?????? ???????????? ???????? ?? KICS for Networks

Метод 1: Настройка типов подсетей

Можно снизить нагрузку, обусловленную работой технологии NIC путем корректного назначения типов подсетей в адресных пространствах, тогда контроль целостности сети будет выполняться только для нужных подсетей и направлений передачи данных, как указано в таблице ниже:

Подсеть отправителя	Подсеть получателя				
	Частная, IT	Частная, OT	Частная, DMZ	Публичная	Link-local
Частная, IT	нет	да	нет	нет	да
Частная, OT	да	да	да	да	да
Частная, DMZ	нет	да	нет	нет	да
Публичная	нет	да	нет	нет	да
Link-local	да	да	да	да	нет

Подробнее в онлайн-справке: https://support.kaspersky.com/KICSforNetworks/4.3/ru-RU/134913.htm

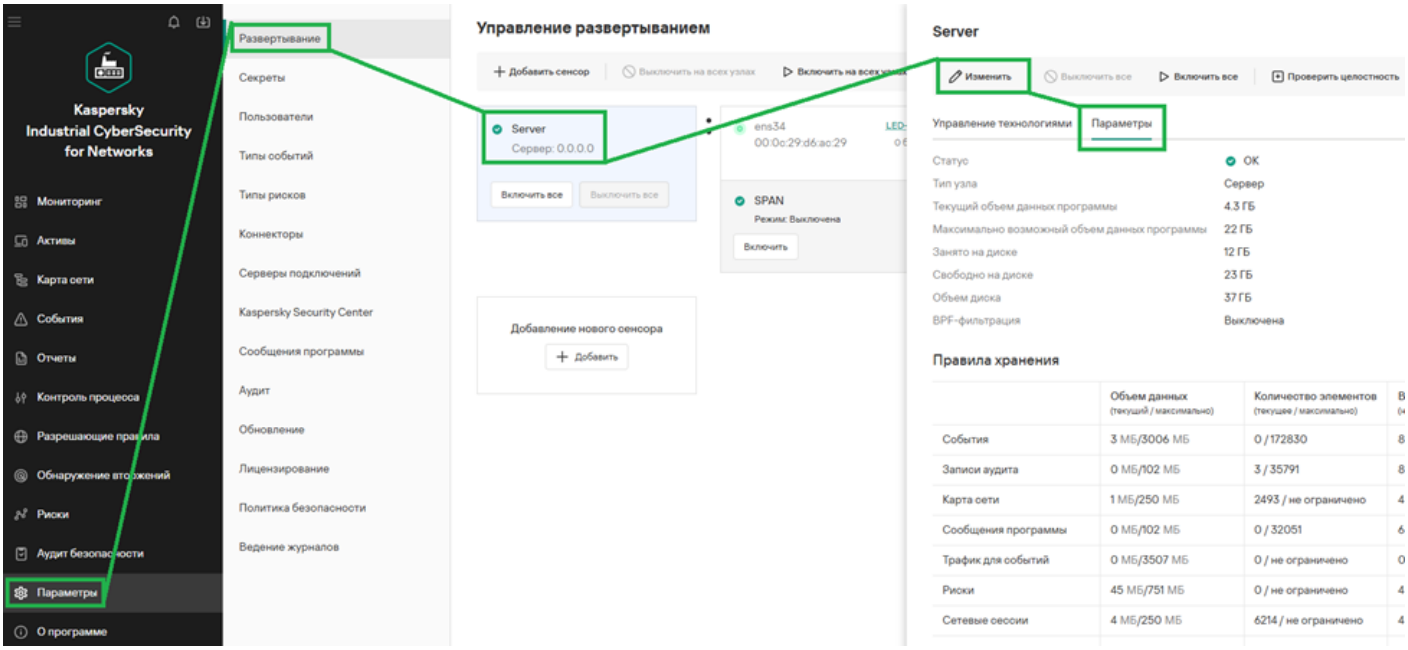
Метод 2: Использование BPF для фильтрации сохраняемого трафика

