Каковы оптимальные методы для использования SenderBase?

Содержание

Введение

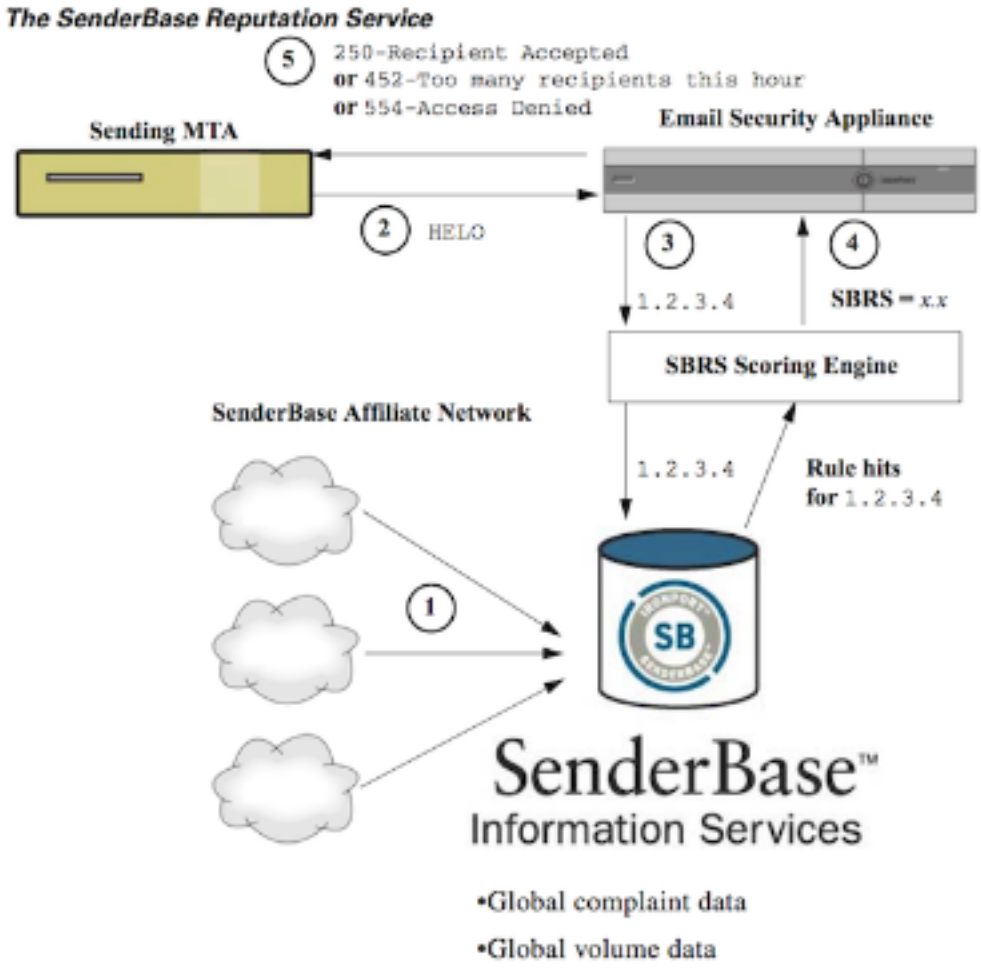
Этот документ описывает оптимальные методы для использования SenderBase.

Каковы оптимальные методы для использования SenderBase?

Сервис Репутации SenderBase (SBRS) предоставляет точное, адаптивный способ для вас, чтобы отклонить или отрегулировать системы, которые, как подозревают, передавали спам на основе соединяющегося IP-адреса удаленного хоста. SBRS возвращает счет на основе вероятности, что сообщение из данного источника является спамом, в пределах от-10 (убеждающийся быть спамом) до 0 к +10 (убеждающийся не быть спамом). Несмотря на то, что SBRS может использоваться в качестве автономного решения для защиты от спама, это является самым эффективным, когда объединено с основанным на содержании сканером для защиты от спама.

Очки SenderBase могут использоваться в таблице доступа к хосту (HAT) на слушателе SMTP для сопоставления входящих соединений SMTP с другой Sender Groups. Каждая Sender Group привязала к нему политику, которая влияет, как обрабатывается входящая электронная почта. Наиболее распространенные вещи сделать с очками SenderBase состоят в том, чтобы или отклонить почту полностью, или отрегулировать подозреваемого отправителя спама.

Можно использовать очки SBRS в HAT, чтобы отклонить или отрегулировать электронную почту. Можно также создать фильтры сообщения для определения "порогов" для очков SBRS для дальнейшей реакции на сообщения, обработанные системой. Приведенный ниже рисунок предоставляет грубую структуру того, как очки SBRS могут использоваться, чтобы заблокировать или отрегулировать подозреваемых отправителей:



1. Филиалы SenderBase передают глобальные данные в реальном времени.
2. Передача MTA открывает соединение с устройством.
3. Устройство проверяет глобальные данные для соединяющегося IP-адреса.
4. Сервис Репутации SenderBase вычисляет вероятность, это сообщение является спамом и назначает Счет Репутаций SenderBase.
5. Устройство возвращает ответ (или отклоняющий электронную почту или регулирующий отправителя) на основе Счета Репутации SenderBase.

