добавляют сроки", добавляют все домены, которые вы хотите обнаружить

спуфинг.

5. Нажмите **Submit** для сохранения изменений словаря.
6. Наконец, нажмите **Commit Changes** для сохранения конфигурации

Пример:



Создайте сообщение фильтр

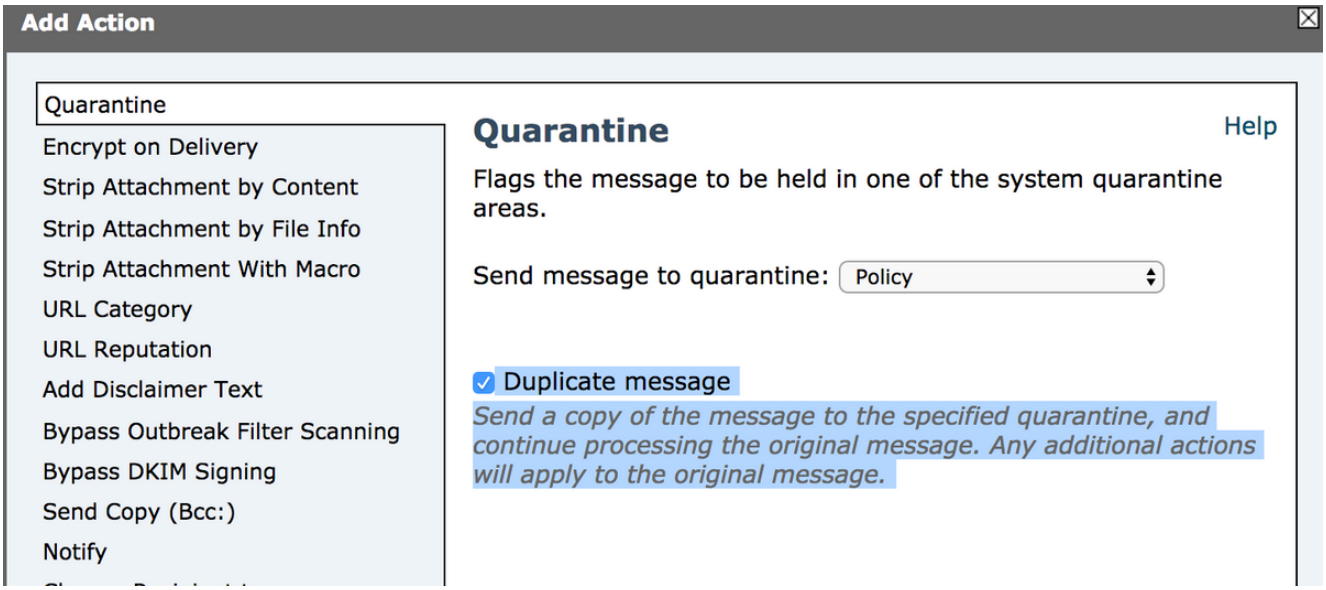
Затем, необходимо будет создать фильтр сообщения для усиления словаря, просто созданного, "VALID_INTERNAL_DOMAINS":

