ОБНОВЛЕНО 20 МАР

Установка и настройка сессионной защиты

Назначение

Сессионная защита — функция платформы DosGate, предназначенная для stateful-обработки сетевого трафика. Она позволяет анализировать соединения на уровне сессий, выявлять аномалии и применять защитные меры до передачи трафика в прикладные сервисы.

Сессионная защита использует базу вредоносных сигнатур для автоматического выявления и блокировки аномального трафика.

Функциональность

- Поддержка: TCP, UDP, SCTP, ICMP, ICMPv6.
- Принудительный разрыв соединений (active-close) без генерации исходящего трафика и без терминирования внутри системы.
- Анализ этапов установки соединения (Handshake).
- Обработка и фильтрация Client-Hello и Server-Hello.
- Контроль TLS SNI (Server Name Indication) и TLS ALPN (Application-Layer Protocol Negotiation).
- Проверка списка поддерживаемых шифров (Cipher List).
- Проверка и валидация контрольных сумм.
- Обнаружение и обработка IP-фрагментации с функцией дефрагментации.
- Поиск JA3 и JA4-отпечатков для анализа шифрованного трафика.
- Поиск TLS Cipher Suites для анализа безопасности и совместимости.

Установка и ввод в эксплуатацию

Внимание! Перед установкой и запуском рекомендуется снять весь продуктивный трафик с платформы.

Настройка конфигурации сессионной защиты

Редактирование конфигурационного файла

Для редактирования конфигурационного файла выполнить команду:

```
nano /etc/dosgate-uh.conf
```

Глобальная конфигурация

Задать глобальные параметры политики обработки сетевого трафика:

```
global:
  traffic-policy:
    good: accept   # Разрешение корректного трафика
    bad: drop      # Отклонение подозрительного трафика
    violate: drop  # Отклонение нарушающего трафика
```

Конфигурация сетевых устройств

Для эффективного управления очередями приема и передачи пакетов настроить параметры сетевых интерфейсов:

```
net:
  ens224:
    rx:
      queues:
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
  ens256:
    tx:
      queues:
        count: 8  # Количество очередей приема
        len: 512  # Длина каждой очереди
```

Настройки захвата трафика

Функция захвата трафика позволяет записывать сетевые пакеты в файлы для последующего анализа:

```
capture:
  path: /var/cache/dosgate-uh/capture      # Директория для сохранения
  filename: cap_${DEV}_${ID}_${NUM}.pcap   # Шаблон имен файлов
  age: 3600                                # Максимальное время хранения файла
(в секундах)
  count: 10                                # Максимальное количество файлов
  size: 10M                                # Максимальный размер файла
```

Конфигурация сбора и экспорта статистики

Статистика помогает отслеживать состояние системы в реальном времени и экспортировать данные в систему мониторинга:

```
stats:
  period: 10                               # Период сбора статистики (в секундах)
  push:
    type: collectd                         # Метод передачи данных
    plugin: unixsock                       # Используемый плагин
    target: /var/run/collectd-unixsock     # Целевой сокет
    stats: all                             # Объем передаваемых данных
    hostname: dosgate-uh01                 # Идентификатор хоста
    queue-len: 0                           # Длина очереди отправки
    period:
      collect: 5                           # Интервал сбора данных (в секундах)
      send: 10                             # Интервал отправки данных (в
секундах)
```

Настройка отслеживания подключений

Параметры контроля соединений позволяют задавать ограничения и определять политику обработки трафика:

```
conntrack:
  limit: 10000000       # Максимальное количество отслеживаемых соединений
  reclaim:
    soft: 80            # Порог мягкого освобождения соединений (в % от лимита)
    hard: 95            # Порог жесткого освобождения соединений (в % от
лимита)
```

Путь к каталогу с реестром профиля приложения

По умолчанию: **/var/lib/dosgate-uh/profiles**

```
application:
  registry: /var/lib/dosgate-uh/profiles
  monitor-fs: true
```

Настройка экспорта фреймов

Обеспечение работы функции экспорта фреймов, которая выполняется в рамках действия dosgate action `-j EXPORT`:

```
frame-export:
  enabled: true         # Включение функции экспорта фреймов
  export-objects: all   # Экспорт всех объектов
```

Установка пакета

```
sudo apt-get update
sudo apt-get install dosgate-uh=1.3.0-1
```

Обработка статистики в collectd

Collectd — служба сбора и передачи метрик. Для передачи статистики сессионной защиты необходимо описание типов метрик и перезапустить службу *collectd*.

