Содержание

8 Как найти абонента за NAT. Работа с abuse letters

Ищем конкретного абонента, на которого пришел внешний abuse. В письме с abuse, как правило, приведен "белый" адрес из NAT-пула, требуется понять кто из абонентов в известное время за этим NAT-пулом ходил на ресурс, где зафиксирована вирусная активность. Нужно сделать **2 шага** — найти в abuse письме необходимые признаки и по ним в GUI CKAT идентифицировать абонента.

Шаг 1. Ищем в письме

1. Адрес из своего NAT-пула (source IP).
2. Адрес атакуемого ресурса (destination IP)
3. Время активности на атакуемом ресурсе *(с учетом часовых поясов!)*

- **Пример 1.**
- **Пример 2.**

Еще из полезного в письме может быть:

1. Причина abuse
2. История abuse (если активность была неоднократной)

Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

Шаг 2. Ищем активность абонента в GUI CKAT

Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

1. Данный NAT-пул заведен на CG-NAT CKAT.
2. Время хранения логов NAT захватывает время abuse-активности. Посмотреть и настроить

Далее в GUI CKAT необходимо открыть раздел NAT flow, выбрать период, завести source и destination IP.

-
-

С найденным абонентом нужно произвести необходимые действия для профилактики дальнейших abuse.