

Практика внедрения BGP Flowspec в сети оператора связи



Дмитрий Онучин



```
root@core# show magic
```

```
class-map type traffic match-all fs_ex  
  match destination-address ipv4 a.b.c.d/32  
  match protocol udp  
  match destination-port 137-139 80 8080  
end-class-map
```

```
policy-map type pbr fs_table_ex  
  class type traffic fs_ex  
    police rate 8000 bps  
  class class-default  
end-policy-map
```

BGP Flowspec

О сервисе:

- **RFC5575**
- Позволяет передавать *Flow Specification* по протоколу BGP
- Можно представить как распределенный access-list на сети провайдера
- Часто используется для предотвращения некоторых видов DDoS атак на четвертом уровне OSI (Amplification/UDP flood).

Flow Specification

Параметры

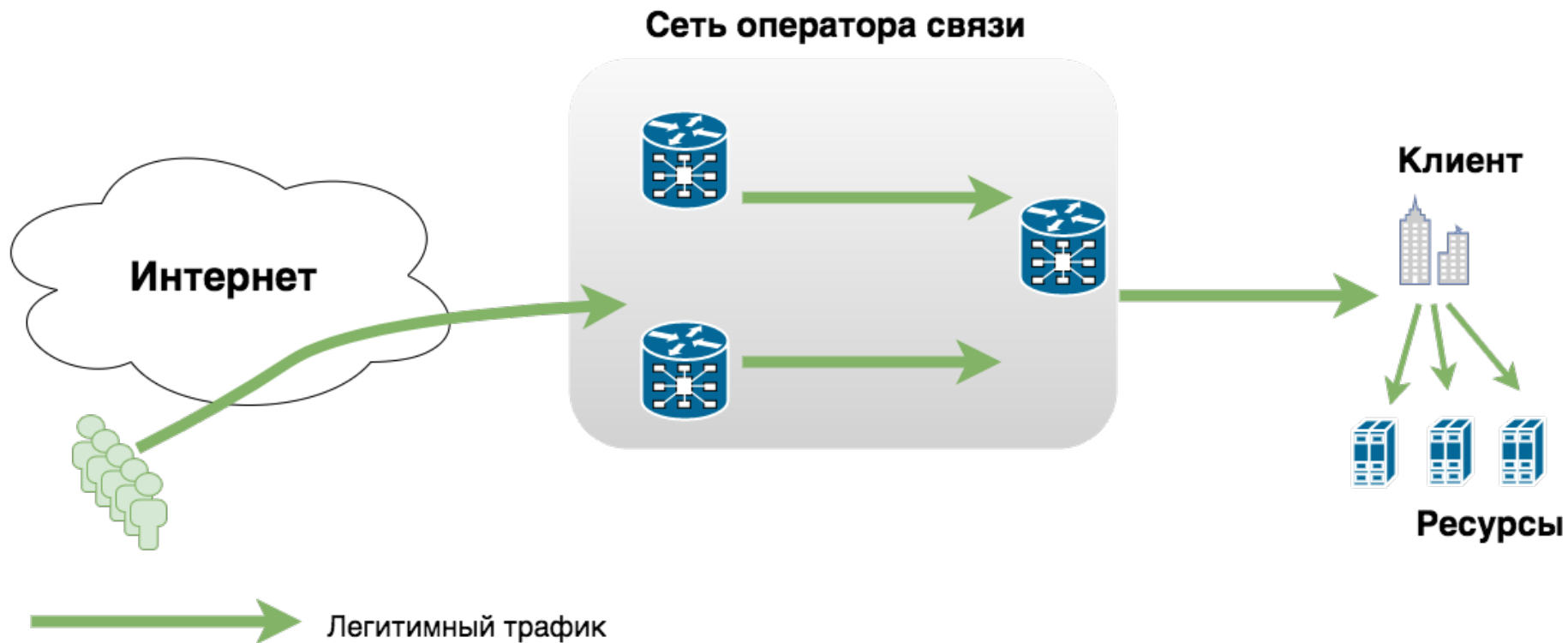
(передаются как NLRI):

1. Destination prefix
2. Source prefix
3. IP protocol
4. Port
5. Destination port
6. Source port
7. ICMP type
8. ICMP code
9. TCP flags
10. Packet length
11. DSCP
12. Fragment

Действия (передаются как extended-community):

- Traffic-rate
- Traffic-action
- Redirect
- Traffic-marking

Типичный сценарий атаки (до ddos)







Типичный сценарий атаки (ddos)

Сеть оператора связи

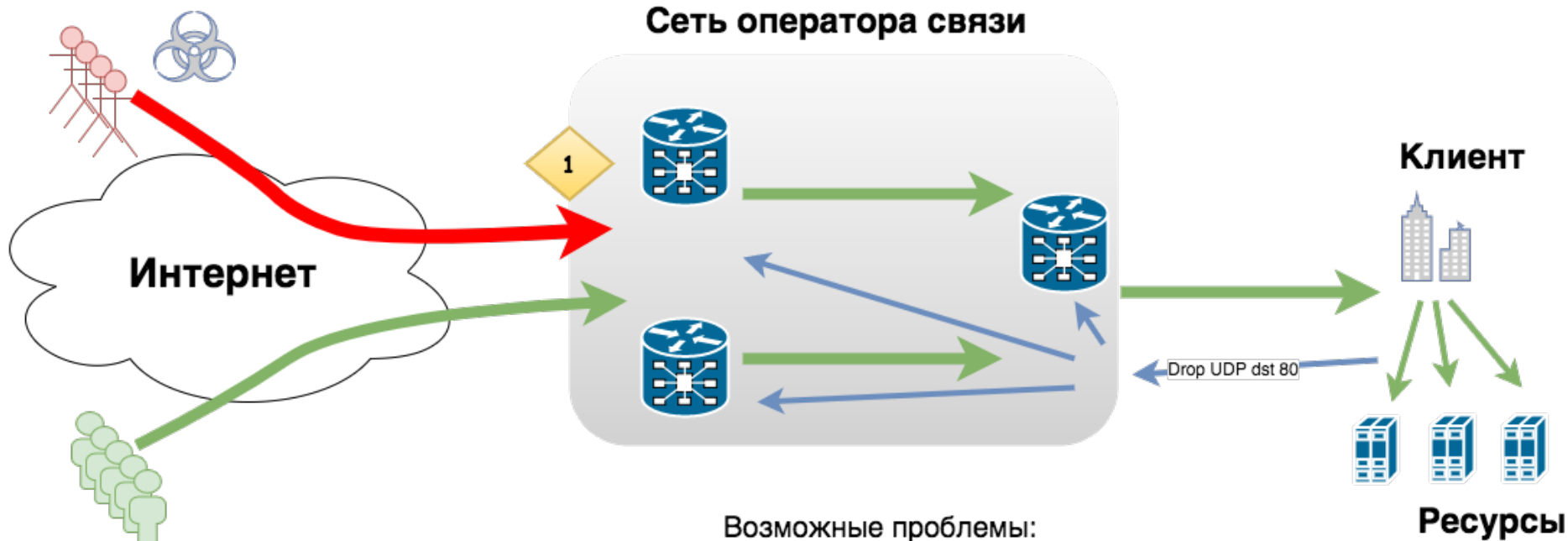


 Легитимный трафик
 Flood/Amplification

Возможные проблемы:

-  1 Переполнение стыков с аплинками
-  2 Переполнение внутренних бэкбонов
-  3 Переполнение стыка с клиентом
-  4 Переполнение канала к ресурсу

Типичный сценарий атаки (используем flowspec)



Возможные проблемы:

1 Переполнение стыков с аппинками

→ Легитимный трафик

→ Flood/Amplification

→ BGP FS правила

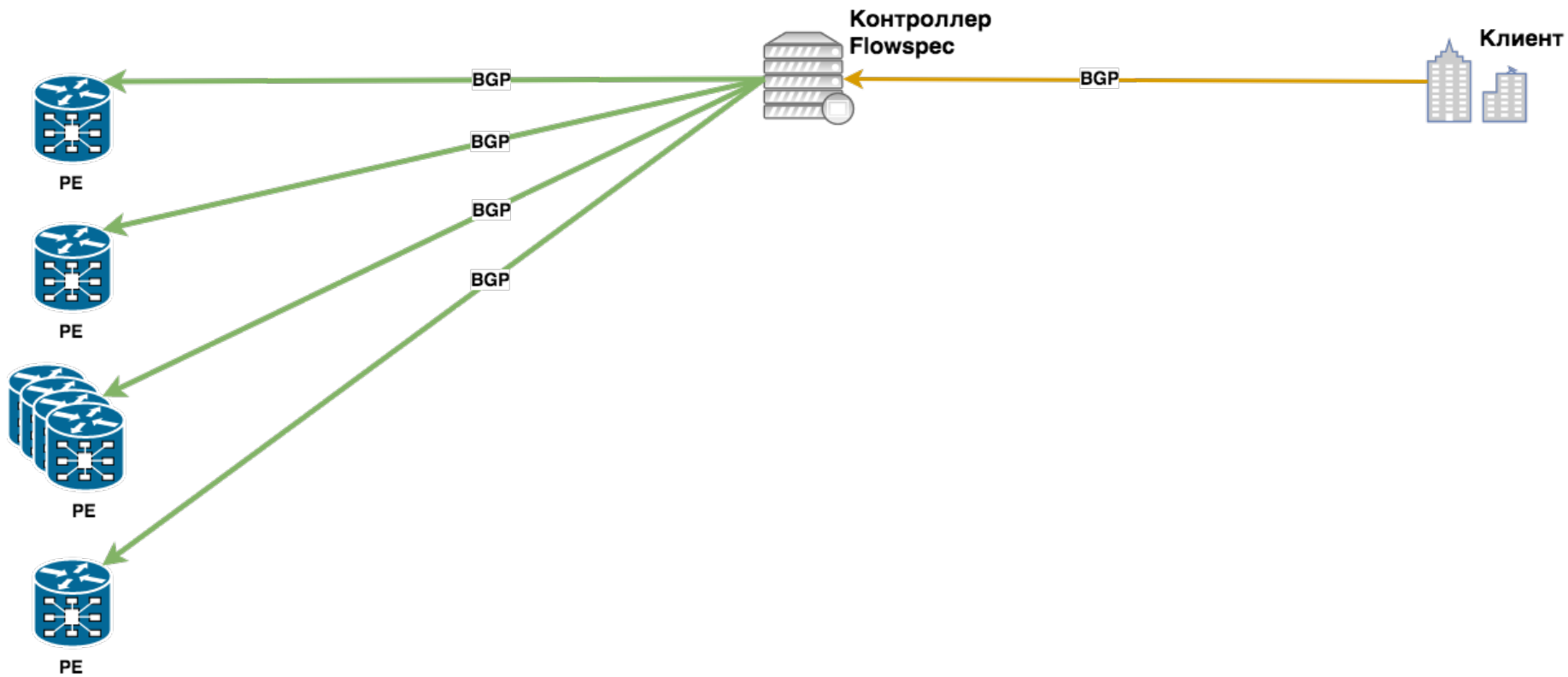
Рассмотренные варианты внедрения


- Включение address-family *IPv4/IPv6 flowspec* на PE маршрутизаторах и клиентских сессиях :
 - Валидация правил? (vendor-specific, more-specific, etc)
 - Возможность «потерять» PE при приеме некорректного правила
 - Необходима поддержка *BGP FS* в «железе»
- Написание ПО(контроллер *BGP FS*):
 - Возможность любого типа валидации
 - Отделение сети оператора от клиентских сессий *BGP FS*
 - Возможность установки правил без аппаратной поддержки у клиента
 - Возможности масштабирования


Валидация правил

- Обязательное наличие **destination prefix**
- **Destination prefix** должен быть лучшим маршрутом в сети оператора, и приниматься с клиентской сессии
- Запрет спецификации портов(*dst/src*) не с протоколами *tcp/udp*
- Запрет указания *tcp-flag* не в протоколе *tcp*
- Запрет указания *icmp-type/code* не в протоколе *icmp*
- Ограничения с учетом используемого оборудования на сети (*vendor-specific*).

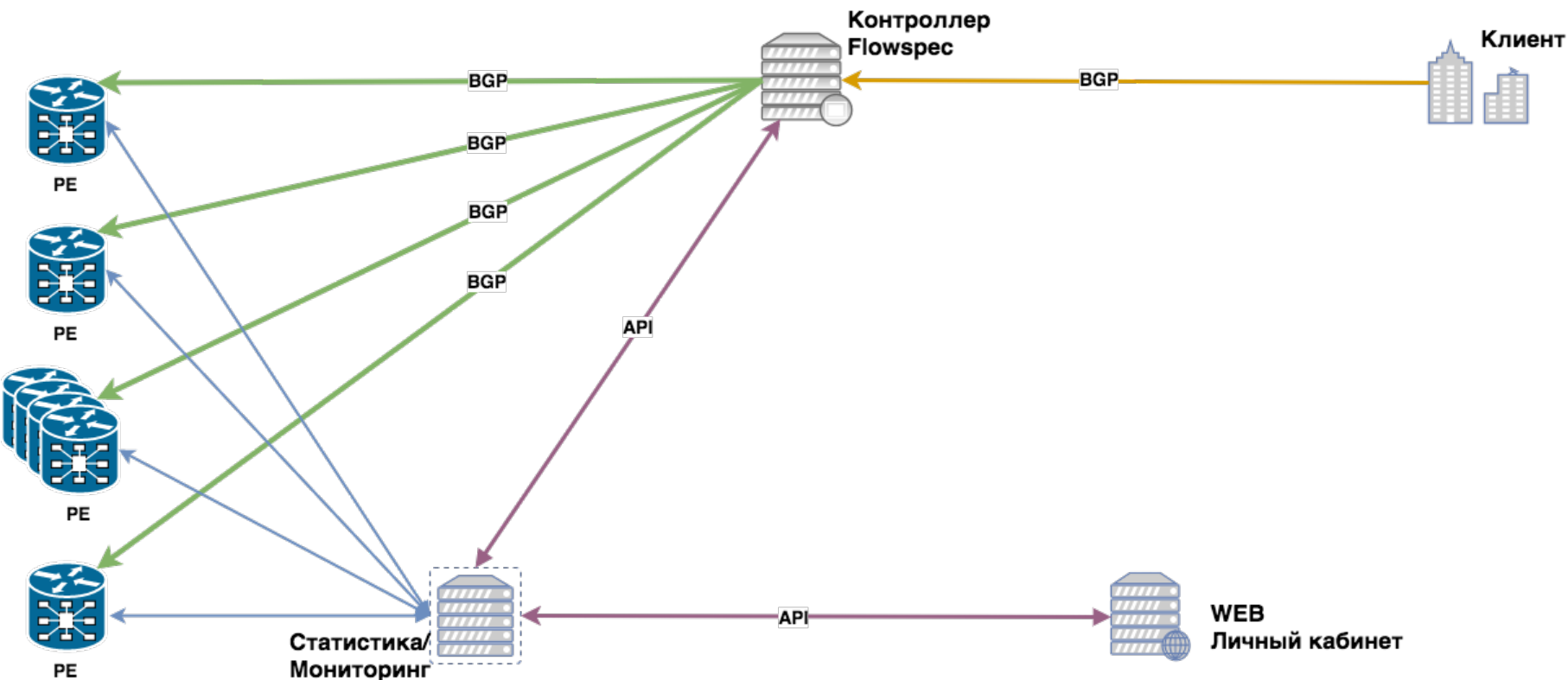
Внедрение BGP Flowspec



Передача правил от клиента контроллеру  BGP

Передача правил от контроллера в сеть  BGP

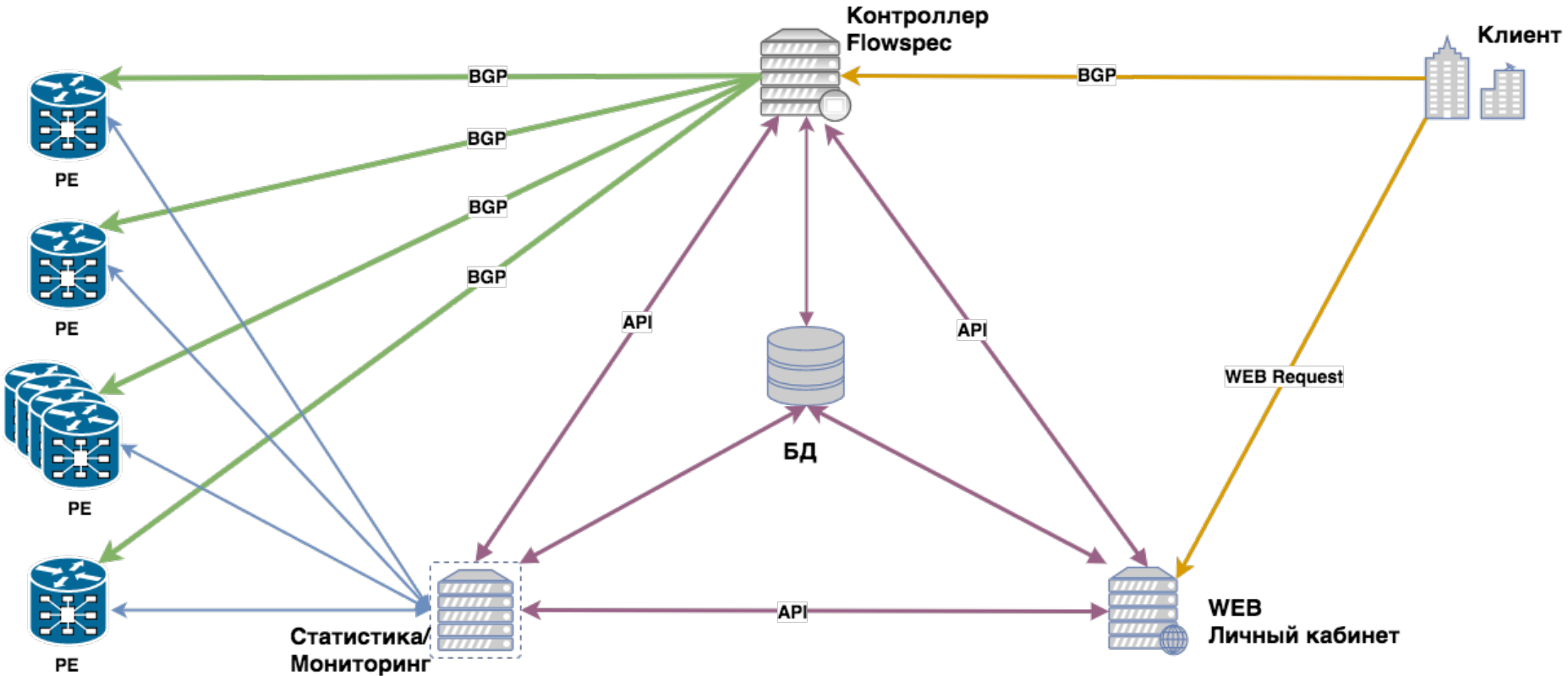
Внедрение BGP Flowspec (+ статистика/мониторинг)



Передача правил от клиента контроллеру — BGP →
Передача правил от контроллера в сеть — BGP →

Сбор статистики — API →
Межсервисное взаимодействие — API →

Внедрение BGP Flowspec (+ web requests)

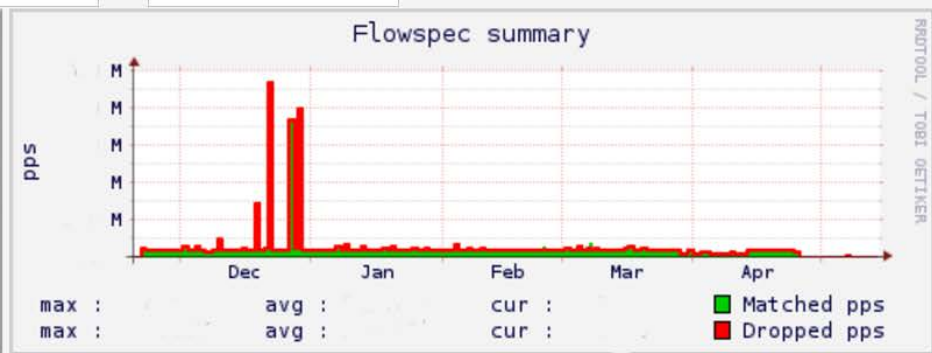
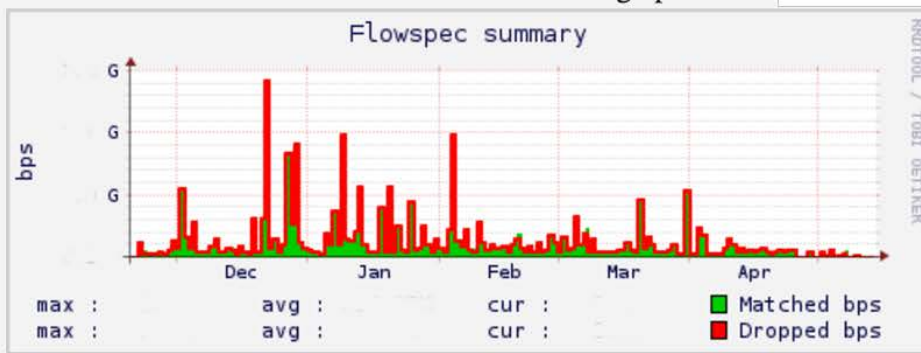


Передача правил от клиента контроллеру — BGP/Web →
Передача правил от контроллера в сеть — BGP →

Сбор статистики — API →
Межсервисное взаимодействие — API →

Статистика и мониторинг

- Съем статистики с маршрутизаторов
- Отправка метрик в систему статистики
- Периодическая ревалидация правил
- Контроль наличия правил в маршрутизаторах



Web портал

- Статистика и управление правилами
- Просмотр истории по выставленным правилам
- Экспорт счетчиков правил (match/drop) в json
- Возможность передавать flowspec:
 - Для клиентов с маршрутизаторами без поддержки bgp flowspec
 - В случае отсутствия доступа к сети/маршрутизатору
 - Просто/быстро/удобно



FlowSpec активен для AS (**0** правил)

Активные правила bgp fs: 0

Активные правила web fs: 6

Add Rule

Установка flowspec через web

dst_prefix:	<input type="text" value="8.8.8.8/32"/>	1.1.1.1/32
police b/s (0 - drop):	<input type="text" value="0"/>	0 76800-100000000000 b/s
proto:	<input type="text" value="tcp"/>	
dst_ports:	<input type="text" value="53,123"/>	80,443,1000-2000 (1-65535)
src_prefix:	<input type="text" value="3.0.0.1/32"/>	2.2.2.2/32
src_ports:	<input type="text" value=""/>	80,443,1000-2000 (1-65535)
tcp_flag:	<input type="text" value="syn"/>	
fragment:	<input type="text" value="any"/>	
icmp_type:	<input type="text" value="any"/>	

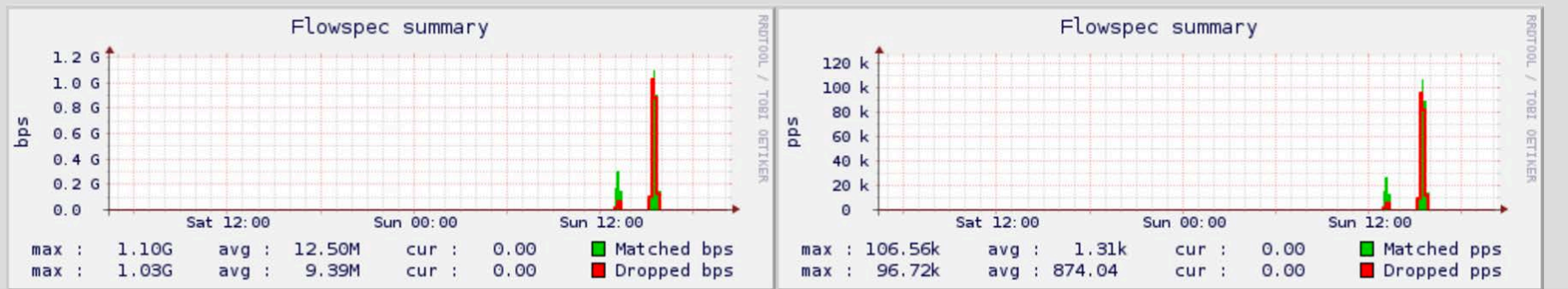
Submit

Cancel

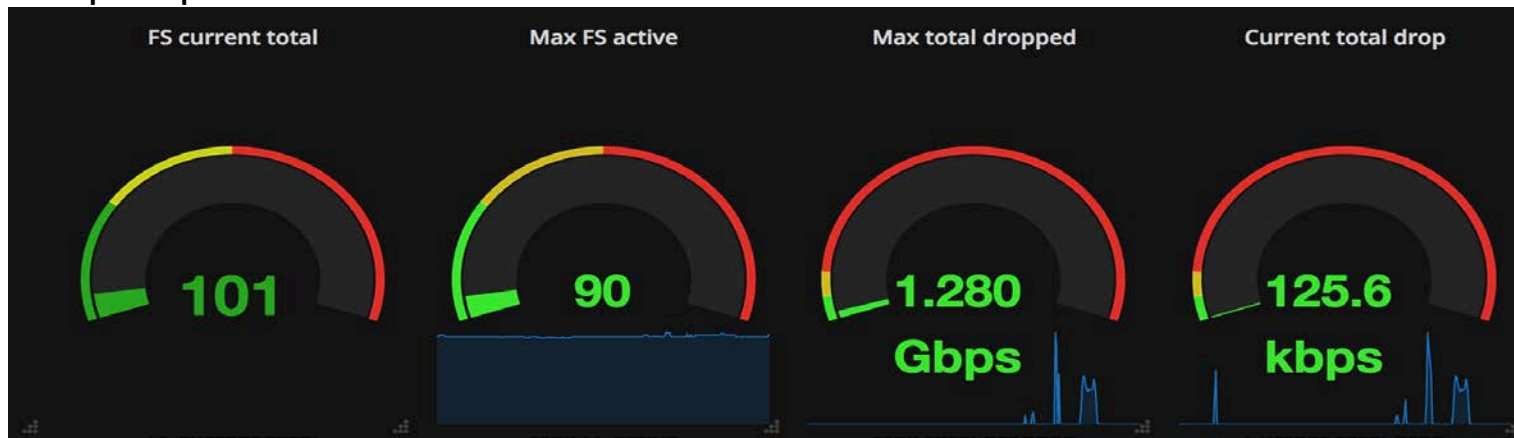
Примеры графиков

У клиентов в личном кабинете:

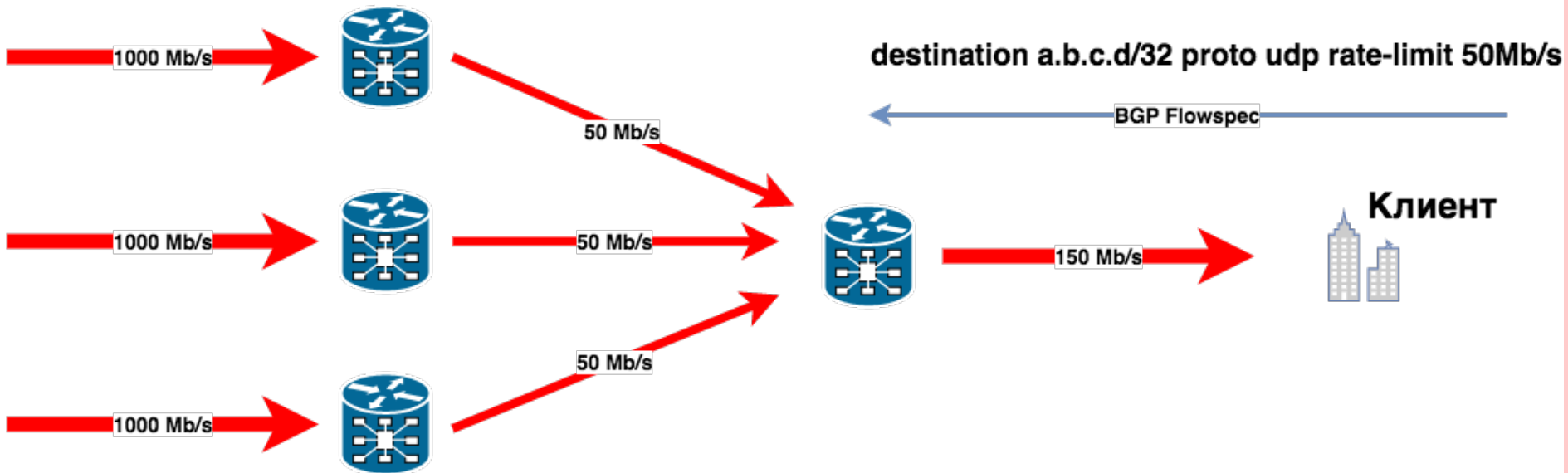
История правил/графики



У администраторов 😊 :



Rate-limit



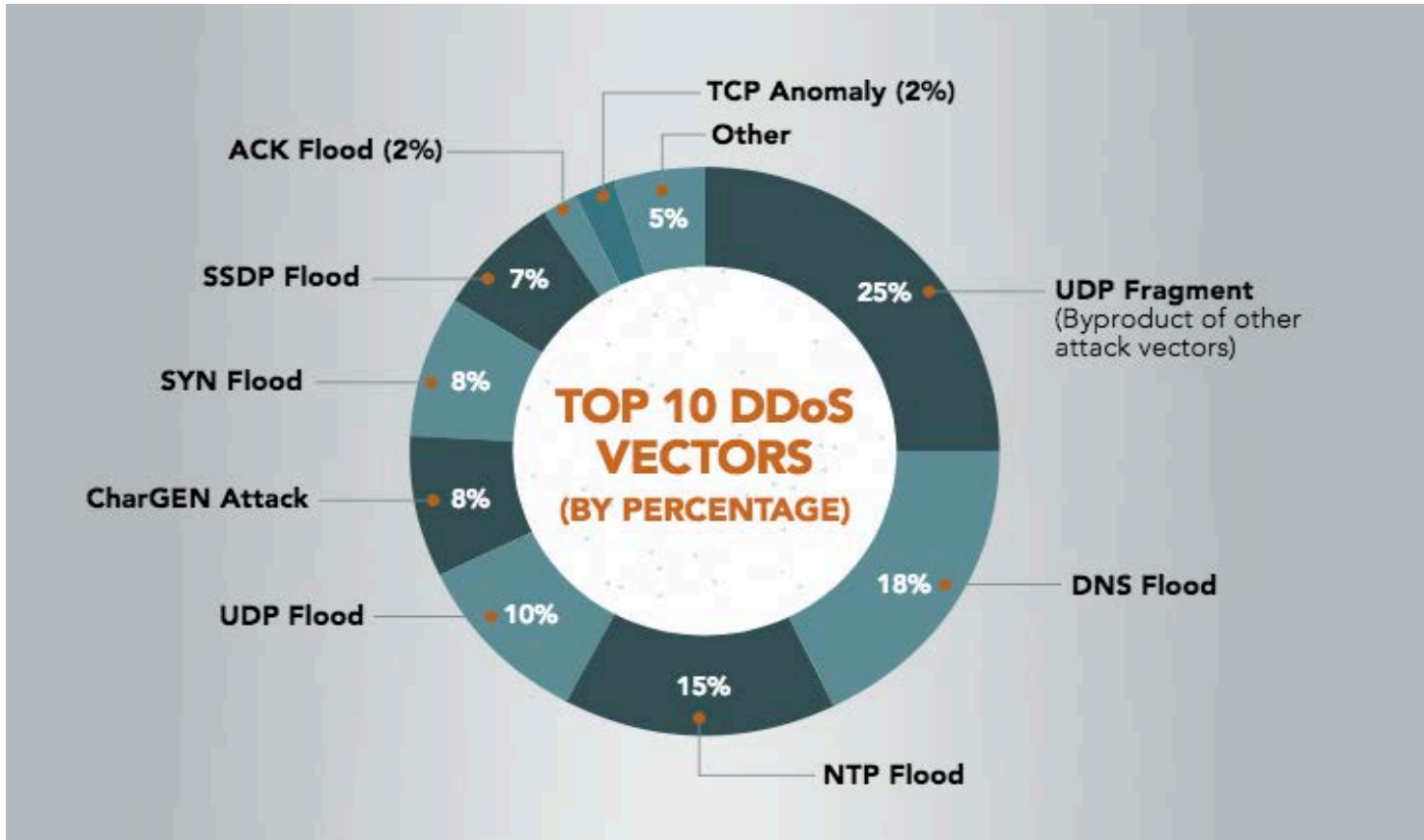
В Cisco ASR9K flowspec применяется на входе -> при наличии N линков(на разных NP) возможны подобные ситуации.

Детектирование DDoS

- Атаки на полосу(UDP Flood/Amplification):
 - BGP Flowspec применим практически ко всем случаям
 - Детектирование достаточно незатратно(Netflow/Sflow), в том числе и на транзите
- Атаки на сетевой стек(Syn/Ack flood, conntrack ...):
 - BGP Flowspec применим редко
 - Детектирование на транзите не всегда возможно
- Application-based атаки:
 - BGP Flowspec неприменим
 - Простое детектирование на транзите невозможно (без DPI и аналитики)

Топ 10 типов ddos атак (АКАМАИ)

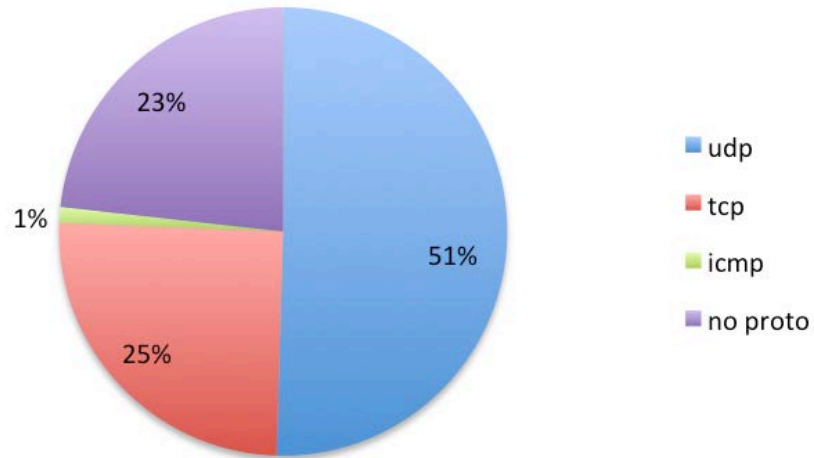
BGP Flowspec применим более чем в 75% случаев



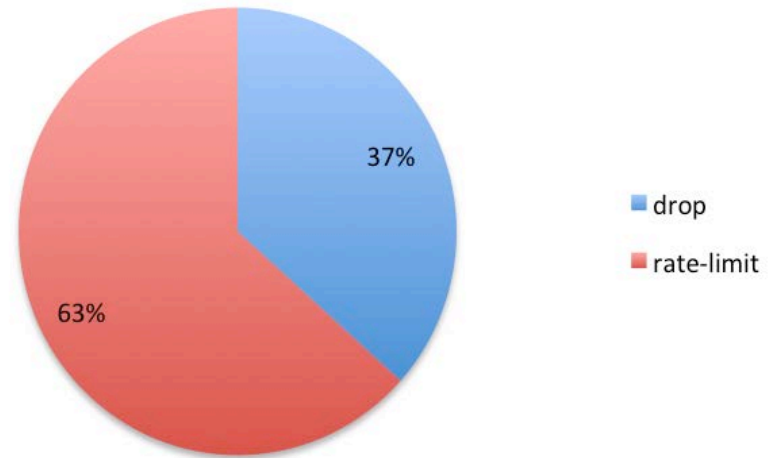
Статистика (Раском)

Выборка из >5000 реальных правил

Используемые протоколы

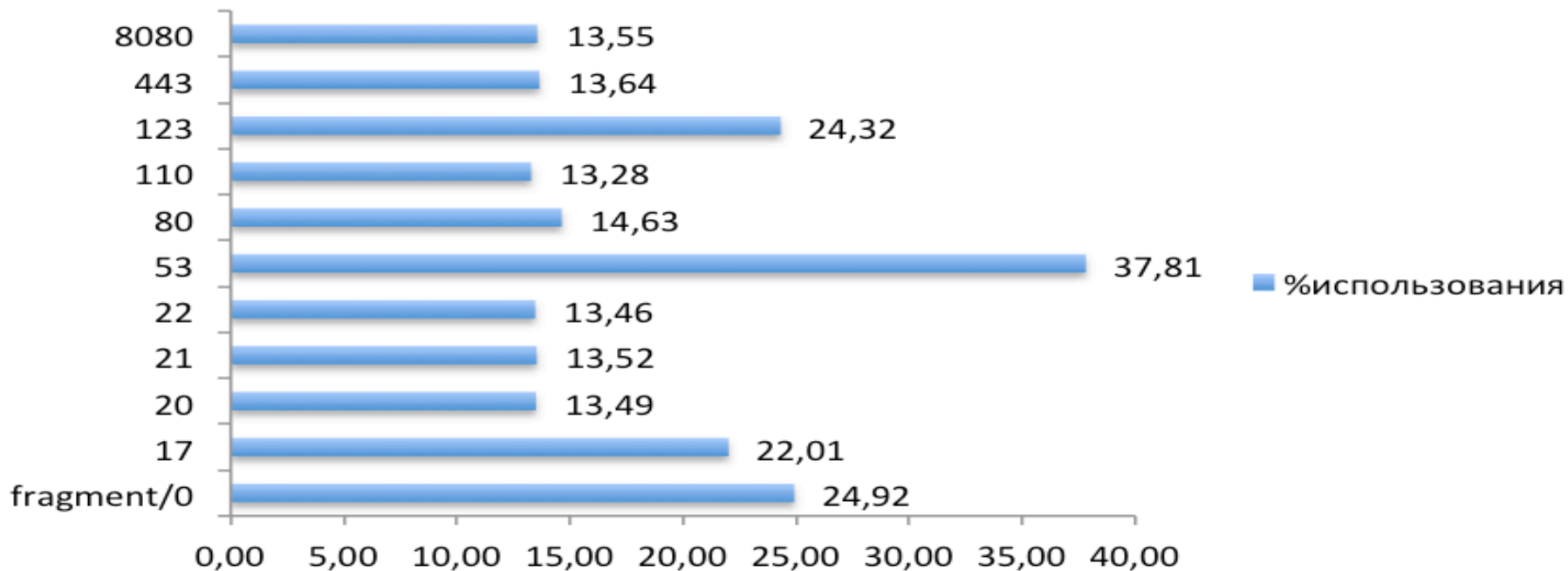


Используемые действия



Статистика (Раском)

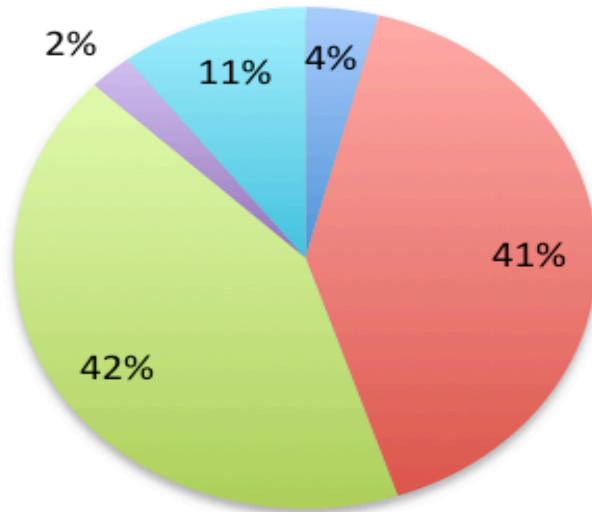
Распределение по портам



Статистика (Раском)

>85% трафика ddos атак, детектированных с помощью BGP Flowspec(клиентские правила) приходят с зарубежных стыков (в основном Tier1 операторы)

Срабатывание по регионам



- Amsterdam
- Frankfurt
- Stockholm
- Saint-Petersburg
- Moscow

Рекомендации

- **Hardware limitation.** Не рекомендуется использовать flowspec в качестве перманентных access-list и всегда убирать неиспользуемые
- **Bad validation.** Не стоит испытывать прочность операторской(вендорной) валидации правил и всегда следовать RFC:
 - Падение ядра сети Cloudflare (match packet-length >64K)
 - Во время тестов некорректными правилами несколько раз потерян Juniper vMX(вылет RPD)
- **Understanding.** Если нет понимания о bgp flowspec и его применениях, то не стоит применять эту услугу.

Планы на развитие

- Введение второго контроллера на базе GoBGP
 - Резервирование
 - Страховка от «багов» ПО
- API
 - Установка/снятие правил
 - Статистика (raw)
 - Информирование/снятие правил по которым нет трафика
- Интеграция с продуктом детектирования атак на базе netflow/sflow
- Доработка web-портала

Конец!



Вопросы и предложения принимаются по email: do@rascom.ru



Дмитрий Онучин
2017

```
root@core# cat flood >  
/dev/null
```