

Internet Umbrella

Руководство пользователя к WEB-интерфейсу
on-line мониторинга



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



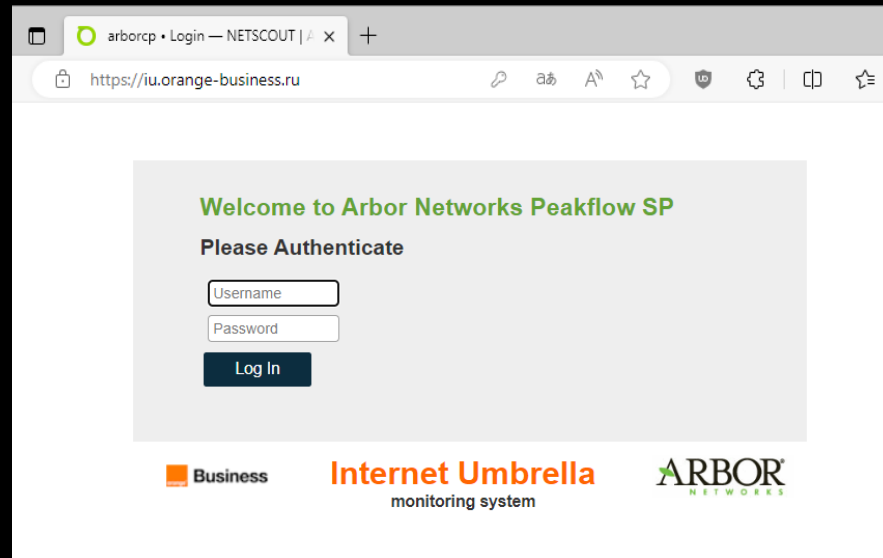
ARBORTM
NETWORKS

WEB-интерфейс ARBOR SP

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

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

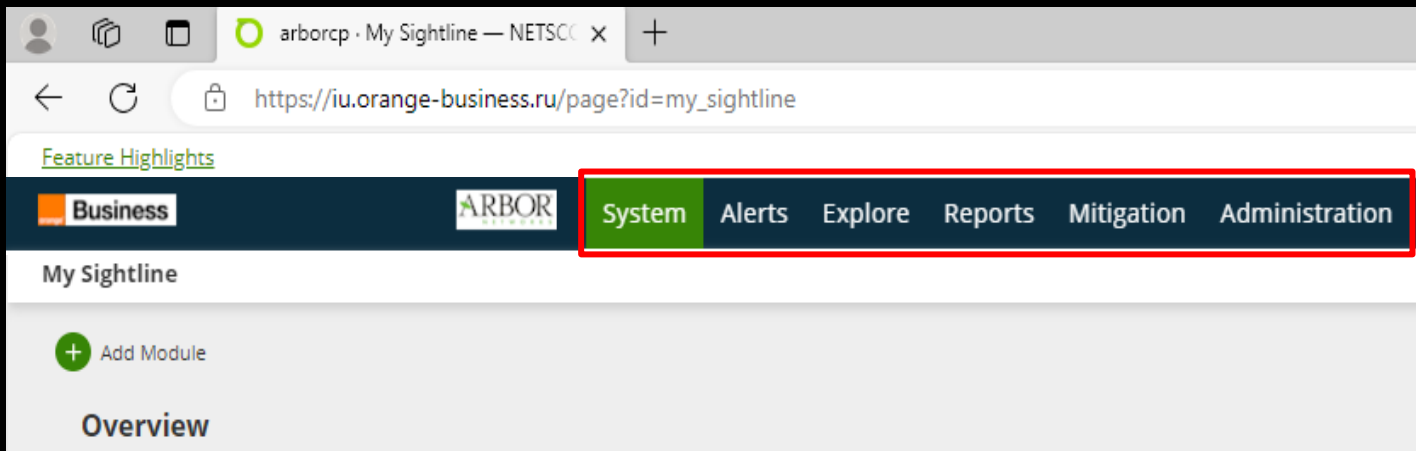
- Для доступа к WEB-интерфейсу требуются **login & password**, которые высылаются **индивидуально каждому** Представителю Клиента на этапе инсталляции Услуги



Важно

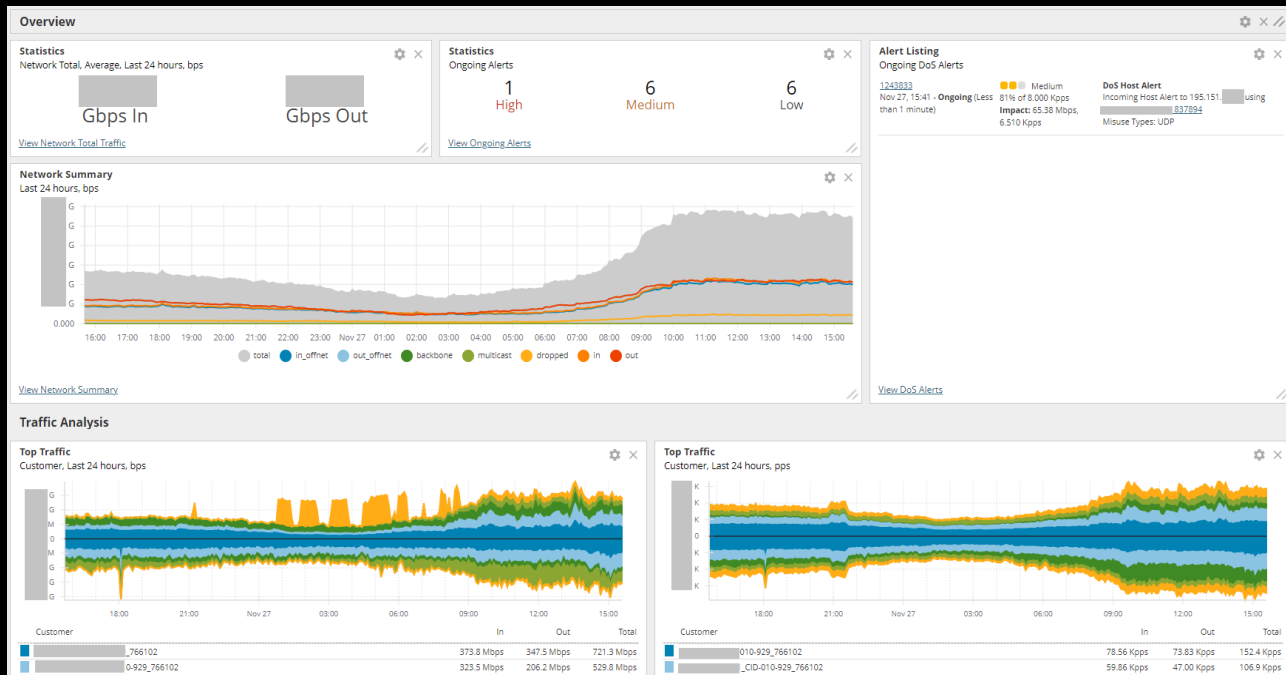
- Обратите внимание, что при вводе реквизитов учитывается регистр!
- Для корректной работы рекомендуется использовать WEB-браузеры Firefox (17ESR и выше) или Internet Explorer (9.0 или 10.0).

