

Содержание

Конфигурация NAT Flow	3
<i>Настройка получения отдельного потока NAT Flow с DPI или NETSTREAM</i>	<i>3</i>
<i>Включение импорта событий NAT из FullFlow</i>	<i>4</i>
<i>Агрегация NAT Flow</i>	<i>5</i>

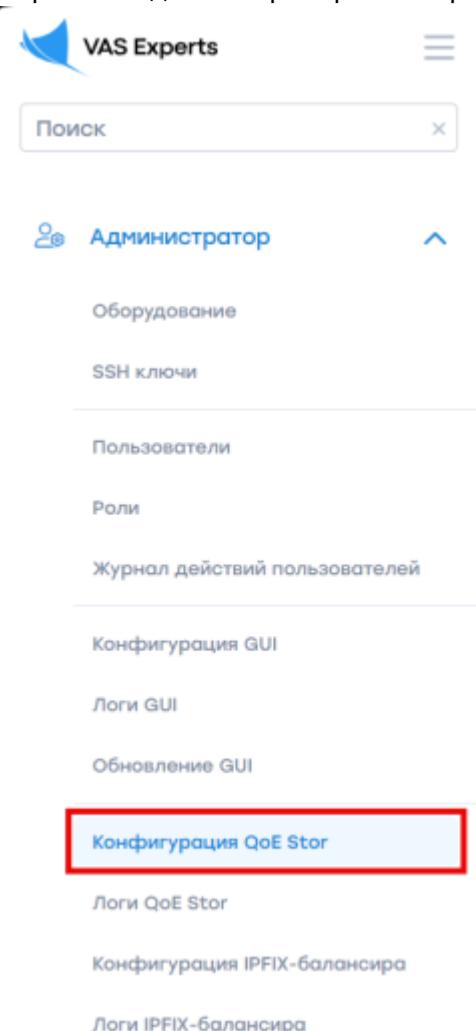
Конфигурация NAT Flow

Есть 3 способа формирования NAT лога в QoE Stor (сервере статистики)

1. Получать NAT Flow отдельным потоком со СКАТ. Для этого на устройстве СКАТ необходимо настроить [экспорт трансляций на внешние коллекторы](#);
2. Получить NAT Flow из Netstream сторонних систем (не СКАТ);
3. Формировать NAT Flow из FullFlow средствами QoE Stor.

Настройка получения отдельного потока NAT Flow с DPI или NETSTREAM

1. Перейти: Администратор → Конфигурация QoE Stor;



2. Перейти в раздел "Ресиверы"; добавить новый ресивер; выбрать "Тип ресивера" — NAT Flow; дозаполнить форму добавления ресивера и нажать кнопку "Применить";

The screenshot shows the 'QoS Stor' configuration interface. The left sidebar lists various configuration sections like 'Фильтрация', 'Общие', 'Настройки Ulr', etc. The main area has tabs for 'Настройки' (selected), 'Ресиверы' (highlighted with a red box), and 'Форма'. A modal window titled 'Ресиверы' is open, showing a table with columns: 'Тип ресивера' (Receiver type), 'Тип порта' (Port type), 'Порт' (Port), 'Ротация в секундах' (Rotation in seconds), 'Ротация по флоу' (Rotation by flow), 'Задержка в секундах' (Delay in seconds), 'Размер очереди' (Queue size), 'Число процессов вставки' (Number of insertion processes), 'Экспорт' (Export), 'Идентификатор DPI' (DPI identifier), 'Балансир' (Balancing), 'Субрессиверы балансира' (Balancing subreceivers), 'Тип супприенников балансира' (Type of balancing suppliers), 'Балансир авто' (Auto balancing), 'Номер ядра балансира' (Balancing core number), and 'Отключено' (Disabled). The 'tcp' row is selected. At the bottom of the modal are 'Отменить' (Cancel) and 'Применить' (Apply) buttons.

3. Перейти в раздел формы "Настройки журнала NAT";
 1. Включить заполнение привязки IP-LGIN из fullflow (FILL_IP_LOGIN_BINDING_FROM_FULLFLOW);
 2. Включить добавление LOGIN в журнал NAT из привязки IP-LGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING).

Администратор > Конфигурация QoS Star

Конфигурация

Сохранить

Настройки журнала NAT

Импорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW)
Включено

Поля для сохранения при агрегировании журнала NAT (NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK)
0x1 - ID протокола, 0x2 - Тип события, 0x4 - IPv4 адрес источника, 0x8 - Порт источника, 0x10 - IPv4 адрес получателя, 0x20 - Порт получателя

Интервал времени для агрегирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL)
15 минут (По умолчанию)

Включить заполнение привязки IP-LINK из fullflow (FILL_IP_LOGIN_BINDING_FROM_FULLFLOW)
Включено

Включить добавление LOGIN в журнал NAT из привязки IP-LINK (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)
Включено

Использовать распределенную таблицу привязки IP-LINK (NAT_USE_DISTR_IP_LOGIN_BINDING)

Включение импорта событий NAT из FullFlow

Для включения импорта событий из FullFlow, передаваемого с DPI в QoE Stor:

1. Перейти: Администратор → Конфигурация QoE Stor;

Поиск

Администратор

Оборудование

SSH ключи

Пользователи

Роли

Журнал действий пользователей

Конфигурация GUI

Логи GUI

Обновление GUI

Конфигурация QoE Stor

Логи QoE Stor

Конфигурация IPFIX-балансиринга

Логи IPFIX-балансиринга

2. Импорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW) — Включить.

Администратор > Конфигурация QoE Stor

Конфигурация

Сохранить

Настройки

Настройки журнала NAT

Импорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW)

Включено

Поля для сохранения при агрегировании журнала NAT (NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK)
0x1 - ID протокола, 0x2 - Тип события, 0x4 - IPv4 адрес источника, 0x8 - Порт источника, 0x10 - IPv4 адрес получателя, 0x20 - Порт

Интервал времени для агрегирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL)
15 минут (По умолчанию)

Включить заполнение привязки IP-LOGIN из fullflow (FILL_IP_LOGIN_BINDING_FROM_FULLFLOW)

Включено

Включить добавление LOGIN в журнал NAT из привязки IP-LOGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)

Включено

Использовать распределенную таблицу привязки IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)

Агрегация NAT Flow

1. Перейти: Администратор → Конфигурация QoE Stor;

Поиск

Администратор

- Оборудование
- SSH ключи
- Пользователи
- Роли
- Журнал действий пользователей
- Конфигурация GUI
- Логи GUI
- Обновление GUI
- Конфигурация QoE Stor**
- Логи QoE Stor
- Конфигурация IPFIX-балансиринга
- Логи IPFIX-балансиринга

2. Выбрать "Настройки журнала NAT" → Выбрать поля для сохранения при агрегации журнала NAT, Интервал времени заполнения лога (по умолчанию 15 минут);

Поиск

Ноды QoE Stor

Сохранить

Настройки

Ресиверы

Фильтрация

Общие

Настройки Ifr

Настройки журнала FULLFLOW

Настройки журнала FULLFLOW AGG

Настройки журнала CLICKSTREAM AGG

Настройки журнала NAT

Настройки журнала ONLINEFLOW

Настройки OpenCellid

Настройки сервиса сбора статистики UPLINK LOAD RATE

Настройки сервиса сбора аномалий в GTP

Список зараженных хостов Касперского

Поля для сохранения при агрегировании журнала NAT (NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK)

Интервал времени для агрегирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL)

15 минут (По умолчанию)

Включить заполнение привязки IP-LOGIN из fullflow (FILL_IP_LOGIN_BINDING_FROM_FULLFLOW)

Включить добавление LOGIN в журнал NAT из привязки IP-LOGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)

Использовать распределенную таблицу привязки IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)

3. Сохранить изменения и перезапустить сервис.