

# Содержание

Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE .....	3
<i>Пример настройки триггера на поиск источника DDOS-атаки типа Flood</i> .....	3
<i>Пример настройки триггера на поиск цели DDOS-атаки типа Flood</i> .....	9
Анализ BotNet .....	11
Фиксация перехода абонента на ресурс конкурента .....	12



# Поиск DDoS атак, BotNet и перехода на конкретный ресурс с использованием триггеров в QoE

Триггеры используются для поиска данных в QoE Stor по заданным параметрам. После срабатывания триггера возможно одно из действий:

- уведомление в GUI
- HTTP действие
- отправка email

Необходимые опции SKAT DPI:

- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- Внедрение и администрирование

## Пример настройки триггера на поиск источника DDOS-атаки типа Flood

### Общая информация триггера

Название триггера *	Важность	Триггер	
DDoS поиск источника	Информация	▼	<input type="radio"/> Выключен
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	▼ 1 час	▼ 1	
Дата начала	Дата окончания	Время начала	Время окончания
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Название триггера «DDoS поиск источника», дни недели - все, частота проверки - 1 час, частота срабатываний триггера - 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

## Запросы

Запросы							
+							
	Название	Отчет		Период с	Период по		
<input checked="" type="checkbox"/> Вкл.	A	Maxi	▼	сейчас - 15 минут	сейчас		🗑

- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 15 минут», период по: «сейчас»



В этом случае будет происходить анализ трафика по выбранной странице в период — последние 15 минут.

## Условия

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
<input checked="" type="checkbox"/> Вкл.	И	A	avg		Время жизни	<=	20
<input checked="" type="checkbox"/> Вкл.	И	A	avg		Сессии	>=	1500

- Добавить "+" 2 поля
- Связка - И
- Функция - avg
- Серия в 1 поле - Время жизни сессии, мс <= 20
- Серия во 2 поле - Сессии >= 1500

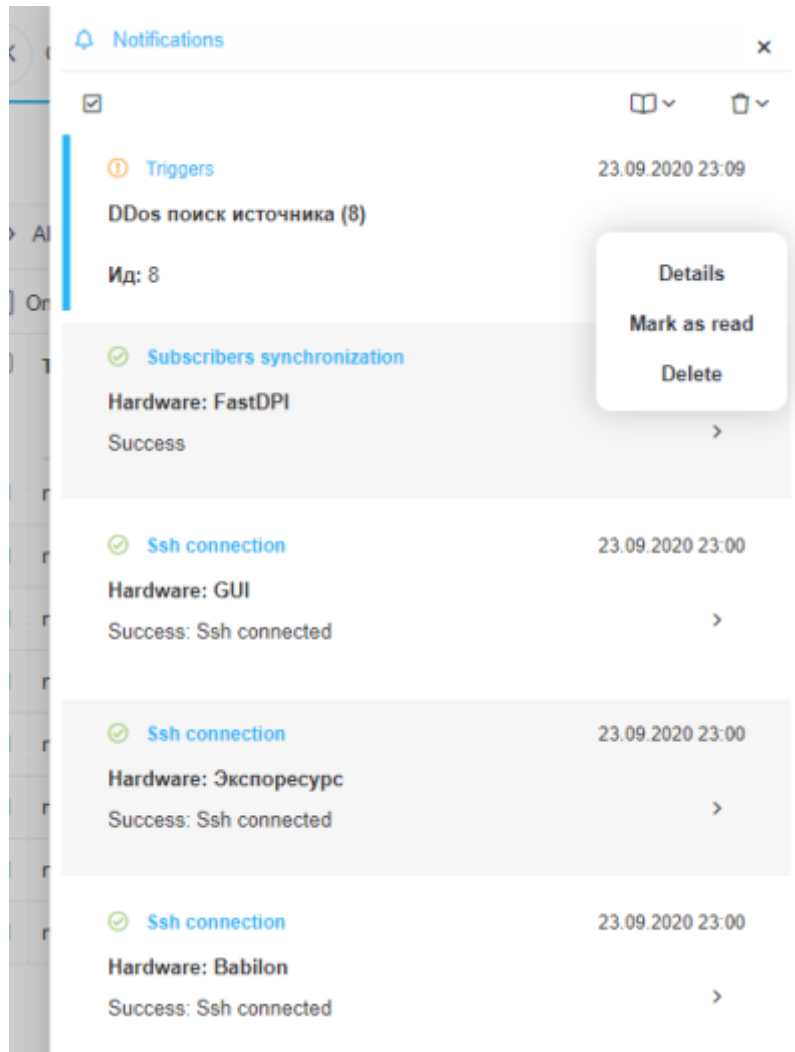


Мы задали условие — для срабатывания триггера необходимо, чтобы были детектированы: И сессии с жизнью меньше или равно 20мс, И с одного IP-хоста было более 1500 сессий.

## Обработка ошибок







Выбрать нотификацию Выбрать — "Детали"

Notifications x

---

← Triggers

---

Status	Read
Notification date	23.09.2020 23:09
Notify type	<span style="color: orange;">ⓘ</span> Warning

---

Notification content

---

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostsIpsWidget

Причины возникновения нотификации:

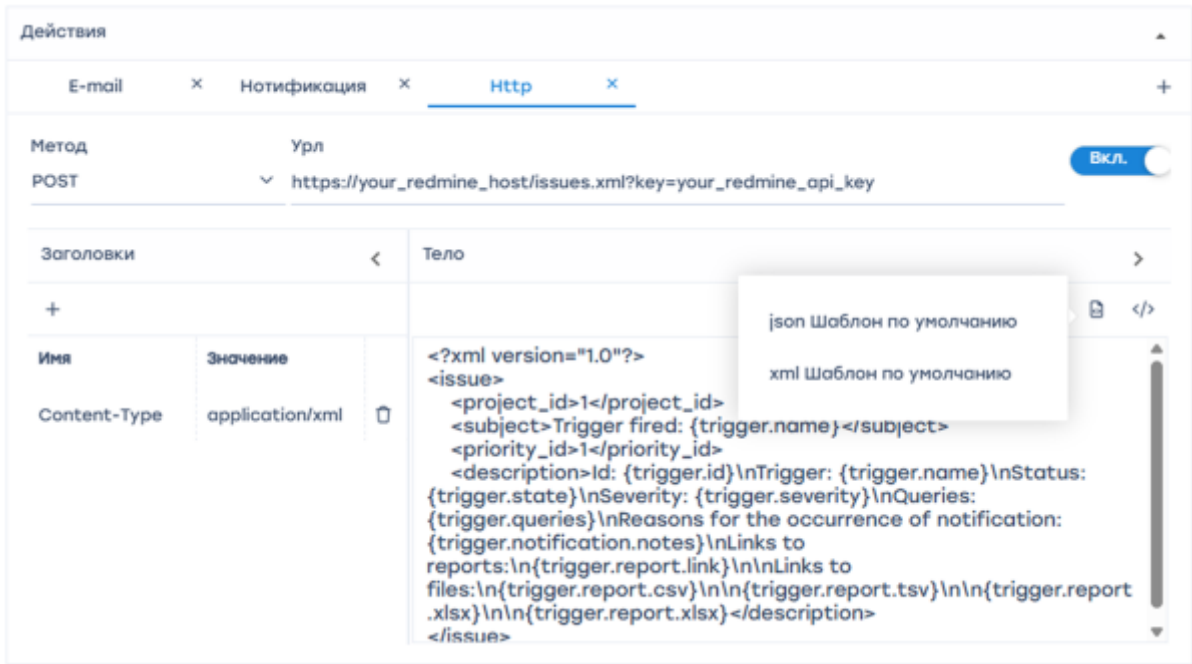
avg(avg\_ses\_lifetime) <= 200000 is true in query A  
avg(sessions\_uniq) >= 1 is true in query A


Ссылки на отчеты:

A: [https://192.168.88.11/#QoEAnyReport/report\\_id=rMeFuKSp316vU1b](https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b)

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

**HTTP действие**



Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)  
Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

## Пример настройки триггера на поиск цели DDOS-атаки типа Flood

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

### Запросы

Запросы

	Название	Отчет	Период с	Период по
<input checked="" type="checkbox"/>	Вкл. A	Махi	сейчас - 15 минут	сейчас

Условия

Связь	Оператор	Значение
<input checked="" type="checkbox"/> Вкл. И	<=	20
<input checked="" type="checkbox"/> Вкл. И	>=	1500

Обработка ошибок

Если нет данных \*  
Нет данных

Действия

Нотификация x

Кому

Поиск

- Сырой полный нетфлоу
- Таблицы
  - Сырой лог
  - Обнаружение атак
  - Топ прикладных протоколов
  - Топ групп прикладных протоколов
  - Топ абонентов
    - По трафику
    - По флоу
    - По времени жизни сессии
    - По абонентам и хостам
    - Махi

в поле отчет выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ абонентов → Махi

## Условия

	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
<input checked="" type="checkbox"/>	Вкл. И	A	avg		Флоу к абоне	>=	10000

Серия — "Объем Flow к абонентам, Пак", >= 10000



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

# Анализ BotNet

От предыдущего примера отличается настройкой 2 и 3 этапов (Запросы и Условия).

## Запросы

Запросы							
+							
	Название	Отчет		Период с	Период по		
<input checked="" type="checkbox"/>	Вкл. А	Махі	▼	сейчас - 15 минут	сейчас		🗑
<input checked="" type="checkbox"/>	Вкл. В	Полный сырой лог	▼	сейчас - 15 минут	сейчас		🗑

- Выбрать Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ прикладных протоколов → Махі для значения "А"
- Сырой полный нетфлоу → Сырой лог → Полный сырой лог для значения "В"

## Условия

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
<input checked="" type="checkbox"/>	Вкл. ИЛИ	В	avg		Порт получат	=	6667
<input checked="" type="checkbox"/>	Вкл. ИЛИ	В	avg		Порт источни	=	6667
<input checked="" type="checkbox"/>	Вкл. ИЛИ	В	avg		Порт получат	=	1080
<input checked="" type="checkbox"/>	Вкл. ИЛИ	В	avg		Порт источни	=	1080
<input checked="" type="checkbox"/>	Вкл. И	А	avg		Флоу	>=	2000

Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "В" со значением "ИЛИ", и Флоу больше или равно 2000.



При этой конфигурации в случае если: хоть на одном из портов (6667/1080) количество проходящих пакетов будет более 2000 в секунду — сработает триггер.



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

# Фиксация перехода абонента на ресурс конкурента

## Общая информация триггера

Общее			
Название триггера *	Важность	Триггер	<input type="checkbox"/> Выключен
Интерес к конкурентам	Информация		
Дни недели *	Частота проверки *	Количество срабатываний	
Пн, Вт, Ср, Чт, Пт, Сб, Вс	1 час	1	
Дата начала	Дата окончания	Время начала	Время окончания

Название триггера «Интерес к конкурентам», дни недели - все, частота проверки - 1 час, частота срабатываний триггера - 1 раз, даты и время начала/окончания не установлены.



Каждый день периодичностью в 1 час будет происходить проверка по условиям описанным ниже.

## Запросы

Запросы						
+						
	Название	Отчет		Период с	Период по	
<input checked="" type="checkbox"/>	Вкл. А	Сырой кликстрим	▼	сейчас - 1 час	сейчас	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Вкл. В	Maxi	▼	сейчас - 1 час	сейчас	<input type="checkbox"/>

- Добавить "+" поле
- Название А  
Выбрать таблицу для сканирования: Сырой кликстрим → Таблицы → Сырой кликстрим
- Название В  
Выбрать таблицу для сканирования: Сырой полный нетфлоу → Таблицы → Обнаружение атак → Топ IP-адресов хостов → Maxi
- Выбрать период с: «сейчас - 1 час», период по : «сейчас»
- В этом случае будет происходить анализ трафика каждый час по выбранным таблицам.

## Условия

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
<input checked="" type="checkbox"/>	Вкл.	ИЛИ	A	avg	Хост	=	*megafon.ru
<input checked="" type="checkbox"/>	Вкл.	И	B	avg	Объем флой	>=	800
<input checked="" type="checkbox"/>	Вкл.	ИЛИ	A	avg	Хост	=	*mts.ru

- Добавить "+" 3 поля
- Первое поле — выбрать таблицу "A"; Связка - "Или"; Функция - "avg"; Серия Хост = \*megafon.ru (или ваш любимый конкурент)
- Второе поле — выбрать таблицу "B"; связка "И"; Функция - "avg"; Серия Объем флой от абонентов >= 800
- Третье поле — выбрать таблицу "A"; Связка - "Или"; Функция - "avg"; Серия Хост = \*mts.ru



Мы задали условие — для срабатывания триггера необходимо, чтобы было детектировано: не менее 800 пакетов (не случайный а осмысленный переход) от абонента к сайту конкурента.

## Обработка ошибок

Обработка ошибок	
Если нет данных *	Если ошибка выполнения или тайм-аут *
Нет данных	Сохранить последнее состояние

- В поле "Если нет данных" — Нет данных
- В поле "Если ошибка выполнения или тайм-аут" — Сохранить последнее состояние.











В этой конфигурации — при отсутствии ошибок никаких данных сохраняться не будет, при их наличии — сохранится информация в виде таблицы о подозрительных сессиях.

## Действия

### E-mail действие



- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать тип нотификации — "Предупреждение"
- При этой настройке будет создана нотификация в СКАТ

Alerts					Alerts actions			
<input type="checkbox"/> Only selected triggers					<input type="checkbox"/> Only selected notifications			
Trigger name	Type	Date	Note		Type	Date	State	
<input type="checkbox"/> Ddos	 Alerting	14.08.2020 13:58:	avg(flow_vol_to_s	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:59:03	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos поиск исто.	 Alerting	14.08.2020 13:58:	avg(avg_ses_lifeti	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:58:23	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos	 Alerting	14.08.2020 13:56:	avg(flow_vol_to_s	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:56:43	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos поиск исто.	 Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:56:05	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos	 Alerting	14.08.2020 13:54:	avg(flow_vol_to_s	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:54:23	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos	 Alerting	14.08.2020 13:52:	avg(flow_vol_to_s	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:52:22	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos поиск исто.	<span>Ok</span>	14.08.2020 13:51:	avg(avg_ses_lifeti	<input type="checkbox"/>	<input type="checkbox"/> notification	14.08.2020 13:50:25	<span>Complete</span>	<input type="checkbox"/>
<input type="checkbox"/> Ddos	 Alerting	14.08.2020 13:50:	avg(flow_vol_to_s	<input type="checkbox"/>				<input type="checkbox"/>