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

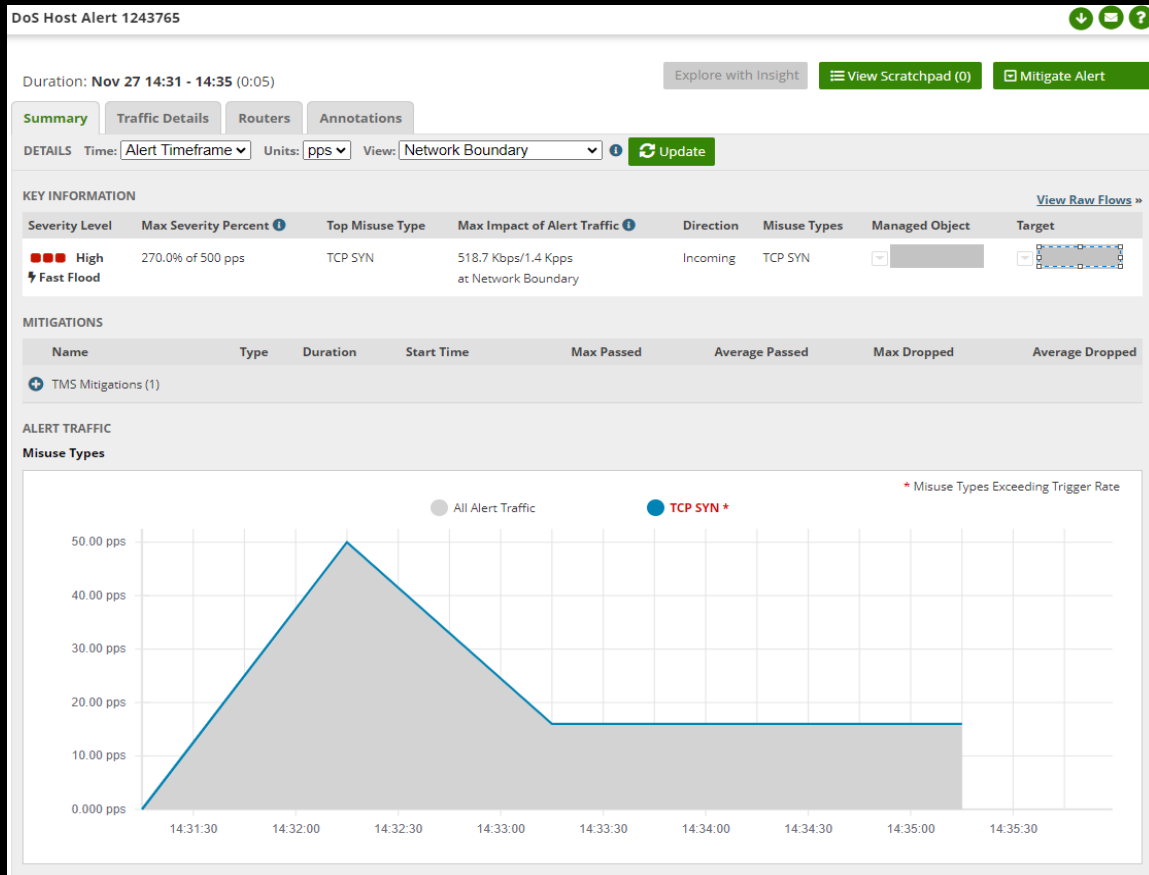
The screenshot displays the ARBOR SP Alerts interface. At the top, there is a navigation bar with tabs for Business, ARBOR, System, Alerts, Explore, Reports, Mitigation, and Administration. A search bar is located on the right. Below the navigation bar, the 'All Alerts' section is active, showing a list of alerts. The interface includes a search bar, a 'Search' button, and a 'Wizard' button. The alert list is organized into columns: ID, Max Impact, Importance, Alert, Start Time, and Classification & Annotations. The first alert (ID 1243836) is a 'DoS Host Alert' with a 'Low' importance level, triggered at Nov 27 15:47. The second alert (ID 1243835) is also a 'DoS Host Alert' with a 'Low' importance level, triggered at Nov 27 15:44. The third alert (ID 1243834) is a 'DoS Host Alert' with a 'Low' importance level, triggered at Nov 27 15:42. The fourth alert (ID 1243833) is a 'DoS Host Alert' with a 'Medium' importance level, triggered at Nov 27 15:41.

ID	Max Impact	Importance	Alert	Start Time	Classification & Annotations
1243836	No Data	Low	DoS Host Alert Incoming Host Alert to 217.12.104.100 using 766102 (parent: 766102) Misuse Types: Total Traffic	Nov 27 15:47 - Ongoing (Less than 1 minute)	Possible Attack The "Total Traffic" host alert signature has been triggered at router "Moscow09.rosprint.net". (expected rate: 10.00 Mbps/3.00 Kpps, observed rate: 5.11 Mbps/3.21 Kpps) (by auto-annotation)
1243835	26.0% of 20 Mbps 5.1 Mbps, 3.2 Kpps	Low	DoS Host Alert Incoming Host Alert to 217.12.98.151 using 929_766102 (parent: 66102) Misuse Types: Total Traffic	Nov 27 15:44 - Ongoing (0:03)	Possible Attack The "Total Traffic" host alert signature has been triggered at router "Moscow09.rosprint.net". (expected rate: 130.00 Mbps/70.00 Kpps, observed rate: 132.22 Mbps/53.63 Kpps) (by auto-annotation)
1243834	40.0% of 20 Mbps 5.7 Mbps, 5.3 Kpps	Low	DoS Host Alert Incoming Host Alert to 217.12.104.100 using 929_766102 (parent: 766102) Misuse Types: Total Traffic	Nov 27 15:42 - 15:46 (0:03)	Possible Attack The "Total Traffic" host alert signature has been triggered at router "Moscow09.rosprint.net". (expected rate: 10.00 Mbps/3.00 Kpps, observed rate: 5.68 Mbps/5.34 Kpps) (by auto-annotation)
1243833	81.0% of 8 Kpps 65.4 Mbps, 6.5 Kpps	Medium	DoS Host Alert Incoming Host Alert to 195.151.27.12 using 837894 Misuse Types: UDP	Nov 27 15:41 - 15:45 (0:03)	Possible Attack The "UDP" host alert signature severity rate configured for 837894 has been exceeded, changing Severity Level from low to medium (expected rate: 8.00 Kpps, observed rate: 6.51 Kpps) (by auto-annotation)

