Содержание

Вопросы и ответы

1. Почему рекомендуется создавать пул не менее чем из 2x или 4x адресов?

Неблокирующий алгоритм диспетчеризации в DPI, распределяющий сессии по рабочим потокам, накладывает ограничение на то, какой белый IP адрес может быть назначен абоненту из пула:

- Чтобы гарантированно абонент получил свой белый адрес, необходимо чтобы в пуле было не меньше адресов, чем рабочих потоков (в типовой конфигурации это 2 для СКАТ-6 и 4 для СКАТ-10 и выше).

Узнать число рабочих потоков можно командой

```
expr $(ps -p `pidof fastdpi` H -o comm|grep wrk|wc -l) / $(ps -p `pidof fastdpi` H -o comm|grep rx|wc -l)
```

- Если в пуле всего один адрес, то не всем абонентам он может быть назначен, а только тем, которые попадут под алгоритм балансировки

2. Как определить, какой белый адрес из пула получит абонент?

Посмотреть, какой белый адрес был назначен серому, можно командой

```
fdpi_ctrl list status --service 11 --ip 192.168.4.20
```

В NAT 1:1 белый адрес выделяется сразу при назначении услуги, в CG-NAT в момент начала сессии

Также выделенный абоненту белый адрес рапортуется в Radius Accounting в целях его логгирования в биллинге.

Заранее предсказать какой-именно адрес будет выдан абоненту из пула невозможно: это зависит от разных факторов и в частности от текущей загрузки пула.

3. После подключения NAT стали отваливаться неактивные SSH сессии

Действительно, время жизни сессии в NAT ограничено, т.к. количество сессий у абонента - ограниченный ресурс и большое количество мертвых сессий в пуле уменьшает производительность NAT и общую.

У NAT нет возможности отличить, умерла сессия аварийно или просто в ней нет никакой активности, и закрывает такие долго висящие сессии по таймауту неактивности. Такое поведение предусмотрено стандартом и поддержано большинством производителей CG-NAT.

В CKAT время жизни сессий можно корректировать следующими параметрами

```
lifetime_flow=60
lifetime_flow_long=600
```

где lifetime_flow_long время жизни в секундах неактивных TCP-сессий, lifetime_flow остальных.

Но не следует делать эти настройки слишком большими, т.к. тогда может слишком разрастись таблица сессий и это повлияет на производительность CG-NAT, а также у абонента может закончится лимит сессий (который задается в параметрах nat пула).

Поэтому при необходимости поддержания долгоиграющих неактивных соединений рекомендуется использовать механизм tcp keep-alive, когда периодически в сессии передается пустой пакет, который сигнализирует, что сессия все еще активна.

Настроить tcp keep-alive можно как индивидуально для приложения на стороне сервера или клиента, так и на уровне операционной системы для всех приложений сразу.

Пример настройки на ssh сервере

```
в файл /etc/ssh/ssh_config добавляем строку
ServerAliveInterval 60
```

Пример настройки на ssh клиенте

```
в файл ~/.ssh/config добавляем строки
Host *
  ServerAliveInterval 60
или в командной строке
ssh -o TCPKeepAlive=yes -o ServerAliveInterval=60 user@example.com
```

Пример настройки для всех приложений в centos

```
в файл /etc/sysctl.conf добавляем строки
net.ipv4.tcp_keepalive_time = 600
net.ipv4.tcp_keepalive_intvl = 60
net.ipv4.tcp_keepalive_probes = 20
```

4. Сколько "серых" IP можно спрятать за одним "белым" в CG-NAT?

Рекомендуется поддерживать соотношение от 1:10 (лучше) до 1:100 (хуже), хотя можно спрятать и тысячу.

Подробнее:

По умолчанию на 1 белом IP для CG-NAT доступны 64512 портов (65535-1023, первые 1024 порта не используются, т.к. являются системными), каждый порт это одна TCP сессия и одна UDP. Количество сессий, которое создают абоненты отличается: физ. лица создают меньше сессий, юр. лица больше (поэтому для юр. лиц нужно использовать отдельный пул с другим лимитами на количество сессий), абонент с торрентом может создать в пике до 1000 сессий.

