ОБНОВЛЕНО 16 МАР

Autopilot

Назначение модуля

Autopilot — это модуль интеллектуального анализа трафика, предназначенный для автоматической генерации правил защиты в реальном времени на основе текущего сетевого трафика. Он помогает оперативно реагировать на атаки, не требуя от администратора глубокого анализа трафика вручную.

Принцип работы

Модуль анализирует сетевой трафик, проходящий через **Сессионную защиту**, и автоматически формирует набор **контрмер**, которые можно применить для нейтрализации угроз. Эти меры строятся на основе математической модели. На выходе **Autopilot** предлагает готовые правила.

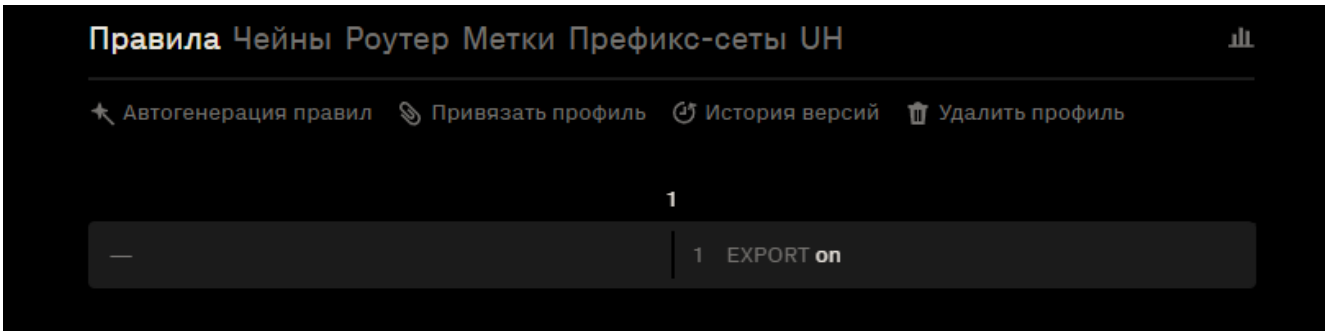
Настройка и запуск

1. Создание правила с действием EXPORT

Отправка трафика на анализ для построения правил автогенерации регулируется действием **EXPORT**. Без активного **EXPORT** трафик не попадёт в анализ, и кнопка **Автогенерация правил** останется недоступной.

Если до **EXPORT** стоит действие **DROP** или **ACCEPT**, то экспортируемых пакетов не будет. Экспортируются только те пакеты, которые проходят через систему (то есть те, что "принимаются", а не блокируются или отбрасываются в следствии применения правил).

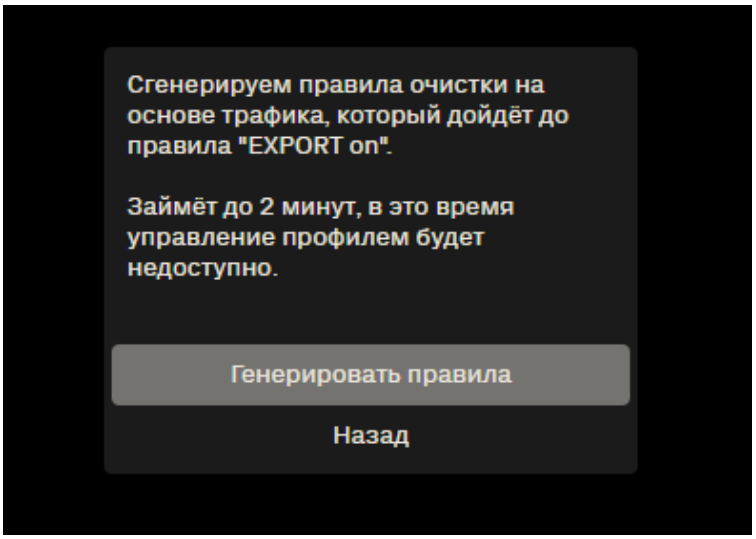
Допускается создание правила без указания **Совпадений**.