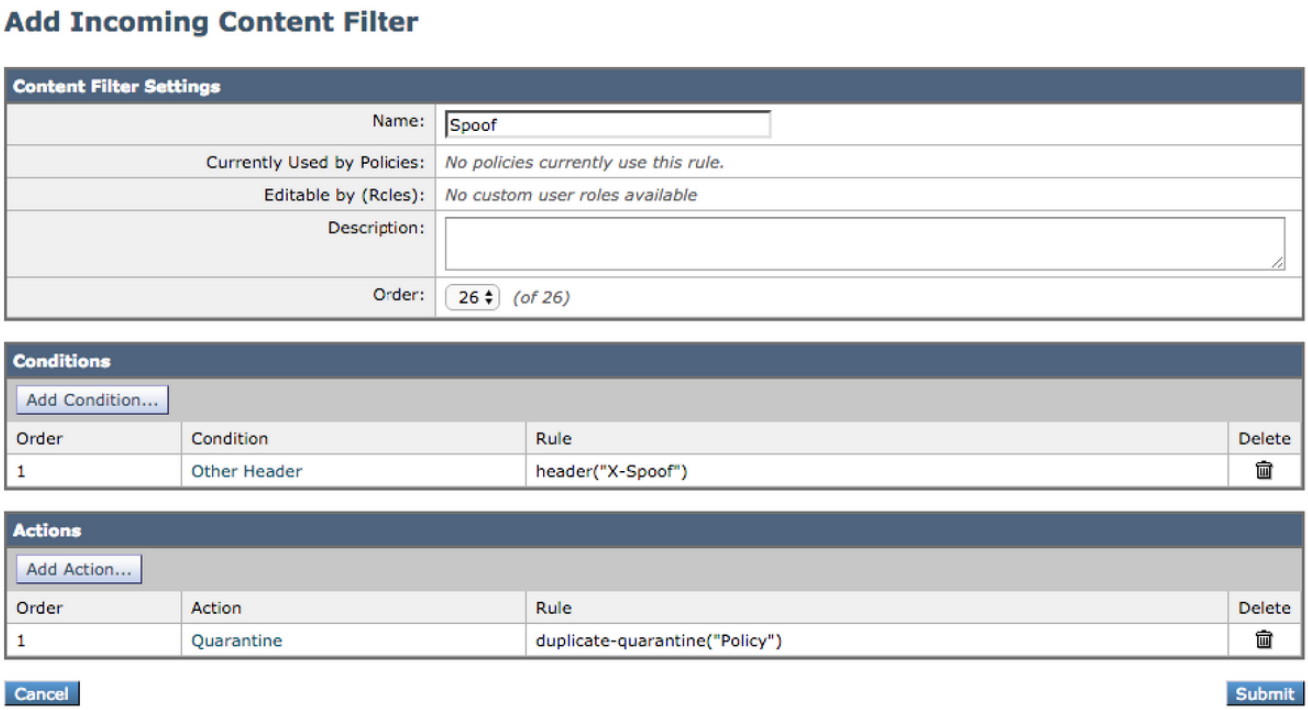
1. Соединитесь с интерфейсом командной строки (CLI) ESA.
2. Выполните **команду Filters.**
3. Выполните **команду New** для создания нового фильтра сообщения.
4. Скопируйте и вставьте следующий пример фильтра, создание редактирует для ваших фактических имен групп отправителя в случае необходимости:

```
mark_spoofed_messages:
if(
(mail-from-dictionary-match("VALID_INTERNAL_DOMAINS", 1))
OR (header-dictionary-match("VALID_INTERNAL_DOMAINS","From", 1)))
AND ((sendergroup != "RELAYLIST")
AND (sendergroup != "MY_TRUSTED_SPOOF_HOSTS")
)
{
```

```
insert-header("X-Spoof", "");
}
```

5. Возвратитесь к основному приглашению CLI и выполните **Передачу** для сохранения конфигурации.
6. Перейдите к GUI> Почтовая Политика> Поступающий Фильтры контента
7. Создайте Входящий Фильтр контента, который принимает меры на X-спуфинге заголовка спуфинга: Добавьте действие: двойной карантин ("Политика").
   Примечание: Двойная функция сообщений, показанная здесь, поддержит копию сообщения и продолжит передавать исходное сообщение получателю.





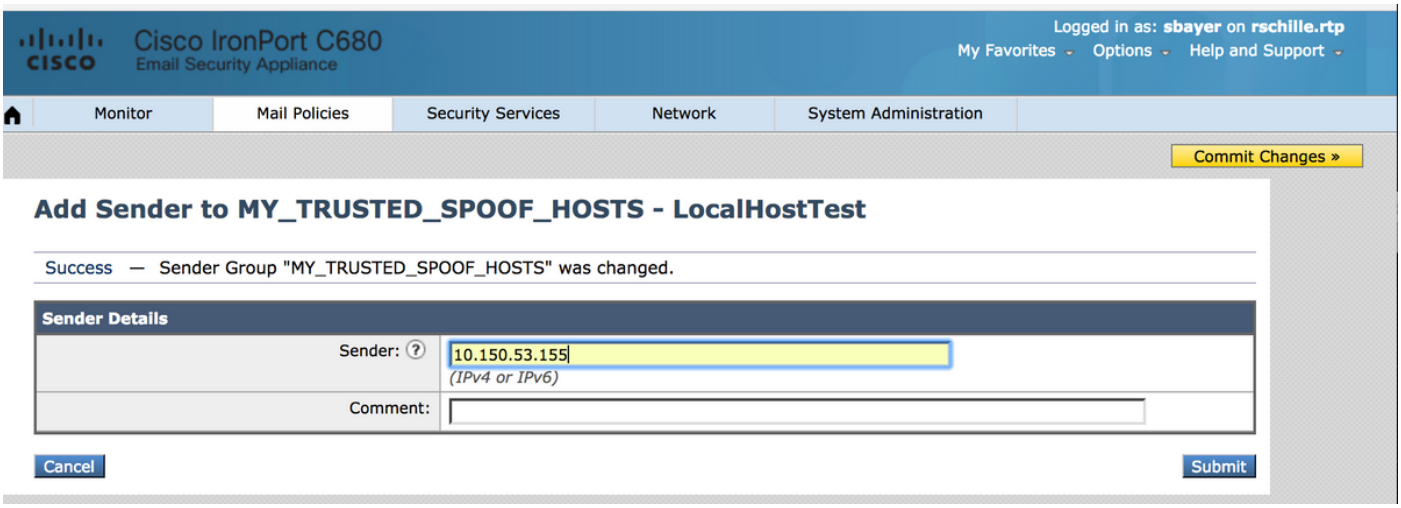
8. Свяжите фильтр контента с политикой входящей почты в GUI> Почтовая Политика> Политика Входящей почты
9. Отправьте и передайте изменения