То, как вы используете очки SBRS, будет зависеть от того, как агрессивный вы хотите быть в предварительной фильтрации электронной почты. Email Security Appliance (ESA) предлагает три других стратегии реализации SenderBase:

- **Консерватор**: консервативный подход к групповым сообщениям со Счетом Репутации SenderBase ниже, чем-7.0, дроссель между-7.0 и-2.0, примените политику по умолчанию между-2.0 и +6.0 и примените доверяемую политику для сообщений со счетом, больше, чем +6.0. Использование этого подхода гарантирует почти нулевую скорость ошибочного допуска при достижении лучшей производительности системы.
- **Умеренный:** умеренный подход к групповым сообщениям со Счетом Репутации SenderBase ниже, чем -4.0, дроссель между-4.0 и 0, примените политику по умолчанию между 0 и +6.0 и примените доверяемую политику для сообщений со счетом, больше, чем +6.0. Использование этого подхода гарантирует очень маленькую скорость ошибочного допуска при достижении лучшей производительности системы (потому что больше почты шунтируется далеко от обработки Защиты от спама).
- **Агрессивный:** агрессивный подход к групповым сообщениям со Счетом Репутации SenderBase ниже, чем-1.0, дроссель между-1.0 и 0, примените политику по умолчанию

между 0 и +4.0 и примените доверяемую политику для сообщений со счетом, больше, чем +4.0. Использование этого подхода, вы могли бы подвергнуться некоторым ошибочным допускам; однако, этот подход увеличивает производительность системы путем шунтирования самого почтового далеко от обработки Для защиты от спама.

График и таблица ниже суммируют эти три политики:

Approach	Characteristics	Whitelist	Blacklist	Suspectlist	Unknownlist
		Sender Base Reputation Score range:			
Conservative	Near zero false positives, better performance	7 to 10	-10 to -4	-4 to -2	-2 to 7
Moderate (Installation default)	Very few false positives, high performance	Sender Base Reputation Scores are not used.	-10 to -3	-3 to -1	-1 to +10
Aggressive	Some false positives, maximum performance. This option shunts the most mail away from Anti-Spam processing.	4 to 10	-10 to -2	-2 to -1	-1 to 4
		Mail Flow Policy:			
All approaches		Trusted	Blocked	Throttled	Accepted

Реализация регулировки SenderBase или блокирования

Лучший способ использовать средства очков SenderBase после простой, методологии с 2 частями. Во-первых, вы выбираете свою политику (например, вы могли запустить с "консервативной" политики выше), и сопоставьте ту политику с Sender Groups. Затем вы сопоставляете те группы отправителя с политикой, которую вы хотите. ESA уже создал матрицу Sender Groups и Почтовой Политики Потока, которая может служить шаблоном для вашей реализации SBRS.

Для реализации SenderBase, регулирующего на основе политики по умолчанию, вы отредактируете четыре группы отправителя (Белый список, Черный список, Suspectlist и Unknownlist) в Почтовой Политике> Обзор таблицы доступа к хосту (HAT). Запустите путем щелчка по группе отправителя "Whitelist". Затем с помощью раскрывающегося меню во вкладке Senders щелкните по "Add Sender" со "Счетом Репутации SenderBase (SBRS)", выбранный. Это добавит линию SBRS к списку отправителей. Заполните свой диапазон счета SBRS (в этом случае 6.0 к 10.0) и нажмите **кнопку отправки**.

Политике для группы отправителя Белого списка "Доверяют". По умолчанию эта политика пропустит обработку для защиты от спама, которая увеличит производительность системы. Поскольку отправители с очень высокими очками SBRS очень вряд ли будут передавать спам, один только этот шаг увеличит пропускную способность. Отредактируйте оставление тремя Sender Groups для добавления очков SBRS, согласно таблице ниже:

Sender Group	Диапазон счета	Результат
Белый список	6 - 10	Известные хорошие отправители не будут просмотрены
Unknownlist	- 2 к +6	Отправители с небольшой информацией будут обычно просматриваться
Suspectlist	- 7 к-2	Отправителей с плохой репутацией в большой степени отрегулируют для сокращения суммы спама, который они могут передать
Черный список	- 10 к-7	Почта от известных спаммеров будет отклонена во время SMTP с 5xx ответ

Когда вы будете сделаны, добавляя диапазоны счета, не забывайте нажимать **"Commit Changes"**. Когда вы добавите SBRS выигрывающие правила к существующим группам отправителя, разместите их в нижней части списка отправителей в любой группе. Вопросы заказа при определении групп отправителя в HAT слушателя, поскольку группы оценены сверху донизу, и в каждой группе, каждое правило, оценены индивидуально, сверху донизу. В HAT первое правило, совпадающее с отправителем, будет использоваться для выбора политики. Если входящее соединение от домена передачи будет иметь определенный счет SBRS и совпадет с диапазоном в правиле в HAT слушателя, то почтовая политика потока будет применена, даже если могли бы также совпасть другие правила далее вниз в списке групп отправителя.

Если ваша политика для помещения отправителей в группы отправителя требует, чтобы все правила non-SBRS были оценены, прежде чем очки SBRS рассматривают, то можно просто добавить четыре новых группы отправителя в конце списка существующих групп отправителя в частности для политики SBRS, совпадающей наряду с их соответствующей политикой.

Дополнительные сведения

- Часто задаваемые вопросы SenderBase
- Cisco Systems – техническая поддержка и документация