Содержание

Введение

По умолчанию Email Security Appliance (ESA) Cisco не предотвращает входящее предоставление сообщений, которые обращены? от? тот же домен, переходящий к тому же домену. Это позволяет сообщениям быть? поддельный? внешними компаниями, которые имеют легитимные дела с клиентом. Некоторые компании полагаются на организацию третьей стороны для отправки электронного письма от имени компании, такой как Здравоохранение, Туристические агентства, и т.д.

Защита спуфинга с помощью Проверки Отправителя

Настройте Почтовую политику потока (MFP)

1. От GUI: **Почтовая Политика> Почтовая Политика Потока> Добавляет Политику...**
2. Создайте новый MFP использование названия, которое релевантно как SPOOF_ALLOW
3. В разделе *Проверки Отправителя* измените конфигурацию *Таблицы исключений Проверки Отправителя Использования* от **По умолчанию Использования** до **ВЫКЛЮЧЕНО**.
4. В **Почтовой Политике> Почтовая Политика Потока> Параметры Политики по умолчанию**, конфигурация *Таблицы исключений Проверки Отправителя Использования* набора к **На**.

Настройте HAT

1. От GUI: **Почтовая Политика> Обзор HAT> Add Sender Group...**
2. Определите имя соответственно к MFP, созданному ранее, т.е. SPOOF_ALLOW.
3. Установите порядок, таким образом, это выше WHITELIST и групп отправителя BLACKLIST.
4. Назначьте политику **SPOOF_ALLOW** на этого Отправителя Параметры группы.
5. Нажмите **Submit и Add Senders...**
6. Добавьте IP или домены для любых третьих сторон, что вы хотите позволить имитировать внутренний домен.

Настройте таблицу исключений

1. От GUI: **Почтовая Политика> Таблица исключений> Добавляет Исключение Проверки Отправителя...**
2. Добавьте локальный домен к Таблице исключений Проверки Отправителя
3. Установите *поведение* **отклонить**

Проверка

На этом этапе почта, приезжающая от *your.domain* до *your.domain*, была бы отклонена, пока отправитель не перечислен в Sender Group SPOOF_ALLOW, поскольку это было бы привязано к MFP , который не использует таблицу исключений проверки отправителя.

Пример этого был бы замечен путем завершения ручного сеанса Telnet слушателю:

553 ответа SMTP являются результатом прямого отклика таблицы исключений согласно конфигурации на ESA от шагов выше.

От почтовых журналов вы видите, что IP-адрес 192.168.0.9 не находится в действительном IP - адресе для корректной группы отправителя:

Позволенный IP-адрес, совпадающий с примером конфигурации от шагов выше , был бы замечен следующим образом:

Дополнительные сведения

- ESA, SMA и Grep WSA с Regex для поиска журналов
- Определение расположения сообщения ESA
- Cisco Systems – техническая поддержка и документация