Создать файл описания типов метрик **/etc/collectd/dosgate-uh-types.db**:

```
sudo touch /etc/collectd/dosgate-uh-types.db
```

Добавить в файл описания метрик следующие определения:

```
xsk_rx_frames frames:COUNTER:0:U
xsk_rx_bytes bytes:COUNTER:0:U
xsk_tx_frames frames:COUNTER:0:U
xsk_tx_bytes bytes:COUNTER:0:U
xsk_rx_drop drop:COUNTER:0:U
xsk_tx_error error:COUNTER:0:U
xsk_frame_alloc bytes:COUNTER:0:U
xsk_frame_alloc_error bytes:COUNTER:0:U
xsk_frame_free bytes:COUNTER:0:U
xsk_partial_writes bytes:COUNTER:0:U
xsk_full_reads bytes:COUNTER:0:U
xsk_opterr bytes:COUNTER:0:U
xsk_fill_frames frames:COUNTER:0:U
xsk_comp_frames frames:COUNTER:0:U
xsk_kick_tx bytes:COUNTER:0:U
xsk_rounds bytes:COUNTER:0:U
xsk_poll bytes:COUNTER:0:U
xsk_poll_nb bytes:COUNTER:0:U
xsk_rx_inv_desc bytes:COUNTER:0:U
xsk_tx_inv_desc bytes:COUNTER:0:U
xsk_rx_ring_full bytes:COUNTER:0:U
xsk_fill_ring_empty bytes:COUNTER:0:U
cap_frames frames:COUNTER:0:U
cap_bytes bytes:COUNTER:0:U
cap_rotates bytes:COUNTER:0:U
cap_errors bytes:COUNTER:0:U
proc_frames frames:COUNTER:0:U
proc_bytes bytes:COUNTER:0:U
proc_dg_error bytes:COUNTER:0:U
proc_frame_error bytes:COUNTER:0:U
proc_frame_verify_error bytes:COUNTER:0:U
proc_frame_mod_error bytes:COUNTER:0:U
proto_buf_alloc bytes:COUNTER:0:U
proto_buf_alloc_error bytes:COUNTER:0:U
proto_buf_destroy bytes:COUNTER:0:U
proto_map_alloc bytes:COUNTER:0:U
proto_map_alloc_error bytes:COUNTER:0:U
proto_map_destroy bytes:COUNTER:0:U
proto_stack_alloc bytes:COUNTER:0:U
proto_stack_alloc_error bytes:COUNTER:0:U
proto_stack_destroy bytes:COUNTER:0:U
tcp_open bytes:COUNTER:0:U
tcp_close bytes:COUNTER:0:U
tcp_seq_late bytes:COUNTER:0:U
tcp_seq_early bytes:COUNTER:0:U
```

```
tcp_large_syn bytes:COUNTER:0:U
tcp_invalid_checksum bytes:COUNTER:0:U
stream_block_alloc bytes:COUNTER:0:U
stream_block_alloc_error bytes:COUNTER:0:U
stream_block_free bytes:COUNTER:0:U
stream_shard_alloc bytes:COUNTER:0:U
stream_shard_alloc_error bytes:COUNTER:0:U
stream_shard_free bytes:COUNTER:0:U
ct_allocated bytes:COUNTER:0:U
ct_destroyed bytes:COUNTER:0:U
ct_alloc_error bytes:COUNTER:0:U
ct_reclaim_soft bytes:COUNTER:0:U
ct_reclaim_soft_scanned bytes:COUNTER:0:U
ct_reclaim_soft_reclaimed bytes:COUNTER:0:U
ct_reclaim_hard bytes:COUNTER:0:U
ct_reclaim_hard_scanned bytes:COUNTER:0:U
ct_reclaim_hard_reclaimed bytes:COUNTER:0:U
ct_collsisions bytes:COUNTER:0:U
ct_collision_reclaimed bytes:COUNTER:0:U
ct_collision_errors bytes:COUNTER:0:U
ct_overlimit bytes:COUNTER:0:U
ct_closed bytes:COUNTER:0:U
ct_timeout bytes:COUNTER:0:U
ct_frames_status_good bytes:COUNTER:0:U
ct_frames_status_bad bytes:COUNTER:0:U
ct_frames_status_violate bytes:COUNTER:0:U
ct_frames_error bytes:COUNTER:0:U
ct_frames_invalid bytes:COUNTER:0:U
tls_create bytes:COUNTER:0:U
tls_free bytes:COUNTER:0:U
tls_records bytes:COUNTER:0:U
tls_handshake bytes:COUNTER:0:U
tls_appdata bytes:COUNTER:0:U
tls_version_error bytes:COUNTER:0:U
tls_length_error bytes:COUNTER:0:U
tls_content_error bytes:COUNTER:0:U
tls_version_missmatch_error bytes:COUNTER:0:U
tls_system_error bytes:COUNTER:0:U
dtls_create bytes:COUNTER:0:U
dtls_free bytes:COUNTER:0:U
dtls_records bytes:COUNTER:0:U
dtls_handshake bytes:COUNTER:0:U
dtls_appdata bytes:COUNTER:0:U
dtls_tls12_cid bytes:COUNTER:0:U
dtls_tls13_uh bytes:COUNTER:0:U
dtls_version_error bytes:COUNTER:0:U
dtls_length_error bytes:COUNTER:0:U
dtls_content_error bytes:COUNTER:0:U
dtls_system_error bytes:COUNTER:0:U
dtls_epoch_error bytes:COUNTER:0:U
dtls_seq_error bytes:COUNTER:0:U
mem_pbuf_alloc bytes:COUNTER:0:U
mem_pbuf_alloc_error bytes:COUNTER:0:U
```

```
mem_pbuf_free bytes:COUNTER:0:U
mem_pbuf_data_alloc bytes:COUNTER:0:U
mem_pbuf_data_alloc_error bytes:COUNTER:0:U
mem_pbuf_data_free bytes:COUNTER:0:U
mem_seg_alloc bytes:COUNTER:0:U
mem_seg_alloc_error bytes:COUNTER:0:U
mem_seg_free bytes:COUNTER:0:U
mem_hash_alloc bytes:COUNTER:0:U
mem_hash_alloc_error bytes:COUNTER:0:U
mem_hash_free bytes:COUNTER:0:U
offenders_alloc bytes:COUNTER:0:U
offenders_alloc_error bytes:COUNTER:0:U
offenders_destroy bytes:COUNTER:0:U
offenders_first bytes:COUNTER:0:U
offenders_known bytes:COUNTER:0:U
offenders_error bytes:COUNTER:0:U
offenders_reg_error bytes:COUNTER:0:U
offenders_queued bytes:COUNTER:0:U
offenders_queue_overflow bytes:COUNTER:0:U
offenders_lost bytes:COUNTER:0:U
offenders_exported bytes:COUNTER:0:U
offenders_handler_miss bytes:COUNTER:0:U
offenders_handler_expired bytes:COUNTER:0:U
offenders_handler_send bytes:COUNTER:0:U
offenders_handler_send_error bytes:COUNTER:0:U
offenders_child_restart_request bytes:COUNTER:0:U
offenders_child_restart bytes:COUNTER:0:U
push_msg_alloc bytes:COUNTER:0:U
push_msg_alloc_error bytes:COUNTER:0:U
push_msg_free bytes:COUNTER:0:U
push_created bytes:COUNTER:0:U
push_create_error bytes:COUNTER:0:U
push_started bytes:COUNTER:0:U
push_socket_error bytes:COUNTER:0:U
push_config_error bytes:COUNTER:0:U
push_connect_start bytes:COUNTER:0:U
push_connect_error bytes:COUNTER:0:U
push_connect_timeout bytes:COUNTER:0:U
push_connect_success bytes:COUNTER:0:U
push_timeout bytes:COUNTER:0:U
push_send_error bytes:COUNTER:0:U
push_send_msgs bytes:COUNTER:0:U
push_enqueued bytes:COUNTER:0:U
push_enqueue_error bytes:COUNTER:0:U
push_rounds bytes:COUNTER:0:U
push_rounds_empty bytes:COUNTER:0:U
defrag_in bytes:COUNTER:0:U
defrag_valid bytes:COUNTER:0:U
defrag_dup bytes:COUNTER:0:U
defrag_invalid bytes:COUNTER:0:U
defrag_out bytes:COUNTER:0:U
defrag_reclaim_soft bytes:COUNTER:0:U
defrag_reclaim_hard bytes:COUNTER:0:U
```

```
defrag_scan_confirmed bytes:COUNTER:0:U
defrag_scan_new bytes:COUNTER:0:U
defrag_reclaim_new bytes:COUNTER:0:U
defrag_confirm_new bytes:COUNTER:0:U
defrag_full bytes:COUNTER:0:U
defrag_error bytes:COUNTER:0:U
defrag_frag_alloc bytes:COUNTER:0:U
defrag_frag_alloc_error bytes:COUNTER:0:U
defrag_frag_free bytes:COUNTER:0:U
defrag_entry_alloc bytes:COUNTER:0:U
defrag_entry_alloc_error bytes:COUNTER:0:U
defrag_entry_free bytes:COUNTER:0:U
defrag_key_error bytes:COUNTER:0:U
defrag_key_id_error bytes:COUNTER:0:U
```

Открыть конфигурационный файл службы *collectd*:

```
sudo nano /etc/collectd/collectd.conf
```

Добавить ссылку на файл с типами метрик:

```
TypesDB "/etc/collectd/dosgate-uh-types.db"
```

Перезапустить службу *collectd*, чтобы применить изменения:

```
sudo systemctl restart collectd
```

Запуск службы сессионной защиты

Сессионная защита реализуется службой *dosgate-uh*. Для управления службой выполните следующие команды:

Запустить службу:

```
sudo systemctl start dosgate-uh
```

Проверить статус службы:

```
sudo systemctl status dosgate-uh
```

Включить автозапуск службы:

```
sudo systemctl enable dosgate-uh
```

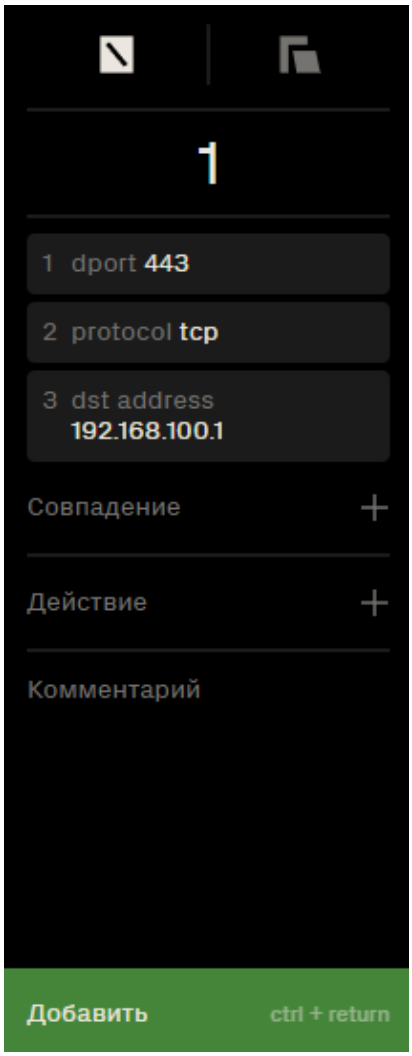
Направление трафика в сессионную защиту

Для передачи сетевого трафика на обработку в сессионную защиту необходимо создать правило фильтрации.

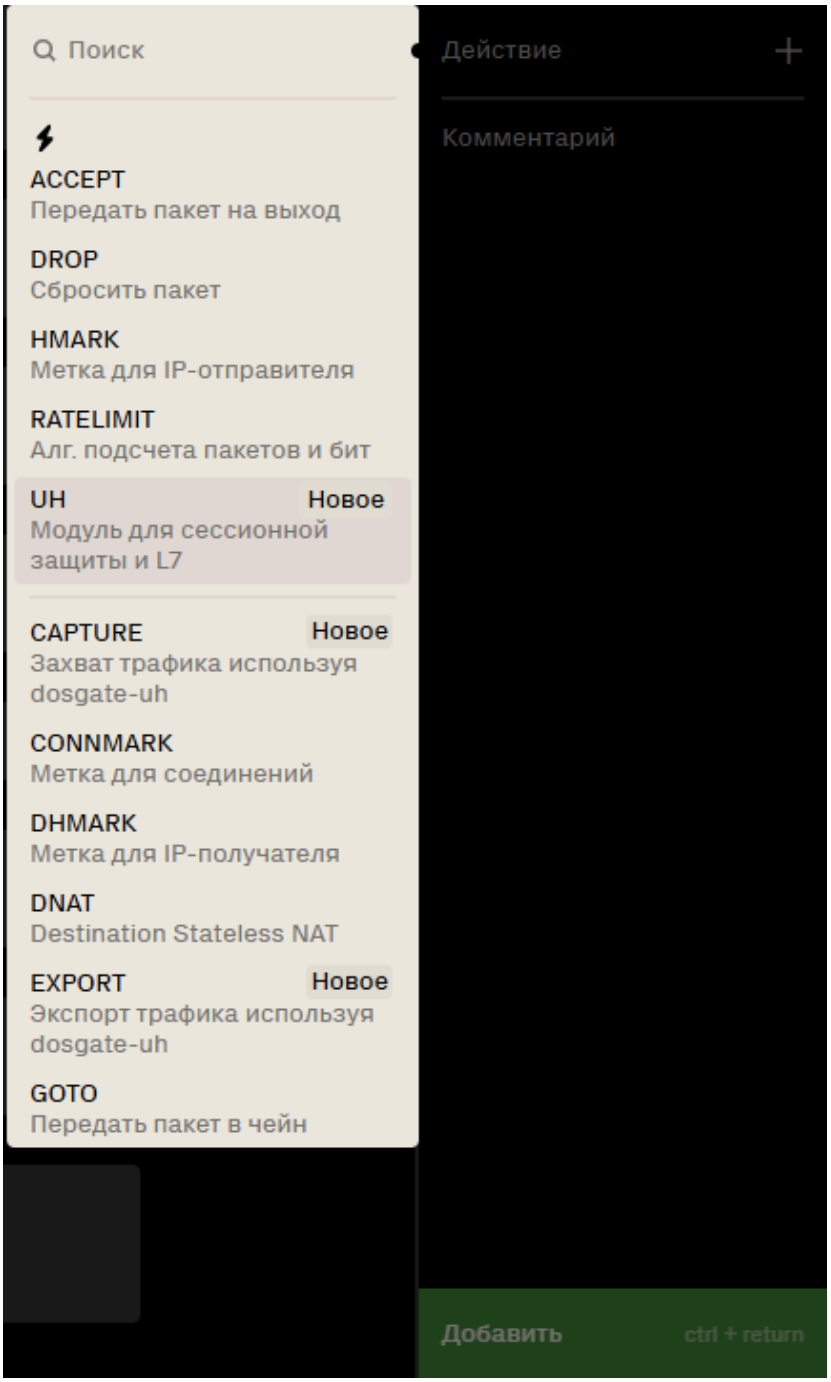
Настройка правила через веб-интерфейс

1. Открыть нужный профиль в DosGate.
2. Создать новое правило:

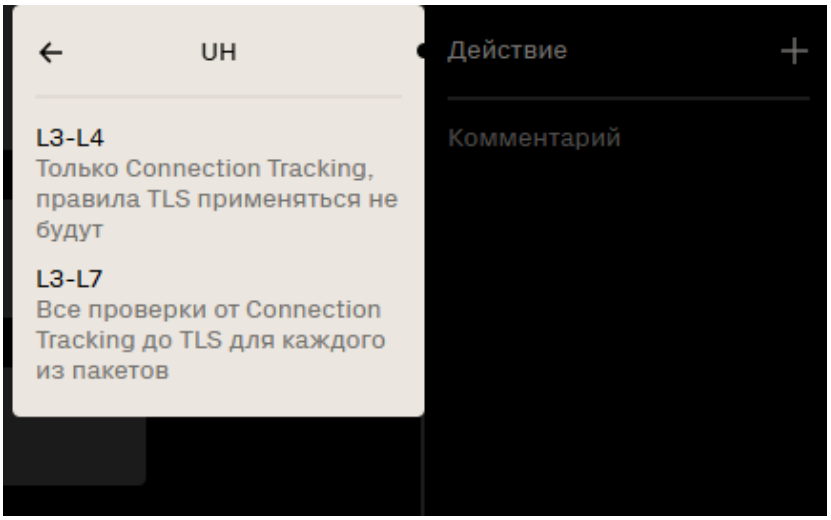
- В поле "Совпадение" указать условия, по которым будет фильтроваться трафик (например, IP-адреса, порты, протоколы):



