Содержание

Введение

Этот документ описывает другие сценарии с Системой политик отправителя (SPF) на Cisco Email Security Appliance (ESA).

Prerequiste

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- Все версии AsyncOS

Что такое SPF?

Система политик отправителя (SPF) является простой почтовой системой проверки, разработанной для обнаружения спуфинга электронной почты путем обеспечения механизма, чтобы позволить получать диспетчеры почты, чтобы проверить, что входящая почта от домена передается от хоста, авторизовавшего администраторами того домена. Список санкционированных отправляющих узлов для домена публикован в записях Системы доменных имен (DNS) для того домена в форме специально отформатированной записи ТЕКСТА. Почтовый спам и фишинг часто используют подделанные адреса отправителя, таким образом публикуя и проверяя, что записи SPF можно считать способами для защиты от спама.

На ESA будет много влияния на производительность?

Из потенциального клиента ЦП не будет огромного влияния на производительность. Однако включение проверки SPF увеличит запросы DNS номера и трафик DNS. Для каждого сообщения ESA, возможно, придется инициировать 1-3 запроса DNS SPF, и это приведет к истекающему кэшу DNS ранее тогда прежде. Поэтому ESA будет генерировать большие запросы для других процессов также.

В дополнение к предыдущей информации запись SPF будет записью.TXT, которая может быть больше тогда обычные записи DNS и могла вызвать некоторый дополнительный трафик DNS.

Как вы включаете SPF?

Эти инструкции от Руководства пользователя Усовершенствования при устанавливании проверки SPF:

Включить SPF / Системно-независимый формат данных (SIDF) на по умолчанию mailflow политика:

1. Нажмите **Mail Policies> Mail Flow Policy**.
2. Нажмите **Default Policy Parameters**.
3. В параметрах политики по умолчанию просмотрите раздел **Характеристик безопасности**.
4. В разделе Проверки SPF/SIDF нажмите **Yes**.
5. Установите уровень соответствия (по умолчанию SIDF-совместим). Эта опция позволяет вам определять который стандарт SPF или проверки SIDF для использования. В дополнение к соответствию SIDF можно выбрать SIDF-compatible, который комбинирует SPF и SIDF.
6. Если вы выбираете уровень соответствия SIDF-совместимых, настраиваете, понижает ли проверка результат **Прохода** идентичности PRA ни к **Одному**, если существует Снова посланный отправитель: или Снова посланный - От: заголовки представляют в сообщении. Вы могли бы выбрать этот параметр для безопасности цели.
7. Если вы выбираете уровень соответствия SPF, настраиваете, выполнить ли тест против идентичности HELO. Вы могли бы использовать эту опцию для улучшения производительности путем отключения проверки HELO. Это может быть полезно, потому что переданное солнцезащитному фактору правило фильтрации проверяет PRA или ПОЧТУ Личности FROM сначала. Устройство только выполняет проверку HELO для уровня соответствия SPF.

Для принятия мер на результатах проверки SPF добавьте фильтр (фильтры) контента:

1. Создайте фильтр контента статуса солнцезащитного фактора для каждого типа проверки SPF/SIDF. Используйте соглашение о записи имен для указания на тип проверки. Например, используйте **Переданный SPF** для сообщений, которые передают проверку SPF/SIDF или **SPF-TempErr** для сообщений, которые не передали из-за переменной ошибки во время проверки. Для получения информации о создании фильтра контента статуса солнцезащитного фактора см. Правило Фильтра контента статуса солнцезащитного фактора в GUI.

2. После того, как вы обрабатываете много сообщений SPF/SIDF-verified, нажмите **Monitor> Content Filters** для наблюдения, сколько сообщений инициировало каждый из фильтров контента SPF/SIDF-verified.

Что делает "Тест Helo" на и от среднего значения? Если Helo протестируют сбои от определенного домена, что произойдет?

Если вы выбираете уровень соответствия SPF, настраиваете, выполнить ли тест против идентичности HELO. Вы могли бы использовать эту опцию для улучшения производительности путем отключения проверки HELO. Это может быть полезно, потому что переданное солнцезащитному фактору правило фильтрации проверяет PRA или ПОЧТУ Личности FROM сначала. Устройство только выполняет проверку HELO для уровня соответствия SPF.

Допустимые записи SPF

Для передачи проверки HELO SPF гарантируйте включение записи SPF для каждого MTA передачи (отдельный от домена). Если вы не будете включать эту запись, то проверка HELO, вероятно, не приведет ни к **Одному** вердикт для идентичности HELO. Если вы замечаете, что отправители SPF к вашему доменному return большое число **Ни одного** вердикты, эти отправители могли не включать запись SPF для каждого MTA передачи.

Если не будет никакого настроенного сообщения/Фильтров контента, сообщение будет передано. Снова, можно принять определенные меры с помощью сообщения/фильтров контента для каждого вердикта SPF/SIDF.

Что лучший путь состоит в том, чтобы включить ему только для одного внешнего домена?

Для включения SPF для определенного домена вы, возможно, должны были бы определить

новый sendergroup с почтовой политикой потока, которой включили SPF; тогда создайте фильтры, как упомянуто ранее.

Можно ли включить проверку SPF для подозреваемого Спама?

Защита от спама Cisco рассматривает довольно много факторов при вычислении очков спама. Наличие записи SPF поддающейся проверке может уменьшить счет спама, но существует все еще шанс получения тех сообщений, пойманных как подозреваемый спам.

Самое лучшее решение состояло бы в том, чтобы добавить IP-адрес отправителя в белый список, OR создает фильтр сообщения для пропуска spamcheck со множественными условиями (удаленный ip, почта - от, заголовок X-skipspamcheck, и т.д.). Заголовок может быть добавлен сервером передачи для определения одного типа сообщений от других.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация