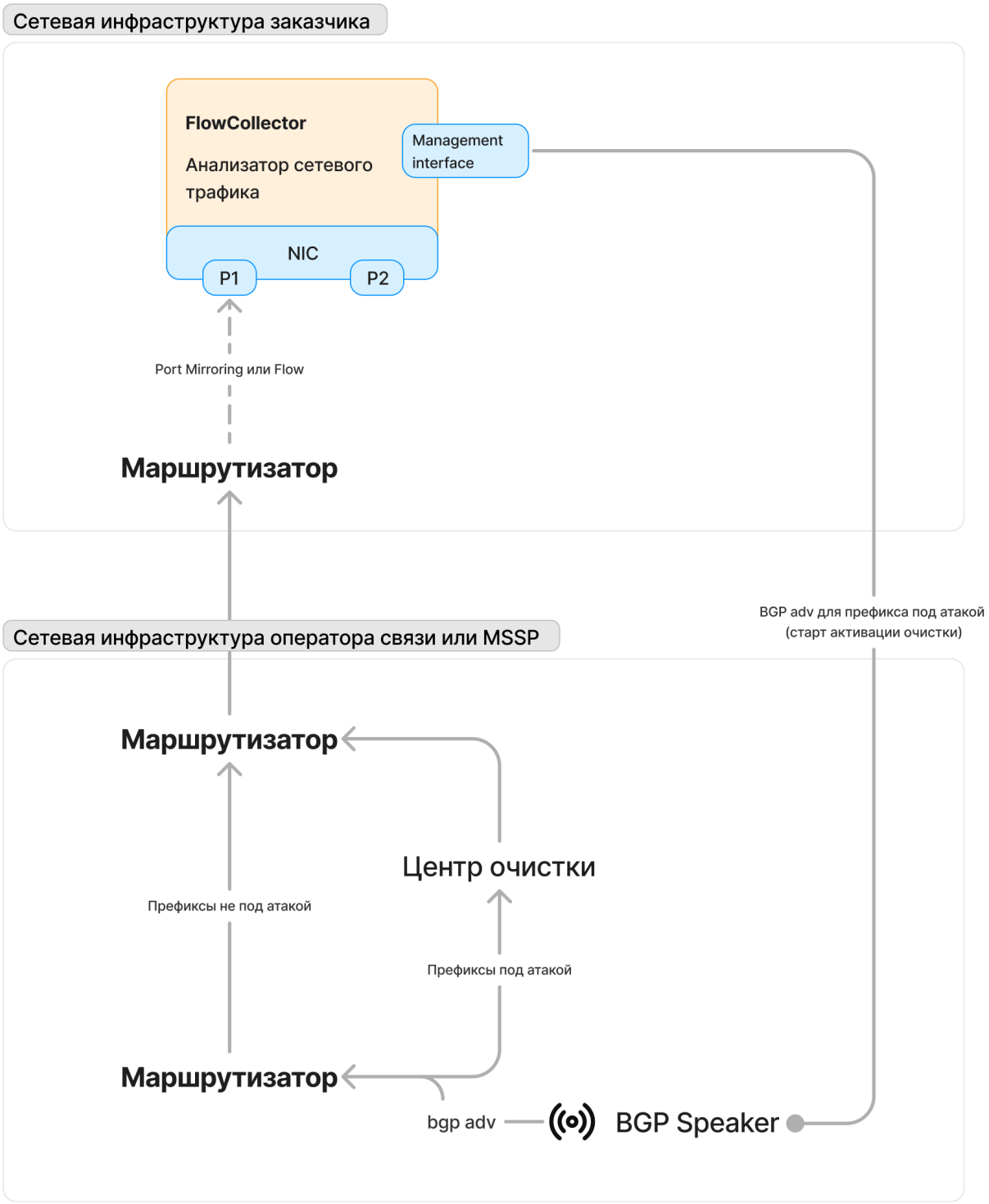
ОБНОВЛЕНО 16 МАР

# Облачная сигнализация (BGP)

Установленный на периметре сетевой инфраструктуры DosGate способен подавить вредоносный трафик до общей пропускной способности входящих каналов связи и производительности локальной инсталляции. В случае переполнения входящих каналов связи или локального центра очистки, FlowCollector может в автоматическом режиме подать сигнал о подключении фильтрации на вышестоящих операторов связи или MSSP (поставщиков услуг защиты).

FlowCollector реализует механизм облачной сигнализации за счет интеграции с GoBGP.




# Настройка сигнализации по BGP

FlowCollector на основании настроенных объектов защиты автоматически определяет начало и конец сетевой аномалии, а также префиксы находящиеся под атакой, которые он направит на вышестоящих операторов связи или MSSP.

## Установите GoBGP

```
sudo apt install gobgpd=3.19.0
```

## Активируйте GoBGP на FlowCollector в файле analyzer.yaml

При детекции сетевой аномалии (DDoS-атаки) - будут активироваться политики указанные в GoBGP

```
gobgp:
  enable: true
  # Хост GoBGP API
  host: localhost
  # Порт GoBGP API
  port: 50051
```

## Конфигурация политик маршрутизации

```
sudo nano /etc/gobgpd.conf
```

Замените в примере конфигурации следующие данные:

- `192.0.100.103` - IP-адрес FlowCollector
- `192.0.100.101` - IP первого BGP соседа
- `192.0.100.102` - IP второго BGP соседа
- `65003` - AS FlowCollector
- `65001` и `65002` - AS BGP соседей
- `192.0.1.101` - nexthop для первого BGP соседа
- `192.0.1.102` - nexthop для второго BGP соседа

```
[global.config]
  as = 65003
  router-id = "192.0.100.103"
  port = 179

[global.apply-policy.config]
```

```
export-policy-list = ["first-export-policy", "second-export-policy"]

[[neighbors]]
  [neighbors.config]
    neighbor-address = "192.0.100.101"
    peer-as = 65001
    [neighbors.ebgp-multihop.config]
      enabled = true

    [[neighbors.afi-safis]]
    [neighbors.afi-safis.config]
      afi-safi-name = "ipv4-unicast"

    [neighbors.transport.config]
      local-address = "192.0.100.103"

    [neighbors.apply-policy.config]
      default-import-policy = "reject-route"
      default-export-policy = "reject-route"

[[neighbors]]
  [neighbors.config]
    neighbor-address = "192.0.100.102"
    peer-as = 65002
    [neighbors.ebgp-multihop.config]
      enabled = true

    [[neighbors.afi-safis]]
    [neighbors.afi-safis.config]
      afi-safi-name = "ipv4-unicast"

    [neighbors.transport.config]
      local-address = "192.0.100.103"

    [neighbors.apply-policy.config]
      default-import-policy = "reject-route"
      default-export-policy = "reject-route"

[[defined-sets.neighbor-sets]]
  neighbor-set-name = "first-neighbor"
  neighbor-info-list = ["192.0.100.101"]

[[defined-sets.neighbor-sets]]
  neighbor-set-name = "second-neighbor"
  neighbor-info-list = ["192.0.100.102"]

[[defined-sets.prefix-sets]]
  prefix-set-name = "allowed-prefixes"
  [[defined-sets.prefix-sets.prefix-list]]
    ip-prefix = "0.0.0.0/0"
    masklength-range = "25..32"

[[policy-definitions]]
```

```
  name = "first-export-policy"
  [[policy-definitions.statements]]
    name = "first-statement"
    [policy-definitions.statements.conditions.match-prefix-set]
      prefix-set = "allowed-prefixes"
    [policy-definitions.statements.conditions.match-neighbor-set]
      neighbor-set = "first-neighbor"
    [policy-definitions.statements.actions]
      route-disposition = "accept-route"
    [policy-definitions.statements.actions.bgp-actions]
      set-next-hop = "192.0.1.101"

[[policy-definitions]]
  name = "second-export-policy"
  [[policy-definitions.statements]]
    name = "second-statement"
    [policy-definitions.statements.conditions.match-prefix-set]
      prefix-set = "allowed-prefixes"
    [policy-definitions.statements.conditions.match-neighbor-set]
      neighbor-set = "second-neighbor"
    [policy-definitions.statements.actions]
      route-disposition = "accept-route"
    [policy-definitions.statements.actions.bgp-actions]
      set-next-hop = "192.0.1.102"
```

## Перезапустите GoBGP

Перезапустите сервис, убедитесь что запустился демон

```
sudo systemctl enable --now gobgpd
sudo service gobgpd restart
sudo service gobgpd status
```

## Перезапустите FlowCollector

Перезапуск сервиса нужен для применения изменений к analyzer.yaml

```
sudo service analyzer restart
sudo service analyzer status
```

## Проверьте активные BGP-сессии

Команда покажет BGP-соседей и статус каждой сессии. Если всё настроено - все сессии должны быть успешно установлены ("Established")

```
sudo gobgp nei
```