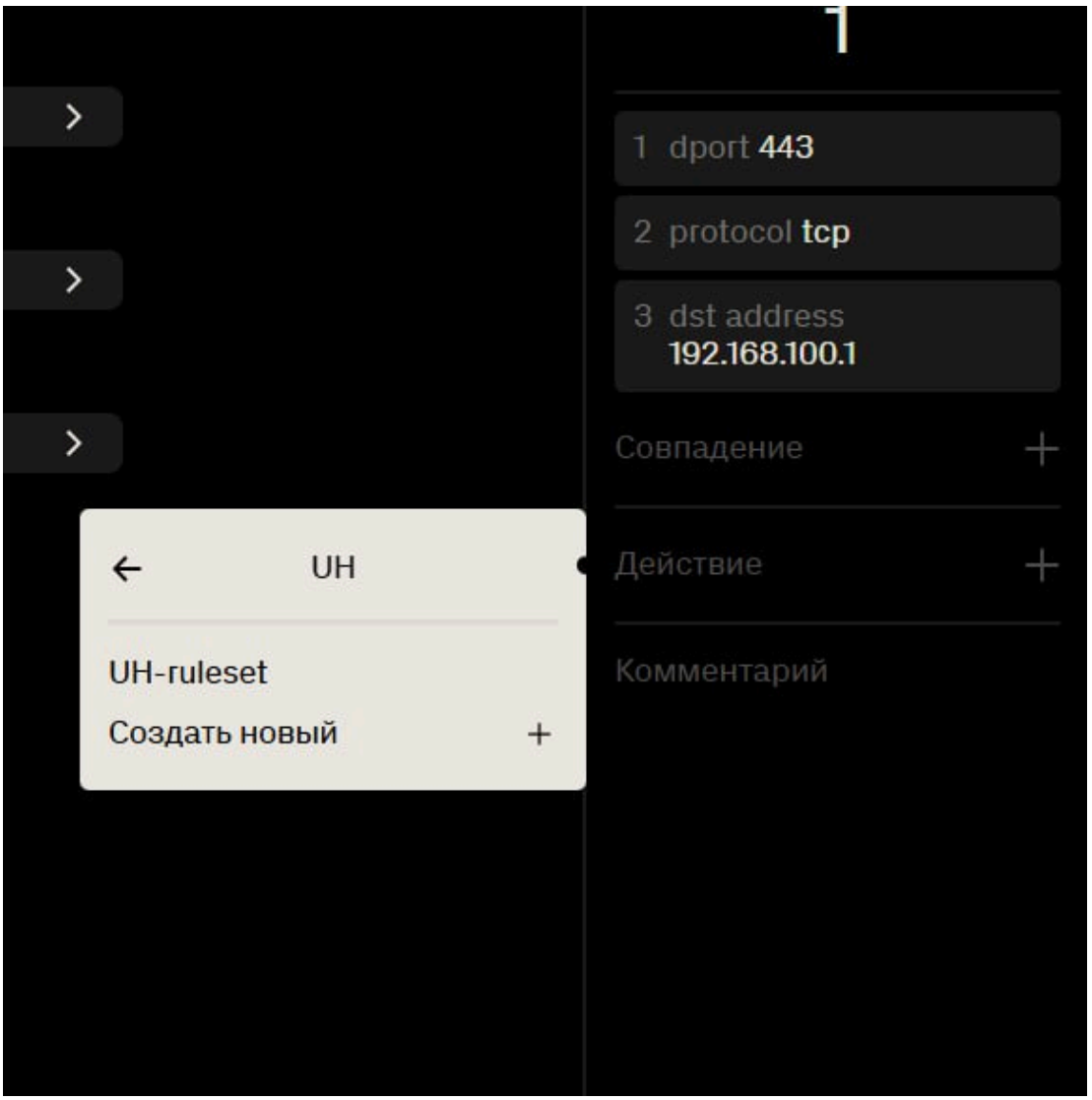
- В поле "Действие" выбрать "UH". Это действие направляет трафик на обработку в сессионную защиту.



