ОБНОВЛЕНО 16 МАР

Управление объектами FlowCollector

Объект — это набор IP-масок получателя, используемых для определения соответствия трафика заданным порогам.

Создание и редактирование объектов через веб-интерфейс

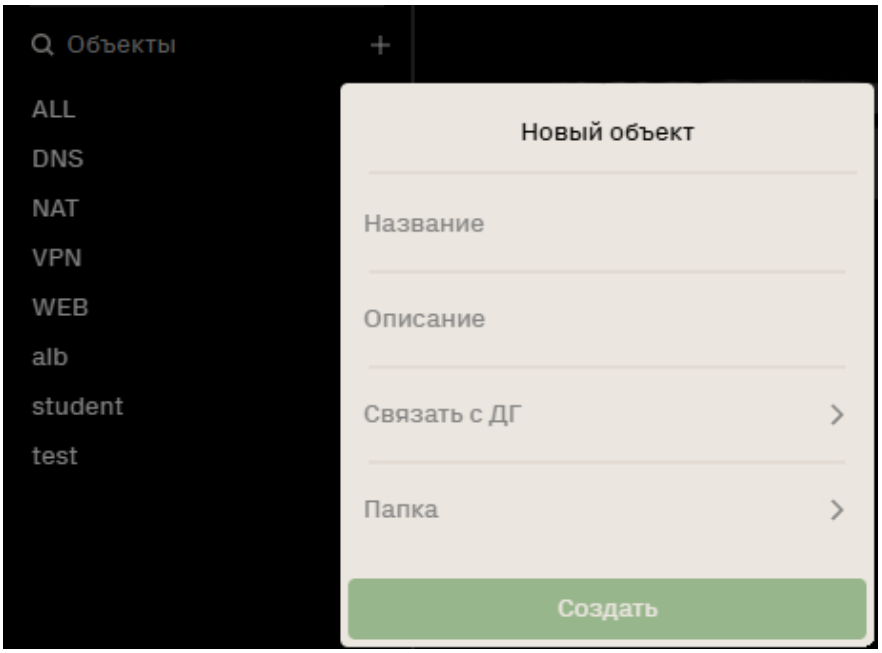
Создание объекта

Для создания нового объекта в системе выполнить следующие действия:

1. На главной странице в разделе **Объекты** нажать кнопку "+".

2. Заполнить следующие поля для создания объекта:

- **Название** - уникальное имя для объекта. Рекомендуется использовать комбинацию из обозначения сегмента инфраструктуры и названия сервиса, например, "zapadniy-filial-web" или "dmz-dns".
- **Описание** - краткое текстовое пояснение, которое поможет понять назначение объекта.
- **Связать с ДГ** - при наличии интеграции между FlowCollector и DosGate объект может быть привязан к профилю DosGate для корреляции событий и мониторинга трафика при обнаружении аномалий.
- **Папка** - для удобства объекты можно сгруппировать в папку, выбрав существующую или создав новую через опцию "Создать папку".



Изменение объекта

Для изменения объекта необходимо нажать правой кнопкой мыши на его названии в общем списке объектов и выбрать пункт **Изменить**. Откроется окно редактирования счётчиков.

Удаление объекта

В объекте предусмотрена возможность его удаления. Для удаления объекта необходимо нажать правой кнопкой мыши на его названии в общем списке объектов и выбрать пункт **Удалить**. После этого объект будет безвозвратно удален из системы.

Создание объекта через конфигурационный файл

Конфигурационный файл — это ещё один способ задания и управления параметрами объектов системы. Каждый объект системы настраивается индивидуально с помощью отдельного YAML-файла, который определяет ключевые параметры и пороговые значения для мониторинга и защиты сети.

Конфигурационные файлы объектов размещаются по пути:

```
/opt/spfc/etc/mo/
```

Допускается создание вложенных директорий для организации конфигураций. Например, конфигурации веб-сервисов можно структурировать следующим образом:

```
/opt/spfc/etc/mo/web/
/opt/spfc/etc/mo/filial1/service1.yaml
/opt/spfc/etc/mo/filial2/service2.yaml
```

Создание конфигурационного файла объекта

Для создания нового объекта выполнить следующую команду:

```
sudo nano /opt/sfpc/etc/mo/new-object.yaml
```

Структура конфигурационного файла объекта

```
name: new-object                                # Имя объекта, чувствительно к регистру

cidrs:                                          # IP-маски получателей объекта. Маска 0.0.0.0/0 не поддерживается
- 1.1.1.0/24
- 1.1.2.0/24

rules:                                          # Блок правил (порогов)
-                                               # Разделитель для правила
  type:                                         # Ключ подсчета трафика, global или local. Local - счетчик для каждого /32 в рамках IP-маски, то-есть, ключем является /32. Используется для детекции точных атак. Может быть оба сразу
  - local
  units:                                        # Единицы измерения. bytes или packets. Может быть оба сразу
  - bytes
  vectors:                                      # Векторы. Может быть несколько векторов сразу
  - total-traffic                               # Любой сетевой пакет (IPv4/IPv6)
  # - dns-flood                                 # UDP или TCP, порт получателя 53
  # - ip-fragment-flood                         # Пакет с установленным битом фрагментации
  # - icmp-flood                                # Протокол ICMP (только IPv4)
  # - tcp-flood                                 # Протокол TCP
```

```
  # - tcp-cwr-flood                          # TCP с флагом CWR (Congestion
Window Reduced, 0x80)
  # - tcp-ece-flood                          # TCP с флагом ECE (ECN-Echo,
0x40)
  # - tcp-urg-flood                          # TCP с флагом URG (Urgent
Pointer, 0x20)
  # - tcp-ack-flood                          # TCP с флагом ACK
(Acknowledgment, 0x10)
  # - tcp-psh-flood                          # TCP с флагом PSH (Push Function,
0x08)
  # - tcp-rst-flood                          # TCP с флагом RST (Reset, 0x04)
  # - tcp-syn-flood                          # TCP с флагом SYN (Synchronize,
0x02)
  # - tcp-fin-flood                          # TCP с флагом FIN (No more data,
0x01)
  # - udp-flood                              # Протокол UDP
  # - total-traffic                          # Любой сетевой пакет (IPv4/IPv6)
  # - invalid-protocol-flood                 # Пакет с идентификатором
протокола 0
  # - chargen-amp                            # UDP, порт источника 19
  # - dns-amp                                # UDP, порт источника 53
  # - ntp-amp                                # UDP, порт источника 123
  # - snmp-amp                               # UDP, порт источника 161
  # - snmptrap-amp                           # UDP, порт источника 162
  # - ldap-amp                               # UDP, порт источника 389
  # - mssql-amp                              # UDP, порт источника 1434
  # - ibm-cics-amp                           # UDP, порт источника 1435
  # - ssdp-amp                               # UDP, порт источника 1900
  # - apple-remote-desktop-amp               # UDP, порт источника 3283
  # - ws-discovery-amp                       # UDP, порт источника 3702
  # - memcached-amp                          # UDP, порт источника 11211
  # - udp-zero-payload-flood                 # UDP-флуд с нулевой полезной
нагрузкой
  # - udp-big-packets-flood                  # UDP-флуд с крупными по размеру
пакетами
  limit-threshold: 250000000               # Тип порога. Их несколько:
                                           #   Limit-threshold - статический
порог, в выбранных единицах измерения (байтах или пакетах)
                                           #   limit-diff - разница между
предыдущим значением (1000 мс.) и настоящим, например, увеличение за секунду на
50000 условных единиц
                                           #   Limit-reldiff - разница между
предыдущим значением (1000 мс.) и настоящим, например, увеличение за секунду в
5 раз (множитель)
                                           #   Можно использовать сразу
несколько, тогда любое из превышенных считается аномалией
- type:                                   # Ключ подсчета трафика
  - global
  units:                                   # Единицы измерения
  - packets
  vectors:                                 # Векторы
  - total-traffic
  - tcp-syn-flood
```

```
  limit-diff: 50000
  limit-threshold: 200000
```

Пример конфигурации объекта

```
name: web-services                          # Имя объекта

cidrs:                                      # IP-маски получателей объекта
- 1.1.1.0/24

rules:                                      # Блок правил (порогов)

-                                           # Объем трафика по любому из
векторов в сторону объекта
  type:
  - global                                  # Тип подсчета — глобальный
  units:
  - bytes                                   # Единицы измерения — байты
  limit-threshold: 2000000000               # Статический порог по суммарному
трафику

-                                           # Объем трафика по любому из
векторов в сторону любого /32
  type:
  - local                                   # Тип подсчета — локальный (по IP)
  units:
  - bytes                                   # Единицы измерения — байты
  limit-threshold: 500000000                # Статический порог на каждый IP

-                                           # DNS-flood
  type:
  - local                                   # Локальный и глобальный подсчет
  - global
  units:
  - bytes                                   # Единицы измерения — байты
  vectors:
  - dns-flood                               # Тип атаки — DNS-флуд
  limit-threshold: 100000000                # Статический порог по DNS-флуду
```

Активация объекта

Для активации объекта необходимо создать символическую ссылку на конфигурационный файл в директории активированных объектов:

```
sudo ln -s /opt/spfc/etc/mo/<file> /opt/spfc/etc/mo.enabled/<file>
```

Перезапустить сервис *analyzer* для активации объекта:

```
sudo systemctl start analyzer
```

Проверить текущий статус службы:

```
sudo systemctl status analyzer
```

Активация объекта считается завершённой после успешного запуска службы и отсутствия ошибок в статусе.