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

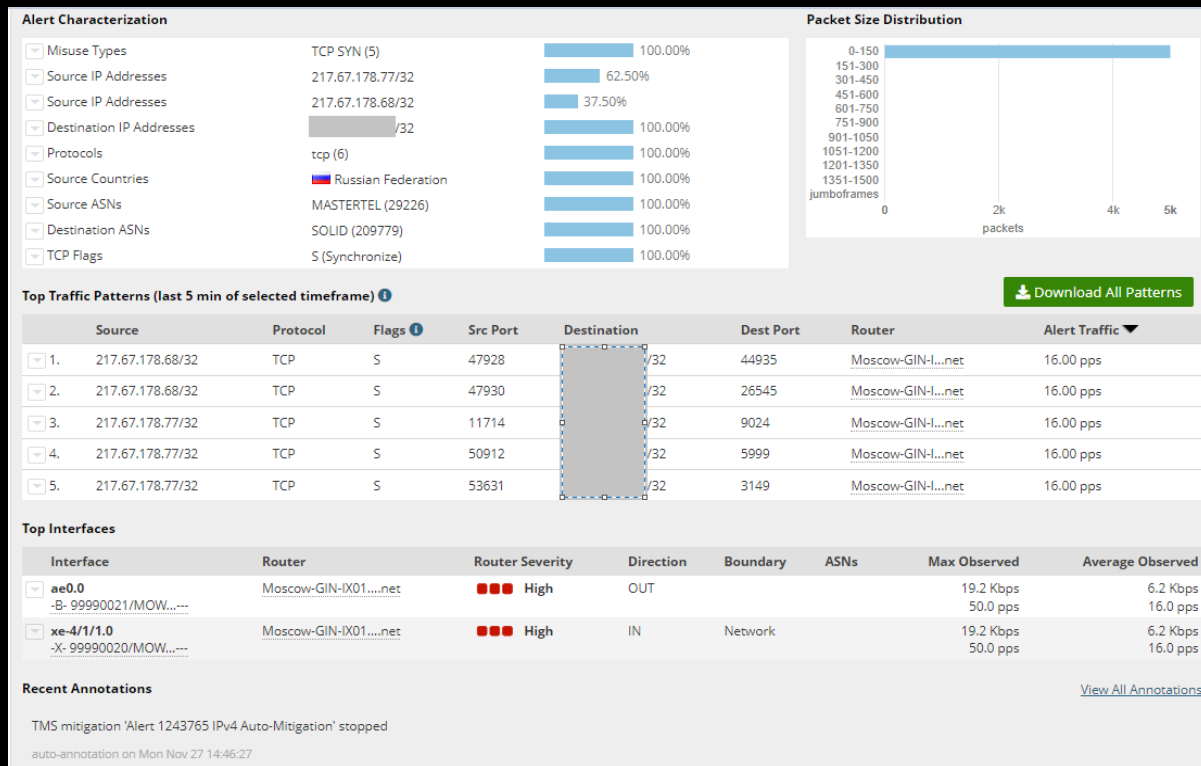
WEB-интерфейс ARBOR SP

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



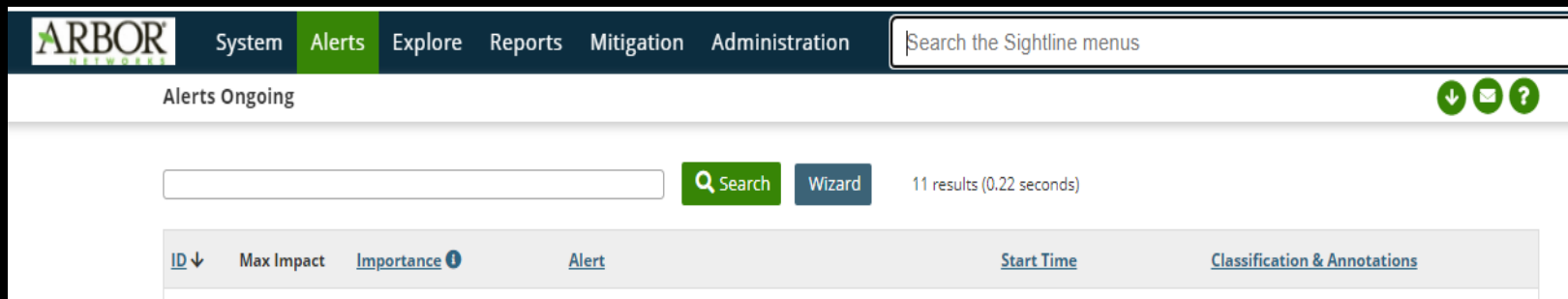
WEB-интерфейс ARBOR SP

- Страницу можно прокрутить вниз для более детальной информации об атаке



WEB-интерфейс ARBOR SP

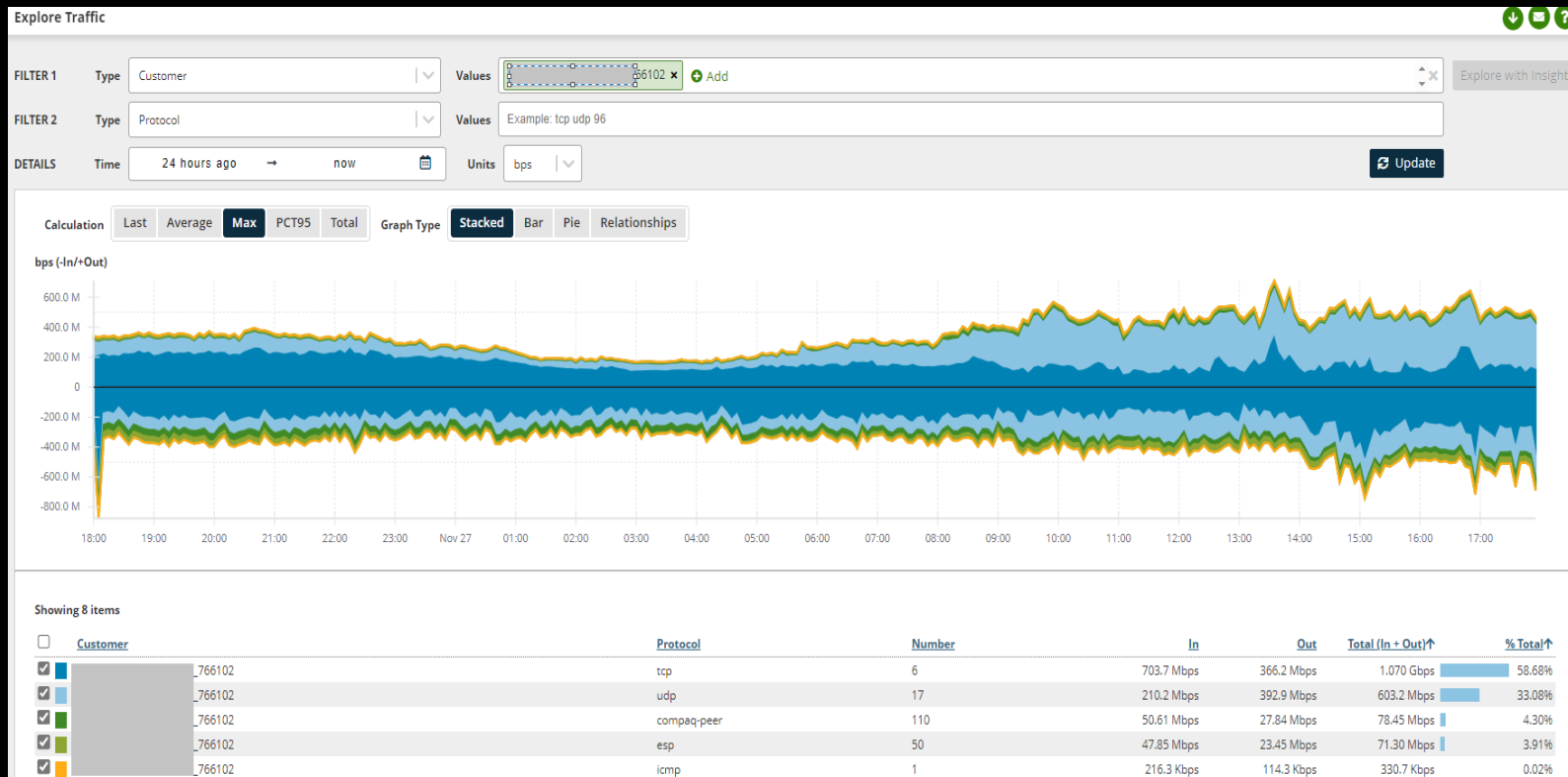
- «Alerts Ongoing» позволяет осуществить поиск определенного события, есть возможность задать параметры поиска через кнопку **Wizard**



