

Содержание

Detecting DDoS attacks, BotNet activity, and visits to specific resources using triggers in QoE 3

Example: configuring a trigger to detect the source of a Flood-type DDoS attack 3

Example: configuring a trigger to detect the target of a Flood-type DDoS attack 9

BotNet analysis 10

Detecting subscriber visits to competitor resources 11

Detecting DDoS attacks, BotNet activity, and visits to specific resources using triggers in QoE

[Triggers](#) are used to search data in QoE Stor based on specified parameters. When a trigger fires, one of the following actions can occur:

- Notification in GUI
- HTTP action
- Email notification

Required SSG DPI options:

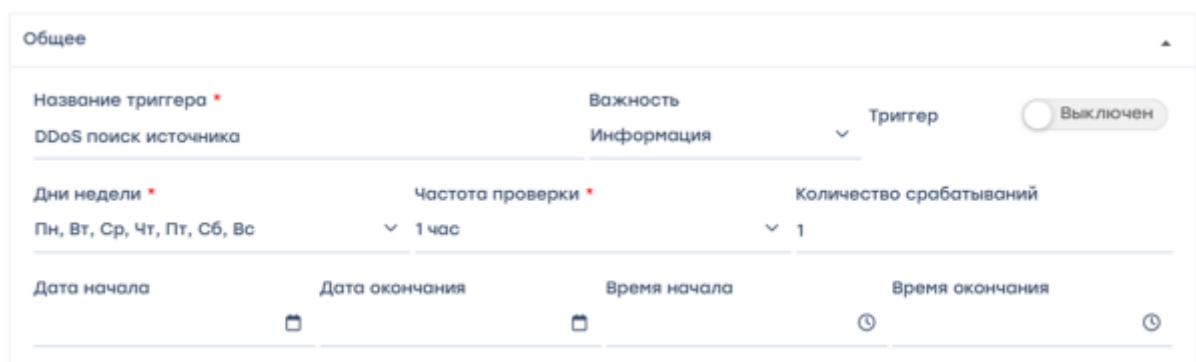
- [Statistics gathering and analysis on protocols and directions](#)
- [Subscriber notifications](#)

Required additional modules:

- [DPIUI2 \(GUI - Graphical User Interface\)](#)
- [Implementation and administration](#)

Example: configuring a trigger to detect the source of a Flood-type DDoS attack

General trigger information



The screenshot shows a configuration window titled "Общее" (General) for a trigger named "DDoS поиск источника" (DDoS source search). The trigger is currently disabled, as indicated by the "Выключен" (Disabled) toggle switch. The configuration includes the following fields:

Название триггера *		Важность	Триггер
DDoS поиск источника		Информация	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

Trigger name: "DDoS source detection", days of the week – all, check frequency – 1 hour, trigger activation frequency – once, start and end times not set.



Every day, the system will perform a check every hour based on the conditions described below.

Queries

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Maxi	▼	сейчас - 15 минут	сейчас	🗑

- Add field
- Name: A
- Select table for scanning: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Select period from “now - 15 minutes” to “now”



In this case, the system analyzes traffic for the selected page during the last 15 minutes.

Conditions

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒ Вкл.	И	A	avg		Время жизни	<=	20
☒ Вкл.	И	A	avg		Сессии	>=	1500

- Add two "+" fields
- Link - AND
- Function - avg
- Condition 1 - session lifetime <= 20 (ms)
- Condition 2 - number of sessions >= 1500



This means the trigger will fire if sessions with lifetimes ≤ 20 ms AND more than 1500 sessions from the same IP host are detected.

Error handling

Действия

E-mail x Нотификация x

Заголовок нотификации
{trigger.name}

Подзаголовок нотификации
{trigger.id}

Тип нотификации
Предупреждение

Сообщение

Ид: {trigger.id}
Триггер: {trigger.name}
Статус: {trigger.state}
Важность: {trigger.severity}

Запросы:
{trigger.queries}

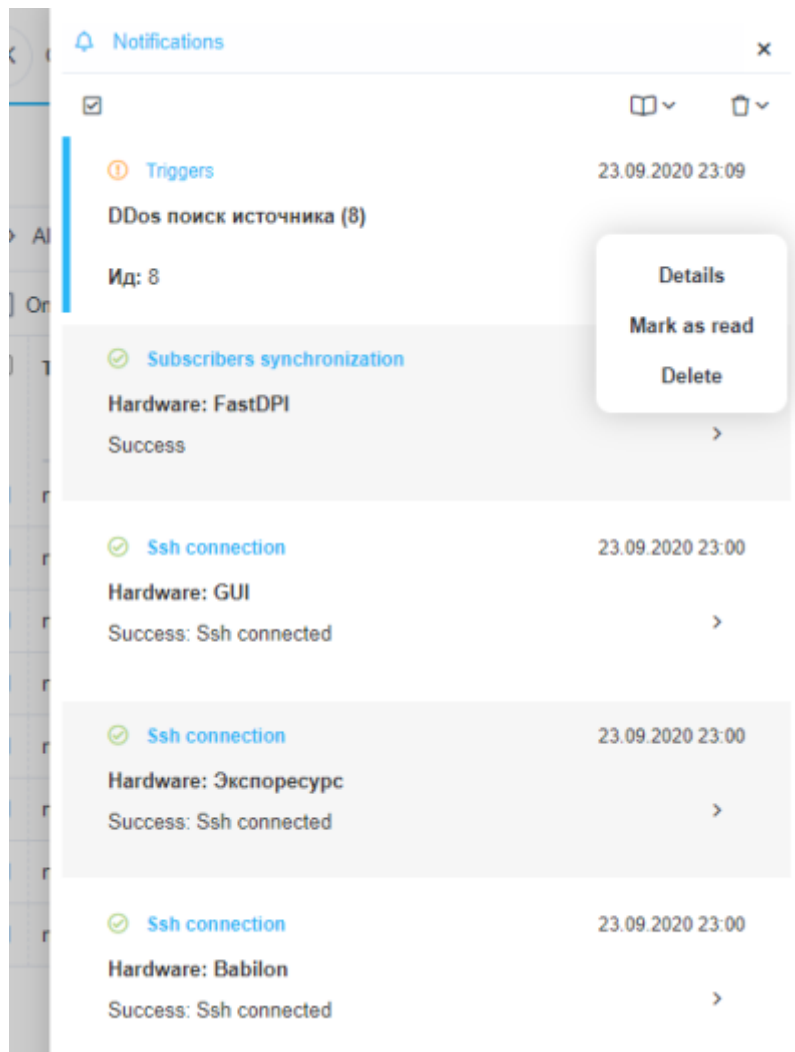
Вкл.

В I U Font Size... Font Family... Font Format

- Click "</>" to auto-fill the form
- Select notification type — “Warning”
- A notification will be created in the SSG system

Alerts					Alerts actions			
Only selected triggers					Only selected notifications			
Trigger name	Type	Date	Note		Type	Date	State	
Ddos	Alerting	14.08.2020 13:58	avg(flow_vol_to_s		notification	14.08.2020 13:59:03	Complete	
DDos поиск исто	Alerting	14.08.2020 13:58	avg(avg_ses_lifeti		notification	14.08.2020 13:58:23	Complete	
Ddos	Alerting	14.08.2020 13:56	avg(flow_vol_to_s		notification	14.08.2020 13:56:43	Complete	
DDos поиск исто	Alerting	14.08.2020 13:55	avg(avg_ses_lifeti		notification	14.08.2020 13:56:05	Complete	
Ddos	Alerting	14.08.2020 13:54	avg(flow_vol_to_s		notification	14.08.2020 13:54:23	Complete	
Ddos	Alerting	14.08.2020 13:52	avg(flow_vol_to_s		notification	14.08.2020 13:52:22	Complete	
DDos поиск исто	Ok	14.08.2020 13:51	avg(avg_ses_lifeti		notification	14.08.2020 13:50:25	Complete	
Ddos	Alerting	14.08.2020 13:50	avg(flow_vol_to_s					

The report link can be obtained from the notifications menu.



Select the notification Click **Details**

 Notifications 

 Triggers

Status	Read
Notification date	23.09.2020 23:09
Notify type	 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

Follow the report link — it will open in a new browser window.

HTTP action

Действия

E-mail x Нотификация x Http x

Метод: POST Урл: Вкл.

Заголовки		Тело
+		
Имя	Значение	<pre><?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></pre>
Content-Type	application/xml	

json Шаблон по умолчанию
xml Шаблон по умолчанию

Click "</>" to auto-fill the form, select the method suitable for your ticket system, and enter the URL address.

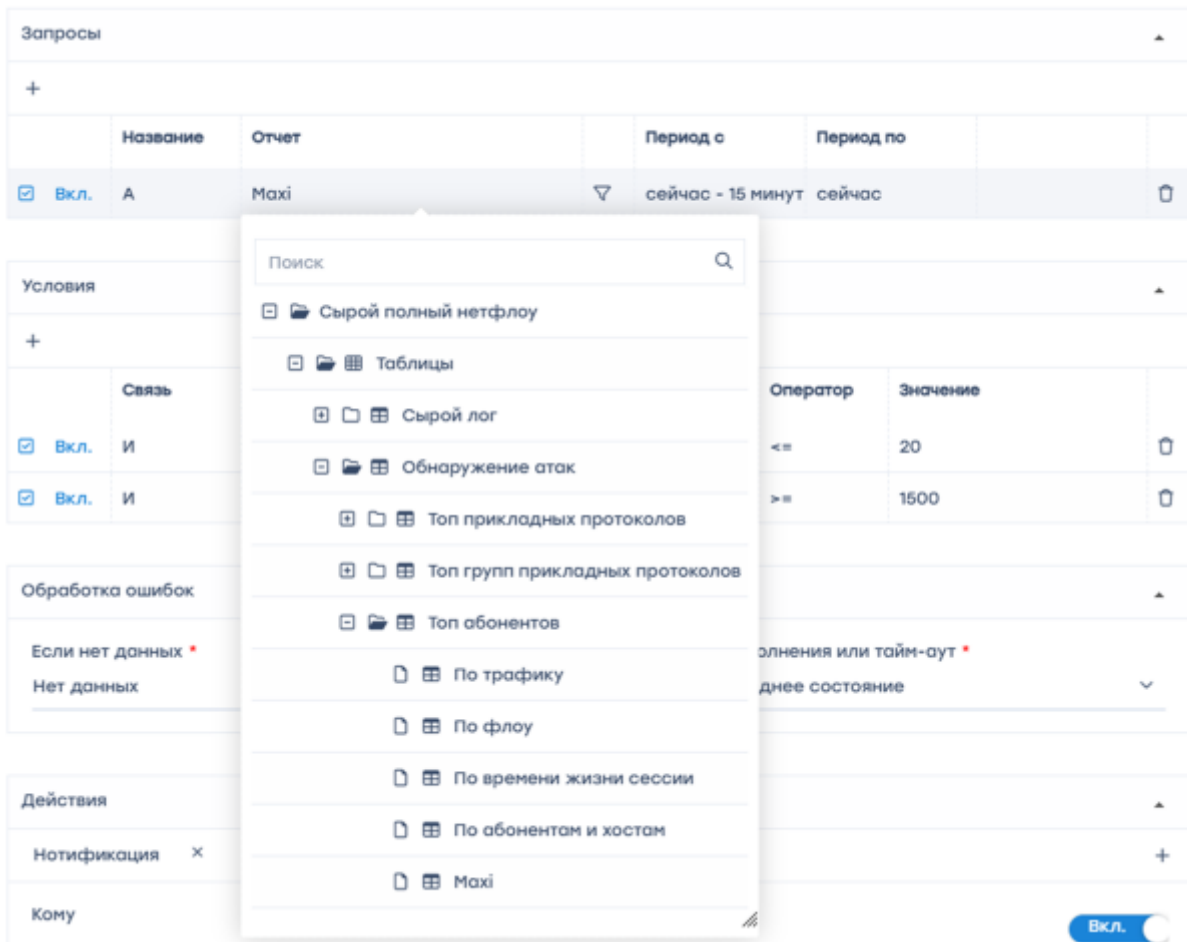


Keep in mind — values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

Example: configuring a trigger to detect the target of a Flood-type DDoS attack

This configuration differs from the previous example in steps 2 and 3 (Queries and Conditions).

Queries



In the report field, select Raw full netflow → Tables → Attacks detection → Top subscribers → Maxi

Conditions

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒ Вкл.	И	A	avg		Флоу к абоне	>=	10000

Series — “Flow volume to subscribers, Pct/s” >= 10000



Values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

BotNet analysis

This configuration differs from the previous example in steps 2 and 3 (Queries and Conditions).

Queries

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Maxi	▼	сейчас - 15 минут	сейчас	🗑
☒ Вкл.	B	Полный сырой лог	▼	сейчас - 15 минут	сейчас	🗑

- Select Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi for “A”
- Raw full network → Tables → Raw log → Full raw log for “B”

Conditions

Условия							
+							
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение
☒ Вкл.	ИЛИ	B	avg		Порт получат	=	6667
☒ Вкл.	ИЛИ	B	avg		Порт источни	=	6667
☒ Вкл.	ИЛИ	B	avg		Порт получат	=	1080
☒ Вкл.	ИЛИ	B	avg		Порт источни	=	1080
☒ Вкл.	И	A	avg		Флоу	>=	2000

Since BotNet often uses ports 6667 and 1080 — add each destination/source port by selecting query “B” with “OR” condition, and Flow Pcts/s >= 2000.



In this configuration, the trigger will fire if on any of the ports (6667/1080) the packet rate exceeds 2000 per second.



Values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.

Detecting subscriber visits to competitor resources

General trigger information

Общее

Название триггера *

Интерес к конкурентам

Важность

Информация

Триггер

Выключен

Дни недели *

Пн, Вт, Ср, Чт, Пт, Сб, Вс

Частота проверки *

1 час

Количество срабатываний

1

Дата начала

Дата окончания

Время начала

Время окончания

Trigger name: “Interest in competitors”, days of the week – all, check frequency – 1 hour, trigger activation frequency – once, start and end times not set.



Every day, the system will perform a check every hour based on the conditions described below.

Queries

Запросы						
+						
	Название	Отчет		Период с	Период по	
☒ Вкл.	A	Сырой кликстрим	☐	сейчас - 1 час	сейчас	☐
☒ Вкл.	B	Maxi	☐	сейчас - 1 час	сейчас	☐

- Add “+” field
- Name A — select table: Raw clickstream → Tables → Raw clickstream
- Name B — select table: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Select period from “now - 1 hour” to “now”
- This setup analyzes traffic hourly based on the selected tables.

Conditions

Условия								
+								
	Связь	Название	Функция	Комбинатор	Серия	Оператор	Значение	
☒ Вкл.	ИЛИ	A	avg		Хост	=	*megafon.ru	
☒ Вкл.	И	B	avg		Объем флюу	>=	800	
☒ Вкл.	ИЛИ	A	avg		Хост	=	*mts.ru	

- Add 3 “+” fields
- First field — select table “A”; Link - “OR”; Function - “avg”; Series Host = *megafon.ru (or your competitor)
- Second field — select table “B”; Link - “AND”; Function - “avg”; Series Flow volume from subscriber, Pct/s >= 800



The trigger will fire if at least 800 packets (indicating a meaningful visit) from a subscriber to a competitor’s website are detected.

Error handling

No data & error handling	
If no data *	If execution error or timeout *
No data	Keep last state

- “If no errors” — no data
- “If there is an error or timeout” — save last state



In this configuration, no data will be saved if there are no errors, but if errors occur, information about suspicious sessions will be saved as a table.

Actions

E-mail action

Actions

Notification x E-mail x

Send to On

Your@email.com

Subject

Trigger fired: {trigger.name}

Message

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

- Click to auto-fill the form
- Enter recipient email address in “To” field



When triggered, an email containing notification details — ID, trigger name, status, and report link (saved state) — will be sent to the specified address.

Notification

Actions

Notification x E-mail x

Notification title On

{trigger.name}

Notification subtitle Notification type

{trigger.id} Warning

Message

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

- Click "</>" to auto-fill the form
- Select notification type — “Warning”
- A notification will be created in the SSG system

Alerts					Alerts actions			
☐ Only selected triggers					☐ Only selected notifications			
Trigger name	Type	Date	Note		Type	Date	State	
☐ Ddos	Alerting	14.08.2020 13:58:	avg(flow_vol_to_s		☐ notification	14.08.2020 13:59:03	Complete	
☐ DDos поиск исто	Alerting	14.08.2020 13:58:	avg(avg_ses_lifeti		☐ notification	14.08.2020 13:58:23	Complete	
☐ Ddos	Alerting	14.08.2020 13:56:	avg(flow_vol_to_s		☐ notification	14.08.2020 13:56:43	Complete	
☐ DDos поиск исто	Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti		☐ notification	14.08.2020 13:56:05	Complete	
☐ Ddos	Alerting	14.08.2020 13:54:	avg(flow_vol_to_s		☐ notification	14.08.2020 13:54:23	Complete	
☐ Ddos	Alerting	14.08.2020 13:52:	avg(flow_vol_to_s		☐ notification	14.08.2020 13:52:22	Complete	
☐ DDos поиск исто	OK	14.08.2020 13:51:	avg(avg_ses_lifeti		☐ notification	14.08.2020 13:50:25	Complete	
☐ Ddos	Alerting	14.08.2020 13:50:	avg(flow_vol_to_s					

The report link can be obtained from the notifications menu.

Notifications

☒

Triggers

DDos поиск источника (8)

Ид: 8

☒

Subscribers synchronization

Hardware: FastDPI

Success

☒

Ssh connection

Hardware: GUI

Success: Ssh connected

☒

Ssh connection

Hardware: Экспересурс

Success: Ssh connected

☒

Ssh connection

Hardware: Babilon

Success: Ssh connected

Details

Mark as read

Delete

Select the notification Click **Details**

Notifications

×

← Triggers

Status	Read
Notification date	23.09.2020 23:09
Notify type	ⓘ 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

Follow the report link — it will open in a new browser window.

HTTP action

Actions

Notification × E-mail × Http × +

Method POST Url https://your_redmine_host/issues.xml?key=your_redmine_api_key On

Headers < Body >

+ 📄 </>

Name	Value	
Content-Type	application/xml	📄

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Сработал триггер: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Ид: {trigger.id}
  Триггер: {trigger.name}
  Статус: {trigger.state}
  Важность: {trigger.severity}

  Запросы:
  {trigger.queries}
</issue>
```

REDMINE JSON
REDMINE XML

- Click "</>" to auto-fill the form
- Select the method suitable for your ticket system and enter the URL address



Keep in mind — values such as session count and packet rate are averaged. Fine-tuning should be performed based on your network specifics.