Классификация DDoS-атак

Александр Лямин,
Highload Lab

?

Метрики

Метрики


0 10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180
180 160 140 120 100 80 60 40 20 0
0 1 2 3 4 5 6

Метрики

Метрики

Метрики

Классификация

DDoS

distributed

*

(an explicit attempt to prevent legitimate users from using service)

Один принцип.

Классификация

DDoS

TCP SYN Flood, TCP SYN-ACK Reflection Flood (DRDoS), TCP Spoofed SYN Flood, TCP ACK Flood, TCP IP Fragmented Attack, HTTP and HTTPS Flood Attacks, INTELLIGENT HTTP and HTTPS Attacks, ICMP Echo Request Flood, UDP Flood Attack, DNS Amplification Attacks *

Различные техники исполнения.

* Классификация DDoS атак, предлагаемая нашими зарубежными коллегами.

Классификация

Классификация

- Зачем классифицировать:
  - Обнаружение атаки
  - Понимание принципа работы
  - Адекватное противодействие
  - Способность отличать атаку от разладки системы

Классификация

Уровень инфраструктуры

1. Канальная емкость
2. Сетевая инфраструктура
3. Стек протоколов
4. Приложение

Мощность атаки

- Как измерять?
  - Объем ботнета
    - Атака на ЖЖ?

Мощность атаки

- Как измерять?
  - Объем ботнета
    - Атака на ЖЖ
    - Объем ботнета – не мера атаки
    - То же самое с остальными параметрами

Мощность атаки

Какова была мощность атаки на Хабрахабр?

Мощность атаки

Мощность атаки

Мощность атаки

Доступность сервиса

- Единственный действительно важный критерий
- Позволяет избежать измерения удава в попугаях

Мощность атаки

Доступность сервиса

Теперь измеряем в попугаях Шредингера.

Доступен для пользователей –
недоступен для ботов.

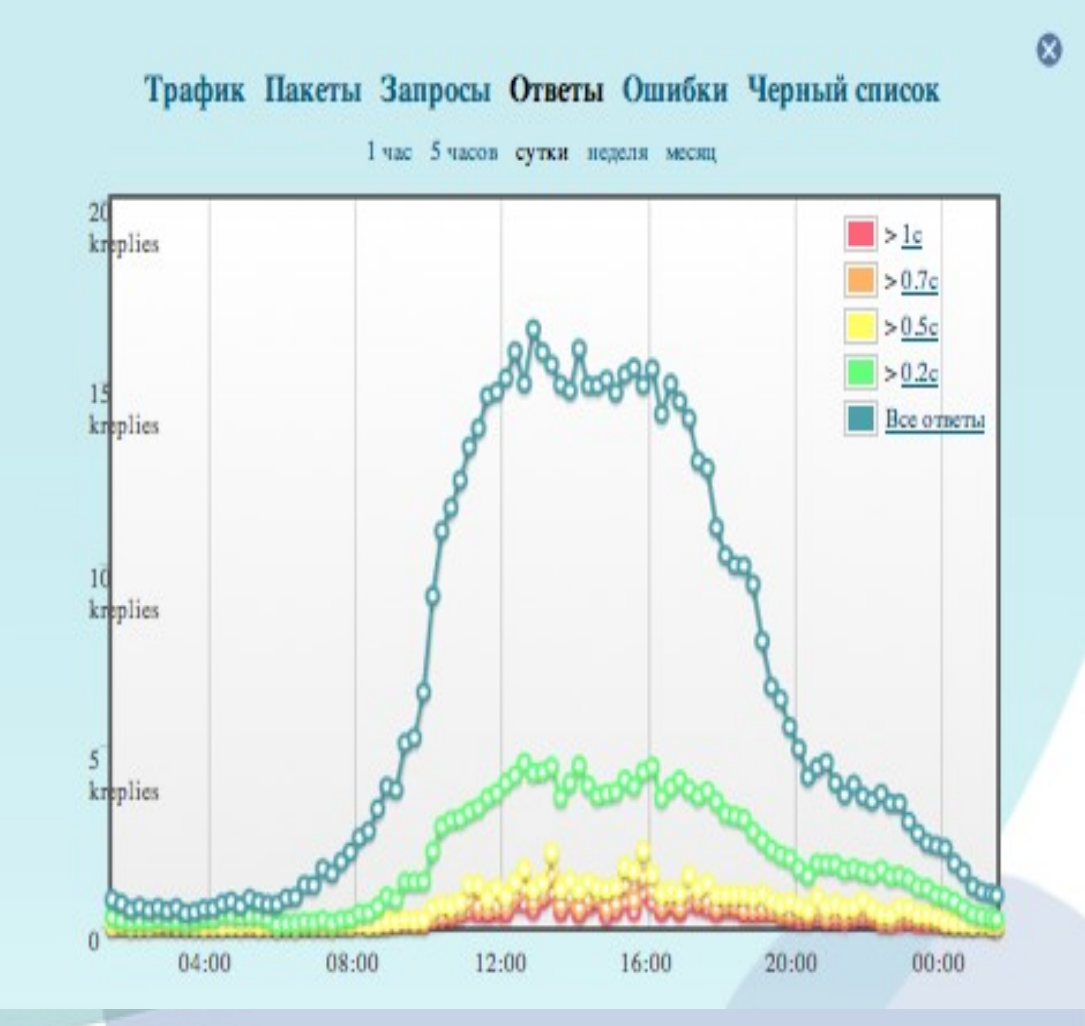
Метрики 2.0

Новые цели

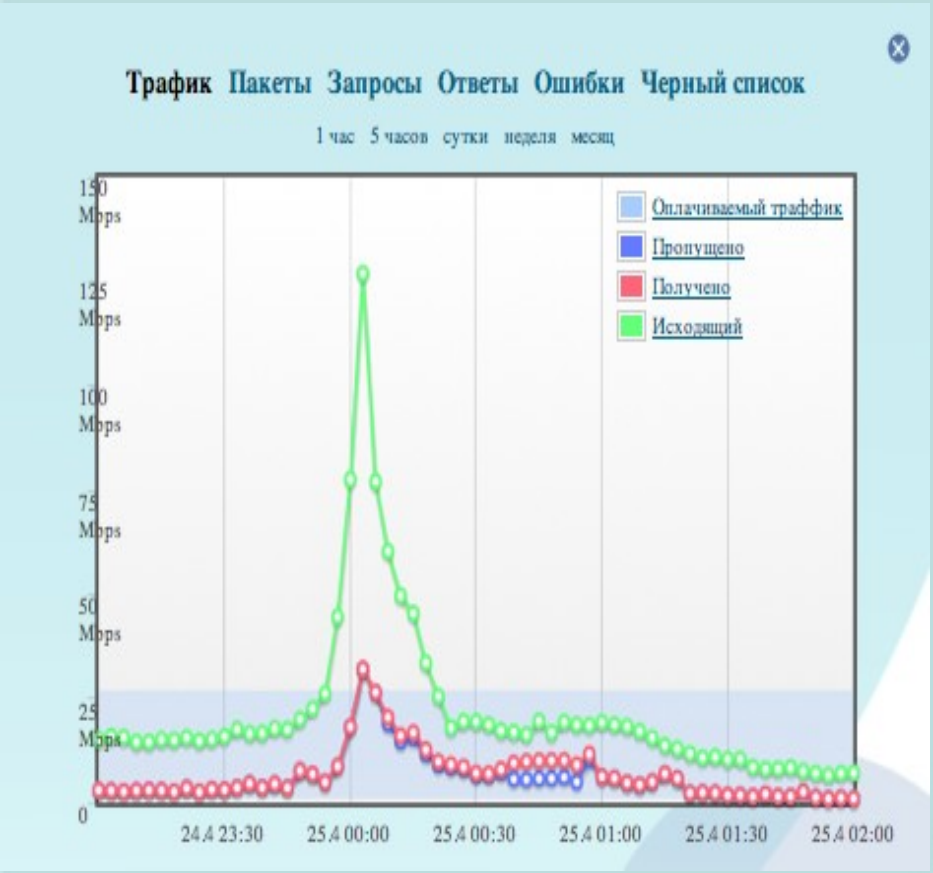
- Обнаружить начало атаки
- Быстро классифицировать
- Оценить масштабы бедствия
- Принять контрмеры

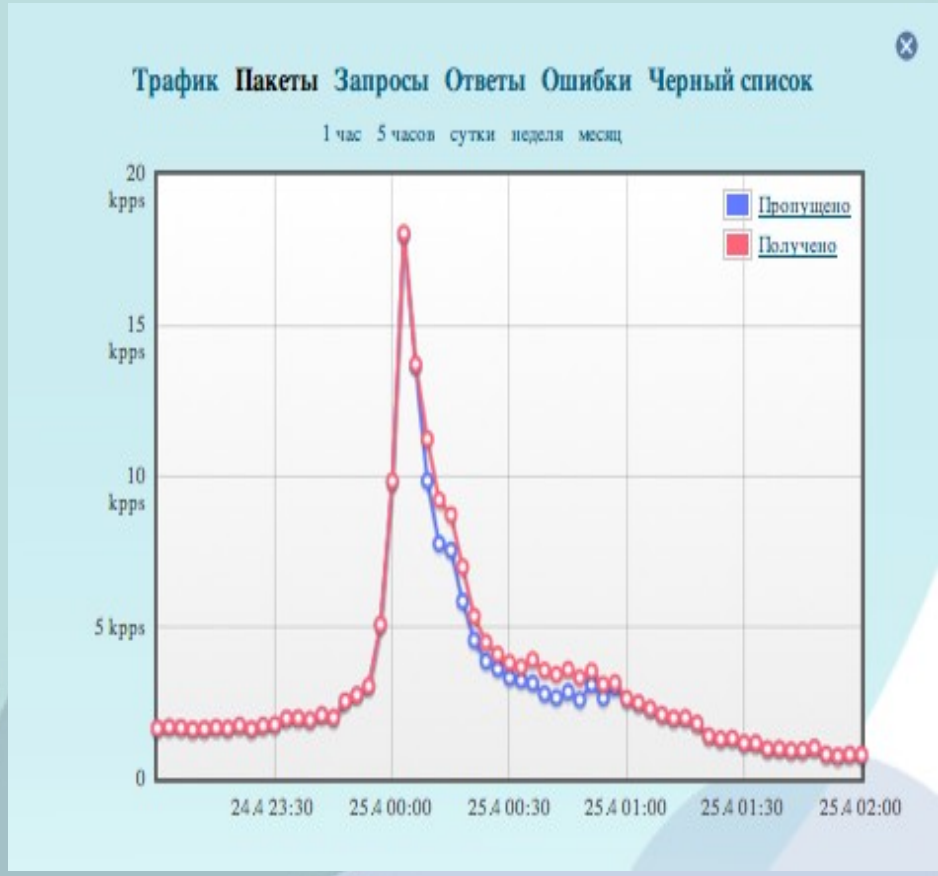
Метрики 2.0

- Трафик (rx/acpt)
- Пакеты (rx/acpt)
- Запросы
- Ответы
- Ошибки
- Стоп-лист

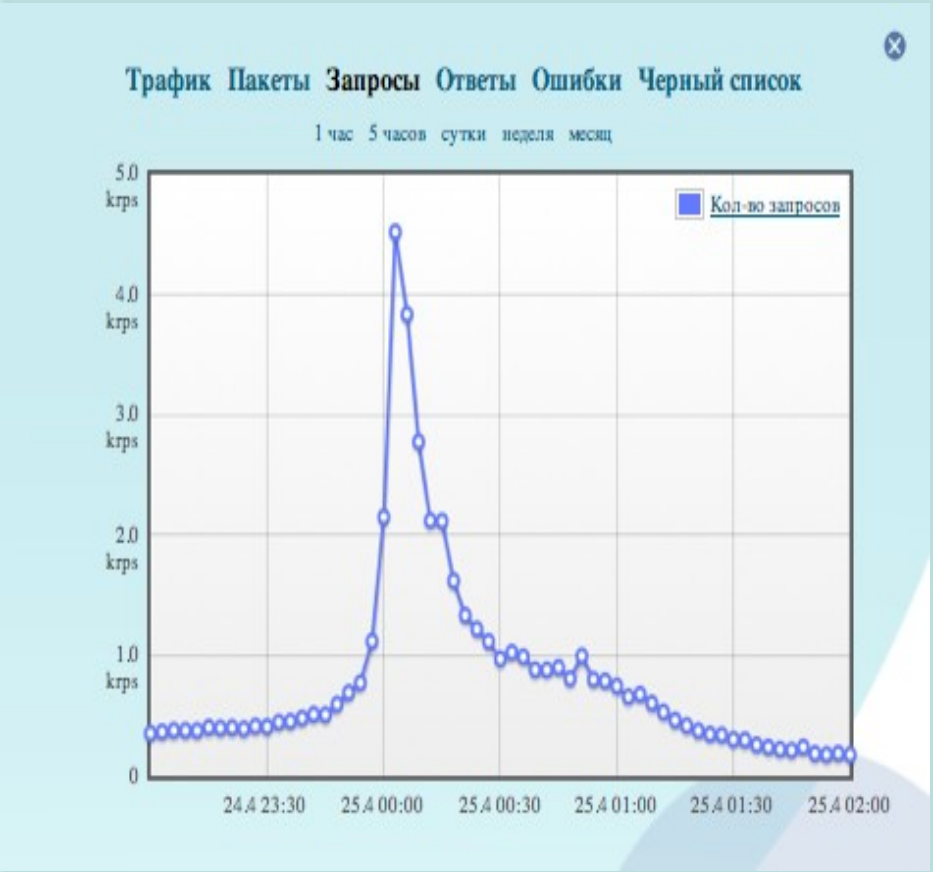


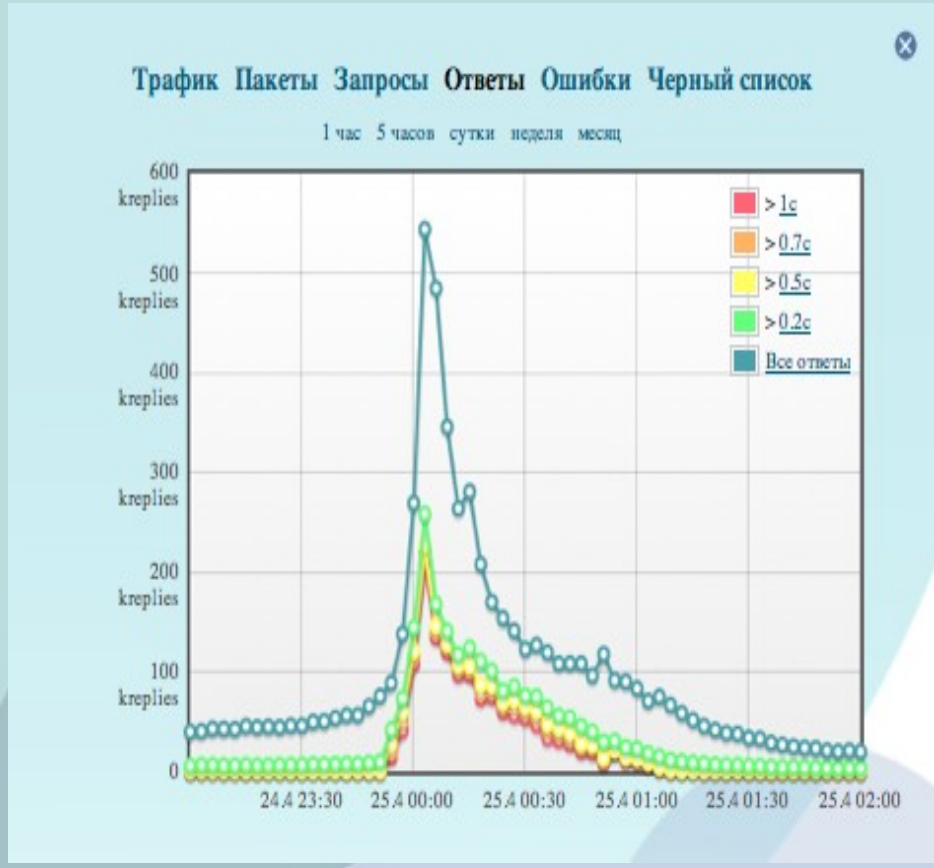
Пример 1


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
150 Mbps
125 Mbps
100 Mbps
75 Mbps
50 Mbps
25 Mbps
0
Оплачиваемый траффик
Пропущено
Получено
Исходящий
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00

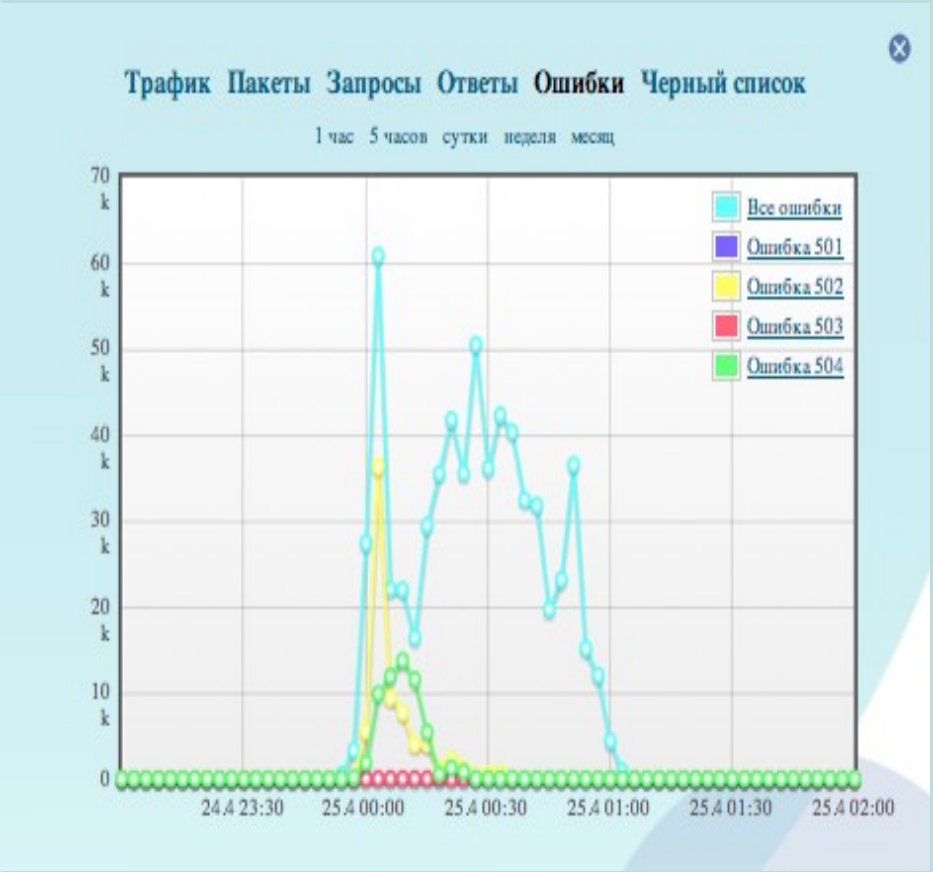

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
20 kpps
15 kpps
10 kpps
5 kpps
0
Пропущено
Получено
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00

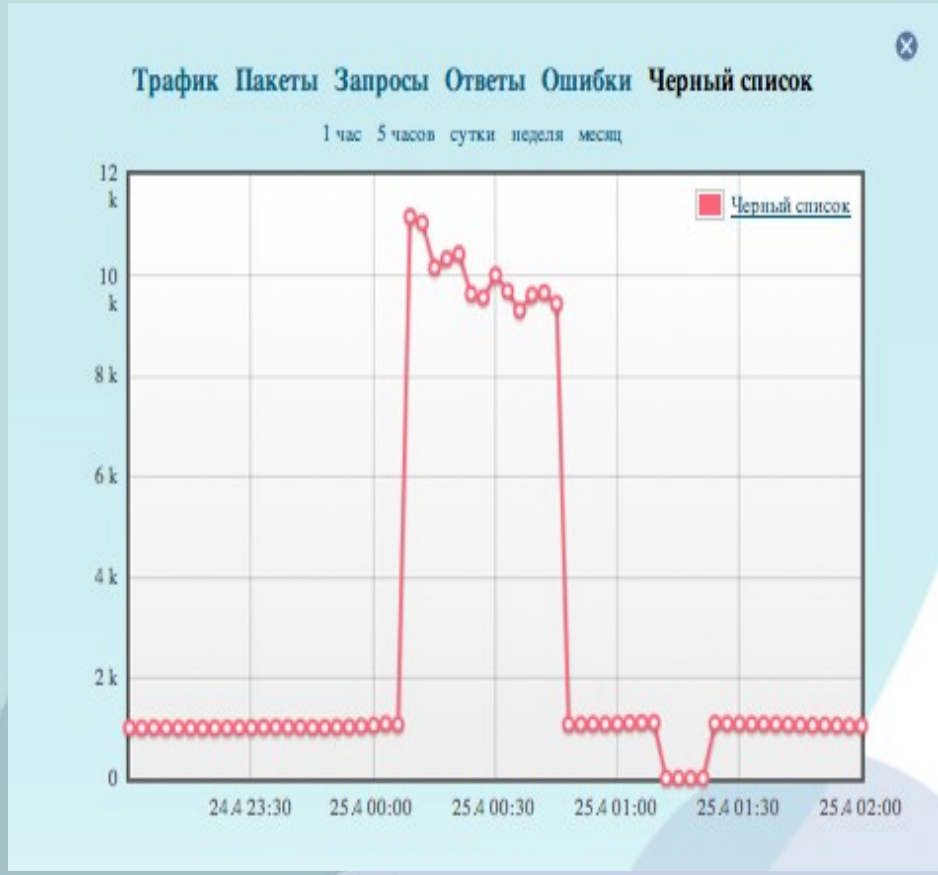
Пример 1


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
5.0 krps
4.0 krps
3.0 krps
2.0 krps
1.0 krps
0
Кол-во запросов
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
600 kreplies
500 kreplies
400 kreplies
300 kreplies
200 kreplies
100 kreplies
0
> 1c
> 0.7c
> 0.5c
> 0.2c
Все ответы
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00

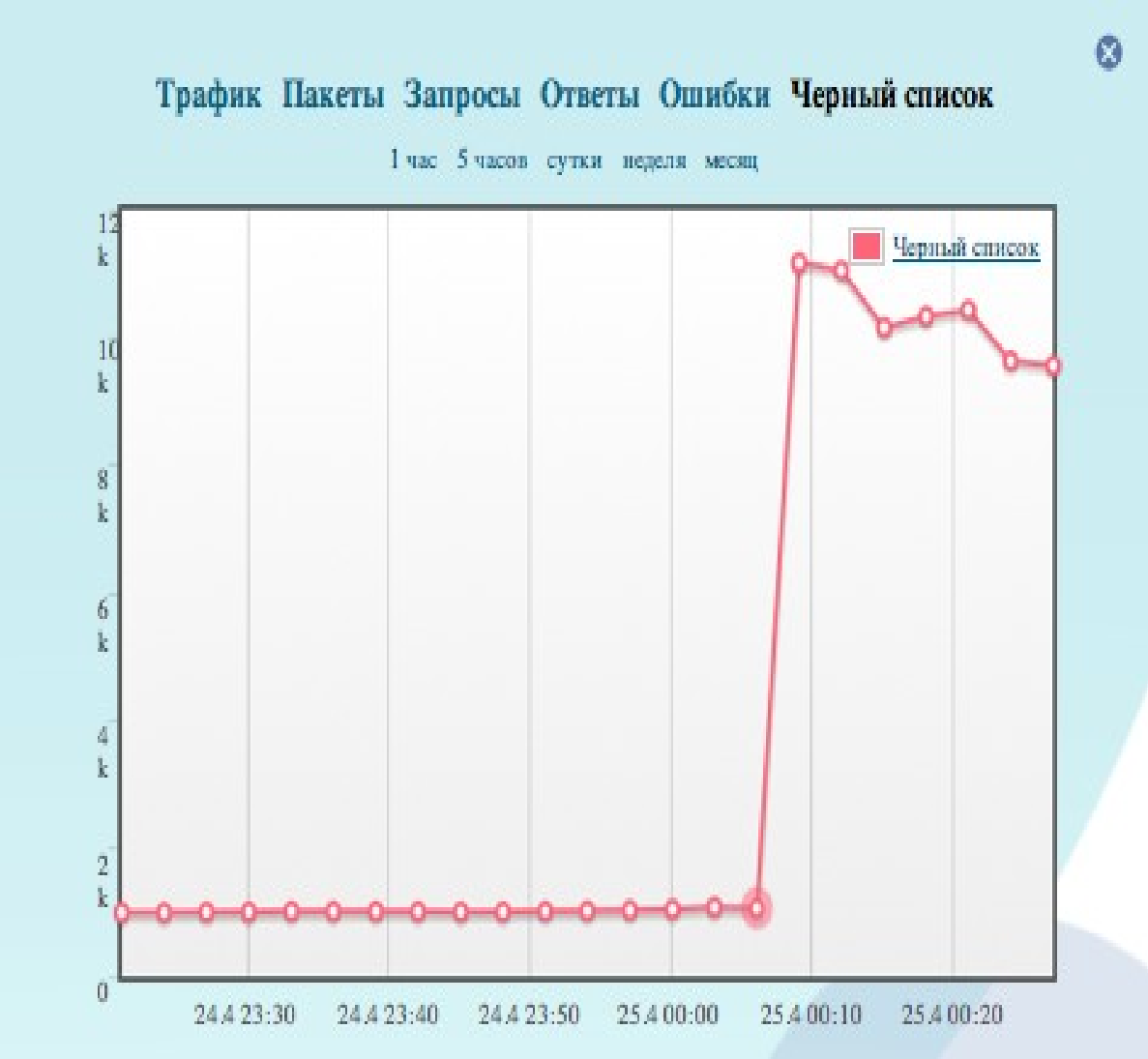
Пример 1


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
70 k
60 k
50 k
40 k
30 k
20 k
10 k
0
Все ошибки
Ошибка 501
Ошибка 502
Ошибка 503
Ошибка 504
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00

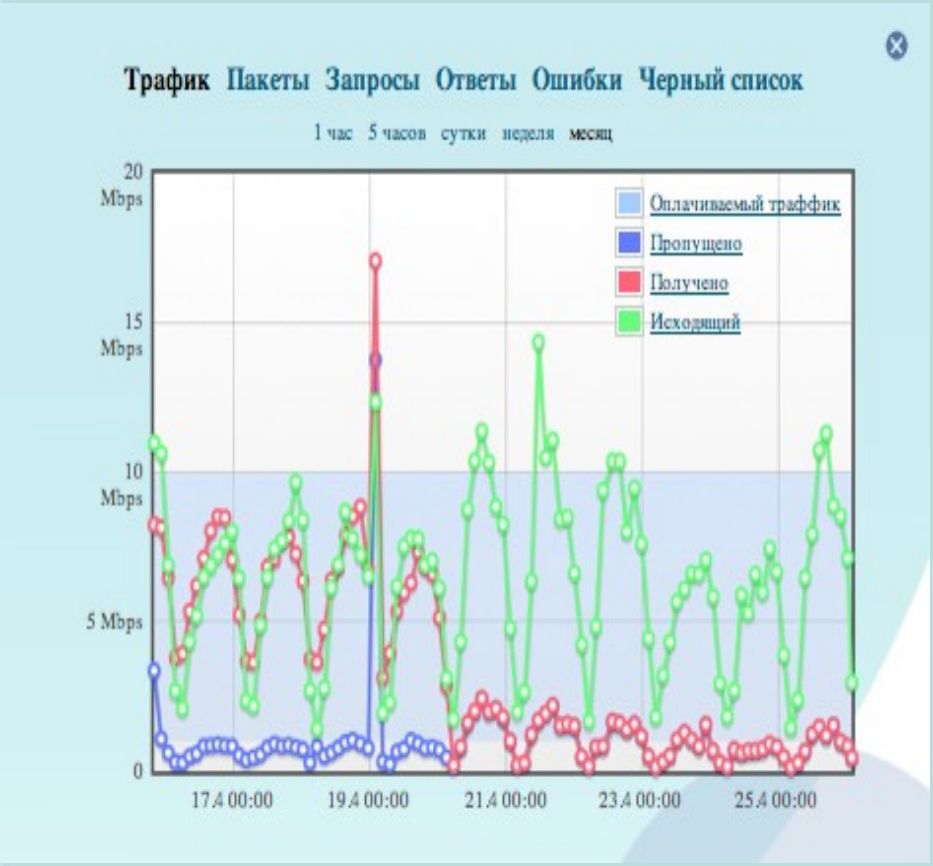

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
12 k
10 k
8 k
6 k
4 k
2 k
0
Черный список
24.4 23:30
25.4 00:00
25.4 00:30
25.4 01:00
25.4 01:30
25.4 02:00

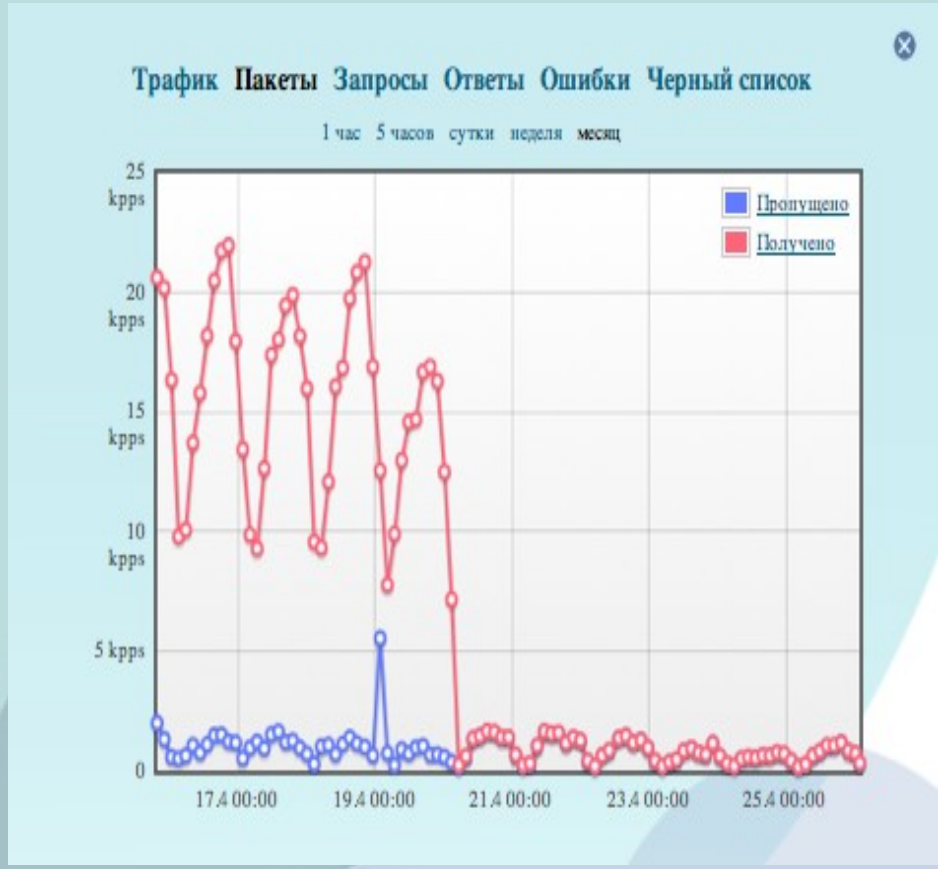
Пример 1

- Что интересно ?
- Почему просто ?
- Почему сложно ?
- Чем опасно ?

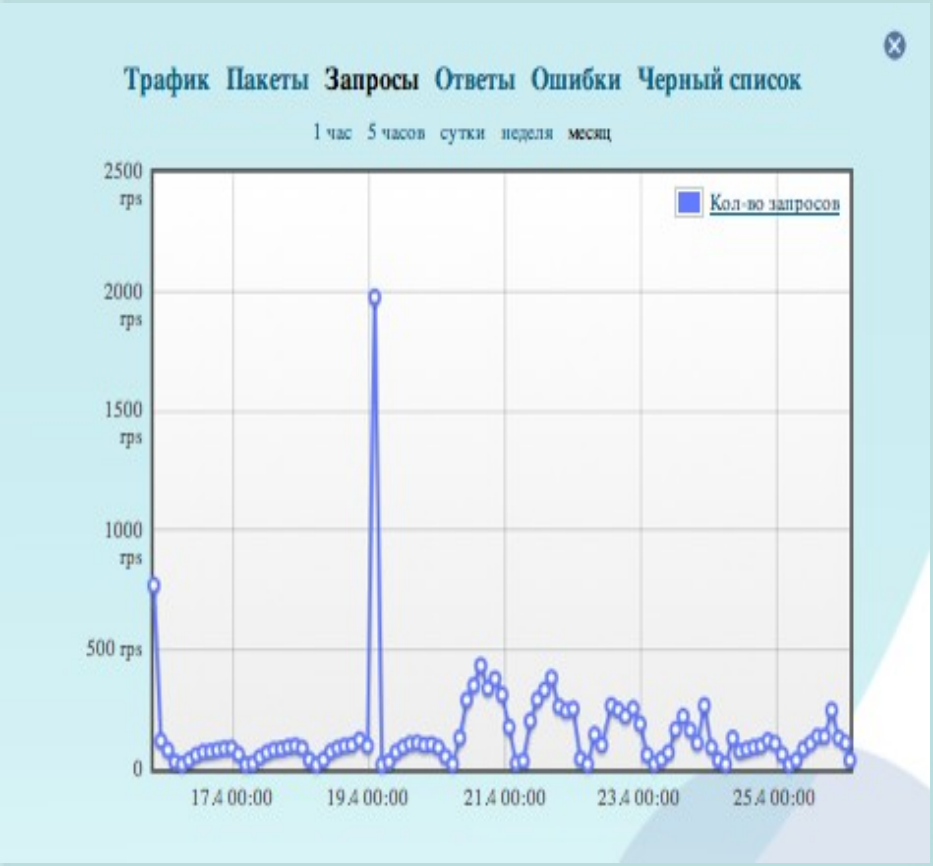


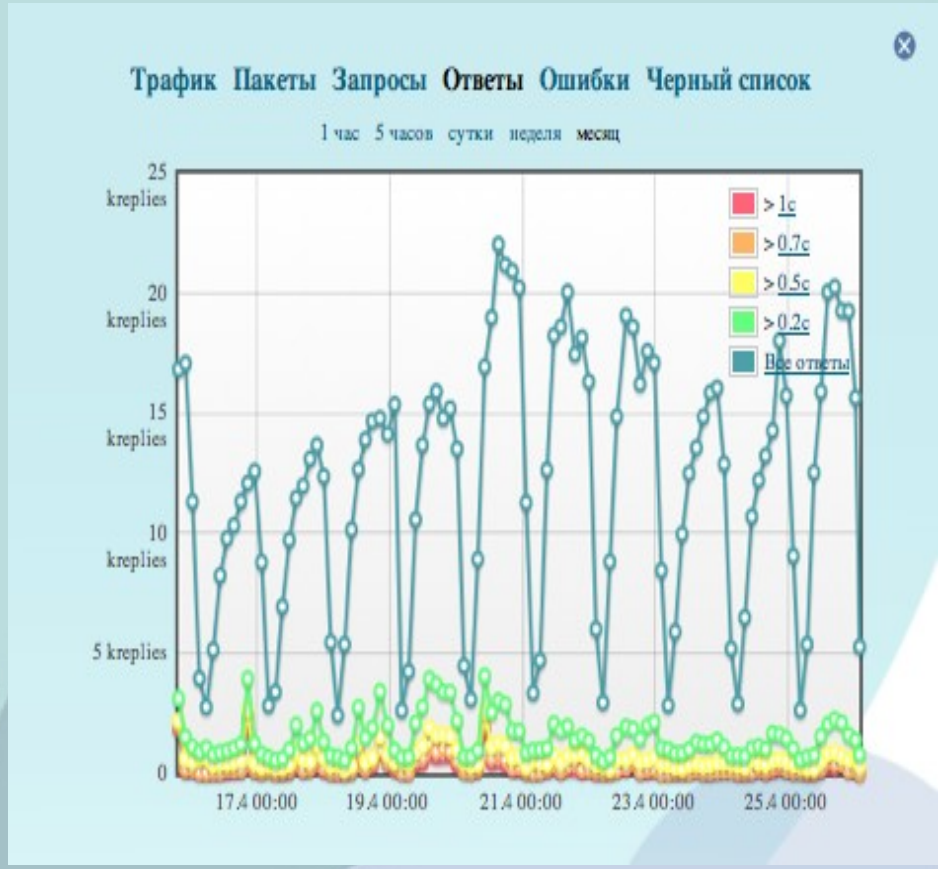
Пример 2


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
20 Mbps
15 Mbps
10 Mbps
5 Mbps
0
Оплачиваемый траффик
Пропущено
Получено
Исходящий
17.4 00:00
19.4 00:00
21.4 00:00
23.4 00:00
25.4 00:00

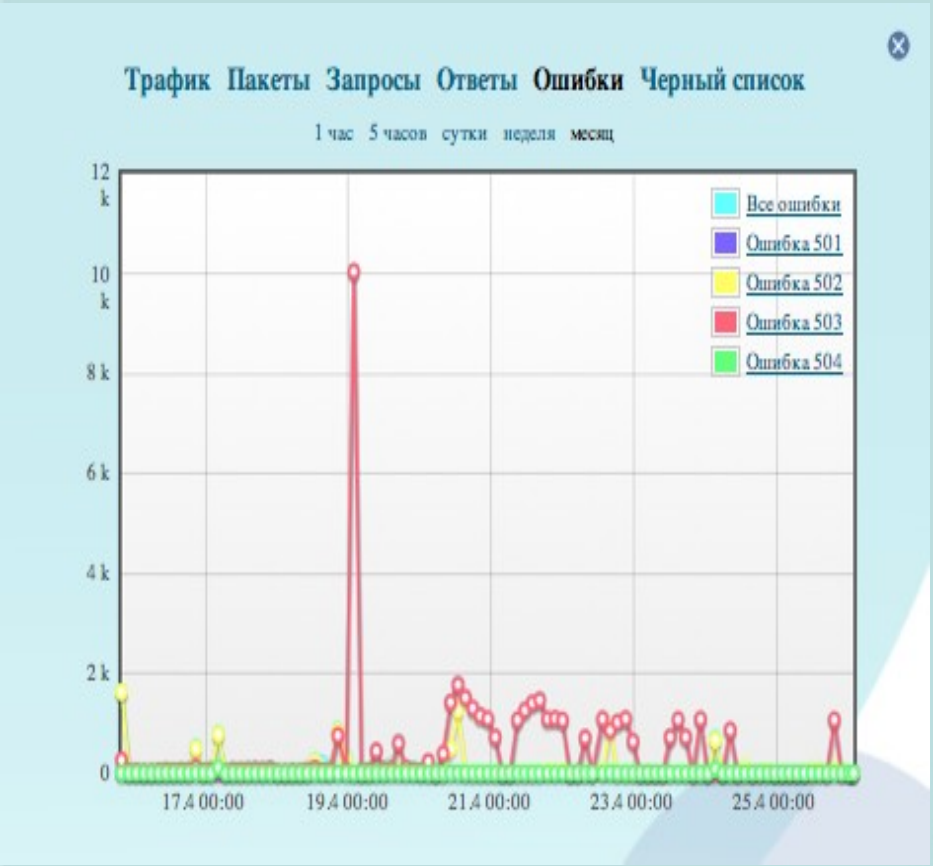

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
25 kpps
20 kpps
15 kpps
10 kpps
5 kpps
0
Пропущено
Получено
17.4 00:00
19.4 00:00
21.4 00:00
23.4 00:00
25.4 00:00

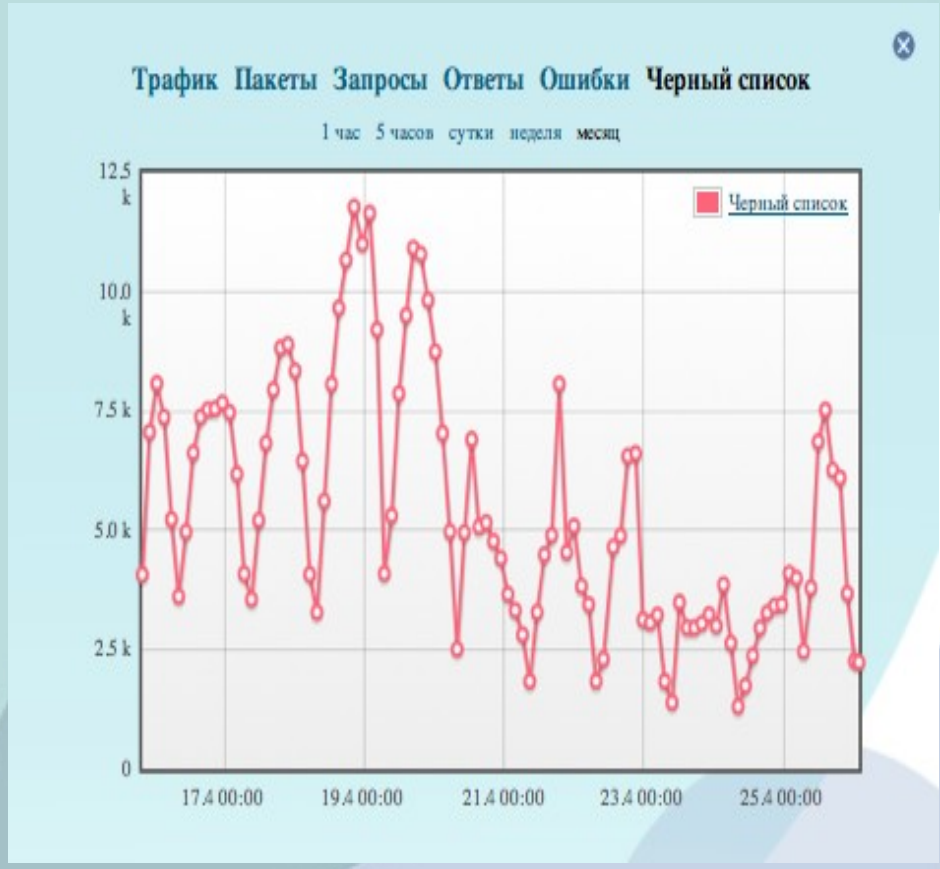
Пример 2


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
2500 rps
2000 rps
1500 rps
1000 rps
500 rps
0
Кол-во запросов
17.4 00:00
19.4 00:00
21.4 00:00
23.4 00:00
25.4 00:00

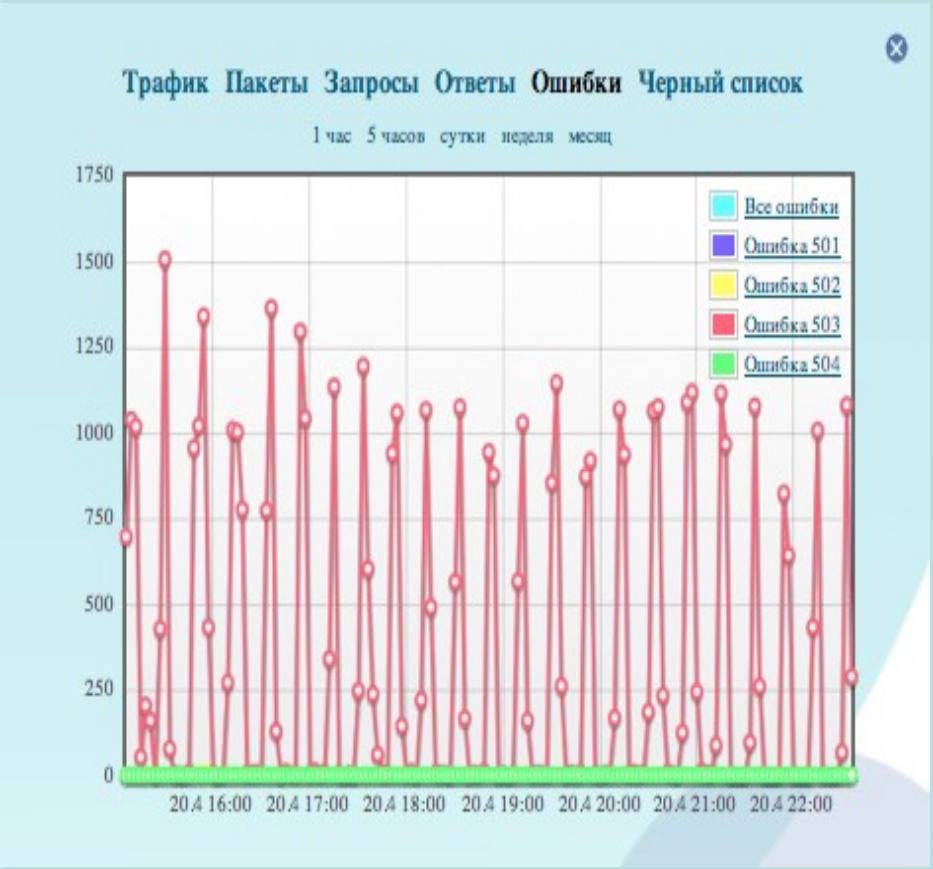

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
25 kreplies
20 kreplies
15 kreplies
10 kreplies
5 kreplies
0
> 1c
> 0.7c
> 0.5c
> 0.2c
Все ответы
17.4 00:00
19.4 00:00
21.4 00:00
23.4 00:00
25.4 00:00

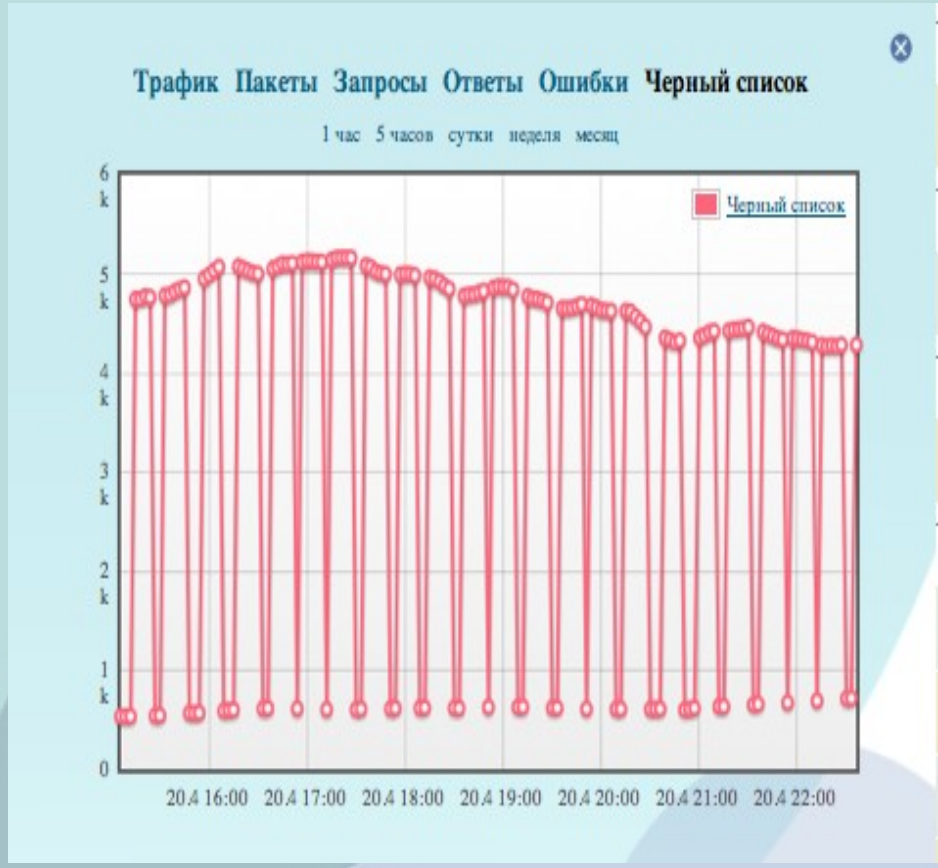
Пример 2


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
12 k
10 k
8 k
6 k
4 k
2 k
0
Все ошибки
Ошибка 501
Ошибка 502
Ошибка 503
Ошибка 504
17.Д 00:00
19.Д 00:00
21.Д 00:00
23.Д 00:00
25.Д 00:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
12.5 k
10.0 k
7.5 k
5.0 k
2.5 k
0
Черный список
17.Д 00:00
19.Д 00:00
21.Д 00:00
23.Д 00:00
25.Д 00:00

Пример 2

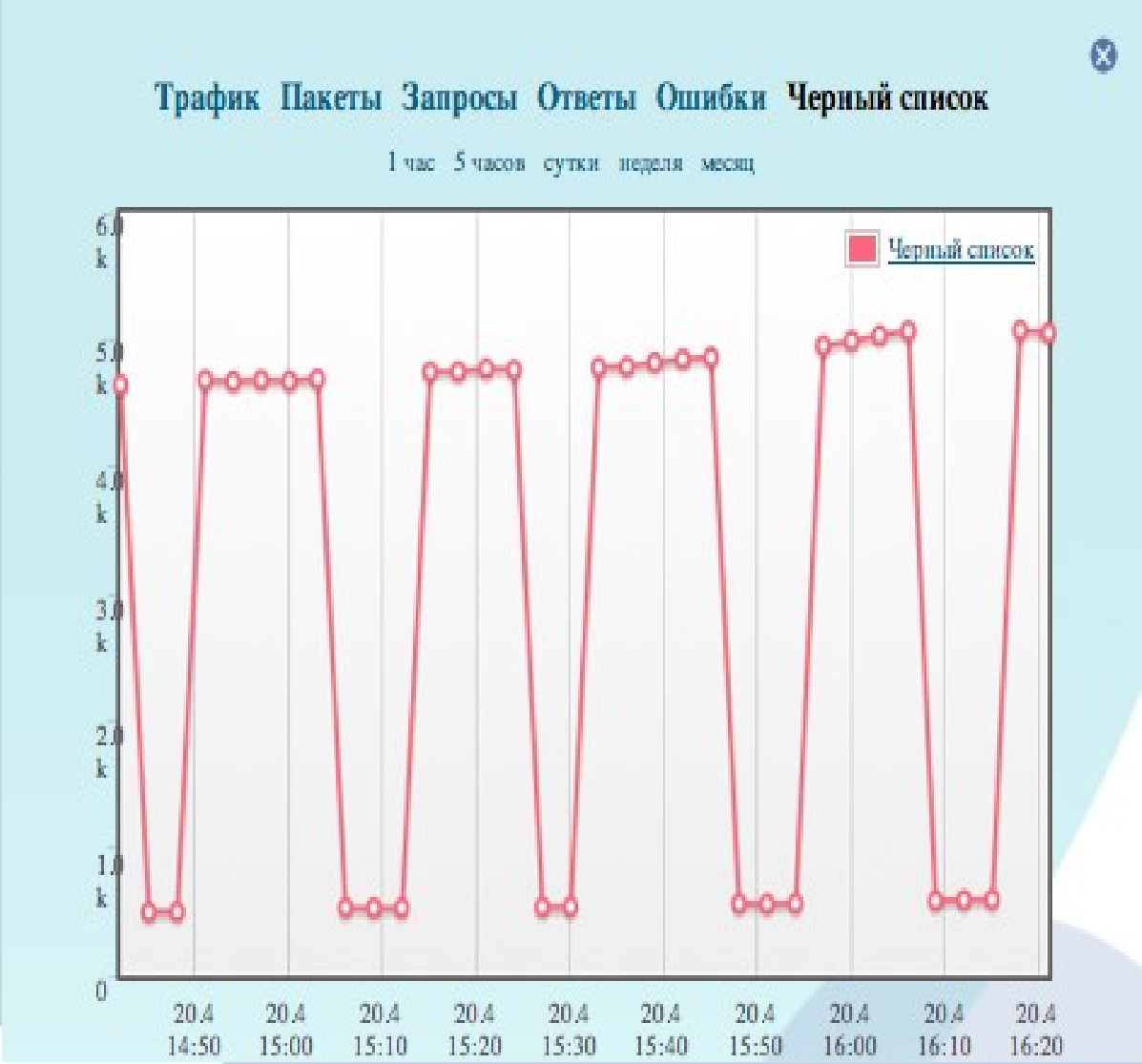




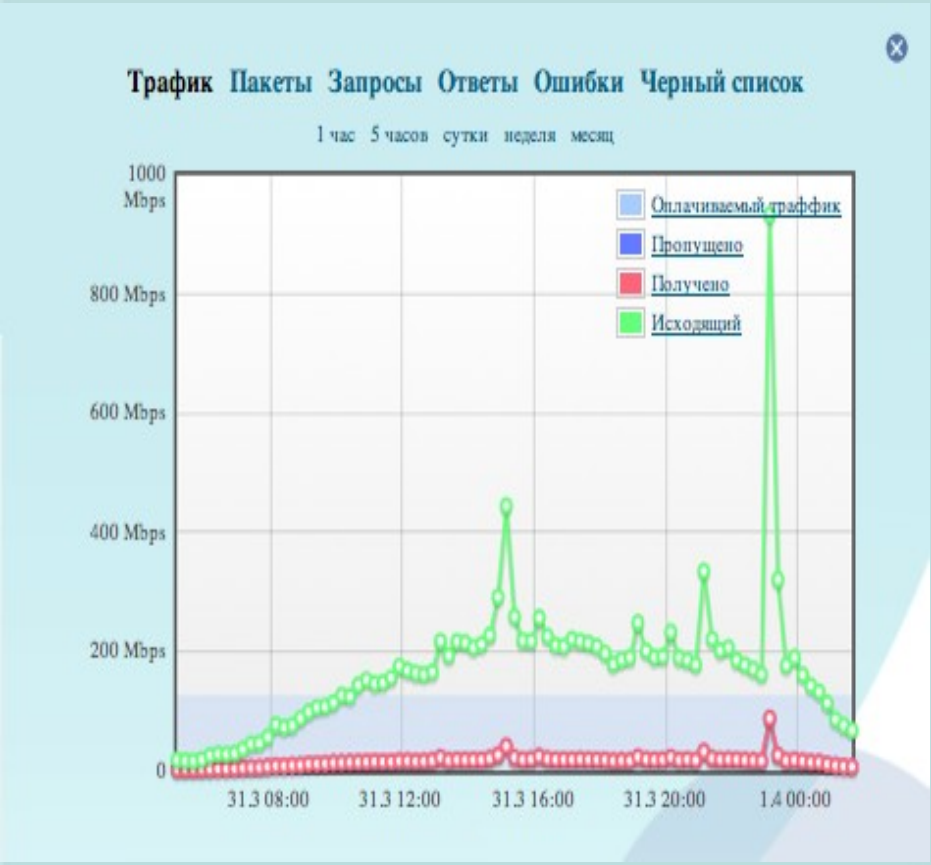
Дьявол в детялях

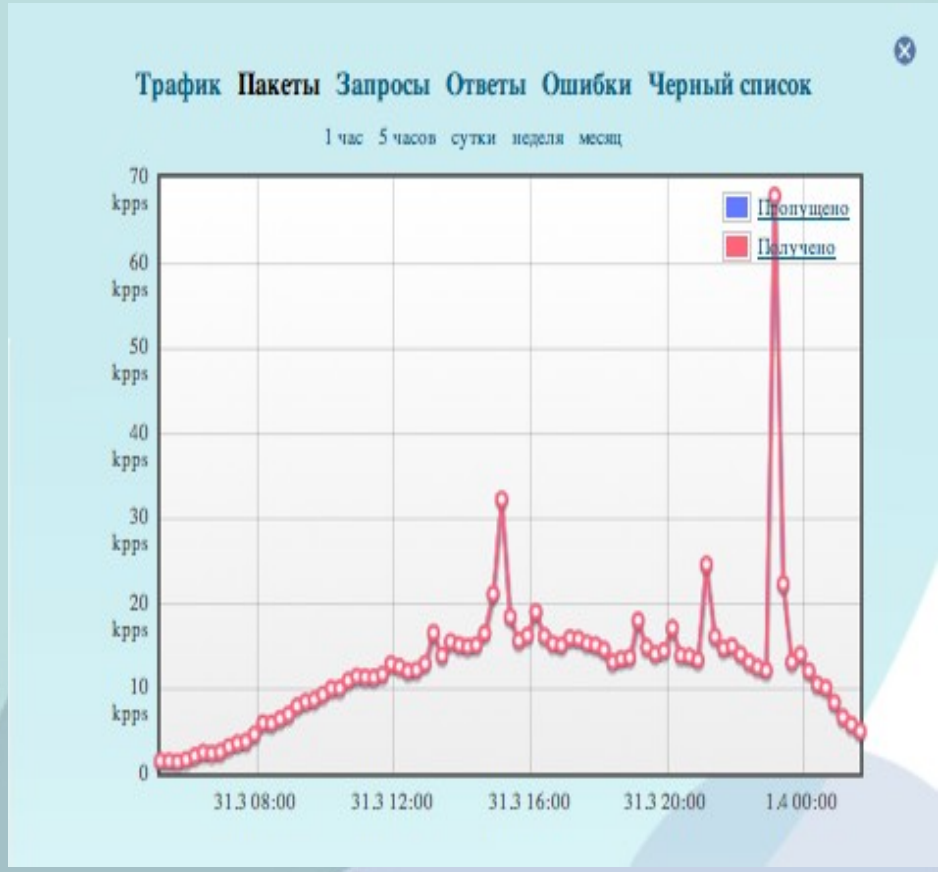
Пример 2

- Что интересно ?
- Почему просто ?
- Чем неприятно ?
- Чем опасно ?

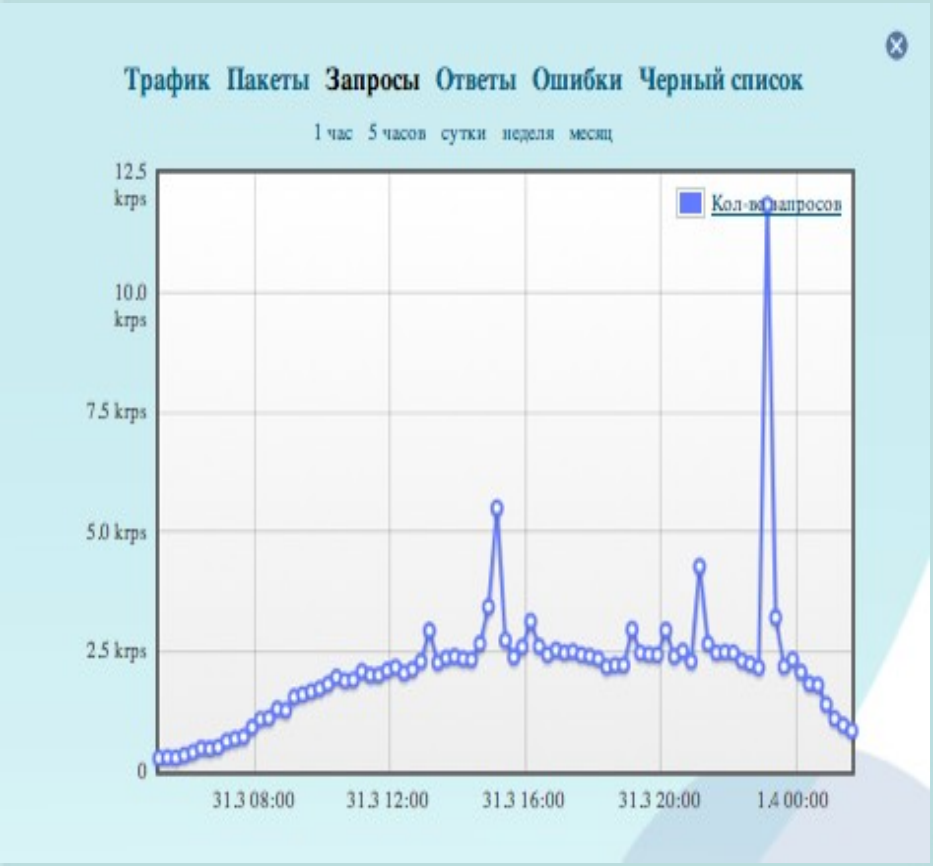


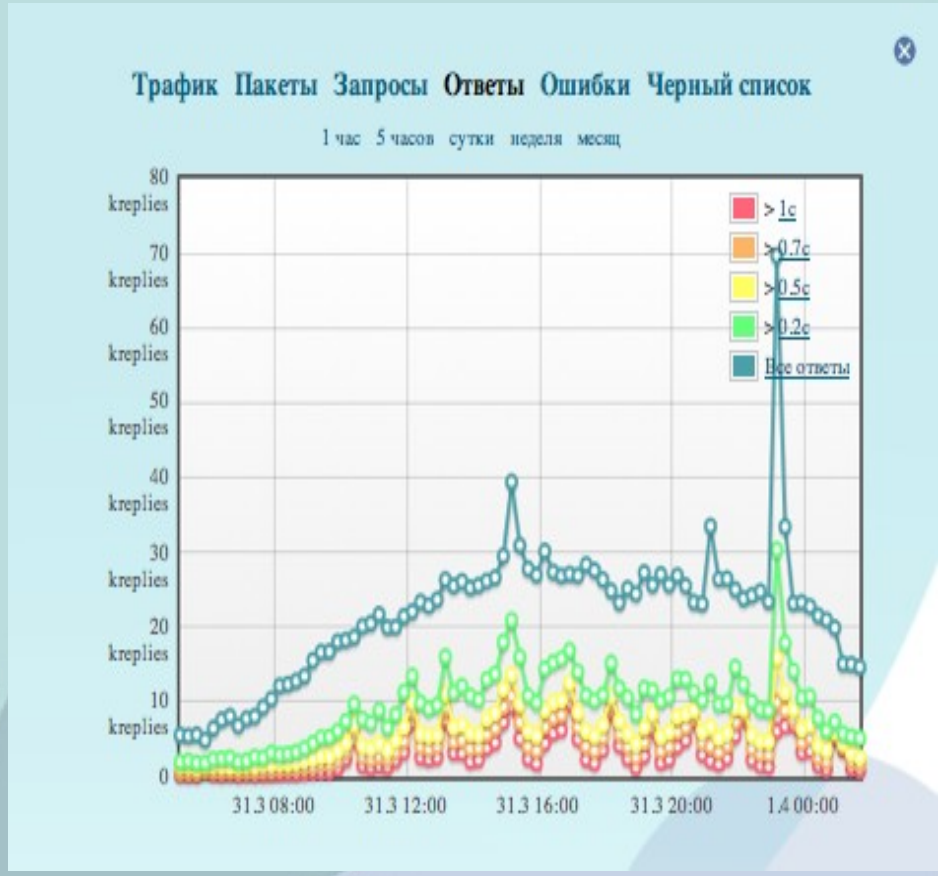
Пример 3


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
1000 Mbps
800 Mbps
600 Mbps
400 Mbps
200 Mbps
0
Оплачиваемый траффик
Пропущено
Получено
Исходящий
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00

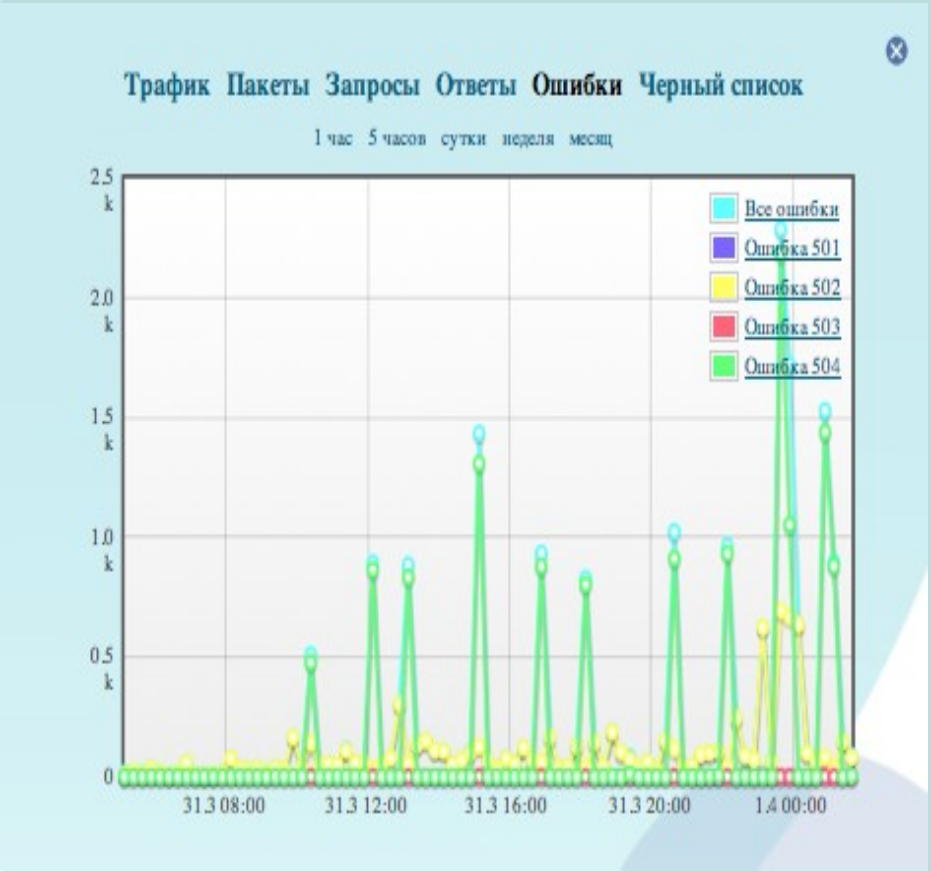

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
70 kpps
60 kpps
50 kpps
40 kpps
30 kpps
20 kpps
10 kpps
0
Пропущено
Получено
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00

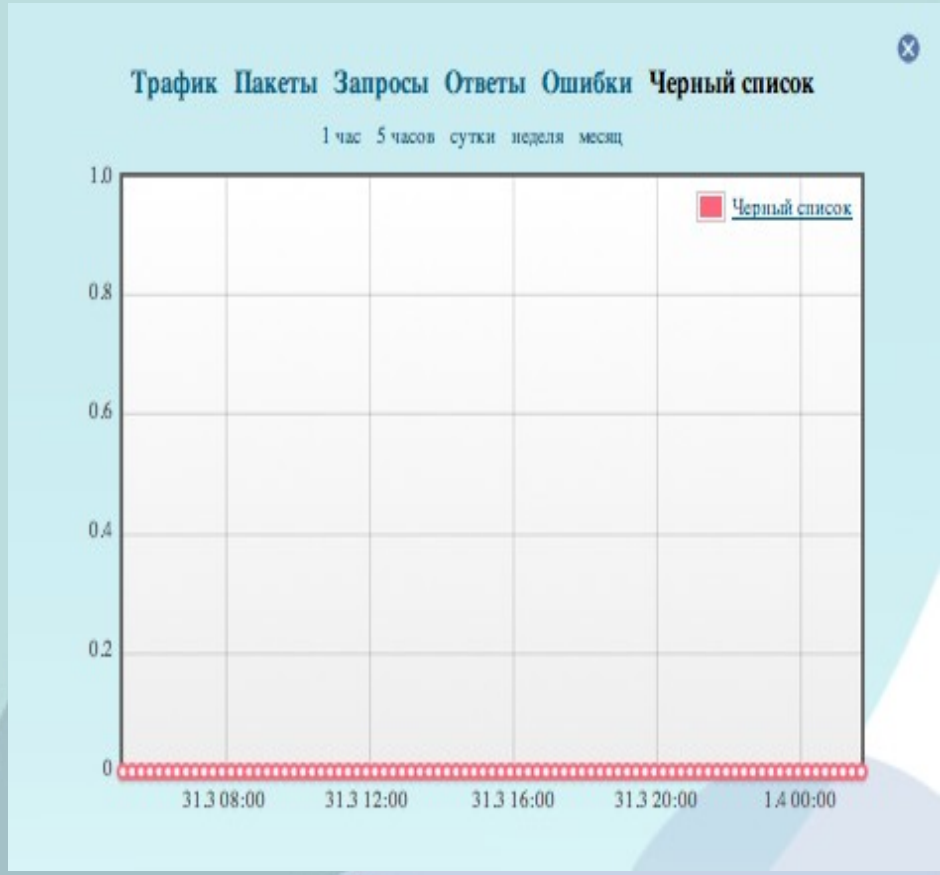
Пример 3


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
12.5 krps
10.0 krps
7.5 krps
5.0 krps
2.5 krps
0
Кол-во запросов
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
80 kreplies
70 kreplies
60 kreplies
50 kreplies
40 kreplies
30 kreplies
20 kreplies
10 kreplies
0
> 1c
> 0.7c
> 0.5c
> 0.2c
Все ответы
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00

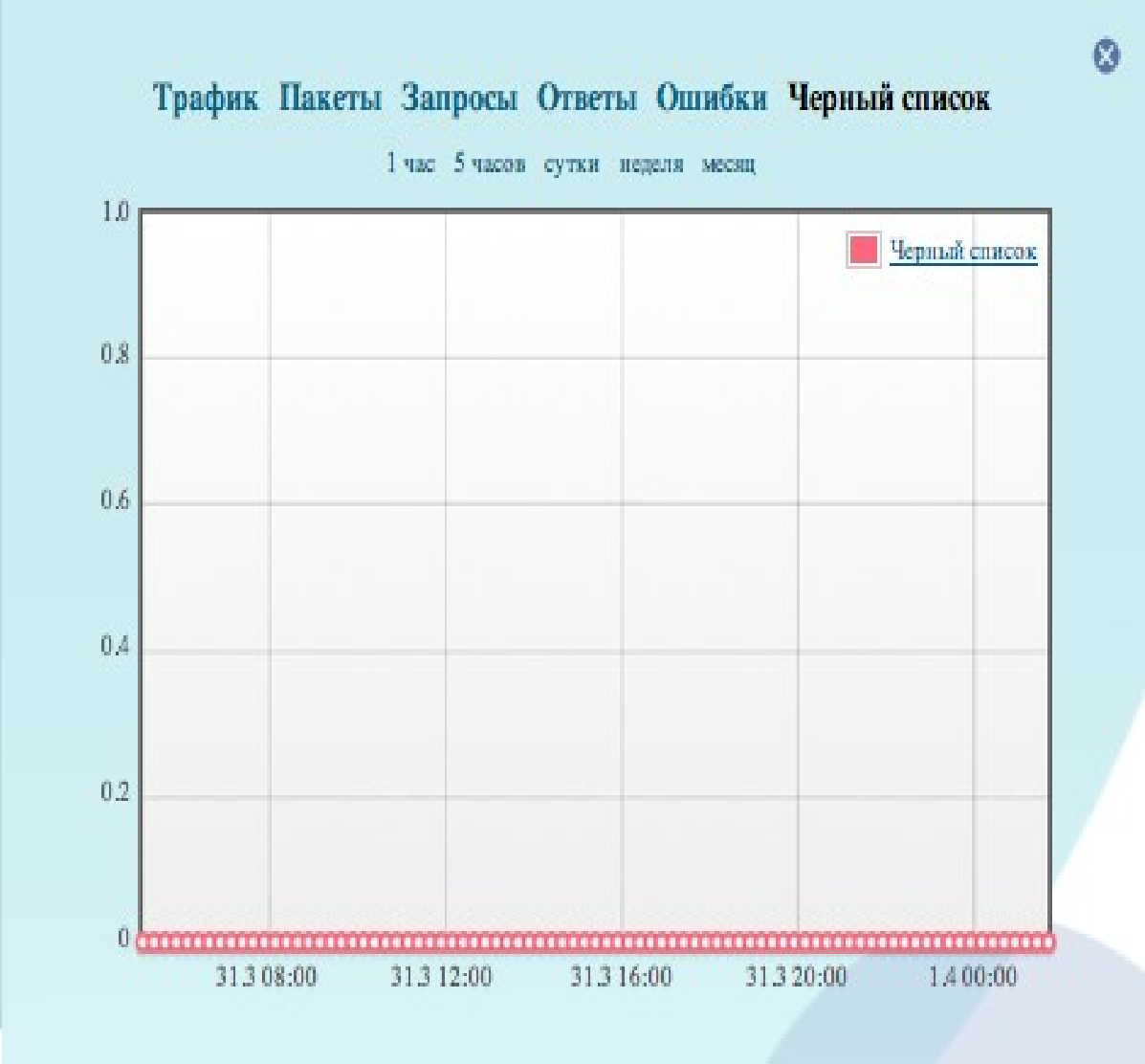
Пример 3


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
2.5 k
2.0 k
1.5 k
1.0 k
0.5 k
0
Все ошибки
Ошибка 501
Ошибка 502
Ошибка 503
Ошибка 504
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
1.0
0.8
0.6
0.4
0.2
0
Черный список
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00

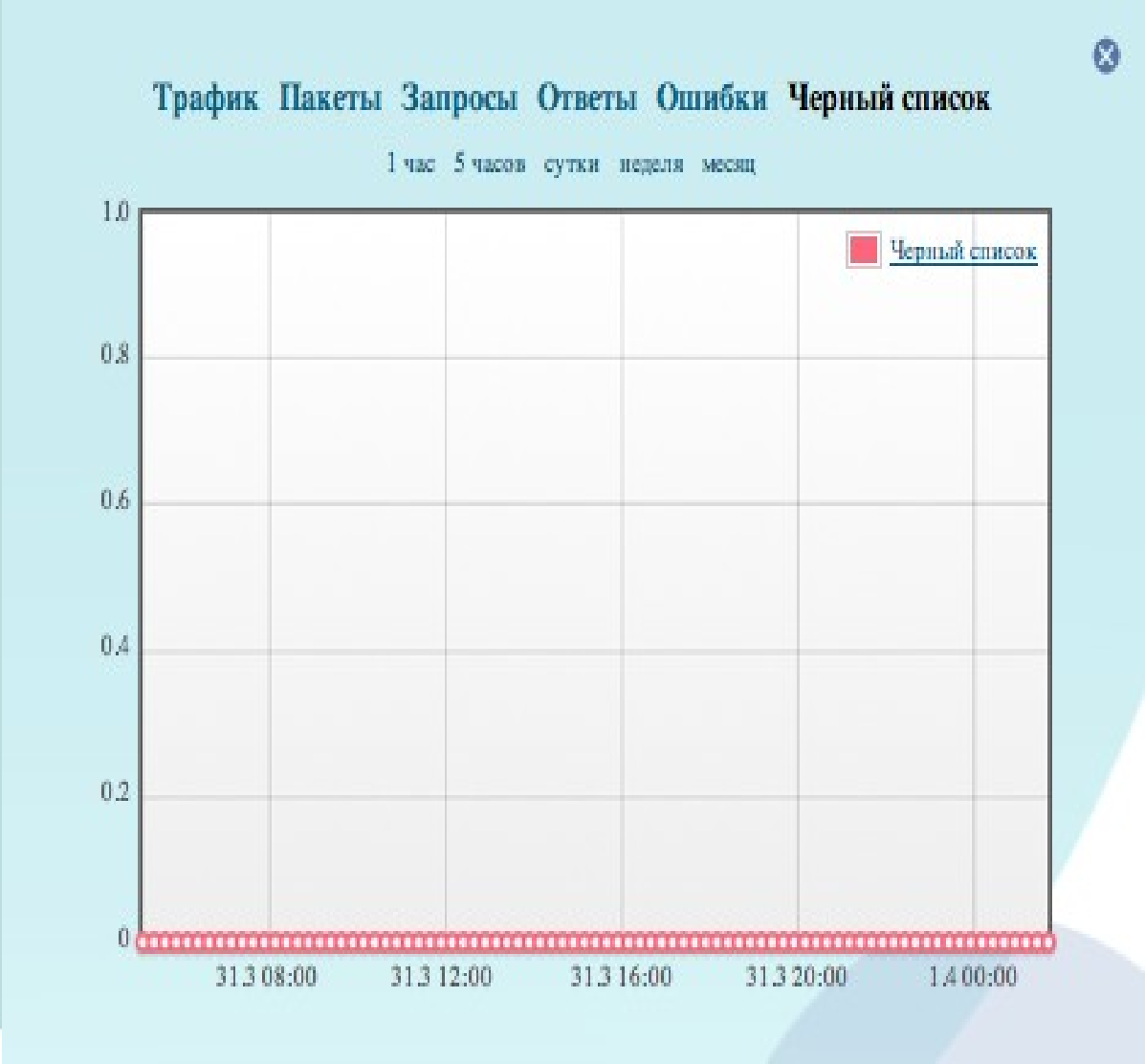
Пример 3

- ????

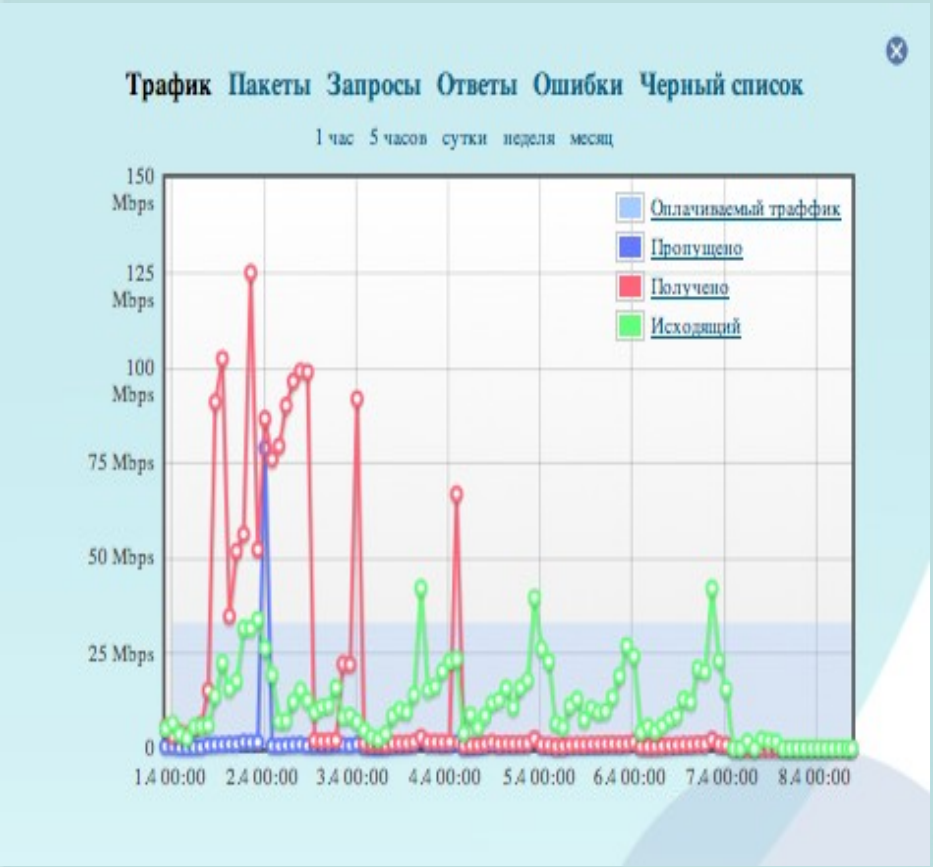

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
1.0
0.8
0.6
0.4
0.2
0
Черный список
31.3 08:00
31.3 12:00
31.3 16:00
31.3 20:00
1.4 00:00

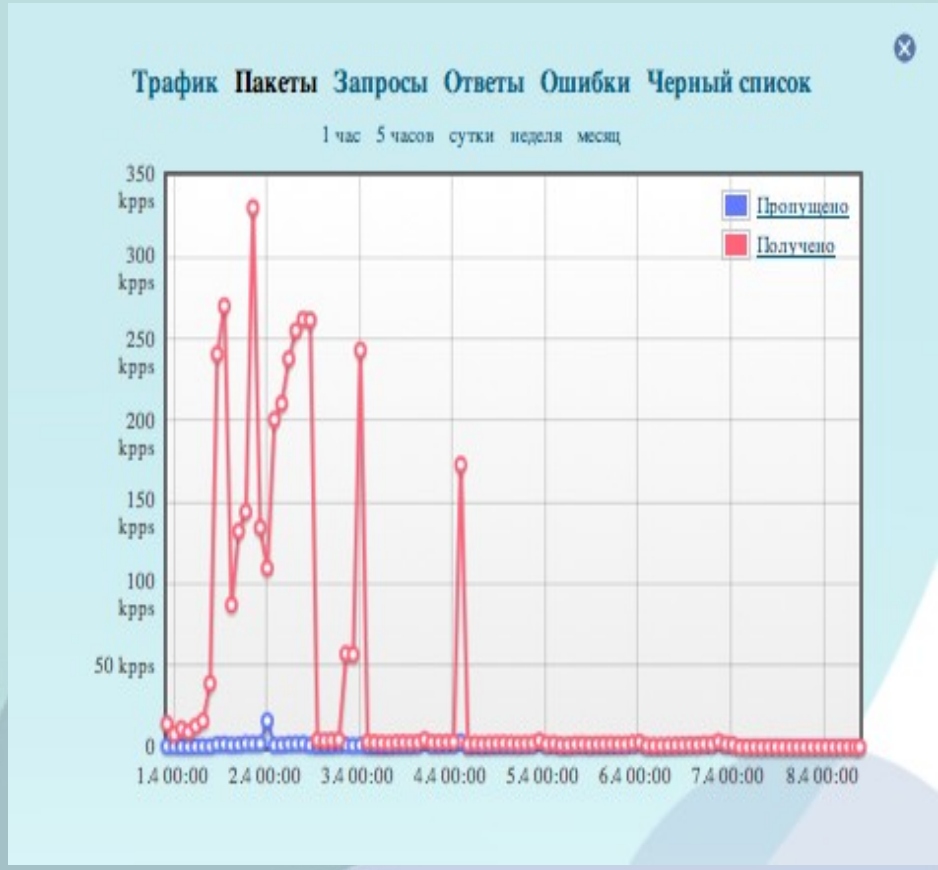
Пример 3

- Телереклама!

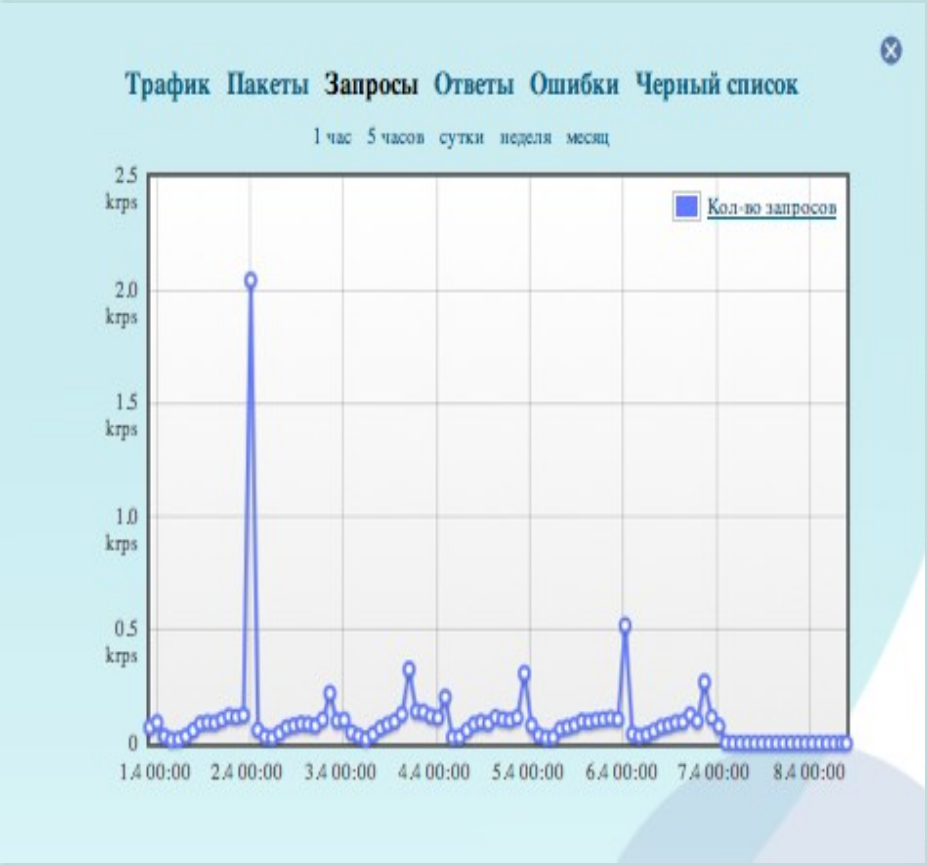


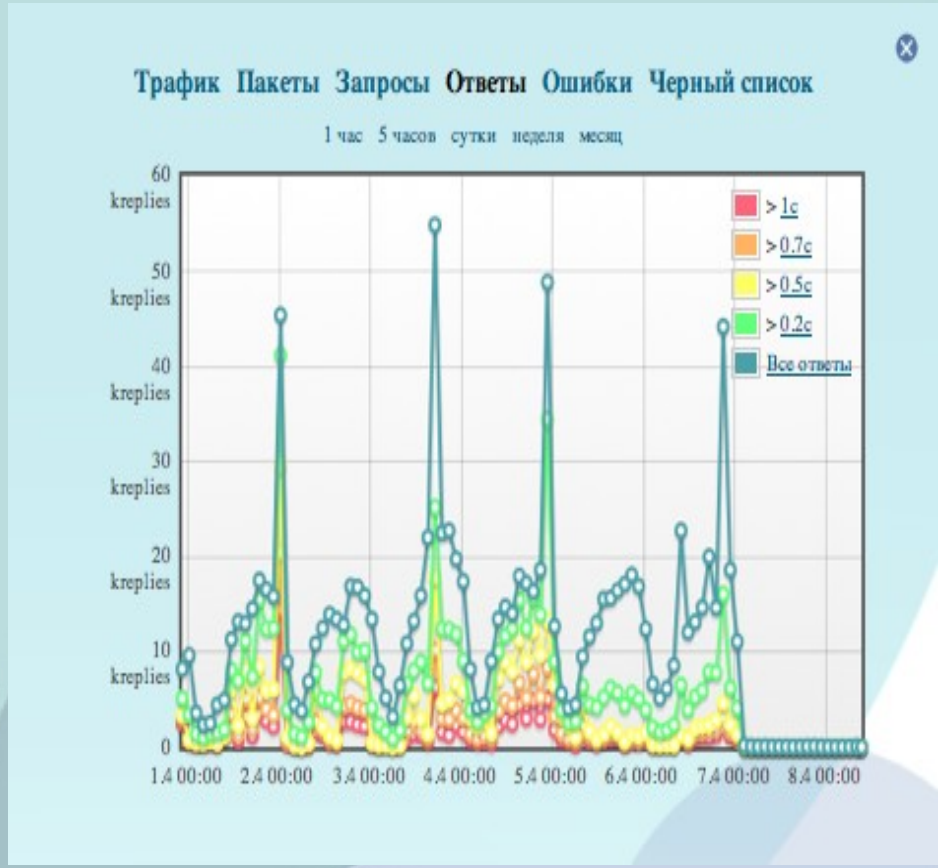
Пример 4


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
150 Mbps
125 Mbps
100 Mbps
75 Mbps
50 Mbps
25 Mbps
0
Оплачиваемый траффик
Пропущено
Получено
Исходящий
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00

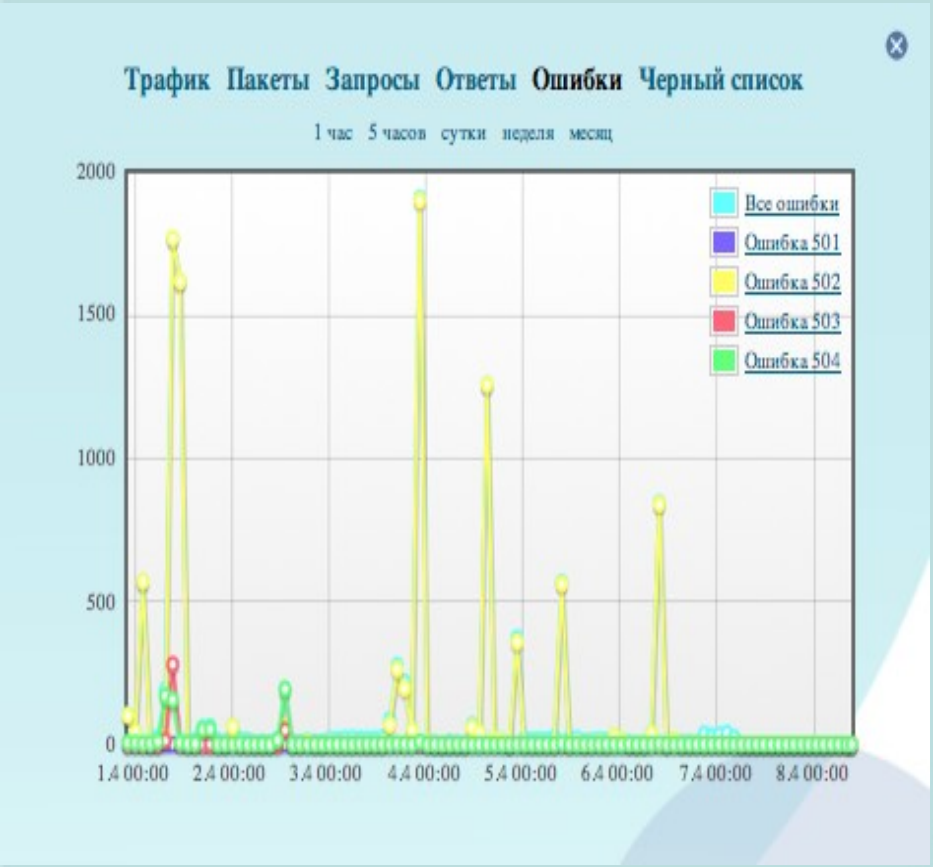

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
350 kpps
300 kpps
250 kpps
200 kpps
150 kpps
100 kpps
50 kpps
0
Пропущено
Получено
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00

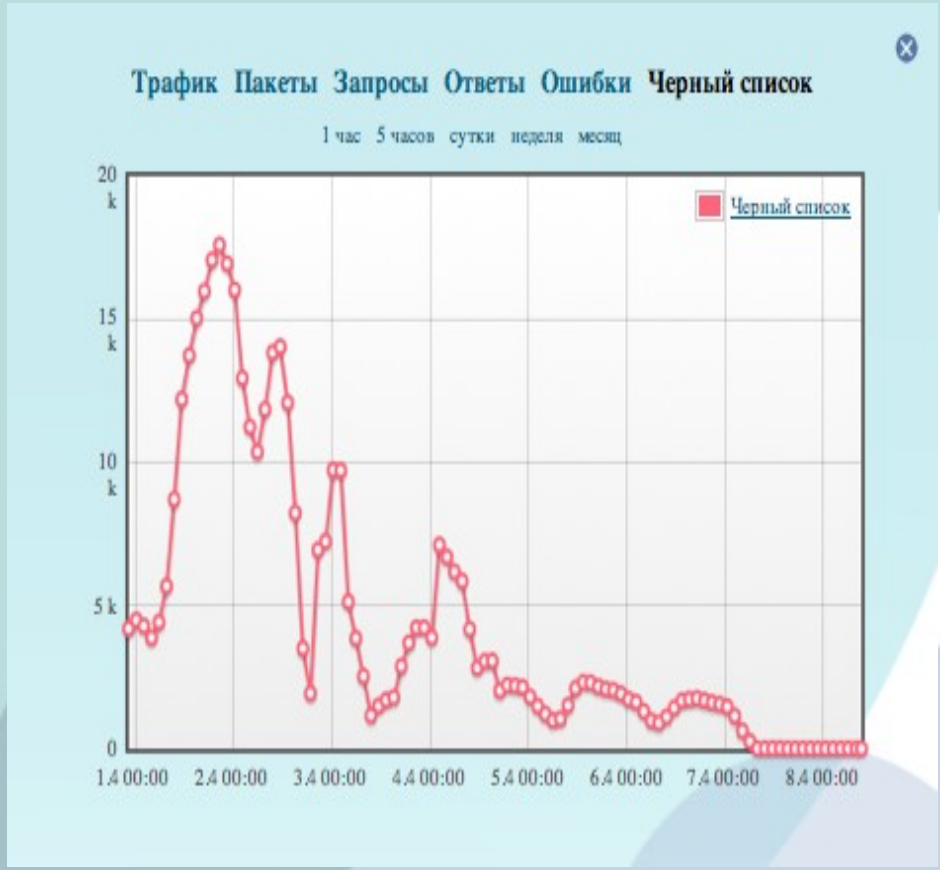
Пример 4


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
2.5 krps
2.0 krps
1.5 krps
1.0 krps
0.5 krps
0
Кол-во запросов
1.4 00:00
2.4 00:00
3.4 00:00
4.4 00:00
5.4 00:00
6.4 00:00
7.4 00:00
8.4 00:00

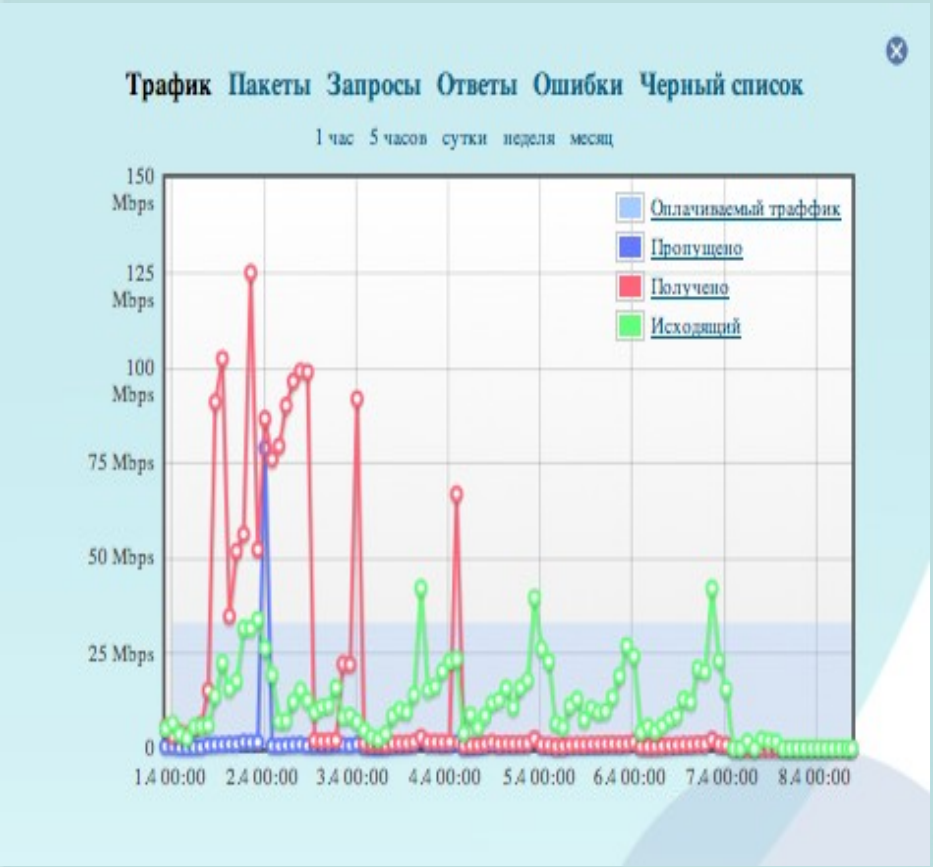

Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
60 kreplies
50 kreplies
40 kreplies
30 kreplies
20 kreplies
10 kreplies
0
> 1c
> 0.7c
> 0.5c
> 0.2c
Все ответы
1.4 00:00
2.4 00:00
3.4 00:00
4.4 00:00
5.4 00:00
6.4 00:00
7.4 00:00
8.4 00:00

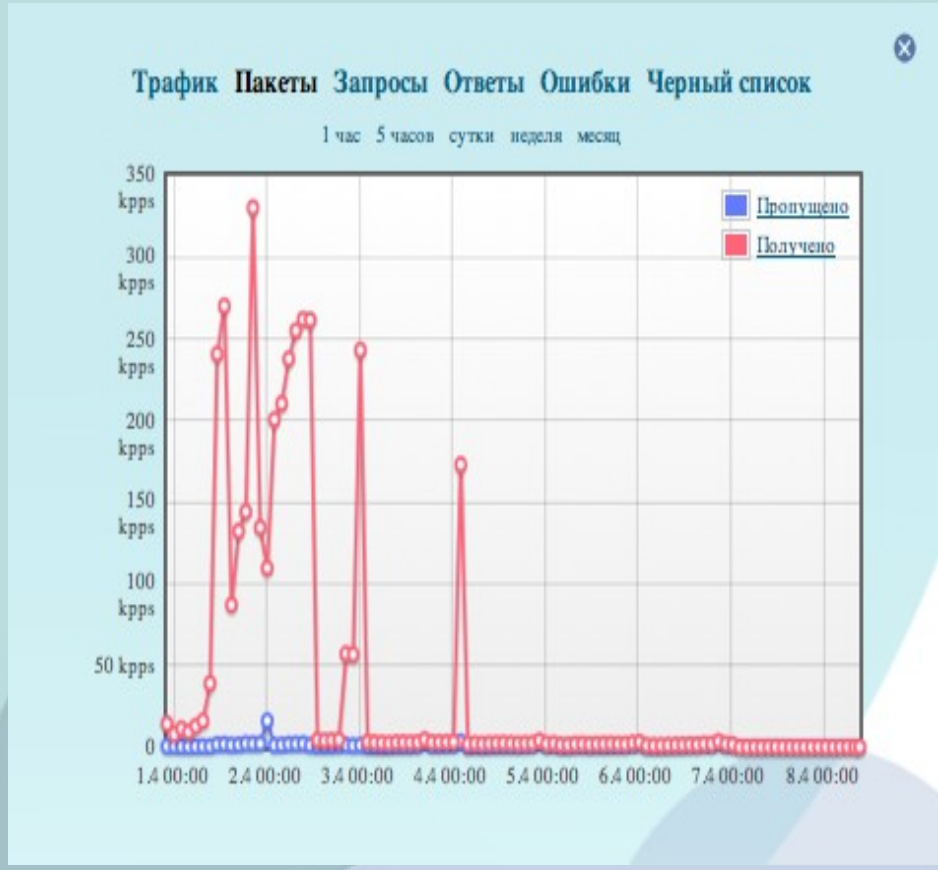
Пример 4


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
2000
1500
1000
500
0
Все ошибки
Ошибка 501
Ошибка 502
Ошибка 503
Ошибка 504
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
20 k
15 k
10 k
5 k
0
Черный список
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00

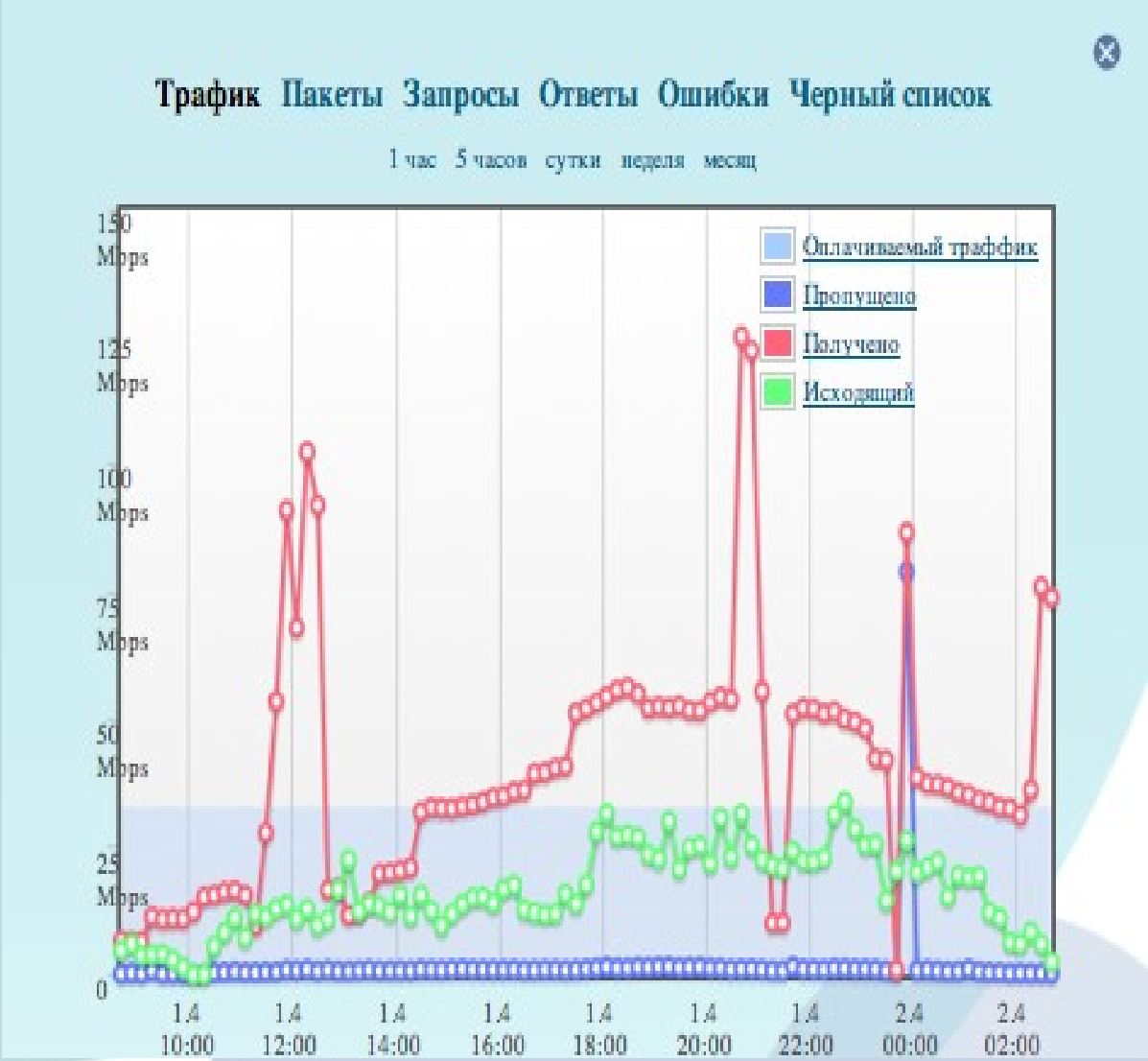
Пример 4


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
150 Mbps
125 Mbps
100 Mbps
75 Mbps
50 Mbps
25 Mbps
0
Оплачиваемый траффик
Пропущено
Получено
Исходящий
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00


Трафик Пакеты Запросы Ответы Ошибки Черный список
1 час 5 часов сутки неделя месяц
350 kpps
300 kpps
250 kpps
200 kpps
150 kpps
100 kpps
50 kpps
0
Пропущено
Получено
1.Д 00:00
2.Д 00:00
3.Д 00:00
4.Д 00:00
5.Д 00:00
6.Д 00:00
7.Д 00:00
8.Д 00:00

Пример 4

- Что интересно?
- Что осталось за кадром ?
- Почему ?



Пример 4

- Компоненты атаки:
  - SYN flood

```
17:28:12.305877 IP 212.58.14.83.30066 > 212.192.255.245.80: S 1680318705:1680318705(0)
17:28:12.305915 IP 212.118.95.136.42761 > 212.192.255.245.80: S 2331650342:2331650342(0)
17:28:12.305944 IP 212.4.252.150.63642 > 212.192.255.245.80: S 1780088629:1780088629(0)
17:28:12.305978 IP 212.123.17.65.53834 > 212.192.255.245.80: S 1363172319:1363172319(0)
17:28:12.306012 IP 212.8.237.44.18701 > 212.192.255.245.80: S 2693728203:2693728203(0)
17:28:12.306053 IP 212.231.103.18.49297 > 212.192.255.245.80: S 1358154416:1358154416(0)
17:28:12.306094 IP 212.75.81.44.38496 > 212.192.255.245.80: S 3995520202:3995520202(0)
17:28:12.306128 IP 212.138.156.170.26992 > 212.192.255.245.80: S 24434248:24434248(0)
17:28:12.306157 IP 212.141.49.99.31961 > 212.192.255.245.80: S 3739325953:3739325953(0)
17:28:12.306191 IP 212.113.33.76.48150 > 212.192.255.245.80: S 4009899498:4009899498(0)
17:28:12.306225 IP 212.240.116.218.22631 > 212.192.255.245.80: S 500296056:500296056(0)
17:28:12.306271 IP 212.141.217.132.37593 > 212.192.255.245.80: S 3638679843:3638679843(0)
17:28:12.306311 IP 212.83.188.232.12937 > 212.192.255.245.80: S 626436486:626436486(0)
17:28:12.306346 IP 212.250.46.138.21007 > 212.192.255.245.80: S 75717416:75717416(0)
17:28:12.306386 IP 212.39.222.26.49161 > 212.192.255.245.80: S 447418041:447418041(0)
17:28:12.306416 IP 212.98.72.17.16639 > 212.192.255.245.80: S 853255599:853255599(0)
17:28:12.306457 IP 212.220.246.162.38560 > 212.192.255.245.80: S 2616693313:2616693313(0)
17:28:12.306493 IP 212.87.83.131.34590 > 212.192.255.245.80: S 2616214561:2616214561(0)
17:28:12.306522 IP 212.216.58.93.14133 > 212.192.255.245.80: S 3699880955:3699880955(0)
17:28:12.306557 IP 212.83.85.136.32100 > 212.192.255.245.80: R 2318562855:2318562855(0)
17:28:12.306577 IP 212.239.239.244.36850 > 212.192.255.245.80: S 3076267411:3076267411(0)
17:28:12.306621 IP 212.152.43.124.60615 > 212.192.255.245.80: S 3621419802:3621419802(0)
17:28:12.306655 IP 212.90.179.139.39460 > 212.192.255.245.80: S 2331627305:2331627305(0)
17:28:12.306683 IP 212.208.132.120.28972 > 212.192.255.245.80: S 947313942:947313942(0)
17:28:12.306714 IP 212.231.67.151.42426 > 212.192.255.245.80: S 203216949:203216949(0)
```

Пример 4

```
17:28:12.305877 IP 212.58.14.83.30066 > 212.192.255.245.80: S 1680318705:1680318705(0)
17:28:12.305915 IP 212.118.95.136.42761 > 212.192.255.245.80: S 2331650342:2331650342(0)
17:28:12.305944 IP 212.4.252.150.63642 > 212.192.255.245.80: S 1780088629:1780088629(0)
17:28:12.305978 IP 212.123.17.65.53834 > 212.192.255.245.80: S 1363172319:1363172319(0)
17:28:12.306012 IP 212.8.237.44.18701 > 212.192.255.245.80: S 2693728203:2693728203(0)
17:28:12.306053 IP 212.231.103.18.49297 > 212.192.255.245.80: S 1358154416:1358154416(0)
17:28:12.306094 IP 212.75.81.44.38496 > 212.192.255.245.80: S 3995520202:3995520202(0)
17:28:12.306128 IP 212.138.156.170.26992 > 212.192.255.245.80: S 24434248:24434248(0)
17:28:12.306157 IP 212.141.49.99.31961 > 212.192.255.245.80: S 3739325953:3739325953(0)
17:28:12.306191 IP 212.113.33.76.48150 > 212.192.255.245.80: S 4009899498:4009899498(0)
17:28:12.306225 IP 212.240.116.218.22631 > 212.192.255.245.80: S 500296056:500296056(0)
17:28:12.306271 IP 212.141.217.132.37593 > 212.192.255.245.80: S 3638679843:3638679843(0)
17:28:12.306311 IP 212.83.188.232.12937 > 212.192.255.245.80: S 626436486:626436486(0)
17:28:12.306346 IP 212.250.46.138.21007 > 212.192.255.245.80: S 75717416:75717416(0)
17:28:12.306386 IP 212.39.222.26.49161 > 212.192.255.245.80: S 447418041:447418041(0)
17:28:12.306416 IP 212.98.72.17.16639 > 212.192.255.245.80: S 853255599:853255599(0)
17:28:12.306457 IP 212.220.246.162.38560 > 212.192.255.245.80: S 2616693313:2616693313(0)
17:28:12.306493 IP 212.87.83.131.34590 > 212.192.255.245.80: S 2616214561:2616214561(0)
17:28:12.306522 IP 212.216.58.93.14133 > 212.192.255.245.80: S 3699880955:3699880955(0)
20:54:48.208569 IP 38.225.42.87.3072 > 212.192.255.235.53: UDP, length 3
20:54:48.208597 IP 248.19.224.57.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208625 IP 5.24.222.74.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208654 IP 203.121.137.9.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208682 IP 139.193.105.11.3072 > 212.192.255.235.53: UDP, length 3
20:54:48.208711 IP 66.191.46.32.3072 > 212.192.255.235.53: UDP, length 3
20:54:48.208743 IP 80.10.52.112.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208770 IP 243.222.179.51.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208798 IP 52.81.7.56.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208828 IP 40.246.172.38.3072 > 212.192.255.235.53: UDP, length 3
20:54:48.208858 IP 95.219.154.6.3072 > 212.192.255.235.53: UDP, length 3
20:54:48.208890 IP 56.180.232.112.1024 > 212.192.255.235.53: UDP, length 3
20:54:48.208919 IP 36.128.252.13.3072 > 212.192.255.235.53: UDP, length 3
17:28:12.306557 IP 212.83.85.136.32100 > 212.192.255.245.80: R 2318562855:2318562855(0)
20:54:48.208975 IP 203.121.137.9.1024 > 212.192.255.235.80: S <1460,[|tcp]>
17:28:12.306577 IP 212.239.239.244.36850 > 212.192.255.245.80: S 3076267411:3076267411(0)
17:28:12.306621 IP 212.152.43.124.60615 > 212.192.255.245.80: S 3621419802:3621419802(0)
17:28:12.306655 IP 212.90.179.139.39460 > 212.192.255.245.80: S 2331627305:2331627305(0)
17:28:12.306683 IP 212.208.132.120.28972 > 212.192.255.245.80: S 947313942:947313942(0)
17:28:12.306714 IP 212.231.67.151.42426 > 212.192.255.245.80: S 203216949:203216949(0)
```

Пример 4

- Компоненты атаки:
  - SYN flood, не выводящий сервер из строя
  - Некорректные закрытия соединений, расходующие ресурсы сервера

Фильтрация атак

- Канальная ёмкость
- Атаки прикладного уровня
- «0-day exploits»
- Интеллектуальные организаторы
- Аутсорсинг компетенций
- Расследование инцидентов?

Расследование

- «Типичное преступление – это когда у юридического лица крадут ключи, по ним формируют платежные поручения. Чтобы клиент не понял, что у него списана большая сумма со счета, на банк начинают DDoS-атаку»

Спасибо!

- Вопросы?
- Alexander Lyamin <al@highloadlab.com>