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

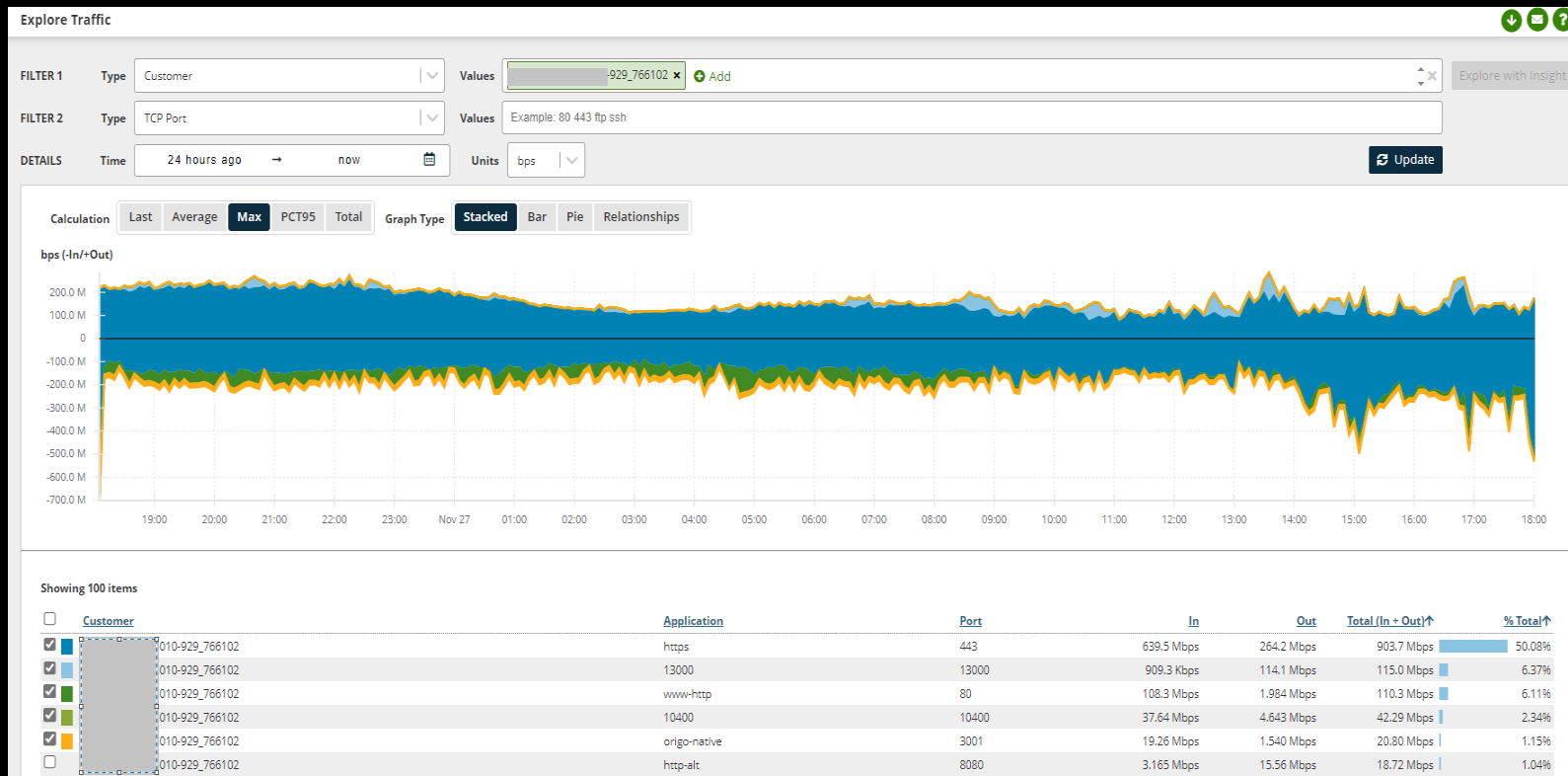
WEB-интерфейс ARBOR SP

Отображение трафика по приложениям



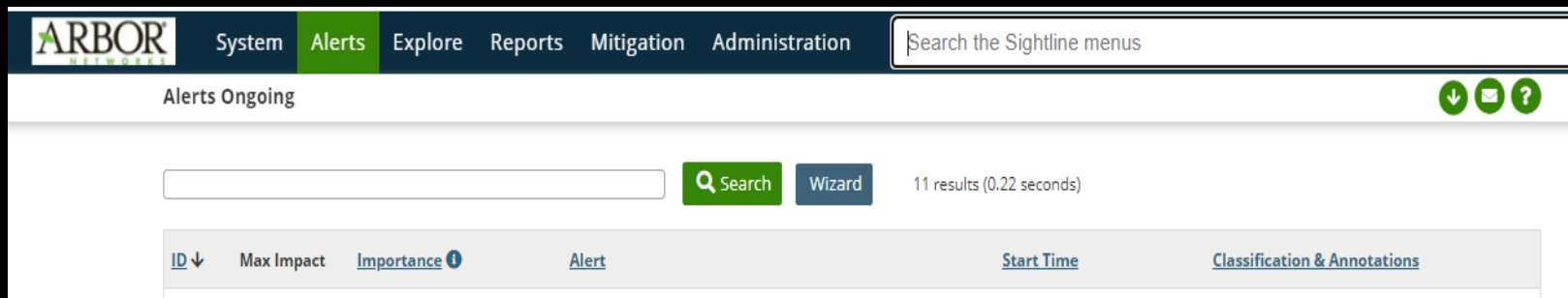
WEB-интерфейс ARBOR SP

Отображение трафика по портам



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

All Mitigations							
		Search	Wizard	100 results (0.65 seconds)			
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