В среднем физическое лицо создает 50-60 одновременно работающих сессий, т.е. 64512/60=1075 физ. лиц можно спрятать за одним серым IP, но на практике такую значительную переподписку использовать не рекомендуется, т.к. многие популярные сервисы (почта, видео, поиск) используют защиту от атак ботнет сетей, основанную на IP адресах. Поэтому если с одного адреса им придет слишком много запросов, они могут принять это за атаку и заблокировать часть запросов или включить капчу, что создаст неудобства для абонентов.

Так же необходимо учесть особенность механизма освобождения портов в NAT Pool:

1. При подключении 11 услуги абоненту назначается Public IP исходя из алгоритма распределения
2. Когда абонент начинает устанавливать сессии, порты берутся из общей очереди СКАТ DPI и закрепляются с определенными тайм-аутами
3. В случае если на конкретном Public IP находится много абонентов, которые начинают конкурировать за свободные порты, абоненты могут начать чувствовать проблемы с доступом.

Рекомендации при создании NAT Pool и эксплуатации:

1. Абонентов, которые находятся в блокировке (5 услуга + полисинг), помещать в отдельный NAT Pool, чтобы они не влияли на работу активных абонентов. Так ведет себя IPhone, к примеру, устанавливает множество сессий в поиске рабочего сервиса.
2. Создавайте разряженные пулы и разделяйте клиентов в разные NAT Pool по типу: Физические лица и Юридические лица.
3. Осуществляйте мониторинг клиентов, которые создают большую нагрузку и проводите с ними работу. Для приема, обработки и хранения NetFlow с DPI предлагаем использовать программный продукт для сбора статистики QoE Store и графический интерфейс DPIUI2. Вы сможете провести анализ трафика абонента и сделать вывод, что его ПК заражен.

5. Как поменять параметры уже существующего и используемого пула?

1) Изменение лимита на количество сессий :

```
fdpi_ctrl load profile --service 11  --profile.name test_nat_2000 --
profile.json '{ "nat_ip_pool" : "111.111.111.0/24", "nat_tcp_max_sessions" :
```

```
2000, "nat_udp_max_sessions" : 2000, "nat_type" : 0 }'
```

Используется команда создания пула, идентичного прежнему, но с другими настройками nat_tcp_max_sessions и nat_udp_max_sessions

2) Добавление дополнительных адресов в пул:

```
fdpi_ctrl load profile --service 11  --profile.name test_nat_2000 --
profile.json '{ "nat_ip_pool" : "111.111.111.0/24,222.222.222.0/25",
"nat_tcp_max_sessions" : 2000, "nat_udp_max_sessions" : 2000, "nat_type" : 0
}'
```

Используется команда создания пула, идентичного прежнему, но с дополнительным пулом, указанным через запятую.

3) Уменьшение пула

В текущей версии не поддерживается динамическое уменьшение размеров пула и исключение из него адресов. В этом случае потребуется освободить пул, удалить и создать его с новыми параметрами.

Для удобства установим jq (утилиту для работы с данными в формате JSON):

```
yum install epel-release yum-utils
yum-config-manager --disable epel
yum --enablerepo epel install jq
```

После чего сохраним информацию об абонентах текущего пула, удалим и создадим пул и подключим к нему абонентов:

```
fdpi_ctrl list all --service 11 --profile.name test_nat_4000 --outformat
json|jq '.lservices[] | .login | select(. != null)' > save_users.txt
fdpi_ctrl list all --service 11 --profile.name test_nat_4000 --outformat
json|jq -r '.lservices[] | .ipv4 | select(. != null)' >> save_users.txt
fdpi_ctrl del all --service 11 --profile.name test_nat_4000
fdpi_ctrl del profile --service 11 --profile.name test_nat_4000
fdpi_ctrl load profile --service 11  --profile.name test_nat_4000 --
profile.json '{ "nat_ip_pool" : "111.111.111.0/30", "nat_tcp_max_sessions" :
4000, "nat_udp_max_sessions" : 4000, "nat_type" : 0 }'
fdpi_ctrl load --service 11 --profile.name test_nat_4000 --file
save_users.txt
```

Не забудьте изменить в командах имя пула и его новые параметры на нужные вам.

6. Как выдать конкретный адрес абоненту с NAT 1:1?