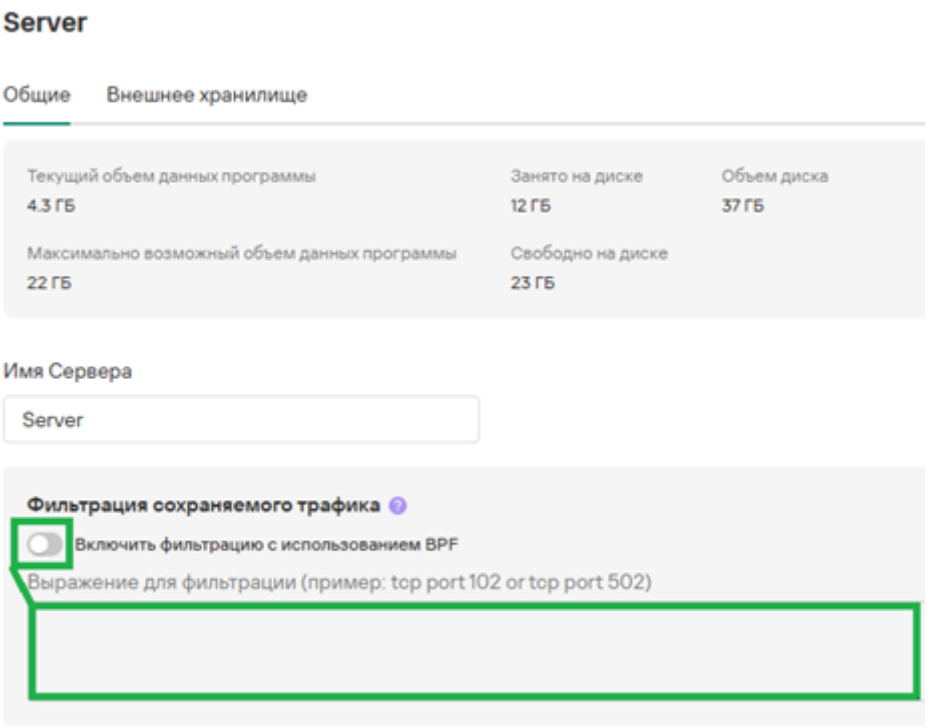
Использование технологии BPF (Berkley Packet Filter) позволяет отсечь заранее неинтересную часть трафика, чтобы не тратить на него ресурсы. Трафик, отсекаемый фильтром, не пишется на диск и никак не анализируется KICS for Networks. Благодаря этому снижается нагрузка на CPU и дисковую подсистему.

Наиболее типичные кейсы применения:

- видеонаблюдение, где объём трафика значительный, но зачастую, не представляющий большой ценности для анализа;
- наличие «неинтересного» корпоративного трафика в анализируемом SPAN-трафике.

Включить BPF-фильтр можно вот где:





Однако при использовании фильтрации вам нужно учитывать, что программа может получать в отфильтрованном трафике не все данные, необходимые для качественного анализа трафика. Вам нужно настроить фильтрацию таким образом, чтобы в файлах дампа трафика сохранялись все сетевые пакеты, которые требуются для анализа трафика в соответствии с функциональностью программы.

Примеры фильтров

Описание	BPF
Исключить TCP трафик с портом 80	not tcp port 80

Описание	BPF
Исключить TCP трафик с портами 80 и 22	not(tcp port 80 or tcp port 21)
Исключить видеонаблюдение RTP	not(udp port 5004 or udp port 5005)
Исключить коммуникации в/из подсети 10.42.0.0/16	not net 10.42.0.0/16
Исключить коммуникации в/из подсетей 10.42.0.0/16 и 192.168.0.0/16	not(net 10.42.0.0/16 or net 192.168.0.0/16)
Исключить TCP трафик с портом 80 только для коммуникаций в подсетях 10.42.0.0/16 и 192.168.0.0/16	not(tcp port 80 and (net 10.42.0.0/16 or net 192.168.0.0/16))

Проверка фильтра

Убедиться в работоспособности и правильности фильтра можно при помощи утилиты tcpdump:

tcpdump -n -r <pcapfile> 'BPF filter text'

