Функция SenderBase правильно позади NAT?

Содержание

[Введение](#)
[Функция SenderBase правильно позади NAT?](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает SenderBase и его функциональность позади Технологии NAT для Cisco Email Security Appliance (ESA).

Функция SenderBase правильно позади NAT?

SenderBase на основе IP сервис репутации, который назначает Сервис Репутации SenderBase (SBRS) очки к IP-адресам. Очки SenderBase колеблются от-10 до +10, который отражает вероятность, что IP-адрес передачи пытается передать спам. Очень отрицательные очки указывают на отправителей, кто, очень вероятно, будет передавать спам; очень положительные очки указывают на отправителей, кто вряд ли будет передавать спам.

Слушатель SMTP на ESA делает запросы счета SBRS с помощью запросов DNS на основе IP-адреса входящего TCP - подключения. Если IP-адрес, который видит почтовое устройство, является "реальным" адресом отправителя, то SBRS функционирует как ожидалось.

> **Примечание:** Если межсетевой экран будет использовать NAT для IP - адреса источника, то это не вставит новый заголовок сообщения, который содержит IP-адрес исходного источника. Без заголовка сообщения, который содержит исходный IP - адрес, не будет работать Входящая Функция ретрансляции. Без информации заголовка для IP - адреса источника ESA не может определить IP-адрес исходного источника.

Большинство предприятий, которые используют NAT, делает так для сокрытия внутренних адресов от Интернета (или потому что у них нет достаточных IP-адресов для работы без функции NAT или NAPT). В тех случаях SenderBase работает успешно, потому что IP-адрес внешнего отправителя не модифицируется ни в каком случае.

Некоторые предприятия с большим количеством топологии сложной сети делают трансляцию сетевых адресов или прокси - подключения к внутренней части их сетей. В тех случаях запросы SenderBase не будут работать должным образом и должны быть отключены на входящем слушателе. (От CLI, **listenerconfig> редактируют> настройка**.)

Если у вас есть сомнение, преобразовываются ли адреса или не или проксируются ли соединения, просто исследуют mail_logs файл (используйте команду CLI, такую как **хвост mail_logs**). Это показывает вам каждое входящее соединение каждому слушателю, и вы быстро будете в состоянии видеть, являются ли IP-адреса, которые видит ESA, от обычного (доступ) в Интернет или нет.

> **Примечание:** Старайтесь посмотреть только на соединения с Общими или Входящими слушателями на журналах почты ESA.

Дополнительные сведения

- Руководства пользователя устройства безопасности электронной почты Cisco
- Cisco Systems – техническая поддержка и документация