## Содержание

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

# 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 CKAT);
- 3. Формировать NAT Flow из FullFlow средствами QoE Stor.

## Настройка получения отдельного потока NAT Flow с DPI или NETSTREAM

1. Перейти: Главное меню → Администратор → Конфигурация сервера QoE Stor → Конфигурация сервера QoE Stor.



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

Конфигурация																			>					
ិ Сохранить ា ④ ာ		C 0 •							Форма		_	Pe	дактор											
© <sub>©</sub> Настройки	۲	Реси	веры																					
Ресиверы	+																							
Фильтрация	lг	Тип р	есивер	a		٦	Тип пор	та			П	орт				Субј 🗇 Тип	🗇 Балк	Hore	м					
Общие	L I	NAT флоу 🗸				, <sup>®</sup> top			~		D 15	1500		۲	tcp									
Настройки Ulr	Ротация в минутах					Ротация в сек			сундах		Р0 Э	Ротация по флоу 0			0	tcp								
Настройки журнала FULLFLOW	Задержка в секундах				ундах Размер очере			очереди			число процессоя		цессов	вставки	-	tcp		~						
Настройки журнала FULLFLOW AGG		0				3	10		© 0				)			tcp		4						
Настройки журнала CLICKSTREAM AGG		Экспорт 10.0.0.2/9920/tcp,10.0.0.3/3440				Иденті tcp,10.0.0.3/3440/L 🕙 -1			нтификатор DPI			Балансир Отключено			, ®	tcp								
Настройки журнала NAT		Субресиверы балансира 10.0.0.2/9920,10.0.0.3/3440 Номер ядра балансира					Субресиверы балансира				•	Тип суб	п субприемников балансира			Бо	Балансир авто				tcp			
Настройки журнала ONLINEFLOW							Номер ядра балансира					cop			~	Стключено С					top			
Настройки журнала DNS AGG	0															tcp								
Настройки OpenCellID			Отменить Применить							top														
Настройки сервиса сбора аномалий в GTP						_										tcp								
Настройки сервиса сбора статистики UPLINK LOAD RATE	ø	Q	Кликст	ı top	15013	2	o	0	400	10		0		30		top								
Список зараженных хостов Касперского		Q	NAT ф	r tcp	1900	10	0	0	o	10		0		10		tcp								
Настройки кластера		O)	DNS db	tcp	15014	1	0	0	0	10		0	188,134.	30		tcp								

- 3. Перейти в раздел формы "Настройки журнала NAT";
  - 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).

=	Администратор > Конфигурация QoE Stor	🚽 💇 /	<b>?**</b>	EK							
Ноды QoE	Конфигурация			>							
	🔁 Сохранить 🕄 🕑 🕤	2 🔲 Форма  Редактор									
Stor	© Настройки	В Настройки журнала NAT									
7	Ресиверы	Импорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW)									
	Фильтрация	Включено	~	1							
	Общие	Поля для сохранения при агрегировании журнала NAT (NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK)									
	Настройки Ulr	0х1 - ID протокола, 0x2 - Тип события, 0x4 - IPv4 адрес источника, 0x8 - Порт источника, 0x10 - IPv4 адрес получателя, 0x20 - Порт	~	U							
	Настройки журнала FULLFLOW	Интервал времени для агрегирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL)									
	Настройки журнала FULLFLOW AGG	יין אווא איזאין איז									
	Настройки журнала CLICKSTREAM AGG	Включить заполнение привязки IP-LOGIN из fullflow (FILL_IP_LOGIN_BINDING_FROM_FULLFLOW) Включено									
	Настройки журнала NAT	Включить добавление LOGIN в журнал NAT из привязки IP-LOGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING) Включено									
	Настройки журнала ONLINEFLOW										
	Настройки журнала DNS AGG	Использовать распределенную таблицу привязки IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)		•							
	Настройки OpenCellID		~	C							
	Настройки сервиса сбора аномалий в GTP			$\triangleright$							
	Настройки сервиса сбора статистики UPLINK LOAD RATE										
	Список зараженных хостов Касперского										
•	Настройки кластера			<b>_</b>							

