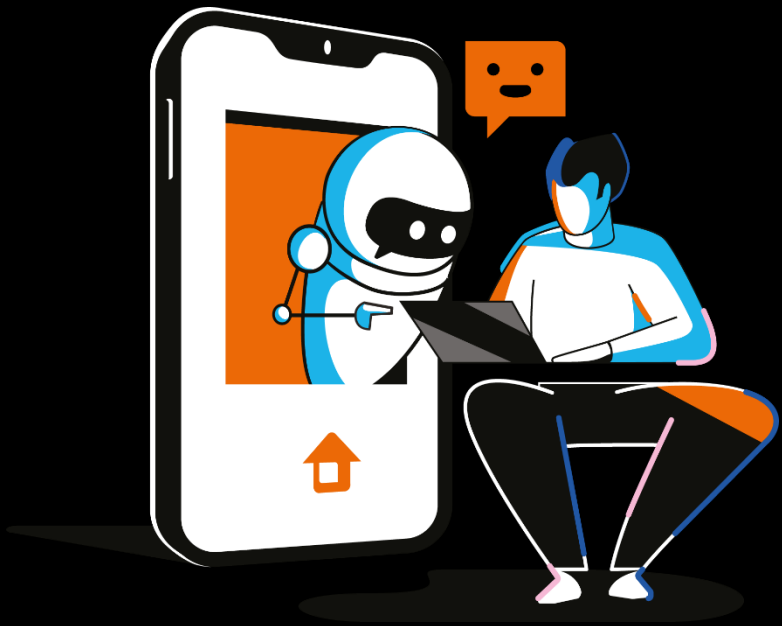
Internet Umbrella

Руководство пользователя к WEB-интерфейсу on-line мониторинга



orange™ Business

Введение

- В рамках Услуги Internet Umbrella (далее – Услуги) Клиенту предоставляется доступ к WEB-интерфейсу, который представляет собой интерфейс с личным кабинетом Клиента для on-line мониторинга.

- Он предназначен для предоставления Представителям Клиента информации о работоспособности Услуги и статистики происходящих событий (Легитимный и Нелегитимный Трафик, типы атак, параметры атак, объем отфильтрованного Трафика, и т.п.).

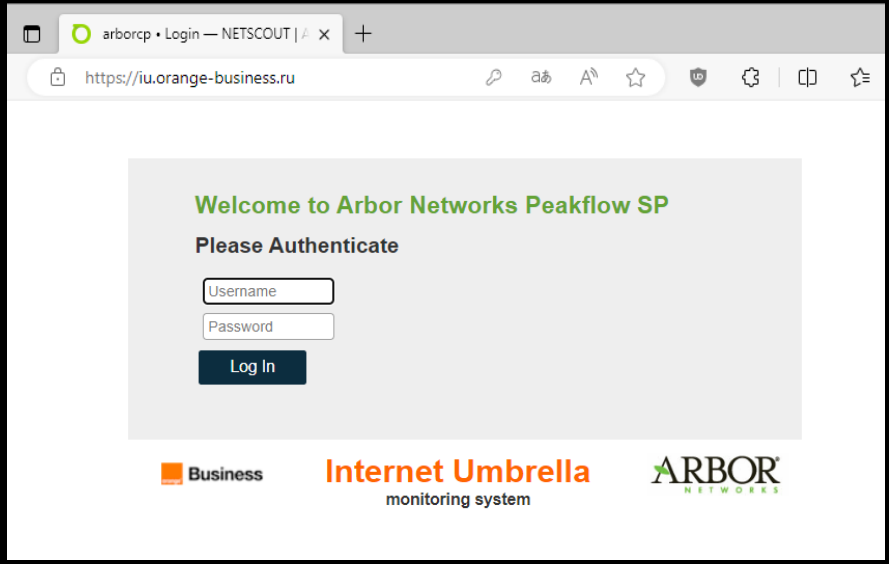
WEB-интерфейс

WEB-интерфейс ARBOR SP

Доступ к WEB-интерфейсу ARBOR SP осуществляется, используя прямую ссылку:

https://iu.orange-business.ru/

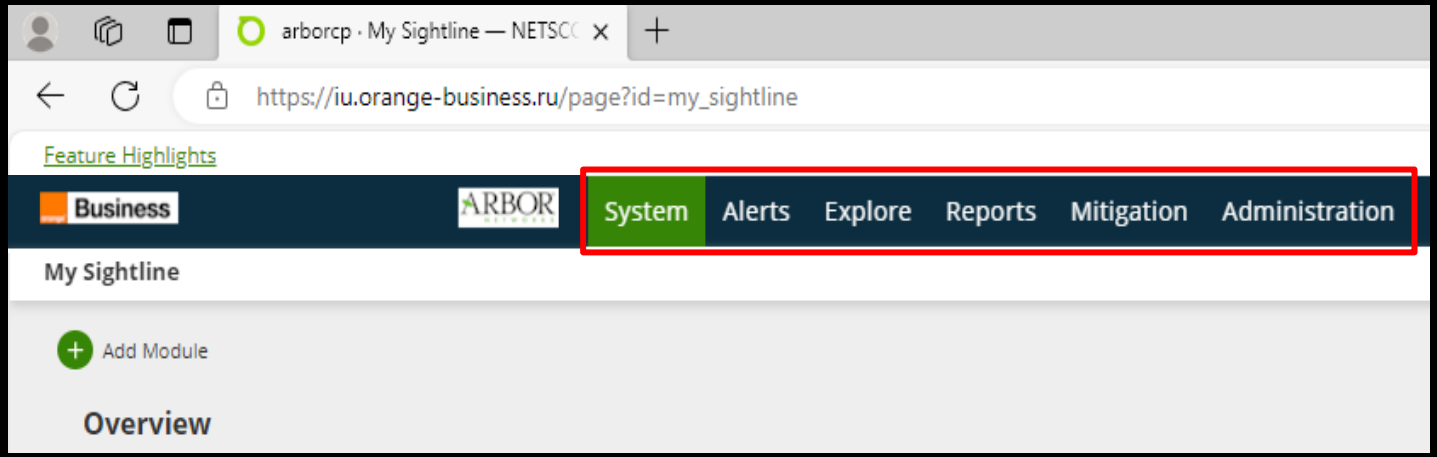
- **Для доступа к WEB-интерфейсу требуются login & password, которые высылаются индивидуально каждому Представителю Клиента на этапе инсталляции Услуги**



Важно

- **Обратите внимание, что при вводе реквизитов учитывается регистр!**
- **Для корректной работы рекомендуется использовать WEB-браузеры Firefox (17ESR и выше) или Internet Explorer (9.0 или 10.0).**