Если у абонента всего один серый адрес и требуется выдать абоненту конкретный белый

адрес, то нужно учитывать зависимость между серыми и белыми адресами, которая накладывается алгоритмом неблокирующей диспетчеризации адресов в DPI.

```
белый_адрес_абонента & mask = серый_адрес_абонента & mask
```

где mask зависит от числа рабочих потоков:

- при 4 рабочих потоках mask=3 (типично для CKAT >= 10)
- при 2 рабочих потоках mask=1 (типично для CKAT <= 6)

Фактически для младших версий CKAT абонентам с четными серыми адресами нужно выдавать четные белые адреса, а нечетными — нечетные. Достаточно учитывать только младший байт NNN в IP адресе XXX.YYY.ZZZ.NNN

Соответственно для старших версий нужно учитывать равенство 2 младших бит IP адреса.

При одном рабочем потоке зависимость между адресами исчезает.

Точное значение маски можно посмотреть в логе DPI:

```
grep nat_hash_mask /var/log/dpi/fastdpi_alert.log
```

Если старт был давно, то выполнить reload

```
service fastdpi reload
```

Т.е. такая частично детерминистическая схема распределения фактически предполагает, что серые адреса тоже будут выдаваться абоненту статически. И в случаях когда в договоре прописана выдача конкретного белого IP адреса и текущий серый адрес абонента не подпадает по указанную выше формулу, то потребуется поменять серый адрес абонента на тот, что формуле соответствует.

Пример для CKAT-20: абоненту с серым адресом 10.0.0.15 требуется выдать белый адрес 188.99.99.27
маска=3
15&3=3 равно 27&3=3 - это значит, такой адрес выдать можно (в противном случае пришлось бы поменять или выдаваемый абоненту серый адрес, или назначаемый ему белый)

Назначаем адрес абоненту командой:

```
fdpi_ctrl load profile --ip 10.0.0.15 --service 11 --profile.json '{
"nat_ip_pool" : "188.99.99.27/32", "nat_type" : 1 }'
```

7. Диагностика NAT

1. В профиле должны быть пулы одного размера[1)]. Правильно:

```
type_profile=1, ref_cnt=0       d3      { "nat_ip_pool" :
```

```
"1.1.2.0/28,1.1.3.0/28", "nat_tcp_max_sessions" : 2000,
"nat_udp_max_sessions" : 2000, "nat_type" : 0 }            11      (0x400)
```

Неправильно:

```
type_profile=1, ref_cnt=0       d3      { "nat_ip_pool" :
"1.1.2.0/28,1.1.3.0/26", "nat_tcp_max_sessions" : 2000,
"nat_udp_max_sessions" : 2000, "nat_type" : 0 }            11      (0x400
```

2. Для абонентов которые в блокировке, следует подключать другой профиль, с другими пулами. Многие сетевые устройства, при блокировке, могут генерировать большое количество запросов, что приводит к использованию свободных портов у публичного адреса.

3. Посмотреть равномерность распределения приватных адресов по публичным адресам в профиле.

```
fdpi_ctrl list all status --service 11 --profile.name nat_pool |grep
whiteip|cut -f7|sort|uniq -c|sort -n
```

4. Посмотреть количество абонентов, которые используют порты сверх значения переменной $P. В среднем абонент использует около 600 портов.

```
fdpi_ctrl list all status --service 11 --profile.name nat_pool | awk 'BEGIN
{FS="[=| }\t]+"}  $15>$P {print $1, $14, $15}' | wc -l
```

5. Посмотреть, как распределились адреса по пулам (подсетям) в профиле.

```
fdpi_ctrl list all status --service 11 --profile.name nat_pool |grep
whiteip|cut -f7|cut -d"." -f1,2,3|sort|uniq -c|sort -n
```

8. Как найти абонента за NAT. Работа с abuse letters

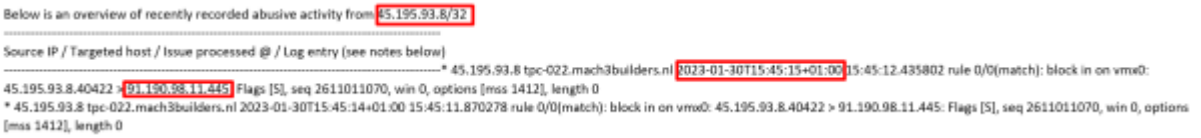
Ищем конкретного абонента, на которого пришел внешний abuse. В письме с abuse, как правило, приведен "белый" адрес из NAT-пула, требуется понять кто из абонентов в известное время за этим NAT-пулом ходил на ресурс, где зафиксирована вирусная активность. Нужно сделать **2 шага** — найти в abuse письме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

