Содержание

Следующие процедуры и рекомендации являются "оптимальными методами" для сокращения суммы спама, проходящего через ESA. Обратите внимание на то, что каждый клиент является другим и что некоторые из этих рекомендаций могут увеличить число легитимных электронных почт, классифицированных как спам (ошибочные допуски).

Базовая настройка

1. Удостоверьтесь, что включена Защита от спама:

   Проверьте, чтобы удостовериться, что весь ваш MX делает запись (включая более низкий приоритет), записи MX передают почту через ESA.Удостоверьтесь, что ваши устройства имеют допустимую характерную черту Для защиты от спама.Гарантируйте, что Защита от спама включена для всей соответствующей политики входящей почты.

2. Проверьте получение обновлений правила для защиты от спама. Проверьте, чтобы подтвердить, что **новые** штампы времени для обновлений под Сервисами безопасности> Защита от спама из прошлых 2 часов.

3. Удостоверьтесь, что сообщения просматриваются Защитой от спама:

   Проверьте выборку пропущенных сообщений спама для следующего заголовка: X-IronPort-Anti-Spam-Result:Если отсутствует тот заголовок:

   Проверьте, чтобы удостовериться, что у вас нет записей Белого списка или фильтров, заставляющих спам обойти сканирование спама (см. ниже).Проверьте, чтобы удостовериться, что сообщения не обходят сканирование, потому что они превышают максимальный размер просмотра сообщений (по умолчанию составляет 262144 байта). Сокращение этой установки не значительно улучшает производительность и может привести к пропущенному SPAM. Во время оценки также важно удостовериться, что значение IPBop совпадает с любыми другими протестированными продуктами.Пройдите каждую запись HAT и подтвердите что "spam_check=on" для всей входящей почтовой политики потока. Пока по умолчанию имеет "spam_check = на", и ни одна из почтовой политики потока явно не выключает его, это настроено должным образом. Обратите особое внимание на ДОВЕРЯЕМЫЕ параметры настройки / параметры настройки WHITELIST. Часто клиенты времен непреднамеренно добавляют отправителя к своему Белому списку, который передает спам - например, путем добавления домена интернет-провайдера, или поддержите партнерские отношения это вперед и спам и легитимная электронная почта группе отправителя WHITELIST.

Сделайте быструю проверку через фильтры сообщения, чтобы удостовериться, что нет никаких фильтров того "пропуска-spamcheck". Если существует, удостоверьтесь, что они делают то, что они должны (учет, что соответствие с одиночным rcpt - к может совпасть на сообщениях с 30 + получатели).

Найдите недавний пример SPAM (время, дата, rcpt, и т.д.), и сошлитесь на mail_logs для наблюдения то, что произошло. Подтвердите, что Защита от спама вынесла отрицательный вердикт.

4. Удостоверьтесь, что вы берете необходимые действия на позитивных сигналах спама. Проверьте Входящую Почтовую Политику для того, как обрабатываются вердикты Для защиты от спама. Удостоверьтесь положительный SPAM и подозревайте, что сообщения отброшены или изолированы в политике по умолчанию, и что вся другая политика или использует поведение по умолчанию или сознательно отвергает по умолчанию.

5. Примените более агрессивные пороги спама, если ошибочные допуски являются меньшим количеством беспокойства, чем пропущенный спам:

   Уменьшите Положительный Порог Спама до 80 (по умолчанию равняется 90), если ошибочные допуски не являются беспокойством об 'определенном' пороге.

   Уменьшите Подозреваемый Порог Спама до 40 (по умолчанию равняется 50), если ошибочные допуски не являются беспокойством о 'подозрительном' пороге.

   Если большинство ваших жалоб на спам прибывает из подмножества получателей, можно создать политику отдельного почтового отправления для этих пользователей с более низкими порогами спама для фильтрации более настойчиво для просто этих получателей.

   Изменения к этим значениям не должны быть внесены слегка, и при этом они не должны быть предписаны ни без каких точных данных установить, каковы repurcussive эффекты будут.

   Кроме того, не обязательно отрегулируйте значения в другом направлении только для предотвращения Ошибочных допусков.Удостоверьтесь, что Ошибочные допуски и Ложные отрицательные отправлены TAC.

6. Оптимизируйте свои параметры настройки SBRS и Политику HAT:

   Большинство организаций является удобным добавлением SBRS-10 к-3.0 к их Черному списку и SBRS-3.0 к 1.0 к их SUSPECTLIST. Более агрессивные клиенты могут поместить в черный список SBRS-10 к-2.0 и добавить-2.0 к-0.6 к SUSPECTLIST.

   В некоторых случаях фактом, что отправитель еще не имеет Счета Репутации SenderBase, является доказательство, что этот отправитель может быть спаммером. Можно добавить SBRS "ни один" непосредственно группе отправителя, которая

получает "Отрегулированную" политику, например группе отправителя SUSPECT.

