Определите и позвольте плохой Счет Репутации SenderBase (SBRS) почтовые серверы

Содержание

Введение

Эта статья описывает, как определить и временно позволить почтовые серверы с плохим Счетом Репутации SenderBase (SBRS) через Email Security Appliance (ESA).

Общие сведения

Фильтрация репутации отправителя является первым уровнем защиты от спама, позволяя вам управлять сообщениями, которые проникают через почтовый шлюз на основе степени доверия отправителя, как определено SBRS. Почтовым серверам с плохим SBRS можно было отклонить их соединения или их возвращенные сообщения, на основе вашего предпочтения.

Проблема

Почтовый сервер соединяется с ESA и сообщается как плохой SBRS , и электронные почты задержаны из-за 554 ответов SMTP, полученных соединяющимся сервером.

Выборка 554 ответа:

```
-----Original Message-----
From: Mail Delivery System [mailto:Mailer-Daemon@example.domain.com]
Sent: 25 April 2013 23:23
To: user@companyx.com
Subject: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

person@example.domain.com
SMTP error from remote mail server after initial connection:
```

```
host gatekeeper.companyx.com [195.195.195.1]: 554-gatekeeper1.companyx.com
554 Your access to this mail system has been rejected due to the sending
MTA's poor reputation. If you believe that this failure is in error, please
contact the intended recipient via alternate means.
```

Решение

Определите плохой почтовый сервер SBRS

Используйте Интерфейс командной строки (CLI), поскольку отслеживание сообщений Графического пользовательского интерфейса (GUI) не делает запись отклоненных соединений по умолчанию.

> **Примечание:** Отслеживание Отклоненных соединений может быть включено в**> Security GUI Сервисы>, Отслеживание сообщений> Включает "Отклоненную Обработку Соединения"**

Используйте **grep** против домена для получения по запросу, все отнеслись данные регистрации против того домена. Для этих выходных данных используемый домен в качестве примера является *test.com*:

```
myesa.local> grep "test.com" mail_logs

Info: New ICID 1512 to Management (10.0.0.1) from 198.51.100.1 connecting host reverse DNS
hostname: smtp1. test.com
Info: MID 6531 ICID 1512 From: test@test.com
```

Затем **grep** ID Входящего соединения (ICID) для извлечения информации о почтовом узле. ICID регистрирует, используется для раскрытия всей информации, такой как: IP-адрес отправляющего узла, DNS проверил имя хоста (при наличии), sendergroup соответствие и связанный счет SBRS:

```
myesa.local> grep "ICID 1512" mail_logs


Tue Mar 10 12:04:29 2015 Info: New SMTP ICID 1512 interface Management (10.0.0.1) address
198.51.100.1 reverse dns host unknown verified smtp1.test.com
Tue Mar 10 12:04:29 2015 Info: ICID 1512 REJECT SG BLACKLIST match sbrs[-10:-3] SBRS -4.0
```

Позвольте плохой почтовый сервер SBRS через ESA

1. От GUI перейдите для **Отправки по почте Политики> обзор HAT**.
2. Click Add Sender Group**...**
3. Назовите Sender Group с понятным именем.
4. Выберите Order так, чтобы это было выше BLACKLIST Sender Group.
5. Выберите или почтовую политику, **ACCEPTED**, или **ОТРЕГУЛИРОВАЛ**.
6. Оставьте все другие поля пустыми.
7. Нажмите **Submit и Add Senders**
8. Добавьте или IP-адрес или Имя хоста DNS хоста (хостов), на который влияют, как расположено от команды grep.
9. **Нажмите кнопку Submit (Отправить)**
10. Рассмотрите обзор HAT и гарантируйте, что новой Sender Group упорядочивают правильно.
11. Наконец, нажмите **Commit** для сохранения всех изменений конфигурации.

Для адреса Отправителя позволены следующие форматы:

- Адреса IPv6 такой как 2001:420:80:1:: 5
- Адреса IPv4 такой как 10.1.1.0
- IPv4 или подсети IPv6, такие как 10.1.1.0/24, 2001:db8::/32
- IPv4 или адрес IPv6 располагаются такой как 10.1.1.10-20, 10.1.1-5, или 2001:db8:: 1-2001:db8:: 10
- Имена хоста, такие как example.com
- Частичные имена хоста, такие как.example.com.

В примере как показано выше, для разрешения любой другой информации о почтовом сервере, заканчивающейся *test.com*, это было бы настроено как:

```
198.51.100.1
smtp1.test.com
.test.com
```

Дополнительные сведения

О компании Cisco SenderBase