Добавьте исключения спуфинга из MY_TRUSTED_SPOOF_HOSTS

Наконец, необходимо будет добавить исключения спуфинга (IP-адреса или имена хоста) к MY_TRUSTED_SPOOF_HOSTS sendergroup.

1. Перейдите через веб-GUI: **Почтовая Политика> Обзор HAT**
2. Нажмите и откройте группу отправителя MY_TRUSTED_SPOOF_HOSTS.
3. Щелкните по "Add Sender..." для добавления IP-адреса, диапазона, имени хоста или частичного имени хоста.
4. Нажмите **Submit** для сохранения изменений отправителя.
5. Наконец, нажмите **Commit Changes** для сохранения конфигурации.

Пример:



Проверка

Проверьте, что Изолируются Поддельные сообщения

Передайте тестовое сообщение, задающее один из ваших доменов как отправитель конверта. Проверьте фильтр, работает как ожидалось путем выполнения дорожки сообщения на том сообщении. Ожидаемый результат - то, что сообщение будет изолировано, потому что мы не создали исключений еще для тех отправителей, кому разрешают имитировать.

```
Thu Apr 23 07:09:53 2015 Info: MID 102 ICID 9 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 Subject 'test1'
Thu Apr 23 07:10:07 2015 Info: MID 102 ready 177 bytes from <user_1@example.com>
Thu Apr 23 07:10:07 2015 Info: MID 102 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:10:11 2015 Info: MID 102 interim verdict using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 using engine: CASE spam negative
Thu Apr 23 07:10:11 2015 Info: MID 102 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:10:11 2015 Info: MID 102 antivirus negative
Thu Apr 23 07:10:12 2015 Info: MID 102 quarantined to "Policy" (message
filter:quarantine_spoofed_messages)
Thu Apr 23 07:10:12 2015 Info: Message finished MID 102 done
```

Проверьте, что отправляются Сообщения об исключениях спуфинга

Отправителями "Исключения спуфинга" являются IP-адреса в вашей группе (группах) отправителя, на которую ссылаются в фильтре выше.

На RELAYLIST ссылаются, потому что он используется ESA для передачи исходящей

почты. Сообщения, передаваемые RELAYLIST , являются, как правило, исходящей почтой, и не включая это создал бы ошибочные допуски или исходящие сообщения, изолируемые фильтром выше.

Пример отслеживания сообщений IP-адреса "Исключения Спуфинга", который был добавлен к MY_TRUSTED_SPOOF_HOSTS. Ожидаемое действие, отправляют и не изолируют. (Этому IP позволяют имитировать).

```
Thu Apr 23 07:25:57 2015 Info: Start MID 108 ICID 11
Thu Apr 23 07:25:57 2015 Info: MID 108 ICID 11 From: <user_1@example.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <test_user@domain.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 Subject 'test2'
Thu Apr 23 07:26:10 2015 Info: MID 108 ready 163 bytes from <user_1@example.com>
Thu Apr 23 07:26:10 2015 Info: MID 108 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Thu Apr 23 07:26:10 2015 Info: MID 108 interim AV verdict using Sophos CLEAN
Thu Apr 23 07:26:10 2015 Info: MID 108 antivirus negative
Thu Apr 23 07:26:10 2015 Info: MID 108 queued for delivery
Thu Apr 23 07:26:10 2015 Info: Delivery start DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: Message done DCID 16 MID 108 to RID [0]
Thu Apr 23 07:26:11 2015 Info: MID 108 RID [0] Response '2.0.0 t58EVG9N031598 Message accepted
for delivery'
Thu Apr 23 07:26:11 2015 Info: Message finished MID 108 done
```

Дополнительные сведения

- ESA поддельная почтовая фильтрация
- Защита спуфинга с помощью Проверки Отправителя