Измените максимальное число получателей в час к 5 для "Отрегулированной" политики.

Полагайте, что создание нескольких "Отрегулированной" политики принуждает другого получателя на пределы часа - например, отправители ограничения скорости с SBRS между-2 и-1 5 получателям в час и отправителей с SBRS между-1 и от 0 до 20 получателей в час.

7. Включите Проверку Отправителя для "Отрегулированной" политики Mailflow:

   Клиенты могут принять решение добавить отправителей с несуществующим или неправильно настроенным DNS группе отправителя SUSPECTLIST.

   Соединение записи PTR хоста не существует в DNS.Соединение поиска записи PTR хоста отказывает из-за временной Ошибки DNS.

   Соединение обратного поиска DNS хоста (PTR) не совпадает с прямым Поиском DNS (A).

   Существует некоторый риск ошибочных допусков от отправителей с DNS неверна настроенного, таким образом, клиенты могут хотеть установить отдельную политику Mailflow, которая возвращает пользовательское 4xx ответ, указывающий, что отклонены сообщения причины.

   Проверьте Онлайновое Руководство пользователя Справки или AsyncOS для получения дополнительной информации о проверке отправителя

8. Включите LDAP, принимают и Защита Атаки Урожая Каталога:

   Много спаммеров посылают электронные письма большому числу недопустимых адресов, таким образом блокируя отправителей, кто передает недопустимым получателям, может также уменьшить спам.

   Если LDAP принимает, уже включено, удостоверьтесь, что Защита Урожая Каталога (DHAP) также настроена для каждого входящего слушателя с максимальными недопустимыми попытками между 5 и 10 на IP.

9. Включите словари содержания:

   Ваш ESA идет с двумя словарями содержания: profanity.txt и sexual_content.txt. В то время как использование этих словарей может генерировать ошибочные допуски, некоторые клиенты нашли, что фильтрация их почтового потока для несоответствующих слов может снизить риск "неправильного человека" получение "неверного адреса электронной почты". Эти фильтры могут только быть применены к "писклявым колесам" путем включения им для группы пользователей в определенной почтовой политике.

10. Сообщите о неправильно классифицированных сообщениях Центру технической поддержки Cisco.

11. Для предотвращения большого числа ошибочных допусков SBRS должен быть отключен для исходящего сканирования. Это вызвано тем, что SBRS посмотрел на репутацию поступить IPs, и во внутренней сети, большинство этих IPs является динамичным. Выполните действия в следующем разделе.

Включите SBNP

1. Удостоверьтесь, что входящая и исходящая почта находится на отдельных слушателях.

2. Отключите поиски SenderBase для исходящей электронной почты на ниже. Чтобы сделать это от GUI, перейдите к Сети> Слушатели, выберите любых исходящих слушателей, выберите "Advanced" и снимите флажок рядом с "Профилированием SenderBase IP использования".

   Участие Сети SenderBase (SBNP) может значительно увеличить эффективность Фильтров Репутации, Защиты от спама и Фильтров Вспышки Вируса. SBNP также не имеет никакого значимого влияния на производительность, если включено при использовании Защиты от спама и очень безопасен.

Обратите внимание на то, что громкость спама, который получает ваша организация, будет изменяться в течение долгого времени. Возможно, что больше спама проходит через ESA просто вследствие того, что вы получаете больше спама, чем в прошлом. Можно отслеживать это поведение в течение долгого времени путем рассмотрения страницы Incoming Mail Overview, и добавление "зашло в фильтрацию репутации", и "сообщения спама обнаружили" элементы строки.

Объяснение SBRS

Большое беспокойство с Ошибочными допусками - то, что могла потеряться важная электронная почта. В этом контексте практике Изоляции или Отбрасывания SPAM Положительная электронная почта проблематична. Если легитимное электронное письмо послано Карантину или папке для спама, оно требует, чтобы упреждающий поиск вошел и "заметил", что ветчина была неправильно классифицирована как спам.

Напротив, черный список и с ограниченной скоростью посылает по электронной почте, заблокированы таким способом, которым отправитель сразу уведомлен. Если этот отправитель НЕ будет спаммером, то они, вероятно, найдут другой способ вступить в контакт с вами. Фактически, как общая политика, блокируясь по умолчанию и затем принимая доверял партнерам на запросе, лучшая позиция для некоторых компаний.

Регулировка, если установлено должным образом, должна крайне редко влиять на партнеров, но обеспечит защиту от доменов, которые заражены вирусами. Регулировка также будет нерасполагающей спаммерам. Мы знаем о способе спаммера, чтобы купить большие числа IP, генерировать достаточно "хорошей" электронной почты, чтобы получить

достойный счет SBRS и затем начать посылать спам. Больший подозрительный диапазон списка должен поймать их, ограничить ущерб, который они наносят и это может в конечном счете заставить их прекращать передавать спам к вашему домену.