MITIGATOR
DDOS PROTECTION

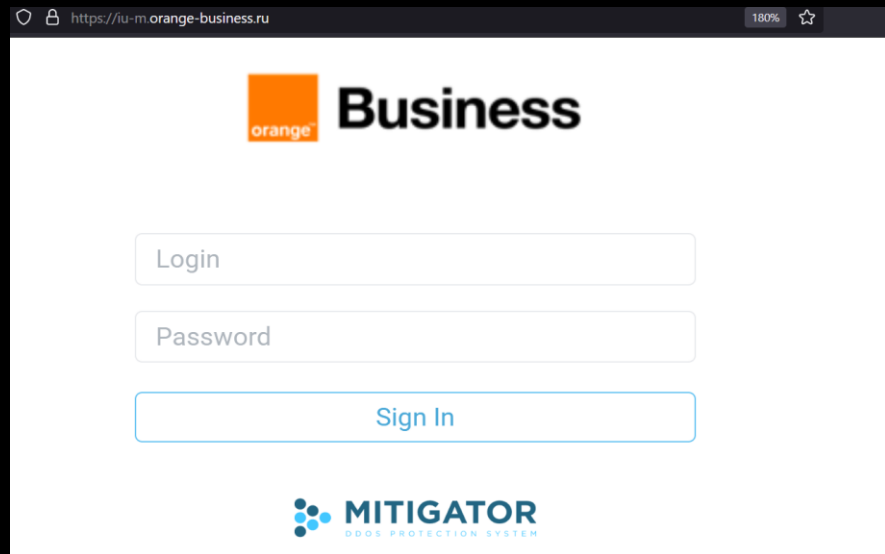
WEB-интерфейс MITIGATOR

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



The screenshot displays a web browser window with the address bar showing <https://iu-m.orange-business.ru>. The page content includes the Orange Business logo, a login form with fields for 'Login' and 'Password', and a 'Sign In' button. The MITIGATOR logo and 'DDOS PROTECTION SYSTEM' text are located at the bottom of the page.

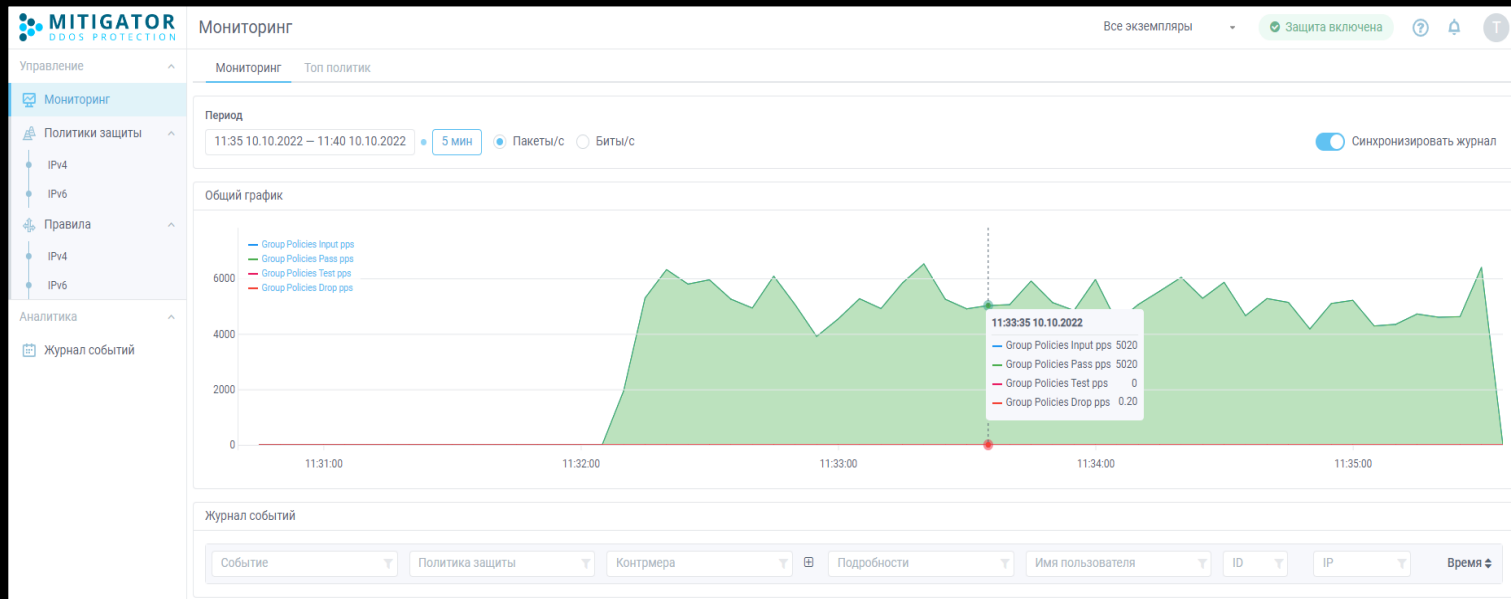
Важно

- 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

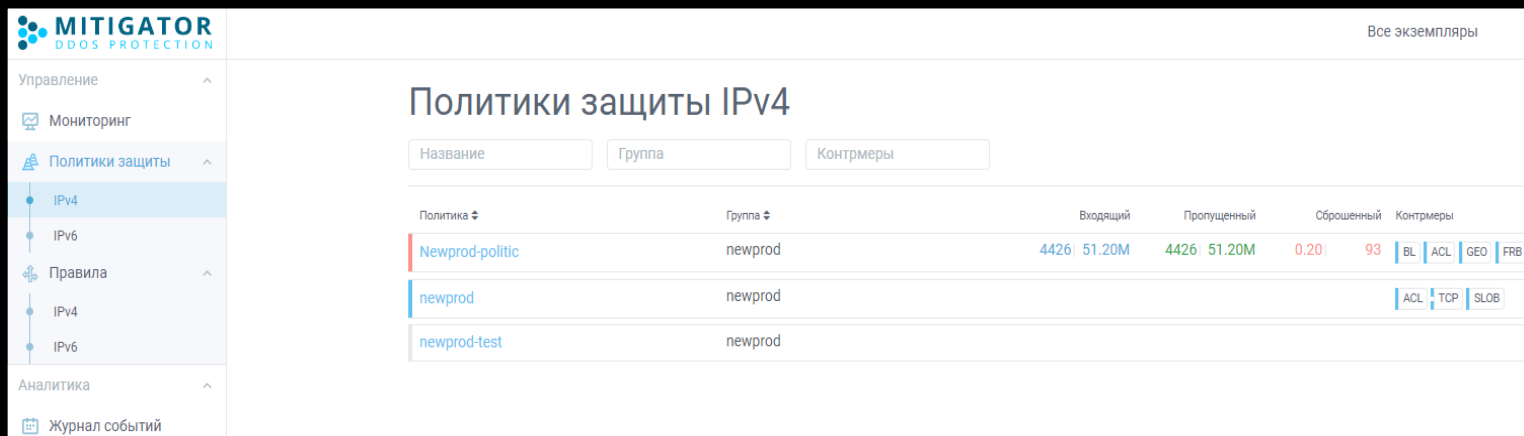
- При входе в систему Вы попадаете на вкладку **Мониторинг (Dahsboard)**, где можно посмотреть сколько трафика (в bps и rps) поступает на защищаемые объекты



WEB-интерфейс MITIGATOR

Политики защиты

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



The screenshot shows the MITIGATOR DDOS PROTECTION web interface. The left sidebar contains navigation links: Управление, Мониторинг, Политики защиты (selected), IPv4 (selected), IPv6, Правила, IPv4, IPv6, Аналитика, and Журнал событий. The main content area is titled 'Политики защиты IPv4' and includes search filters for 'Название', 'Группа', and 'Контрмеры'. Below the filters is a table with columns: Политика, Группа, Входящий, Пропущенный, Сброшенный, and Контрмеры. The table lists three policies: 'Newprod-politic', 'newprod', and 'newprod-test', all belonging to the 'newprod' group. The 'Newprod-politic' row shows incoming traffic of 4426 and 51.20M, and dropped traffic of 4426 and 51.20M. The 'newprod' row shows a drop rate of 0.20 and 93 dropped packets. The 'newprod-test' row shows no traffic. The 'Контрмеры' column lists active countermeasures: BL, ACL, GEO, FRB for 'Newprod-politic'; ACL, TCP, SLOB for 'newprod'; and no countermeasures for 'newprod-test'.

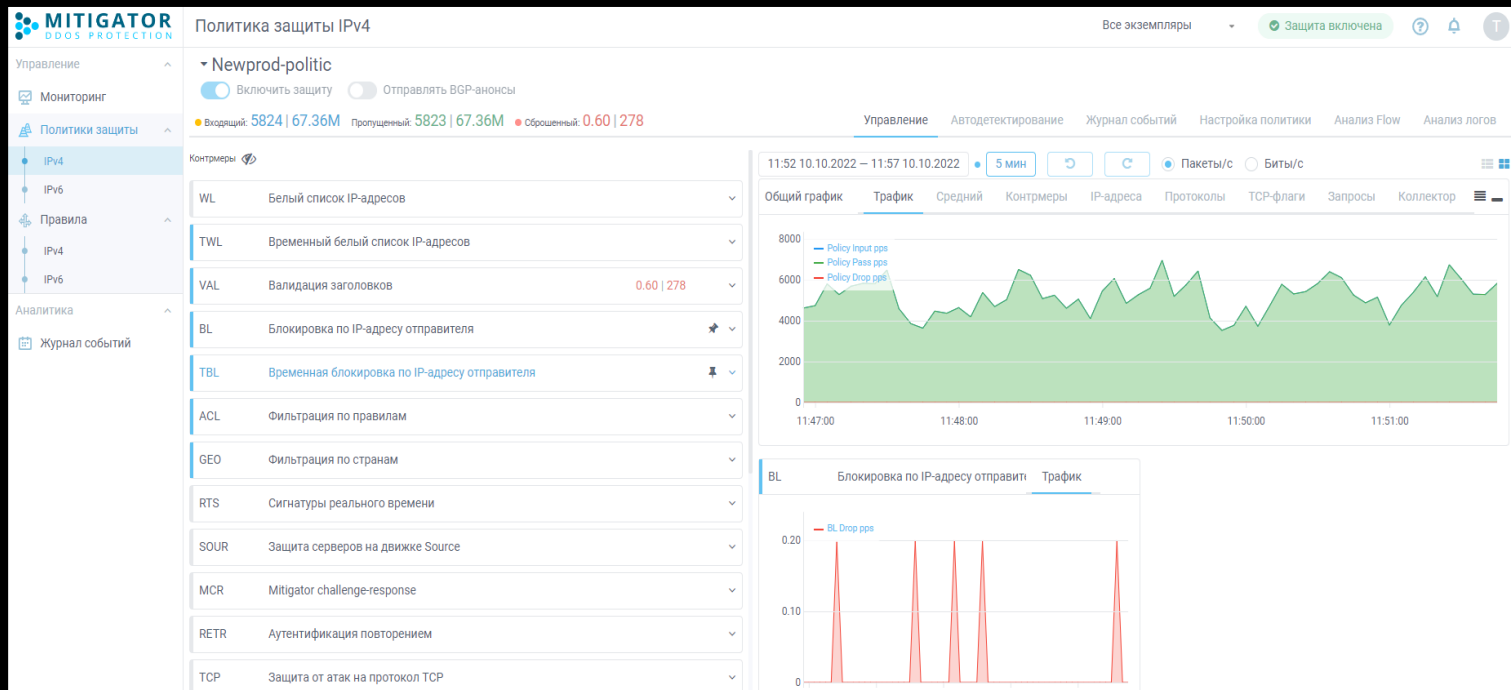
Политика	Группа	Входящий	Пропущенный	Сброшенный	Контрмеры
Newprod-politic	newprod	4426 51.20M	4426 51.20M	0.20 93	BL ACL GEO FRB
newprod	newprod				ACL TCP SLOB
newprod-test	newprod				