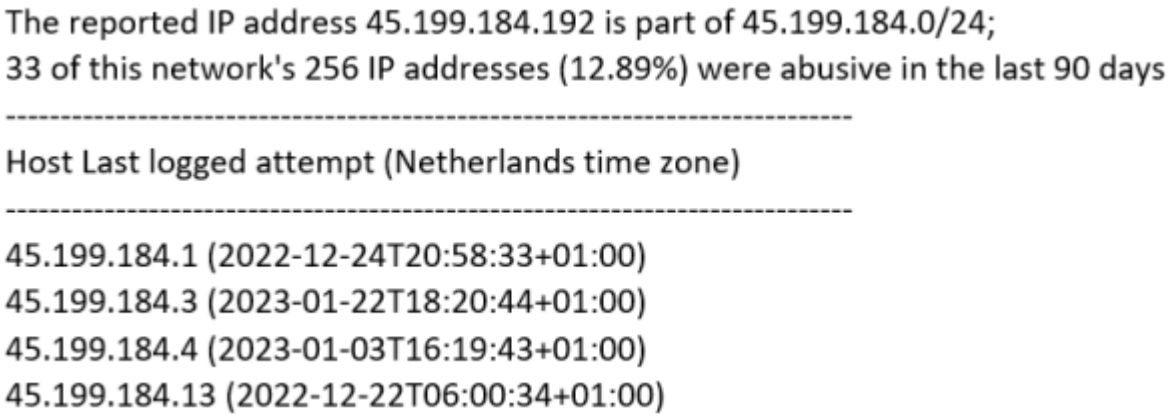
- **Пример 1.**

- **Пример 2.**



Еще из полезного в письме может быть:

1. Причина abuse
   Date: 2023-02-27T00:53:34+01:00
   Source: 45.199.184.192
   Type of Abuse: Portscan/Malware/Intrusion Attempts
   Logs: 00:53:29.425121 rule 0/0(match): block in on vmx0: 45.199.184.192.65001 > 91.190.98.8.59891: Flags [S], seq 3803861910, win 0, options [mss 1412], length 0
2. История abuse (если активность была неоднократной)



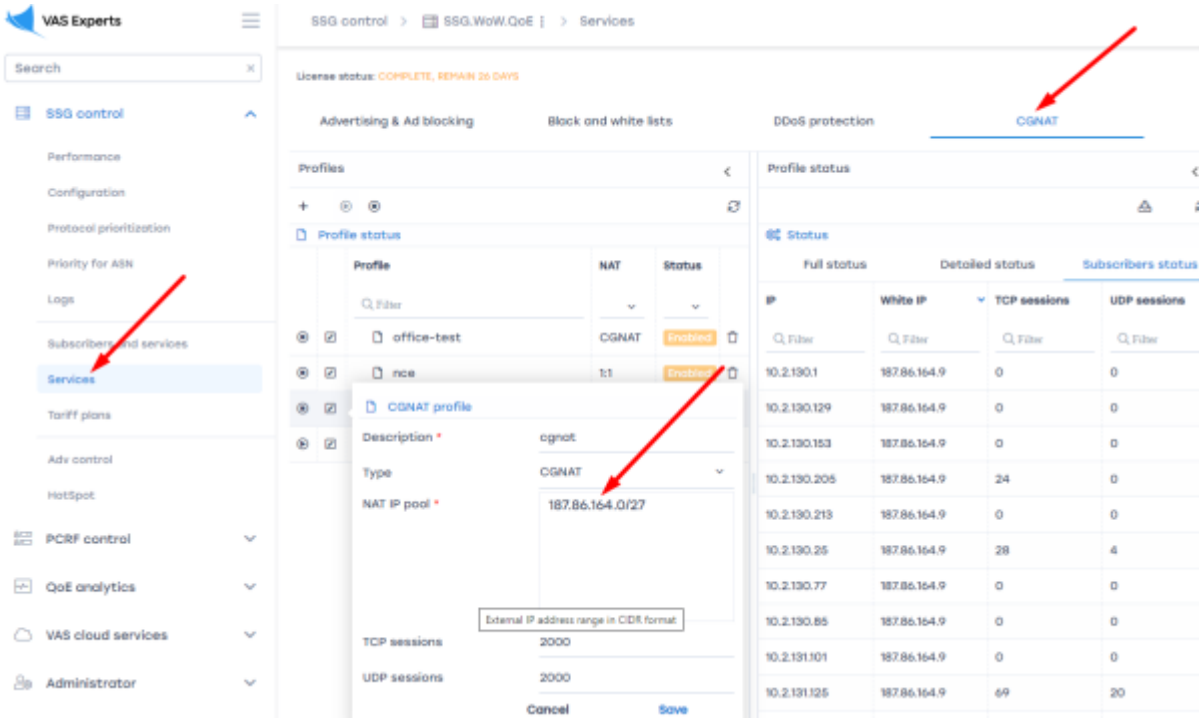
Это может помочь понять масштаб проблемы и выявлять аналогичные проблемы в сети.

Шаг 2. Ищем активность абонента в GUI CKAT

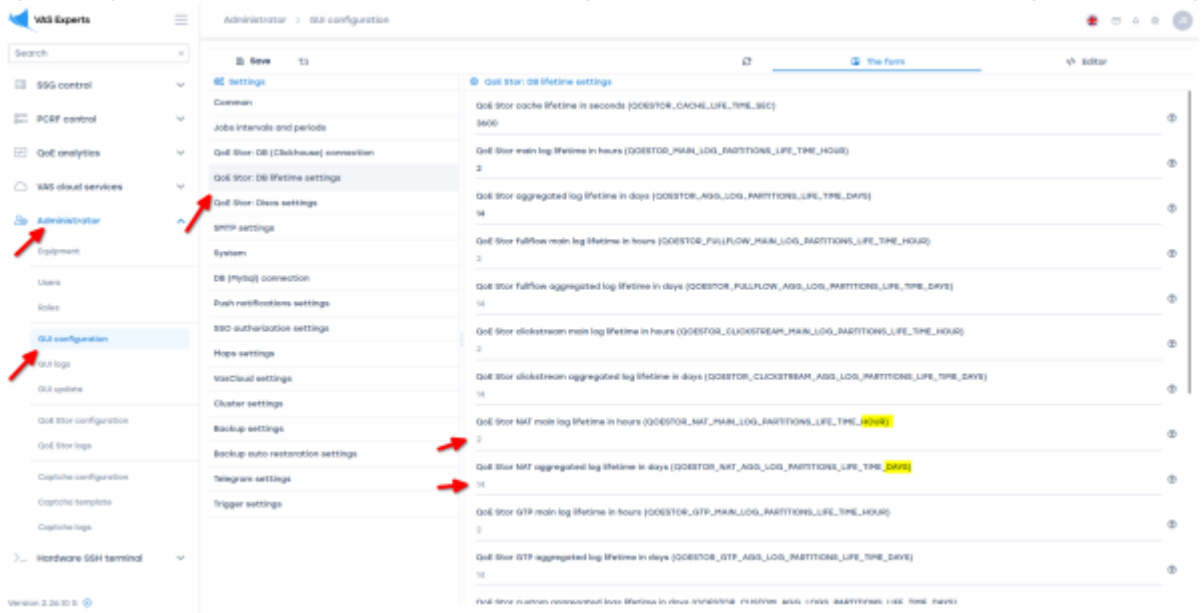
Задача — определить по логам, какой абонент за NAT-пулом (source IP), указанным в письме, в это время обращался к адресу destination IP.

Перед началом поиска стоит проверить 2 факта:

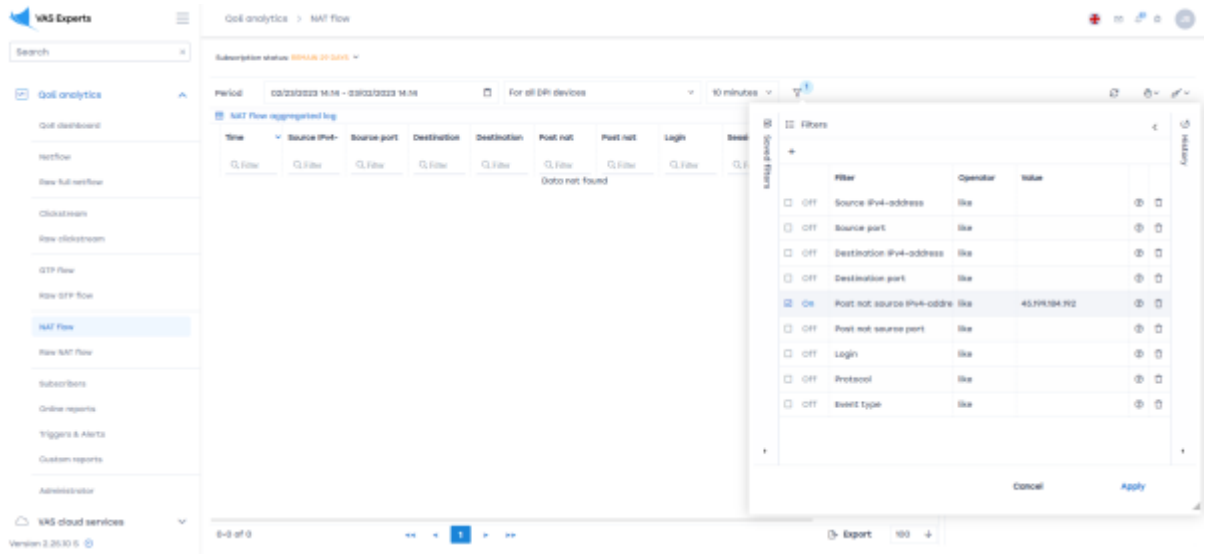
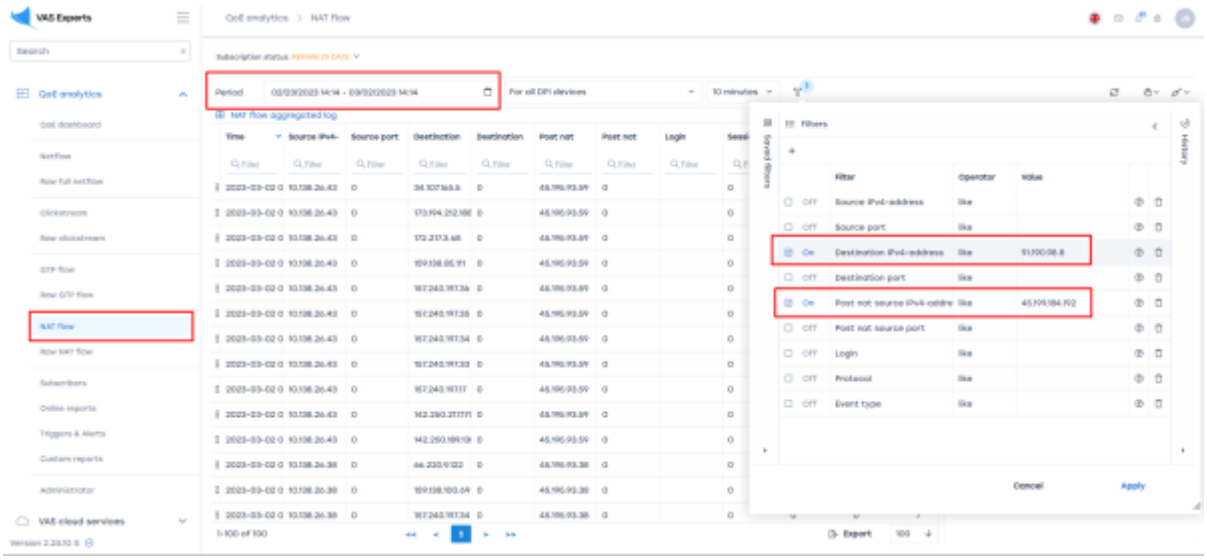
1. Данный NAT-пул заведен на CG-NAT CKAT.



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.

1)

начиная с 12 версии это требование больше не актуально