- Выбрать вариант обработки трафика:



- Выбрать существующий UH или создать новый:



Примечание: подробнее о первичной настройке UH можно узнать в Руководстве пользователя

- При необходимости оставить комментарий к правилу и нажать зеленую кнопку **Добавить**.

Нажать **Применить**, чтобы правило вступило в силу. После этого трафик будет направляться в сессионную защиту.

Настройка правила через CLI

Для добавления правила выполнить следующую команду:

```
dgctl -u profile://<arena-name>/<profile-name> -c insert -- -m protocol tcp -m dst 192.168.100.1 -m dport 443 -j PASS uh app tls 1
```

Параметры команды:

- `<arena-name>` — имя арены в соответствии с файлом конфигурации `/etc/dosgate.conf`
- `<profile-name>` — имя профиля, используемого для обработки трафика
- `-m protocol tcp` — *(опционально)* указание протокола. По умолчанию можно направлять весь трафик
- `-m dst 192.168.100.1` — *(опционально)* фильтрация по IP-адресу получателя
- `-m dport 443` — *(опционально)* фильтрация по целевому порту
- `-j PASS` — действие, разрешающее передачу трафика на обработку в сессионную защиту
- `uh app tls` — параметры, указывающие на применение профиля `tls` для обработки
- `1` - ID политики приложения в файле policy

При необходимости направить весь трафик без дополнительных условий, создать правило без параметров `-m`:

```
dgctl -u profile://<arena-name>/<profile-name> -c insert -- -j PASS uh app tls 1
```

Диагностика и устранение проблем при запуске сессионной защиты

Работа службы сессионной защиты *dosgate-uh* зависит от сетевого драйвера и версии ядра операционной системы. При возникновении проблем рекомендуется выполнить

предварительные диагностические шаги и проверки, описанные ниже.

Предварительные действия перед внесением изменений

Перед выполнением изменений рекомендуется выполнить следующие шаги, чтобы избежать сбоев в работе:

1. **Перенаправление продуктивного трафика**
   Перед внесением изменений убедиться, что трафик направляется в обход DosGate.
2. **Остановка служб**
   Полностью остановить работающие службы *dosgate* и *dosgate-uh*:

```
sudo systemctl stop dosgate
sudo systemctl stop dosgate-uh
```

3. **Отключение XDP-программ**
   Для всех задействованных интерфейсов отключить XDP-программы:

```
sudo ip link set dev <interface_name> xdp off
```

где `<interface_name>` — имя сетевого интерфейса.

Действия перед запуском после внесения изменений

После выполнения настроек очистить кэш и подготовить систему к запуску:

```
rm -rf /sys/fs/bpf/dosgate
```

```
dgadm --batch=uh -y
```

Отключение zero-copy для службы dosgate-uh

В случае возникновения проблем с обработкой трафика попробуйте отключить режим zero-copy в файле конфигурации **/etc/dosgate-uh.conf**:

```
net:
  enp59s0f0:
    nozc: 1
  tx:
    ....
```

При отключении zero-copy рекомендуется активировать функцию **Оффендеры**.
Она позволяет блокировать IP-адреса вредоносных ботов на уровне *dosgate*, снижая нагрузку на службу *dosgate-uh*, особенно при использовании ресурсоемких алгоритмов.
Следует учитывать, что отключение zero-copy **снижает производительность службы dosgate-uh примерно в 2,1 раза.**

Перевод DosGate в generic-режим

Этот режим обладает сниженной производительностью, но может обеспечить корректную работу в средах, где использование XDP невозможно или нестабильно. Для изменения режима открыть конфигурационный файл **/etc/dosgate.conf** и задать параметр:

```
daemon:
    xdp-mode: generic
```

После изменения конфигурации перезапустить службу *dosgate*:

```
sudo systemctl restart dosgate
```

Связанные разделы

Сессионная защита