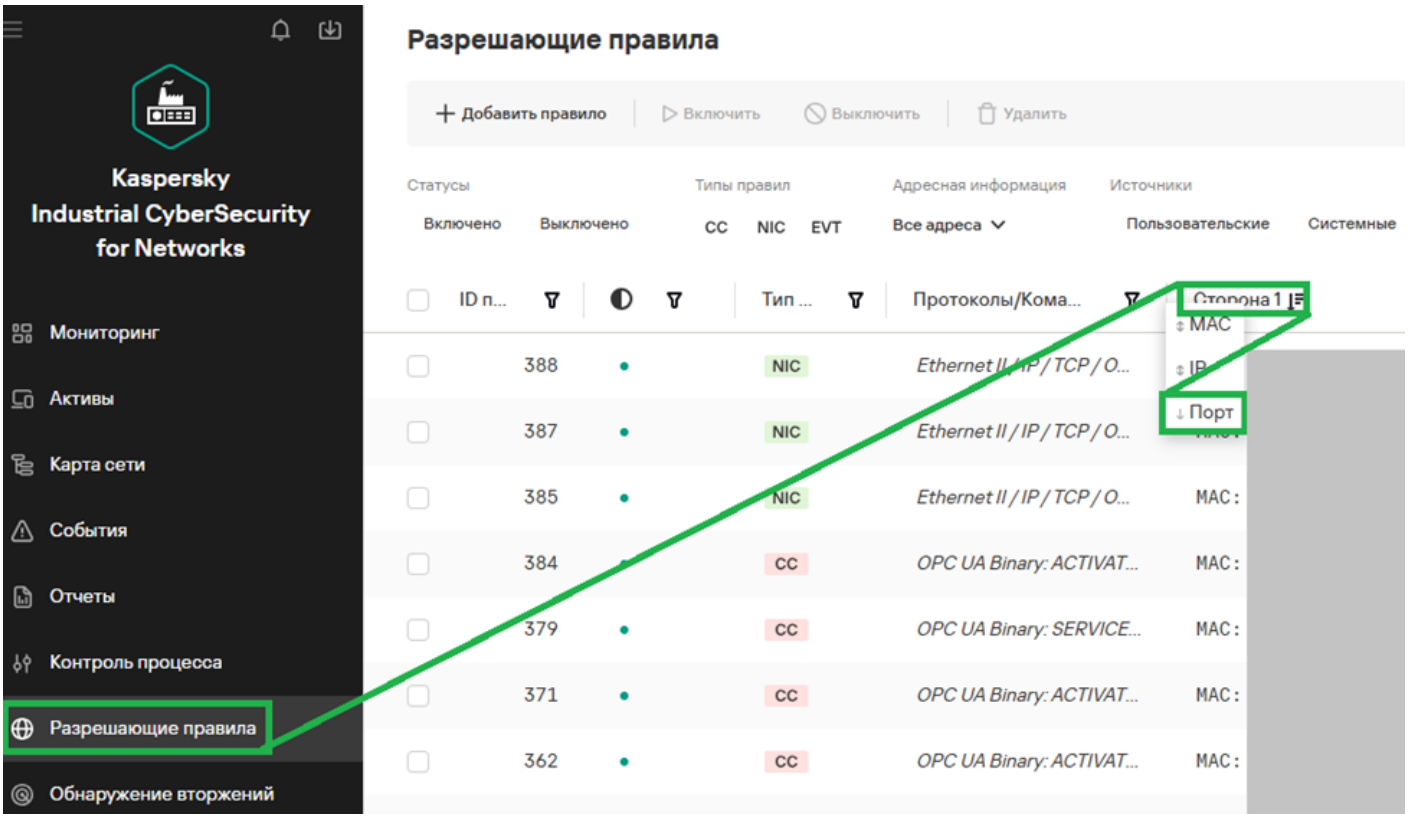
например

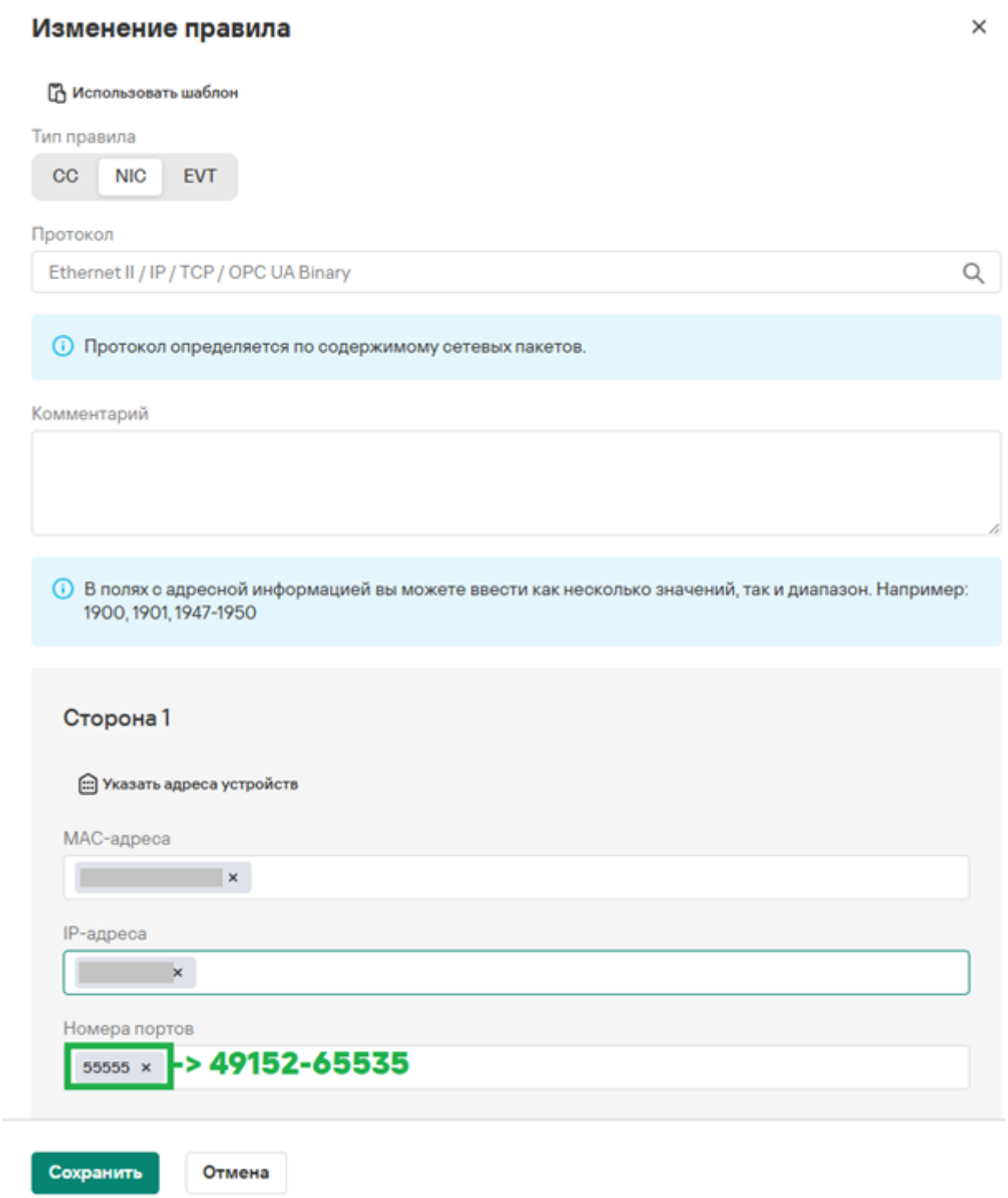
tcpdump -n -r capture.pcap 'udp portrange not 6970-6973'

Метод 3: Оптимизация разрешающих правил

Большое количество разрешающих правил может создавать повышенную нагрузку на продукт, поэтому следует контролировать их количество в период обучения KICS for Networks. Часто, большое количество разрешающих правил обусловлено тем, что для каждой новой сессии на отправителе выбирается случайный порт из динамического диапазона 49152-65535 (RFC 6335), поэтому для таких правил можно вместо конкретного порта, например, 55555 указать диапазон 49152-65535, после чего KICS for Networks предложит удалить все частные правила, подходящие под это - более общее. Удобно это сделать следующим образом:

Отсортировать разрешающие правила по убыванию портов.


Kaspersky Industrial CyberSecurity for Networks
Мониторинг
Активы
Карта сети
События
Отчеты
Контроль процесса
Разрешающие правила
Обнаружение вторжений
Разрешающие правила
Добавить правило
Включить
Выключить
Удалить
Статусы
Включено
Выключено
Типы правил
CC
NIC
EVT
Адресная информация
Все адреса
Источники
Пользовательские
Системные
ID п...
Тип ...
Протоколы/Кома...
Сторона 1
MAC
IP
Порт
388 NIC Ethernet II / IP / TCP / O...
387 NIC Ethernet II / IP / TCP / O...
385 NIC Ethernet II / IP / TCP / O... MAC :
384 CC OPC UA Binary: ACTIVAT... MAC :
379 CC OPC UA Binary: SERVICE... MAC :
371 CC OPC UA Binary: ACTIVAT... MAC :
362 CC OPC UA Binary: ACTIVAT... MAC :