WEB-интерфейс ARBOR SP

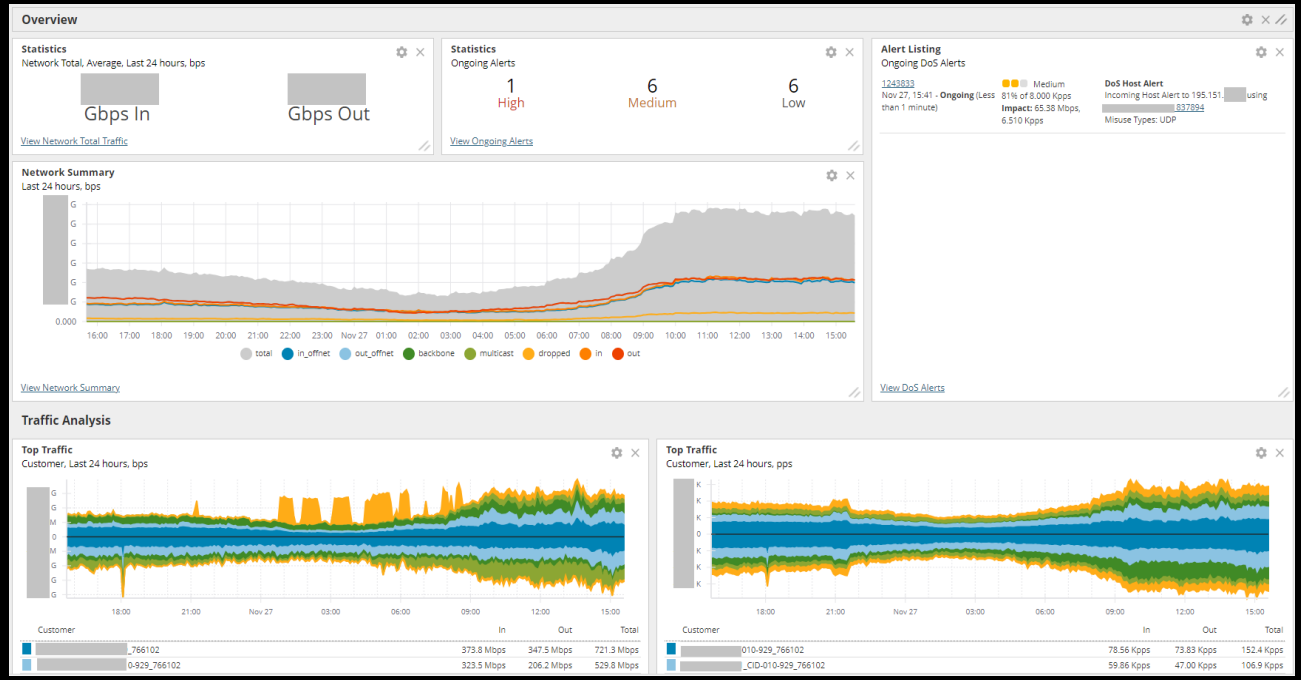


- После успешной авторизации пользователь получает доступ к интерфейсу системы мониторинга Услуги.

- В открывшемся окне браузера, непосредственно под логотипами компаний Orange Business и Arbor Networks, находится панель управления, на которой размещены управляющие кнопки: System, Alerts, Explore, Reports, Mitigation, Administration.

WEB-интерфейс ARBOR SP

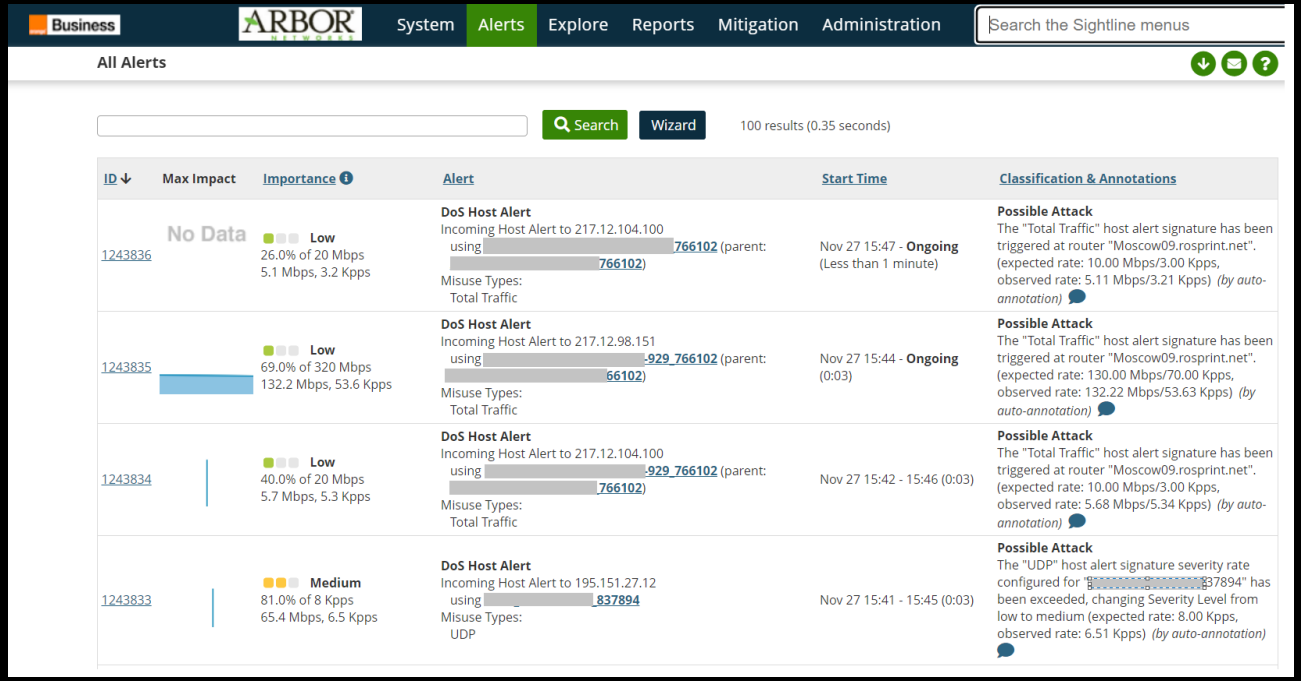
System



- **Первая страница интерфейса, на которую попадает пользователь после авторизации, отображает общий статус о защите объекта и уведомления о текущих угрозах. Данная страница доступна по кнопке System на панели управления.**

