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

Содержание

Введение

Этот документ описывает, как управлять спуфингом электронной почты на ESA Cisco и как создать исключения для пользователей для отправки имитировавших электронных писем.

Предварительные условия

Требования

Ваш ESA должен обрабатывать и поступление/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 карантина имитировал электронную почту и контакт за исключениями.
- **Карантин политики**: используемый для хранения имитировавших электронных почт временно прежде, чем решить освободить, или поставить, сообщение. Полагайте, что добавление IP-адреса освобожденных сообщений к WHITELIST предотвращает будущие сообщения от этого отправителя от ввода карантина политики.
- **WHITELIST**: 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 ваш WHITELIST Sendergroup 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 этот sendergroup, предположение - то, что сообщение не является поддельным сообщением.

  Примечание: Если или sendergroup называют чем-то другим, чем **WHITELIST** или **RELAYLIST**, необходимо будет модифицировать фильтр с соответствующим названием sendergroup. Также, если у вас есть множественные слушатели, у вас может также быть несколько WHITELIST.

Общие сведения

Спуфинг включен по умолчанию на ESA Cisco. Существует несколько допустимых причин для разрешения других доменов передать от Вашего имени. Вы могли бы хотеть полагать, что управление имитировало электронные почты путем изоляции имитировавших сообщений, прежде чем они будут отправлены, например.

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

Что такое Почтовый Спуфинг?

Почтовый спуфинг является созданием сообщений электронной почты с подделанным адресом отправителя.

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?

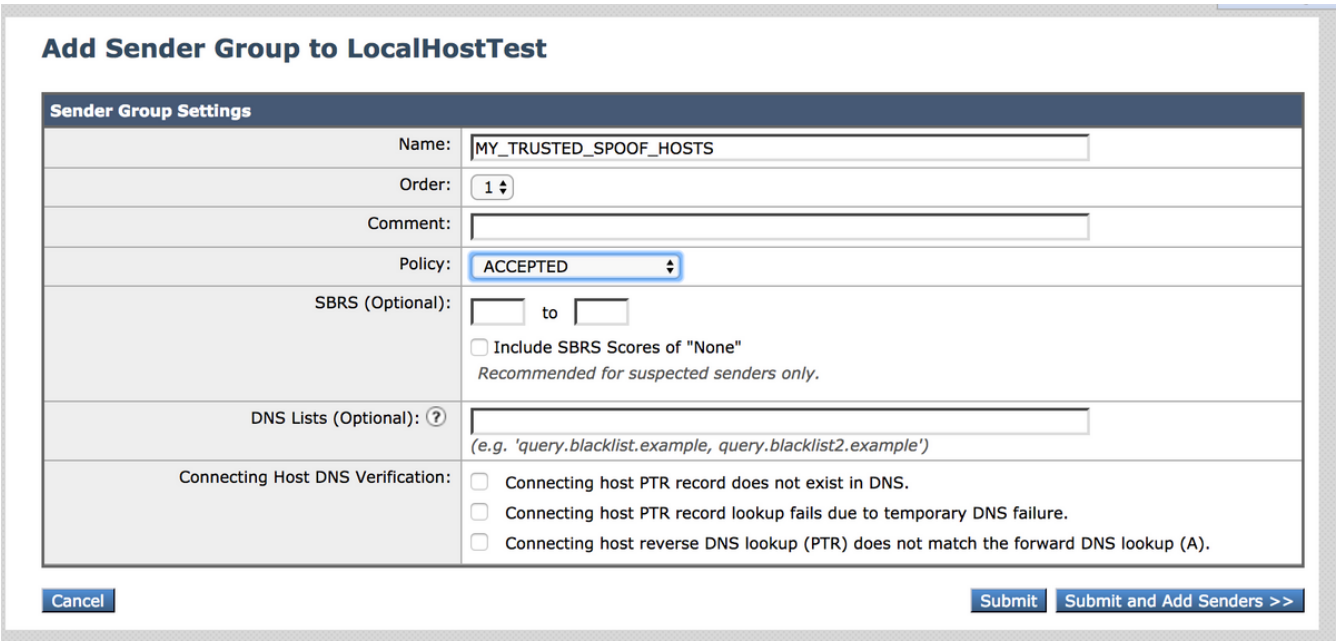
Когда реализация сообщения просачивается эта статья, имитировавшие сообщения передаются карантину политики. Для добавления исключения просто добавьте IP отправителя к WHITELIST.

Настройка

Создайте словарь

из всех ваших доменов, для которых вы хотите отключить спуфинг на ESA

- В GUI Перейдите для **Отправки по почте Политики> Словари.**
- Нажмите Add **словарь.**
- В Поле имени задают **VALID_INTERNAL_DOMAINS**, например.
- Под добавляют сроки, добавляют все домены, для которых требуется отключить спуфинг.
- **Отправьте и передайте изменения.**
-



Создайте сообщение фильтр

Усиливать словарь **VALID_INTERNAL_DOMAINS**

Соединитесь с консолью Интерфейса командной строки (CLI) вашего устройства и введите **фильтры** команды для получения меню монтеров сообщения.