#### Включение импорта событий NAT из FullFlow

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

1. Перейти: Главное меню → Администратор → Конфигурация сервера QoE Stor → Конфигурация сервера QoE Stor;

	VAS Experts								
Поиск									
2	Администратор								
	Оборудование								
	SSH ключи								
	Пользователи								
	Роли								
	Журнал действий пользователей								
	Конфигурация GUI								
	Логи GUI								
	Обновление GUI								
[	Конфигурация QoE Stor								
	Логи QoE Stor								
	Конфигурация IPFIX-балансира								
	Логи IPFIX-балансира								

٢

2. Импорт событий NAT из fullflow (NAT\_IMPORT\_FROM\_FULLFLOW) — Включить.



#### Агрегация NAT Flow

1. Перейти: Главное меню → Администратор → Конфигурация сервера QoE Stor →

Конфигурация сервера QoE Stor;

	VAS Experts	≡
Пои	ICK	×
20	Администратор	^
	Оборудование	
	SSH ключи	
	Пользователи	
	Роли	
	Журнал действий пользователей	
	Конфигурация GUI	
	Логи GUI	
	Обновление GUI	
[	Конфигурация QoE Stor	
	Логи QoE Stor	
	Конфигурация IPFIX-балансира	
	Логи IPFIX-балансира	

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

$\boldsymbol{\prec}$	VAS Experts	=	Администратор > Конф	игурация QoE Stor	😠 A A 🖉	þ						
По	иск	×	Ноды QoE Stor <	QoE Stor < Kondpurypouve								
800	правление РСКР	Ť	QoE Stor	🗑 Сохранить 🖽 🕑 🗇	C 🕼 Форма 🥠 Редактор							
-1-	QoE аналитика	~		8¢ Настройки	В Настройки журнала NAT							
~	Cenercu VAS cloud	~		Ресиверы	Инпорт событий NAT из fullflow (NAT_IMPORT_FROM_FULLFLOW)							
				Фильтрация	Включено 🗸 🕐							
20	Администратор	^		Общие	Поля для сохранения при агрегировании журнала NAT (NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK)							
	Оборудование			Настройки Ulr	0х4 - IPv4 адрес источника, 0х10 - IPv4 адрес получателя, 0х20 - Порт получателя, 0х40 - IPv4 адрес источника после 🗸 🖤							
	Пользователи			Настройки журнала FULLFLOW	Интервол времени для огрегирования логов NAT (NAT_AGG_LOG_GROUP_TIME_INTERVAL) 15 минут (По унолчание) v @							
	Роли			Настройки журнала FULLFLOW AGG								
	Журнал действий пользователей			Настройки журнала CLICKSTREAM AGG	включить заполнение привизки и>-codin из тыптоw (Fitt_и>_codin_виолид_FROM_FottP-tow)							
				Настройки журнала NAT	Включить добовление LOGIN в журнол NAT из привязки IP-LOGIN (NAT_ADD_LOGIN_FROM_IP_LOGIN_BINDING)							
	конфигурация сол			Настройки журнала ONLINEFLOW	~ ®							
	/IONA GUI			Настройки OpenCellID	Использовать распределенную таблицу привяжи IP-LOGIN (NAT_USE_DISTR_IP_LOGIN_BINDING)							
	Обновление GUI			Настройки сервиса сбора аномалий в GTP	~ @							
	Конфигурация QoE Stor			Настройки сервиса сбора статистики UPLINK LOAD RATE								
	Логи QoE Stor			Список зараженных хостов Касперского								
	Конфигурация САРТСНА											
	Темплейт САРТСНА											
	Логи CAPTCHA											
>_	SSH терминал устройства	×										

3. Сохранить изменения и перезапустить сервис.