Получить ссылку на отчет можно через меню нотификаций

**Notifications** x

📖 ▾ 🗑️ ▾

ⓘ **Triggers** 23.09.2020 23:09

**DDos поиск источника (8)**

**Ид: 8**

**Details**

**Mark as read**

**Delete**

✔ **Subscribers synchronization**

**Hardware: FastDPI**

Success >

✔ **Ssh connection** 23.09.2020 23:00

**Hardware: GUI**

Success: Ssh connected >

✔ **Ssh connection** 23.09.2020 23:00

**Hardware: Экспоресурс**

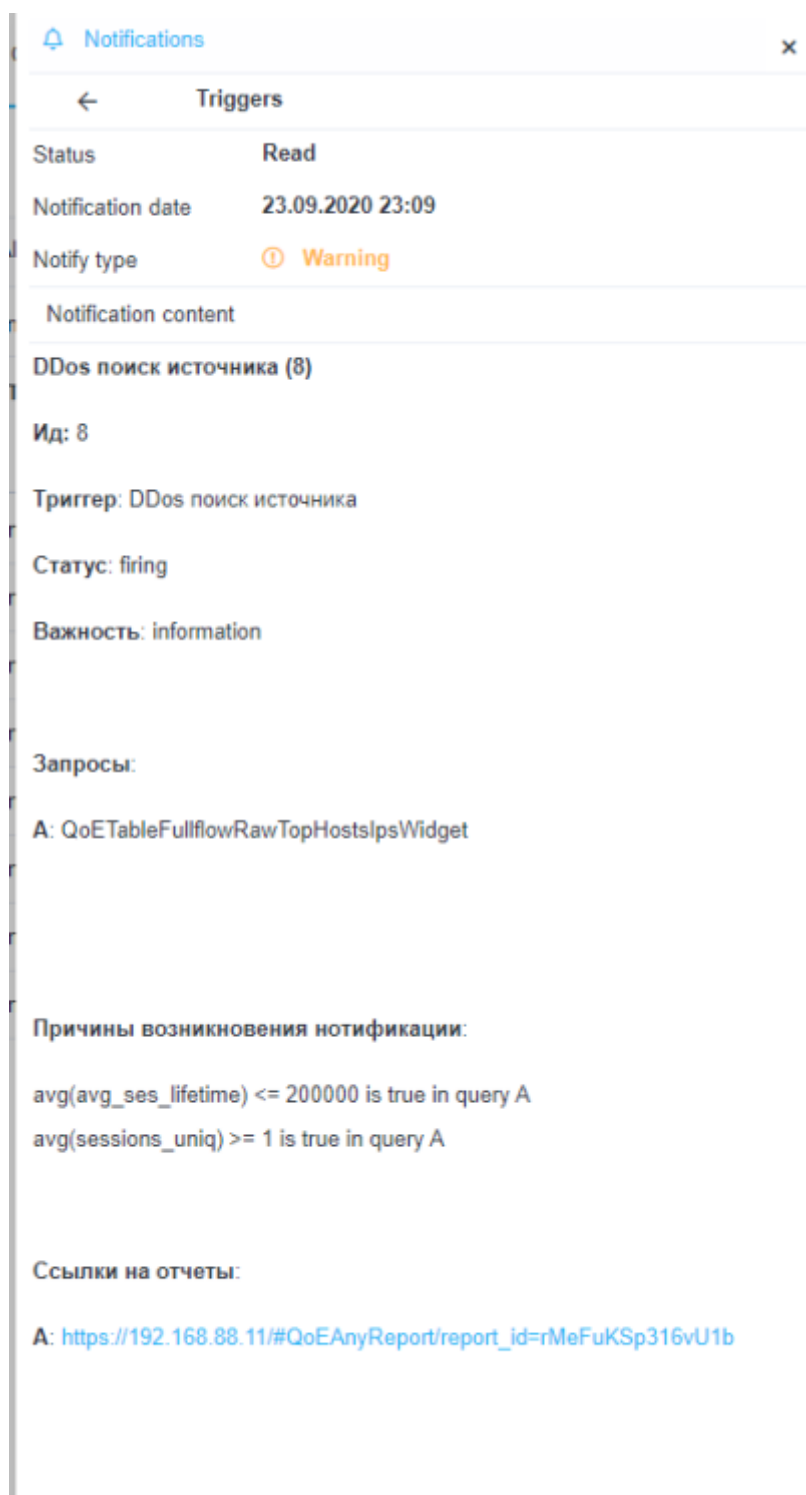
Success: Ssh connected >

✔ **Ssh connection** 23.09.2020 23:00

**Hardware: Babilon**

Success: Ssh connected >

Выбрать нотификацию Выбрать — "Детали"



The screenshot shows a 'Notifications' window with a title bar containing a bell icon, the text 'Notifications', and a close button 'x'. Below the title bar is a header with a back arrow and the text 'Triggers'. The main content area displays the following details:

Status	Read
Notification date	23.09.2020 23:09
Notify type	<span style="color: orange;">ⓘ</span> Warning

Notification content

DDos поиск источника (8)

Ид: 8

Триггер: DDos поиск источника

Статус: firing

Важность: information

Запросы:

A: QoETableFullflowRawTopHostsIpsWidget

Причины возникновения нотификации:

avg(avg\_ses\_lifetime) <= 200000 is true in query A  
avg(sessions\_uniq) >= 1 is true in query A

Ссылки на отчеты:

A: [https://192.168.88.11/#QoEAnyReport/report\\_id=rMeFuKSp316vU1b](https://192.168.88.11/#QoEAnyReport/report_id=rMeFuKSp316vU1b)

Перейти по ссылке на отчет — отчет откроется в новом окне браузера.

**HTTP действие**

Действия

E-mail × Нотификация × Http ×


Метод: POST  
Урл: `https://your_redmine_host/issues.xml?key=your_redmine_api_key` Вкл.

Заголовки < Тело >

Имя	Значение
Content-Type	application/xml

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Trigger fired: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Id: {trigger.id}\nTrigger: {trigger.name}\nStatus:
{trigger.state}\nSeverity: {trigger.severity}\nQueries:
{trigger.queries}\nReasons for the occurrence of notification:
{trigger.notification.notes}\nLinks to
reports:\n{trigger.report.link}\n\nLinks to
files:\n{trigger.report.csv}\n\n{trigger.report.tsv}\n\n{trigger.report
.xlsx}\n\n{trigger.report.xlsx}</description>
</issue>
```

json Шаблон по умолчанию  
xml Шаблон по умолчанию

- Для автоматического заполнения — кликнуть  (автоматическое заполнение формы)
- Выбрать метод наиболее приемлемый для вашей ticket-системы и ввести URL адрес



Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.