Вставьте и введите фильтр сообщения ниже.

```
>filters
...
[]> new

Enter filter script. Enter '.' on its own line to end.

quarantine_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 !=
"WHITELIST")) {
                                quarantine("Policy");
                            }
```

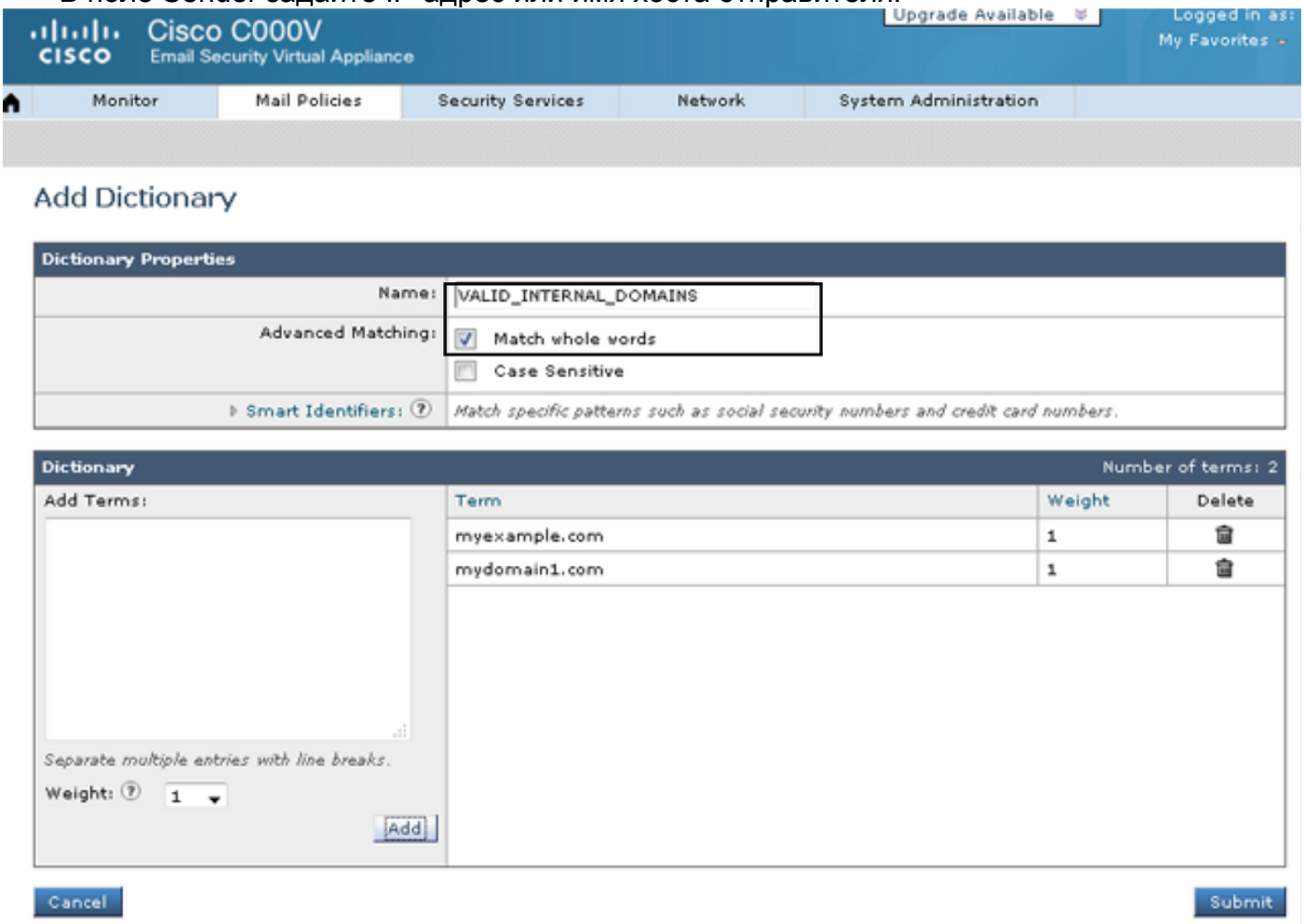
```
.
1 filters added.
```

Подвергнитесь и изменения Передачи

```
>commit
```

Добавьте исключения спуфинга из WHITELIST

- Перейдите к **Политике Почты** GUI**> Обзор HAT.**
- Откройте **WHITELIST** Sendergroup.
- В поле Sender задайте IP-адрес или имя хоста отправителя.



Подвергнитесь и изменения Передачи

```
>commit
```

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: <sbayer@cisco.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 <sbayer@cisco.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 вашем sendergroups, на который 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 WHITELIST. 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: <sbayer@cisco.com>
Thu Apr 23 07:26:02 2015 Info: MID 108 ICID 11 RID 0 To: <sbayer@cisco.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 <sbayer@cisco.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