Содержание

Введение

Этот документ описывает ошибки обычной конфигурации на Email Security Appliance (ESA).

Каковы ошибки обычной конфигурации на ESA?

Устанавливаете ли вы новую оценку или просматриваете существующую конфигурацию, можно сослаться на этого чек-листа ошибок обычной конфигурации.

1. ШЛЯПА

- Не помещайте положительные очки SBRS как +5 или +7 в WHITELIST. Диапазон 9.0-10.0 был бы в порядке, но включая более низкие очки только сделает его более вероятно, что пройдет спам.
- Отключите UNKNOWNLIST, Проверку DNS Отправителя Конверта и Подключающий Проверку DNS Хоста, пока вы действительно не нуждаетесь и понимаете их.
- Вместо того, чтобы изменить размер сообщения и другие параметры настройки политики в каждой Почтовой Политике Потока, перейдите к Почтовому Меню политик Потока и выберите последний параметр, "Параметры Политики по умолчанию".
- Предельные максимальные числа подключений к три для большинства отправителей, и делают это по умолчанию для новой Почтовой Политики Потока.
- Проверьте, что очки SenderBase от-10.0 до-2.0 включены в BLACKLIST. Документация и мастера настройки чрезмерно консервативны; у нас в настоящее время нет ошибочных допусков в этом диапазоне.

2. Политика

- Политика названия после, кто получает их, не, что они делают. Назовите любые фильтры контента в честь того, что они делают и используют сокращения как Q_basic_attachments, D_spoofers, Strip_Multi-среды, где Q означает карантин и отбрасывание средств D.

- Политика ня по умолчанию должна "Использовать Настройки по умолчанию" для Защиты от спама, Anit-вируса, Фильтров контента и Фильтров Вспышки кроме того, где вам действительно нужны специальные параметры настройки. Не воссоздавайте те параметры настройки в каждой политике если необязательно.

- Удалите галочку "У зараженных прикреплений отбрасывания", или иначе вы передадите много пустых электронных почт, где был разделен вирус.

- Параметры антивирусной защиты для исходящего должны уведомить отправителя, не получателя

- Фильтры вспышки и Защита от спама должны быть отключены на исходящем

3. Входящие реле

Если "Монитор> Обзор" показывает соединения от ваших собственных серверов и доменов, необходимо добавить их к Входящей настройке Реле. Очень общая ошибка, при использовании GUI, должна думать, что вы включили Входящую Функцию ретрансляции, когда все, что вы сделали, добавляют записи в таблицу. Кроме того:

- Добавьте специальную HAT Sender Group для них, выше WHITELIST, для создания отчетов о целях. Не выберите ограничение скорости, или DHAP, но спам и обнаружение вирусов в порядке.

- Добавьте фильтр сообщения для соответствия с действием политики BLACKLIST. Пример:

В редких случаях, где вы повторно вводите Электронную почту (например, повторно обрабатывая почту межабонента через входящую почтовую политику), ваш фильтр должен будет также освободить интерфейс повторного закачивания. Обычно это не необходимо.

4. DNS

Много клиентов вынуждают ESA сделать запрос их внутренних серверов DNS из привычки. В большинстве установок 100% записей DNS, в которых мы нуждаемся, находятся в Интернете, не в Internal DN. Имеет больше смысла сделать запрос интернет-корневых серверов, уменьшая передающую загрузку на Internal DN.

5. Сообщение и фильтры контента

Наиболее распространенная ошибка состоит в том, чтобы вставить соответствующие Фильтры контента условий, где они не требуются. Большинство фильтров должно перечислить некоторые действия, но условие должно быть оставлено незаполненное. Фильтр всегда будет *истинен* и будет всегда работать. Вы управляете, какие пользователи/политика получают эти действия путем создания новой политики Входящей или Исходящей почты по мере необходимости и применения этого фильтра к политике. Вот неправильные и корректные примеры:

- Это - почти всегда ошибка использовать rcpt - для условия в фильтре сообщения. Корректная процедура должна записать входящий фильтр контента и сделать его определенным для индивидуального пользователя путем добавления основанной на получателе Политики Входящей почты.

- Это - почти всегда ошибка иметь тест фильтра контента для присутствия прикрепления, затем отбросить прикрепление. Корректный метод должен всегда отбрасывать то прикрепление, не тестируя на его присутствие.

- Это - почти всегда ошибка использовать, поставляют (). Поставьте средства пропускают любые остающиеся фильтры, затем поставляют. Если вы просто хотите поставить, не пропуская остаток фильтров, никакое явное действие не требуется (подразумеваемый, поставляют).

7. Открытое релейное предотвращение

Некоторые сервисы проверят, чтобы видеть, принимает ли ваш Агент передачи сообщений (MTA) адреса, которые потенциально могли привести к открытым релейным условиям. Начиная с отъезда вашего MTA, поскольку функционирующее открытое реле плохо, эти узлы могут добавить вас к черным спискам, пока вы не отклоняете эти опасные адреса в диалоге SMTP.

Добавьте специальную HAT Sender Group для них, выше WHITELIST, для создания отчетов о целях. Не выберите ограничение скорости или DHAP, но позвольте спам и обнаружение вирусов.

- Изменитесь на Строгий Парсинг Адреса (Свободный, по умолчанию). Это необходимо для предотвращения дважды, входит в систему адреса.

- Отклонение (не разделяют), недопустимые символы. Это также необходимо для предотвращения дважды, входит в систему адреса.

- Отклонение (не принимают) литералы, и вводит следующие символы: * %! \\/?

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация