

Содержание

Поиск DDoS атак 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
<i>Анализ BotNet</i>	10
<i>Фиксация перехода абонента на ресурс конкурента</i>	11

Поиск DDoS атак 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:

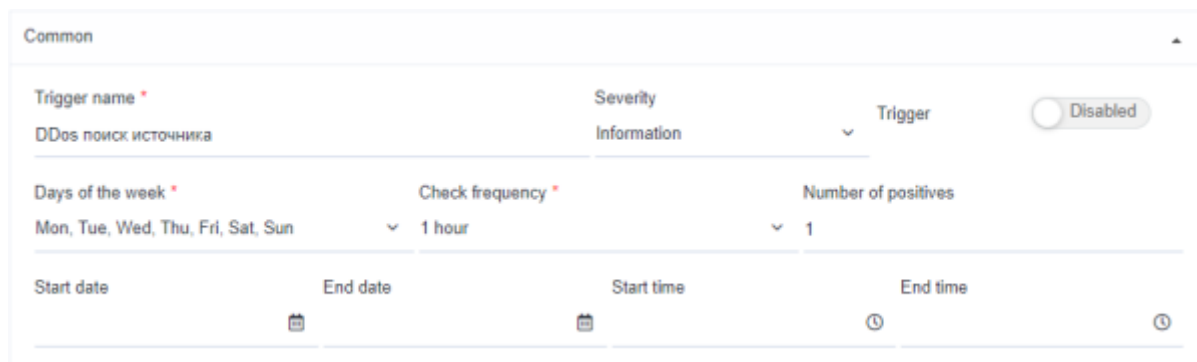
- Сбор и анализ статистики по протоколам и направлениям
- Уведомление абонентов

Необходимые дополнительные модули:

- DPIUI2 (GUI - Графический интерфейс управления)
- QoE Stor (Модуль сбора статистики)

Пример настройки триггера на поиск источника DDOS-атаки типа Flood

Общая информация триггера



Common			
Trigger name *	Severity	Trigger	
DDos поиск источника	Information	Trigger	Disabled
Days of the week *	Check frequency *	Number of positives	
Mon, Tue, Wed, Thu, Fri, Sat, Sun	1 hour	1	
Start date	End date	Start time	End time

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

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Maxi		now - 15 minute	now	

- Добавить поле
- Название A
- Выбрать таблицу для сканирования: Raw full netflow → Tables → Attacks detection → Top hosts IPs → Maxi
- Выбрать период с: «now - 15minute», период по : «now»



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

Условия

Conditions							
+							
	Bind	Query name	Function	Combinator	Series	Operator	Value
☒ On	AND	A	avg		Session lifetime	<=	20
☒ On	AND	A	avg		Sessions	>=	1500

- Добавить "+" 2 поля
- Связка - И
- Функция - avg
- Серия в 1 поле - время жизни сессии <= 20(мс)
- Серия во 2 поле - количество сессий >= 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

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

- В поле "Если нет ошибок" — нет данных
- В поле "Если есть ошибка или таймаут" — 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

Е-mail действие

Actions

Notification

E-mail

Send to

Your@email.com

Subject

Trigger fired: {trigger.name}

Message

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

- Для автоматического заполнения — кликнуть по иконке "</>" (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты
- При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние)