WEB-интерфейс ARBOR SP

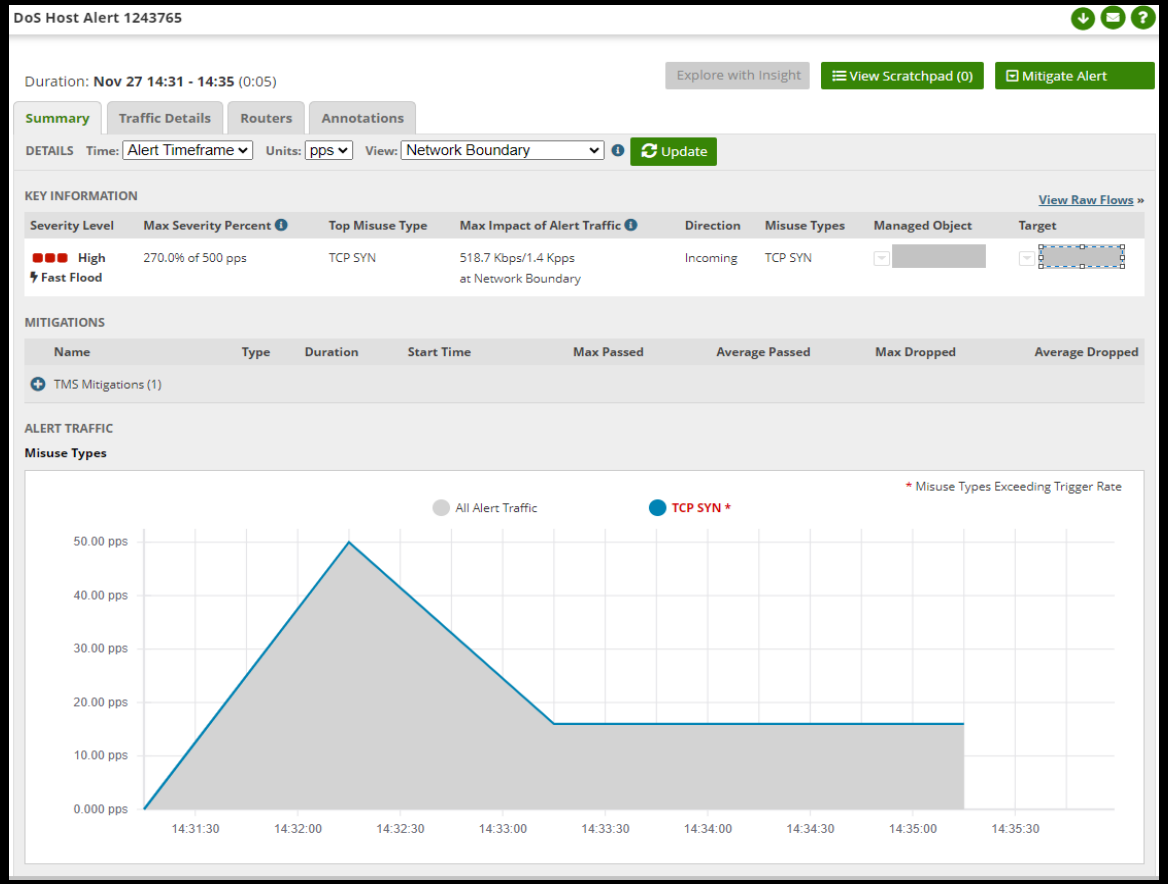
Alerts



- Кнопка Alerts позволяет выбрать две опции «All Alerts» и «Alerts Ongoing».
- Опция «All Alerts» - позволяет просмотреть историю событий списком:

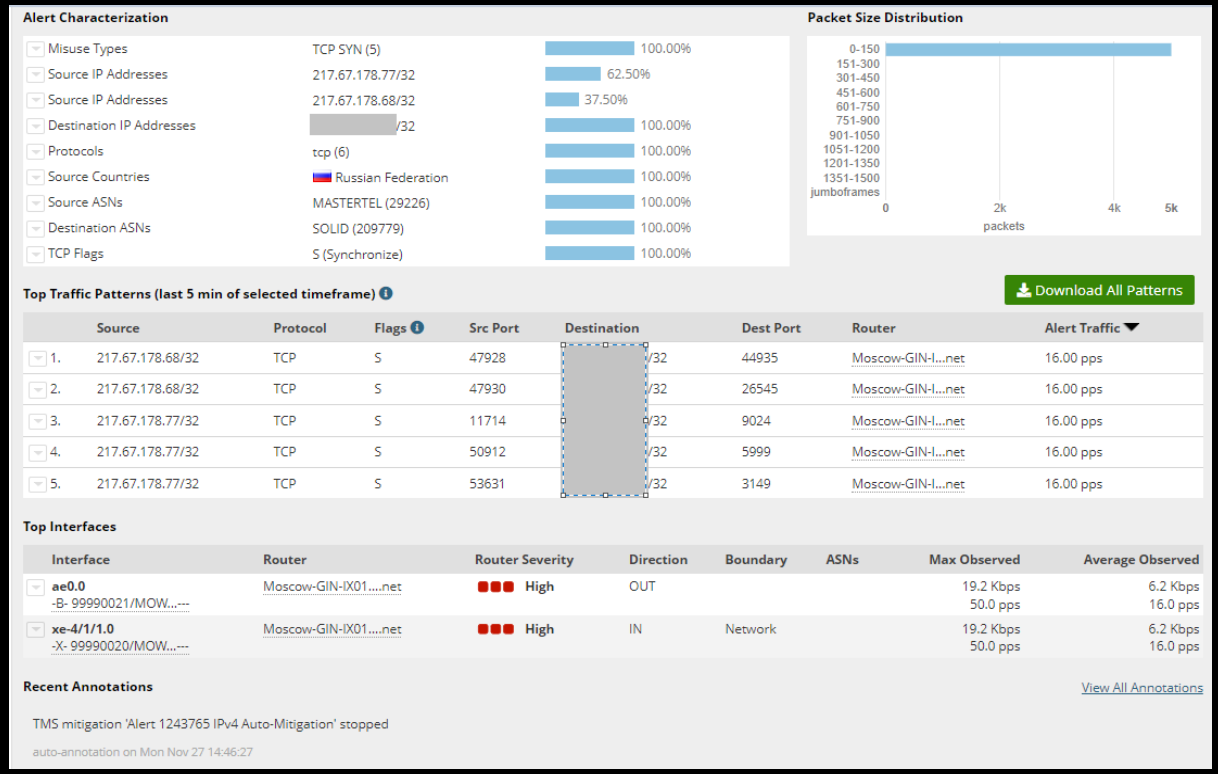
WEB-интерфейс ARBOR SP

- После нажатия «левой кнопкой» мыши на иконку интересующего графика, предоставляется детальная информация об атаке



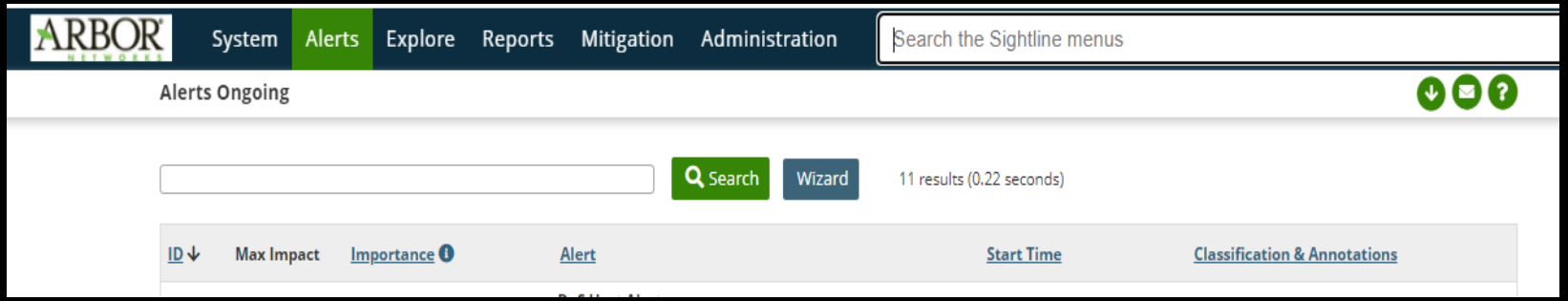
WEB-интерфейс ARBOR SP

- Страницу можно прокрутить вниз для более детальной информации об атаке



WEB-интерфейс ARBOR SP

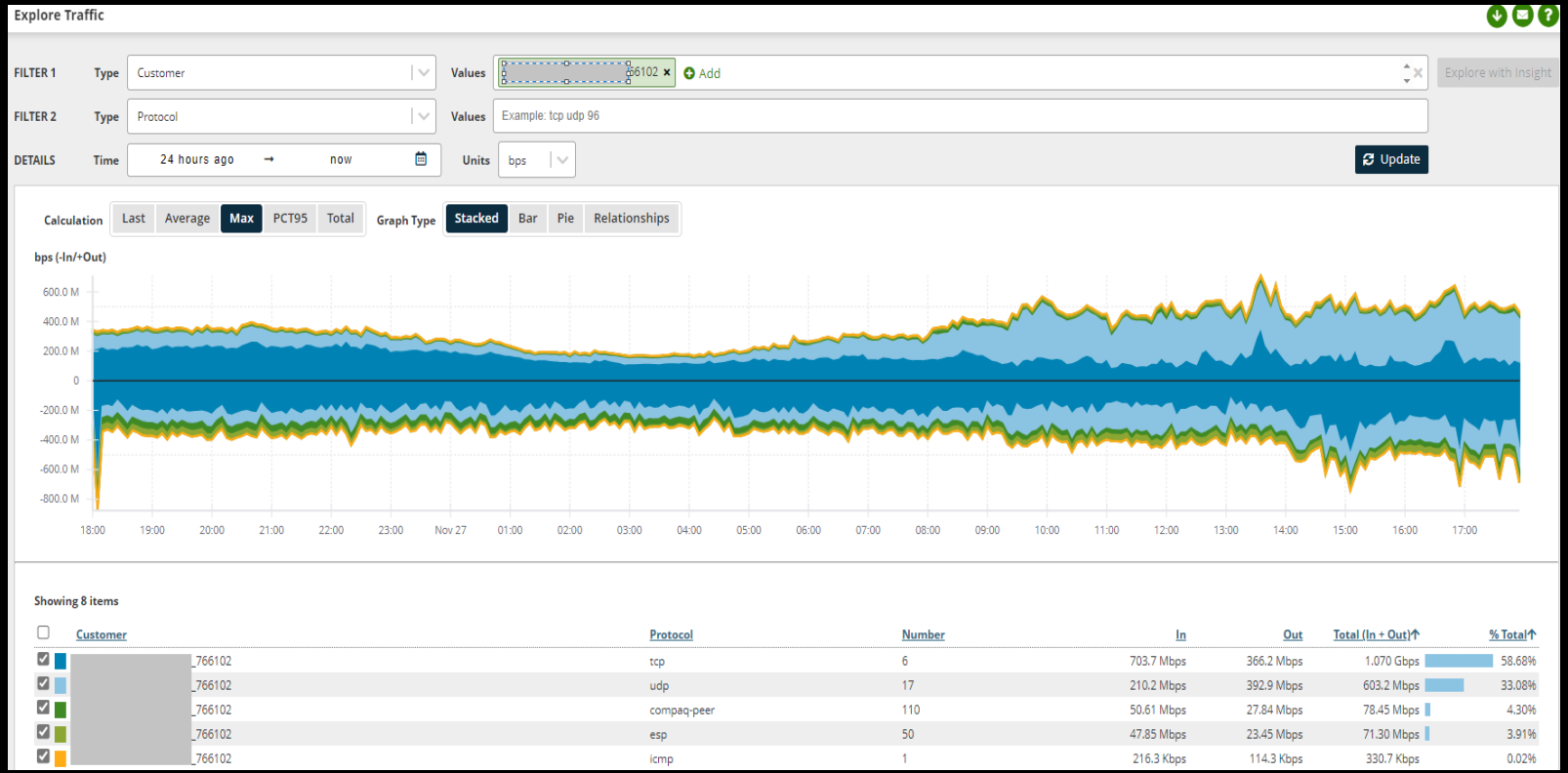
- **«Alerts Ongoing» позволяет осуществить поиск определенного события, есть возможность задать параметры поиска через кнопку Wizard**



- **Wizard позволяет выбрать несколько опций для графического отображения трафика по протоколам, приложениям, IP-адресам и т.п. за выбранный период времени**