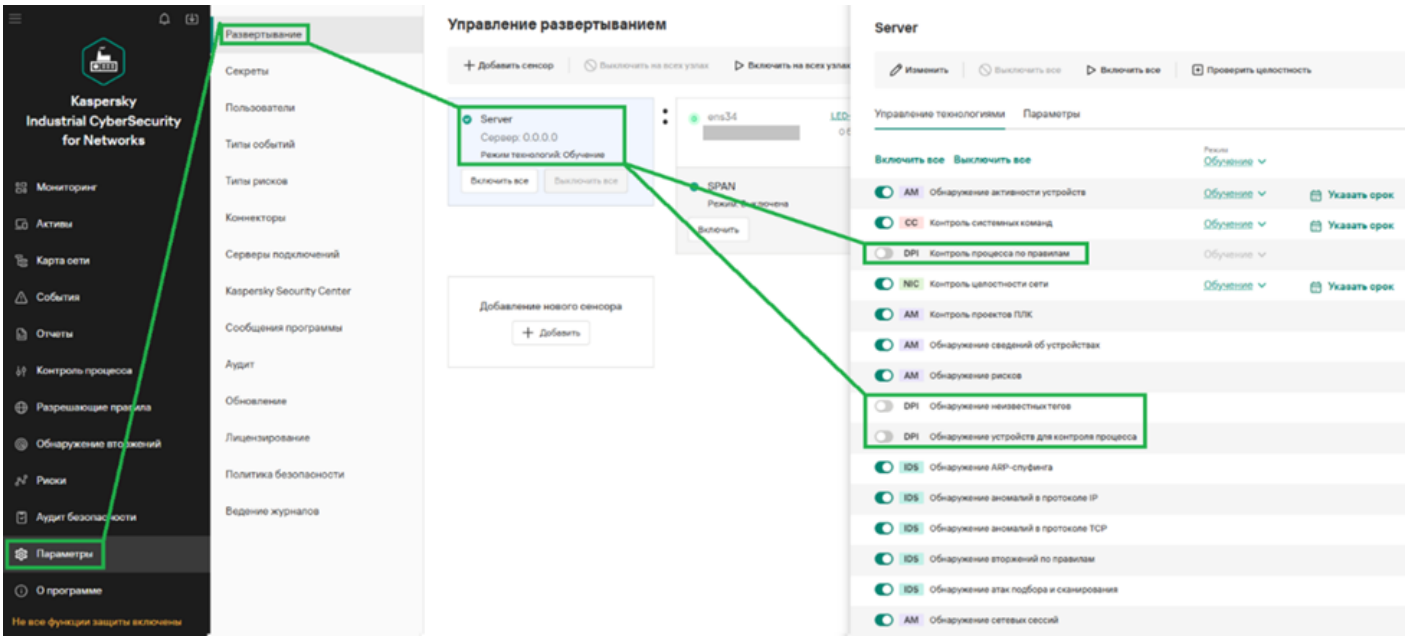


Метод 4: Выделение достаточного места под сырой трафик

Если выделить мало места для хранения файлов дампа трафика, то сервер будет хуже переносить пиковые нагрузки - во время таких нагрузок часть трафика может быть не проанализирована. Кроме того, чем больше выделено места под дампы трафика, тем за больший период времени этот трафик можно будет запросить при расследовании инцидентов. Например, при скорости 100 Мбит, 1 ТБ выделенного пространства позволит сохранить трафик за последние 22 часа.

Метод 5: Отключение ненужных технологий

Для снижения нагрузки на сервер можно отключить технологии детектирования, которые всё равно не планируется использовать в контексте мониторинга конкретной системы АСУ ТП. Наиболее частый случай отключение технологий DPI, если не планируется контролировать технологические параметры.



Метод 6: Оптимизация архитектуры

Для оптимизации нагрузки на сервер рекомендуются следующие архитектурные решения:

- весь трафик подавать на сенсоры, чтобы предварительная обработка трафика выполнялась на них;
- на сенсорах задействовать не более 4 точек мониторинга из 8 доступных.

Revision #2
Created 20 November 2025 13:42:05 by Sergey Malyugin
Updated 4 August 2026 11:43:48 by Boris Doroshenko