Нотификация

Actions

Notification

E-mail

Notification title

{trigger.name}

Notification subtitle

{trigger.id}

Notification type

Warning

Message

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

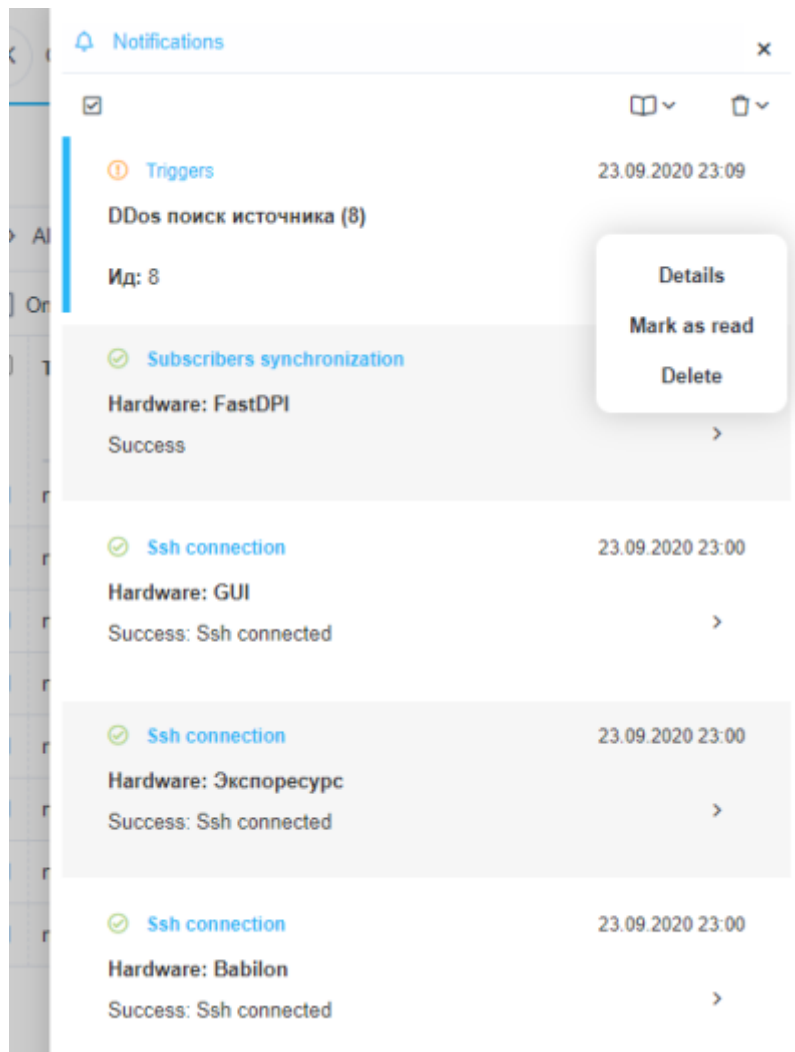
Важность: {trigger.severity}

Запросы: {trigger.queries}

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

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				

Получить ссылку на отчет можно через меню нотификаций



Выбрать нотификацию Выбрать — "Детали"