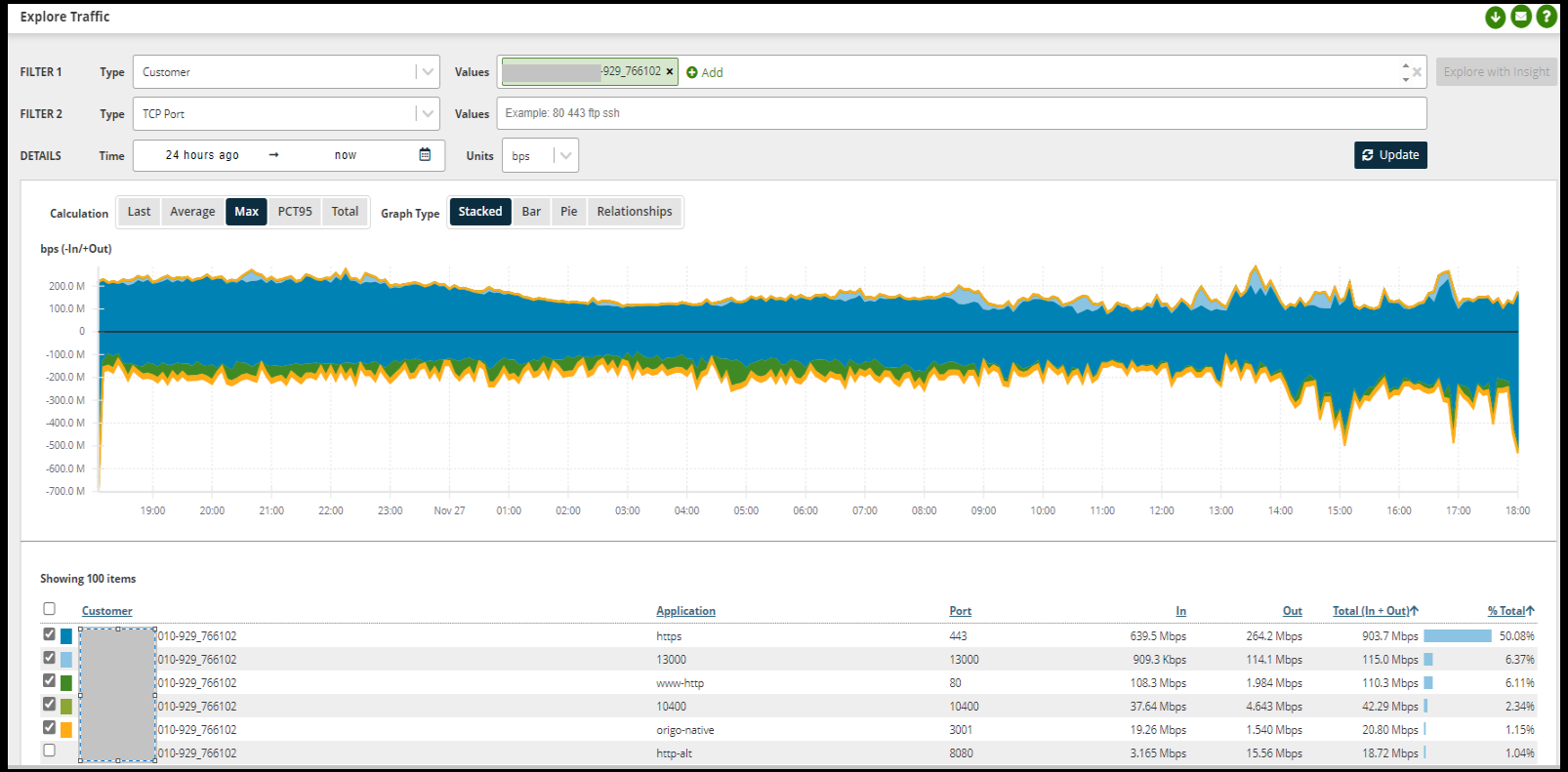
WEB-интерфейс ARBOR SP

Отображение трафика по приложениям



WEB-интерфейс ARBOR SP

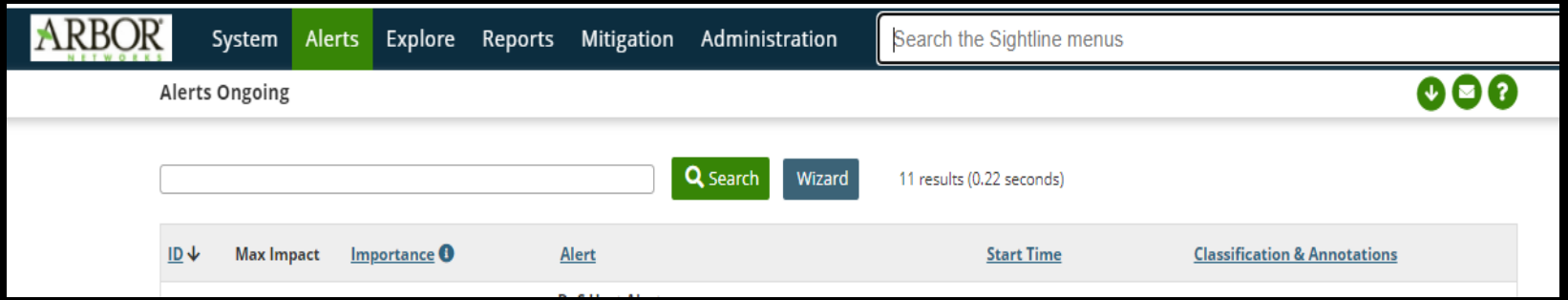
Отображение трафика по портам



Customer	Application	Port	In	Out	Total (In + Out)	% Total
010-929_766102	https	443	639.5 Mbps	264.2 Mbps	903.7 Mbps	50.08%
010-929_766102	13000	13000	909.3 Kbps	114.1 Mbps	115.0 Mbps	6.37%
010-929_766102	www-http	80	108.3 Mbps	1.984 Mbps	110.3 Mbps	6.11%
010-929_766102	10400	10400	37.64 Mbps	4.643 Mbps	42.29 Mbps	2.34%
010-929_766102	origo-native	3001	19.26 Mbps	1.540 Mbps	20.80 Mbps	1.15%
010-929_766102	http-alt	8080	3.165 Mbps	15.56 Mbps	18.72 Mbps	1.04%

WEB-интерфейс ARBOR SP

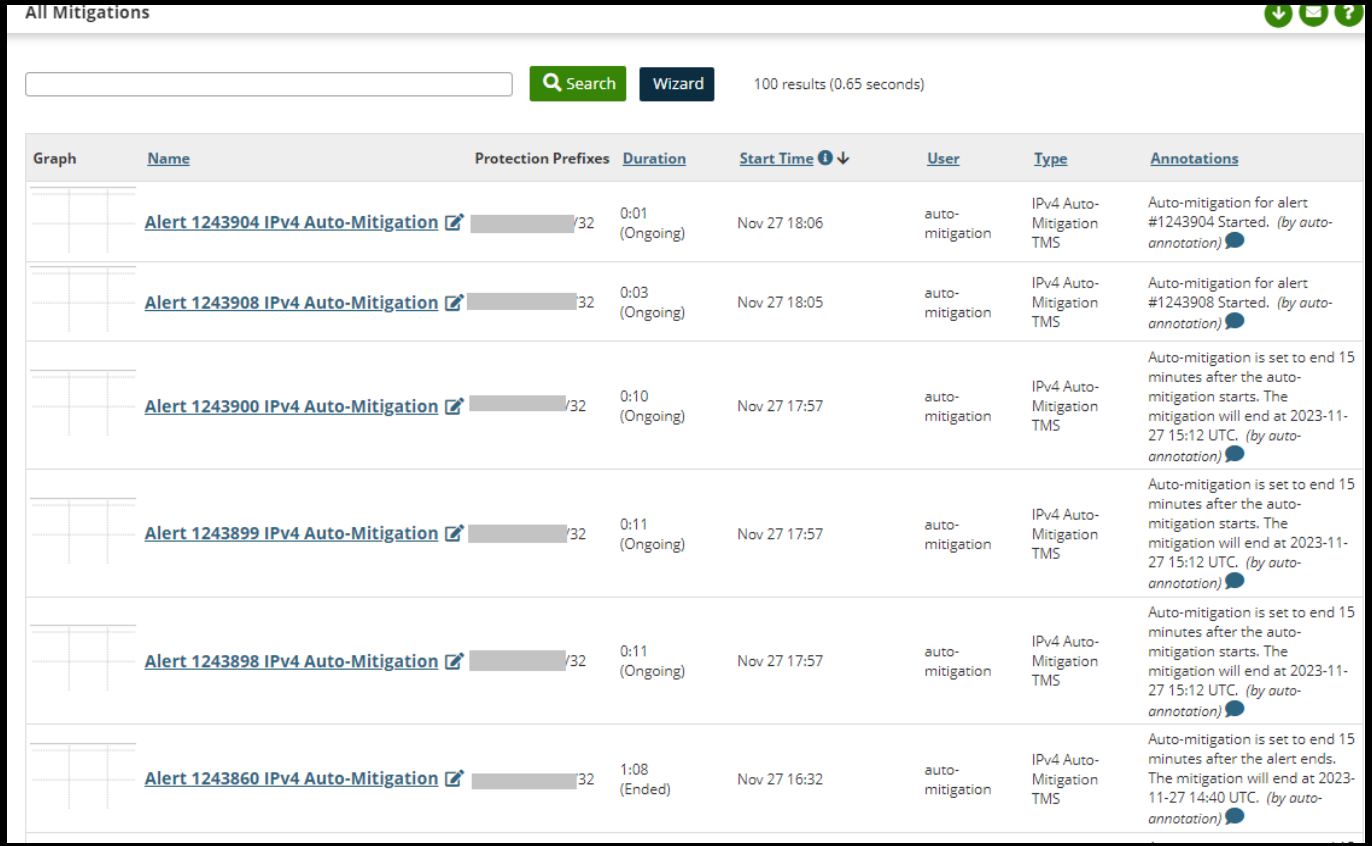
- Кнопка Mitigation позволяет показать список событий в период подавления атак



- С детальной информацией о применяемых методах подавления паразитного трафика можно ознакомиться в WEB-интерфейсе MITIGATOR

WEB-интерфейс ARBOR SP

События Mitigation



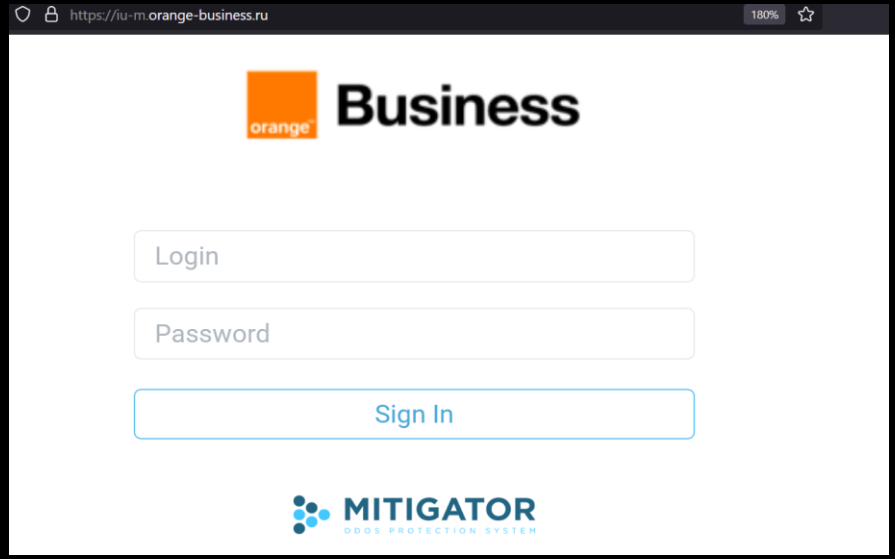
Graph	Name	Protection Prefixes	Duration	Start Time	User	Type	Annotations
	Alert 1243904 IPv4 Auto-Mitigation	/32	0:01 (Ongoing)	Nov 27 18:06	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation for alert #1243904 Started. *(by auto-annotation)*
	Alert 1243908 IPv4 Auto-Mitigation	32	0:03 (Ongoing)	Nov 27 18:05	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation for alert #1243908 Started. *(by auto-annotation)*
	Alert 1243900 IPv4 Auto-Mitigation	/32	0:10 (Ongoing)	Nov 27 17:57	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation is set to end 15 minutes after the auto-mitigation starts. The mitigation will end at 2023-11-27 15:12 UTC. *(by auto-annotation)*
	Alert 1243899 IPv4 Auto-Mitigation	/32	0:11 (Ongoing)	Nov 27 17:57	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation is set to end 15 minutes after the auto-mitigation starts. The mitigation will end at 2023-11-27 15:12 UTC. *(by auto-annotation)*
	Alert 1243898 IPv4 Auto-Mitigation	/32	0:11 (Ongoing)	Nov 27 17:57	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation is set to end 15 minutes after the auto-mitigation starts. The mitigation will end at 2023-11-27 15:12 UTC. *(by auto-annotation)*
	Alert 1243860 IPv4 Auto-Mitigation	32	1:08 (Ended)	Nov 27 16:32	auto-mitigation	IPv4 Auto-Mitigation TMS	Auto-mitigation is set to end 15 minutes after the alert ends. The mitigation will end at 2023-11-27 14:40 UTC. *(by auto-annotation)*

WEB-интерфейс

WEB-интерфейс MITIGATOR

Доступ к WEB-интерфейсу MITIGATOR осуществляется, используя прямые ссылки:

Москва https://iu-m.orange-business.ru/
Новосибирск https://iu-n.orange-business.ru/



- **Для доступа к WEB-интерфейсу требуются login & password, которые высылаются индивидуально каждому Представителю Клиента на этапе инсталляции Услуги**

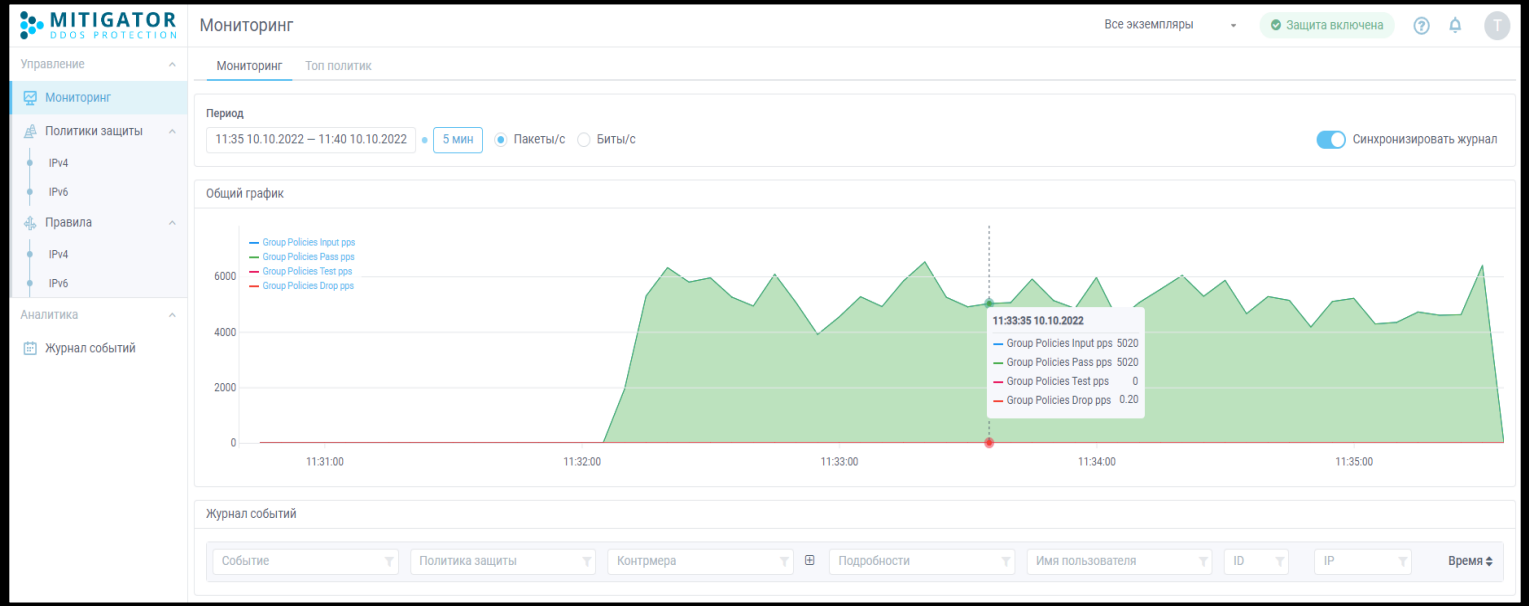
Важно

- **Обратите внимание, что при вводе реквизитов учитывается регистр!**
- **Для корректной работы рекомендуется использовать WEB-браузеры Firefox (17ESR и выше) или Internet Explorer (9.0 или 10.0).**

WEB-интерфейс MITIGATOR

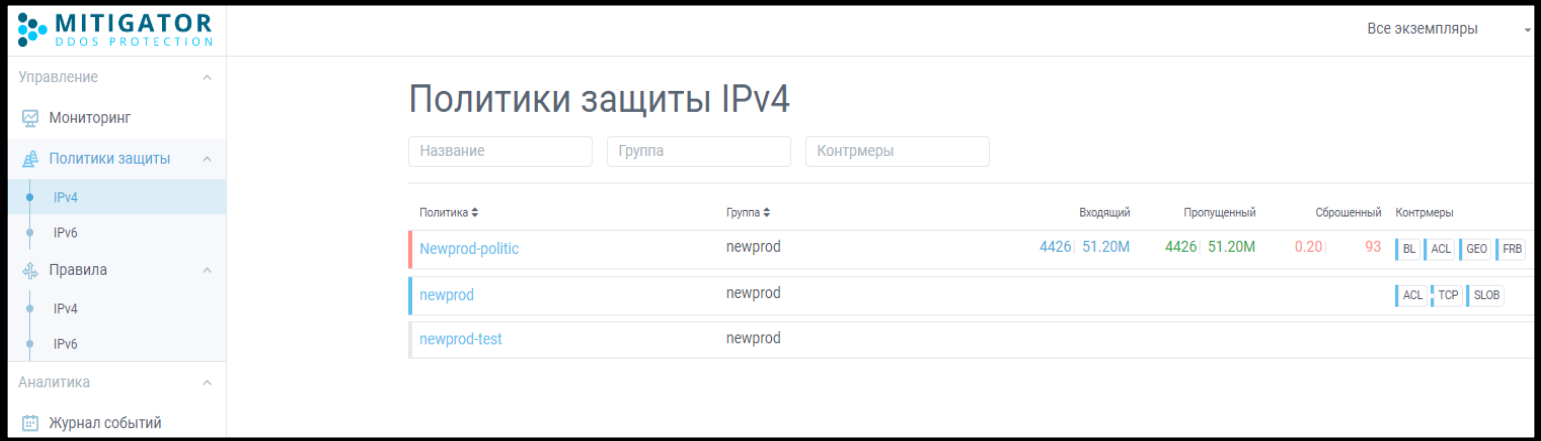
Мониторинг защищаемых объектов

- При входе в систему Вы попадаете на вкладку **Мониторинг (Dahsboard)**, где можно посмотреть сколько трафика (в bps и pps) поступает на защищаемые объекты



WEB-интерфейс MITIGATOR
Политики защиты

- При нажатии на «Политики защиты/IPv4» появляется возможность увидеть используемые политики защиты

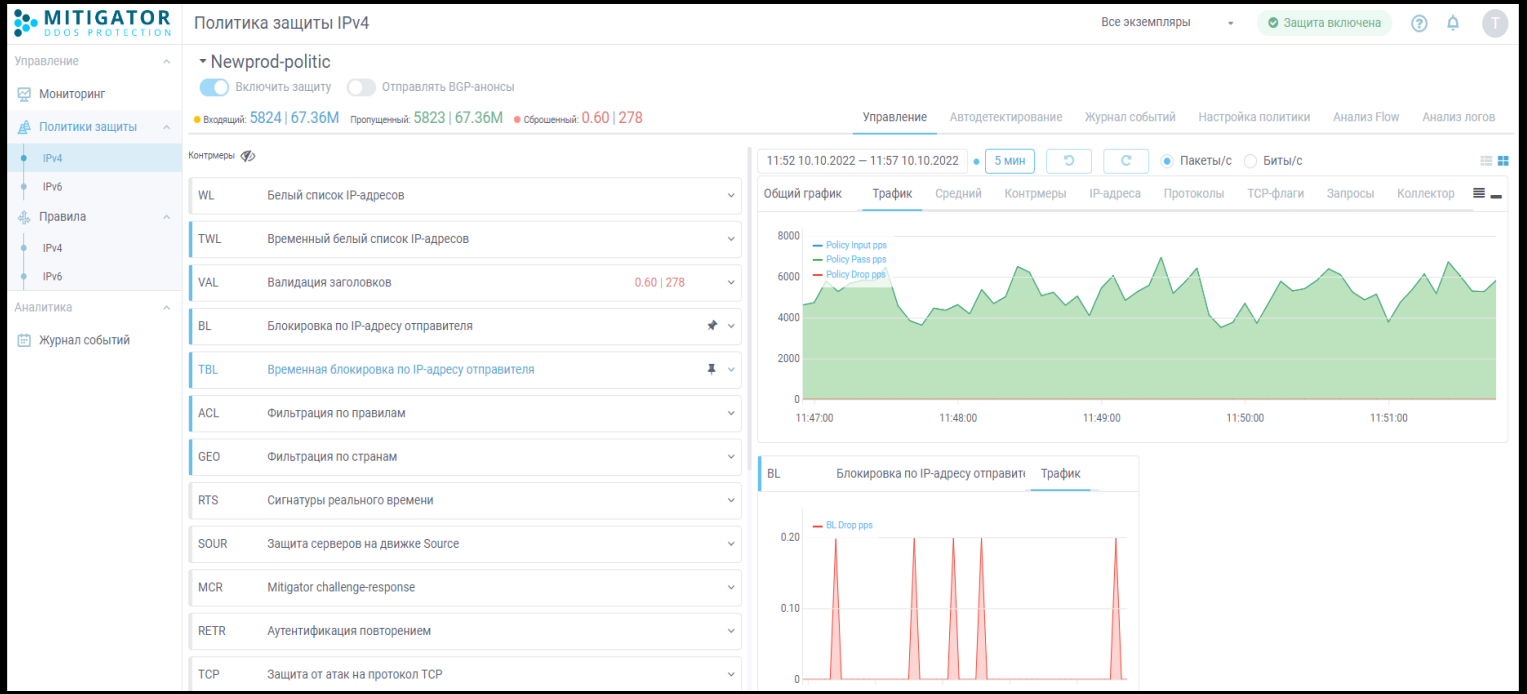


- По изменяющимся значениям (bps и pps) входящего, пропущенного и сброшенного трафика можно увидеть, какие политики в данный момент работают, также показан список контрмер, используемых в отображаемых политиках.

WEB-интерфейс MITIGATOR

Политики защиты

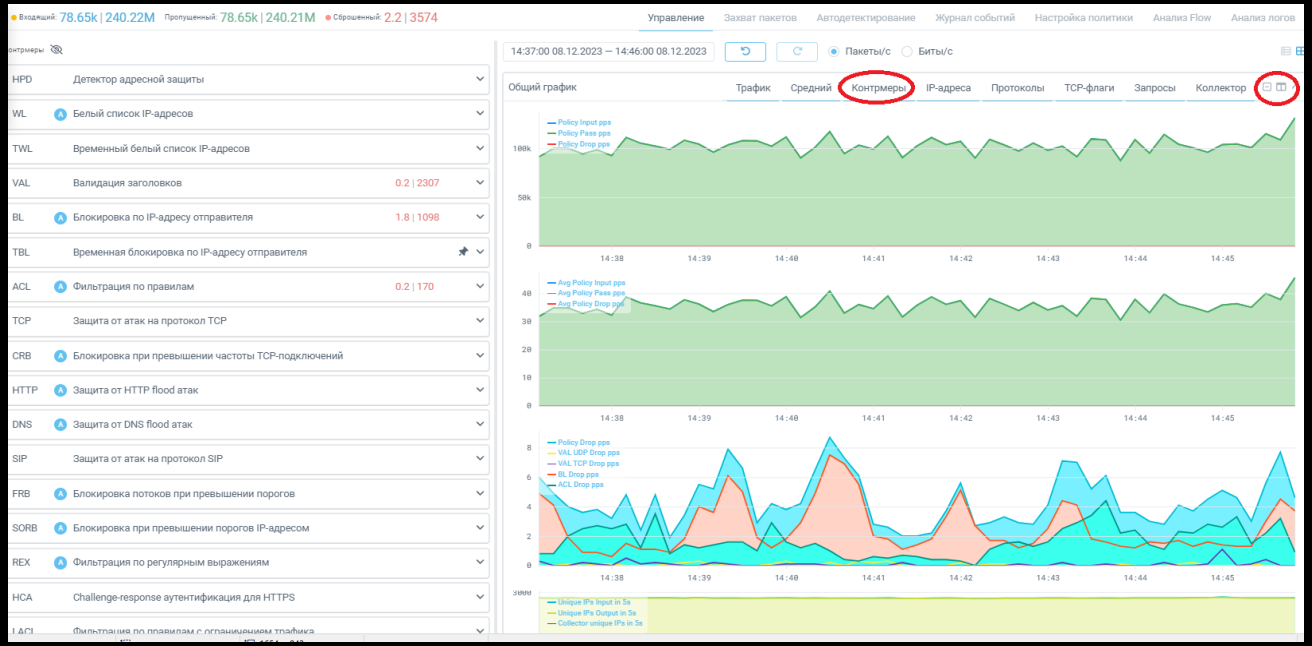
- При нажатии на Политику открывается список используемых контрмер в политике



WEB-интерфейс MITIGATOR

Политики защиты

- Над графиком можно перейти во вкладку **Контрмеры**, чтобы посмотреть детально

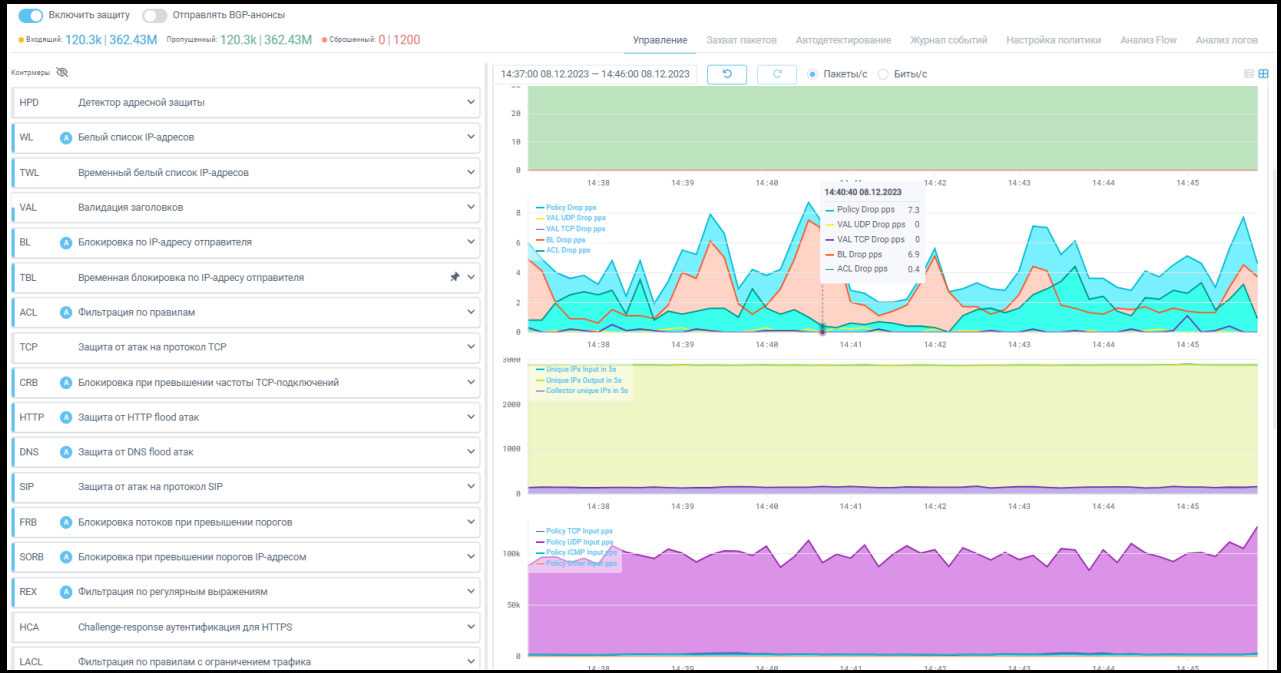


- В правом верхнем ряду (выделено на рисунке) можно нажать на кнопку сортировки, после чего будут **доступны графики сброшенного трафика** по включенным контрмерам

WEB-интерфейс MITIGATOR

Графики сброшенного трафика

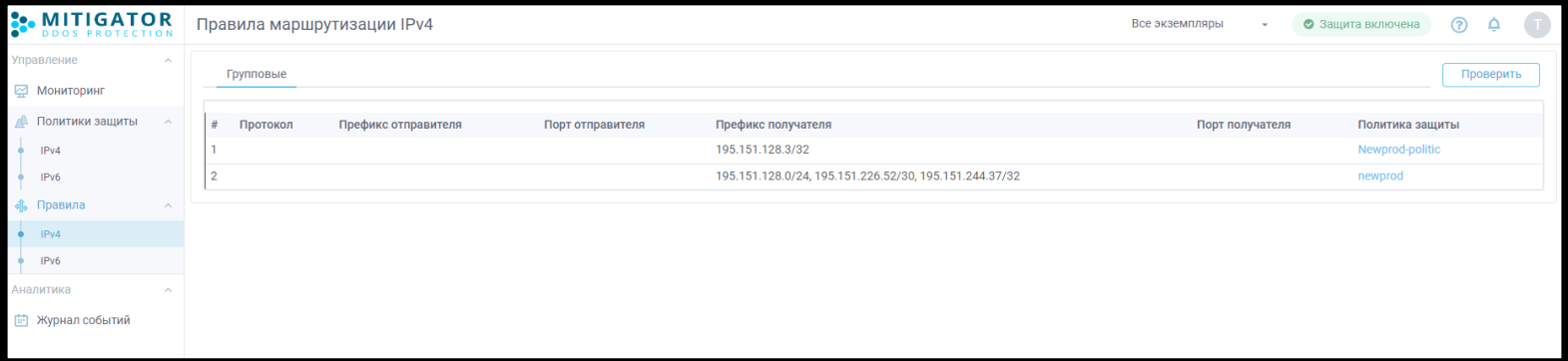
- При наведении курсора на график сброшенного в контрмере трафика появляется табличка с информацией о том, какой трафик сбрасывается, также указываются значения bps и pps трафика



WEB-интерфейс MITIGATOR

Правила маршрутизации для префиксов

- В разделе **Правила маршрутизации IPv4** можно увидеть правила маршрутизации для защищаемых префиксов



- Здесь можно увидеть **порядок применения правил**, которые направляют трафик в **соответствующие политики**. Порядок правил настраивают, начиная от более специфичных к более общим, иначе весь трафик пройдет по общему правилу, не дойдя до специфичного

Thank you!