2. Запуск генерации правил

В интерфейсе станет активной кнопка

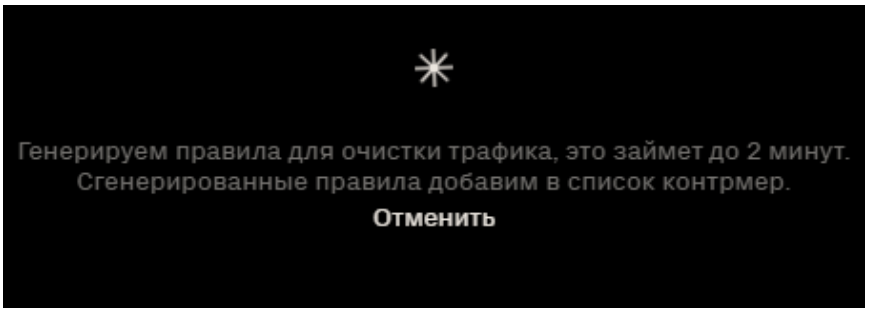
Нажать кнопку — запустится процесс сбора и анализа трафика на основе экспортируемых пакетов. На экране отобразится уведомление:



Ограничения при генерации контрмер:

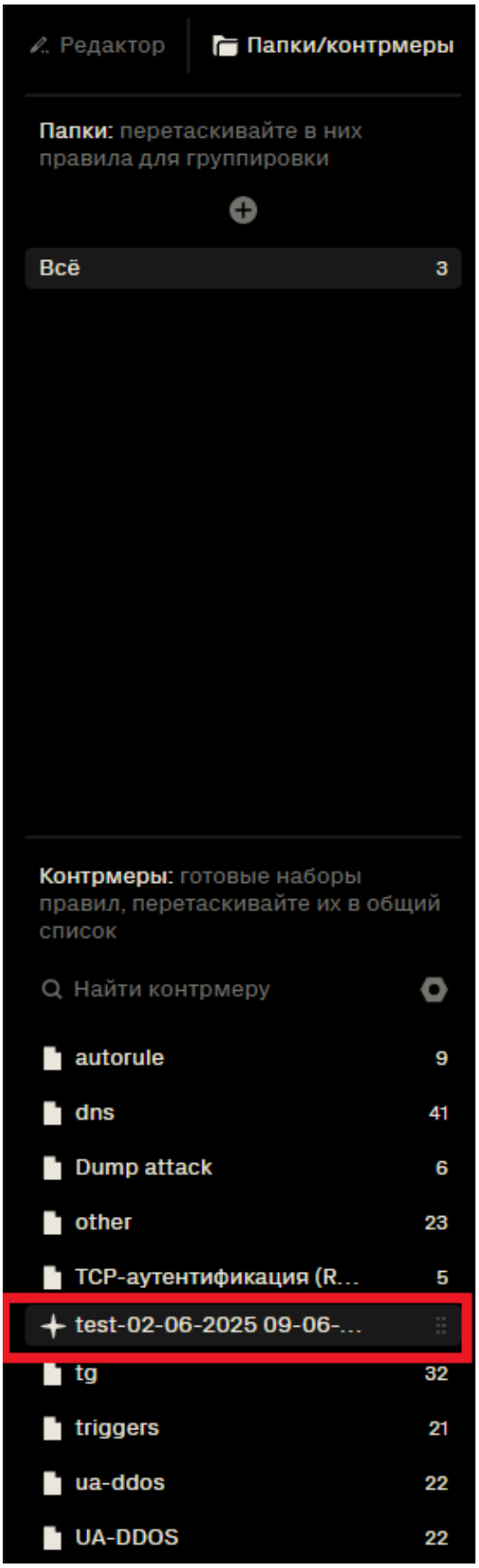
- Во время выполнения автогенерации контрмер редактирование правил **блокируется для профиля**, на котором запущена генерация. Это связано с тем, что модуль анализирует трафик с учётом текущей политики фильтрации, заданной профиле.
- **Одновременная генерация контрмер невозможна** — запуск автогенерации правил поддерживается только для одного профиля в один момент времени.

Нажать кнопку **Генерировать правила** для подтверждения запуска процесса. После подтверждения интерфейс отобразит статус выполнения:

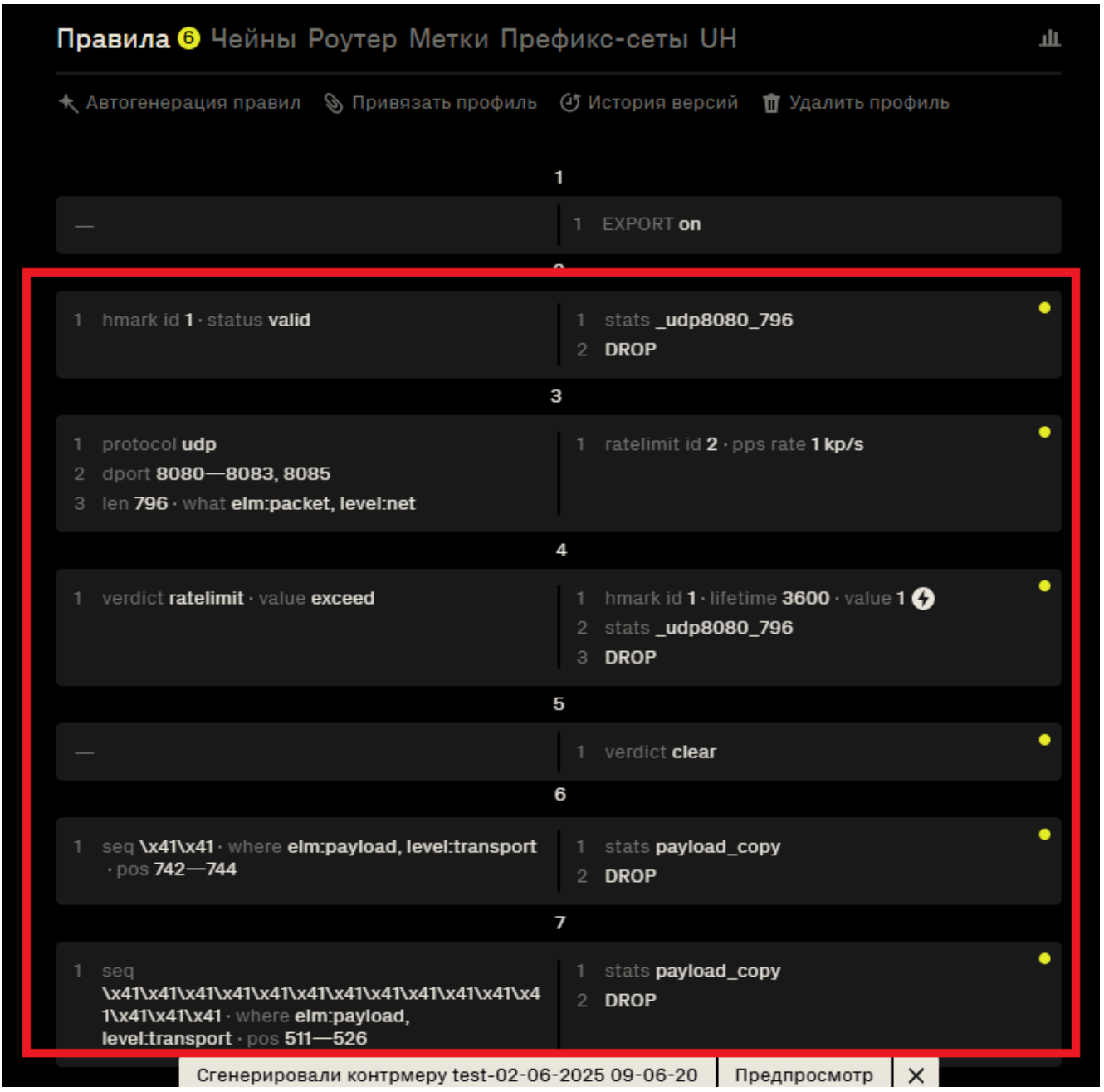


3. Получение и применение сгенерированных правил

После завершения генерации сгенерированный набор правил автоматически сохраняется в разделе **Контрмеры**, доступном во вкладке **Папки/контрмеры** на боковой панели интерфейса. Название набора формируется автоматически и включает имя исходного профиля, дату и время генерации.



Для применения набора необходимо перенести его в рабочий профиль. После переноса допускается просмотреть содержимое правил и внести корректировки. Далее нажать жёлтую кнопку **Применить** для активации изменений.


Правила 6 Чейны Роутер Метки Префикс-сеты UH
Автогенерация правил
Привязать профиль
История версий
Удалить профиль
1
— 1 EXPORT on
2
1 hmark id 1 · status valid
1 stats _udp8080_796
2 DROP
3
1 protocol udp
2 dport 8080—8083, 8085
3 len 796 · what elm:packet, level:net
1 ratelimit id 2 · pps rate 1 kp/s
4
1 verdict ratelimit · value exceed
1 hmark id 1 · lifetime 3600 · value 1
2 stats _udp8080_796
3 DROP
5
— 1 verdict clear
6
1 seq \x41\x41 · where elm:payload, level:transport · pos 742—744
1 stats payload_copy
2 DROP
7
1 seq \x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41 · where elm:payload, level:transport · pos 511—526
1 stats payload_copy
2 DROP
Сгенерировали контрмеру test-02-06-2025 09-06-20
Предпросмотр