 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

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

HTTP действие

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

Body:

```
<?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

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

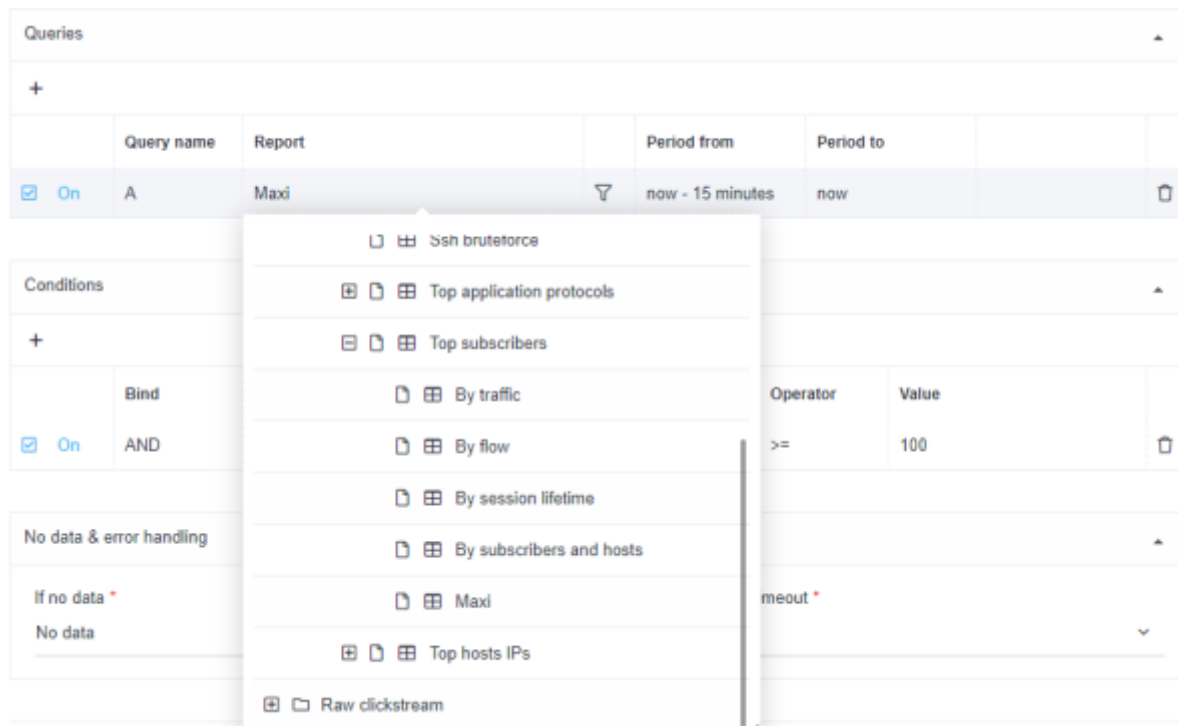


Стоит понимать — значение количества устанавливаемых сессий, количества входящих пакетов и т.д. приведены усредненно. Более точная настройка должна производиться с учетом особенностей вашей сети.

Пример настройки триггера на поиск цели DDOS-атаки типа Flood

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

Запросы



в поле отчет выбрать Raw full netflow → Tables → Attacks detection → Top subscribers → Maxi

Условия

Conditions							
+							
	Bind	Query name	Function	Combinator	Series	Operator	Value
☒ On	AND	A	avg		Flow volume to	>=	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

Queries						
+						
	Query name	Report		Period from	Period to	
☒ On	A	Maxi	🔍	now - 15 minute	now	🗑
☒ On	B	Full raw log	🔍	now - 15 minute	now	🗑

- Выбрать Raw full netflow → Tables → Attacks detection → Top application protocols → Maxi для значения "A"
- Raw full network → Tables → Raw log → Full raw log для значения "B"

Условия

Conditions							
+							
	Bind	Query name	Function	Combinator	Series	Operator	Value
☒ On	OR	B	avg		Destination port	=	6667
☒ On	OR	B	avg		Source port	=	6667
☒ On	OR	B	avg		Destination port	=	1080
☒ On	OR	B	avg		Source port	=	1080
☒ On	AND	A	avg		Flow, Pkts/s	>=	2000

Т.к. BotNet чаще всего использует порты 6667 и 1080 — добавить каждый порт назначения/источника выбрав запрос "B" со значением "ИЛИ", и Flow Pkts/s 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

Conditions								
+								
	Bind	Query name	Function	Combinator	Serie	Operator	Value	
☒ On	OR	A	avg		Host	=	*megafon.ru	
☒ On	AND	B	avg		Flow volume fro	>=	800	
☒ On	OR	A	avg		Host	=	*mts.ru	

- Добавить "+" поле 3 поля
- Первое поле — выбрать таблицу "А"; Связка - "Или"; Функция - "avg";Серия Host = *megafon.ru(или ваш любимый конкурент)
- Второе поле — выбрать таблицу "Б"; связка "И"; Функция - "avg";Серия Flow volume from subscriber, Pct/s >= 800



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

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

- В поле "Если нет ошибок" — нет данных
- В поле "Если есть ошибка или таймаут" — 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

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}

- Для автоматического заполнения — кликнуть (автоматическое заполнение формы)
- В поле "Кому" — указать адрес электронной почты



При этой настройке, при срабатывании триггера на указанный адрес электронной почты будет отправлена вся информация о нотификации: ИД, название триггера, статус, ссылка на отчет (сохраненное состояние).

Нотификация

Actions

Notification x E-mail x

Notification title On

{trigger.name}

Notification subtitle

{trigger.id}

Notification type

Warning

Message

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

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

Alerts				
☐ Only selected triggers				
Trigger name	Type	Date	Note	
☐ Ddos	Alerting	14.08.2020 13:58:	avg(flow_vol_to_s	☐
☐ DDos power victo	Alerting	14.08.2020 13:58:	avg(avg_ses_lifeti	☐
☐ Ddos	Alerting	14.08.2020 13:56:	avg(flow_vol_to_s	☐
☐ DDos power victo	Alerting	14.08.2020 13:55:	avg(avg_ses_lifeti	☐
☐ Ddos	Alerting	14.08.2020 13:54:	avg(flow_vol_to_s	☐
☐ Ddos	Alerting	14.08.2020 13:52:	avg(flow_vol_to_s	☐
☐ DDos power victo	Ok	14.08.2020 13:51:	avg(avg_ses_lifeti	☐
☐ Ddos	Alerting	14.08.2020 13:50:	avg(flow_vol_to_s	☐

Получить ссылку на отчет можно через меню уведомлений

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

Hardware: GUI

Success: Ssh connected >

Ssh connection

Hardware: Экспоресупс

Success: Ssh connected >

Ssh connection

Hardware: Babilon

Success: Ssh connected >

Выбрать нотификацию Выбрать — "Детали"

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

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

HTTP действие

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}
```

REDMINE JSON
REDMINE XML

- 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.