- По изменяющимся значениям (bps и rps) 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

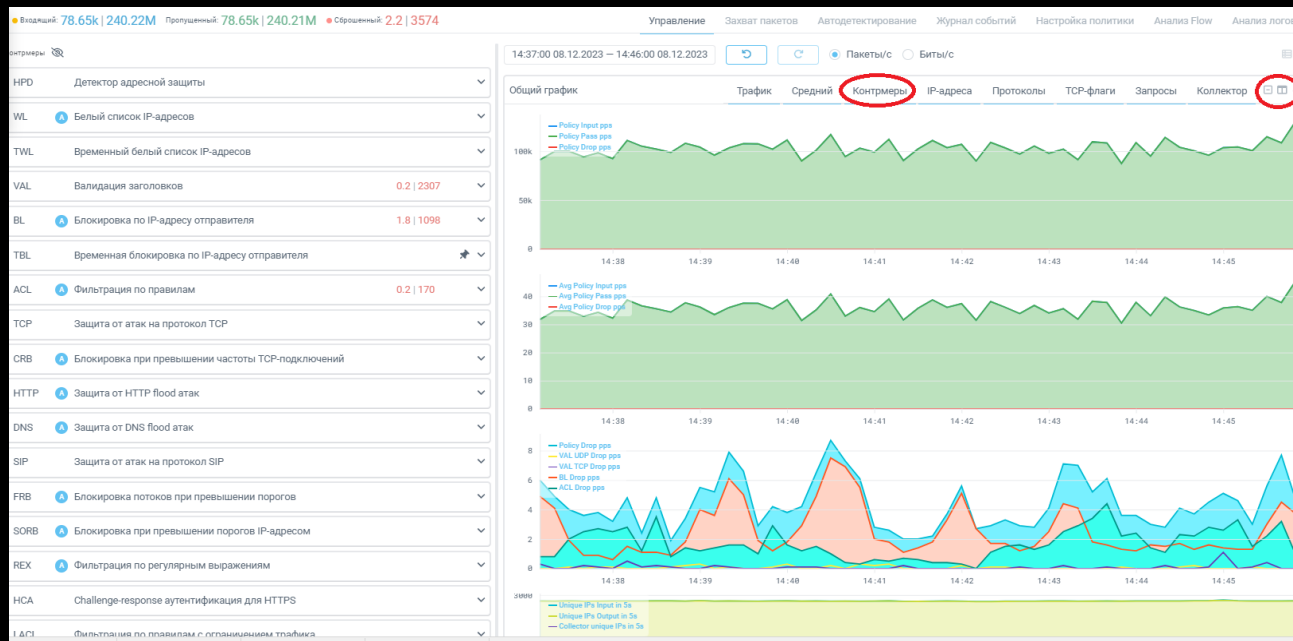
- При нажатии на **Политику** открывается список используемых контрмер в политике



WEB-интерфейс MITIGATOR

Политики защиты

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

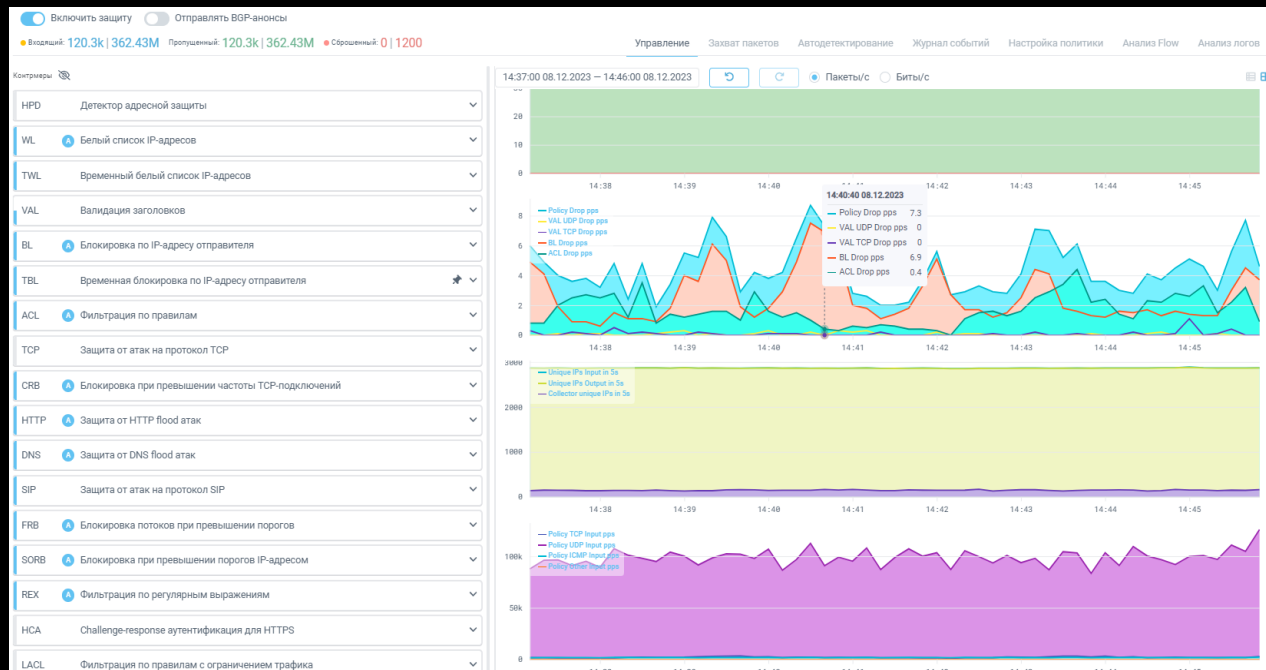


- В правом верхнем ряду (выделено на рисунке) можно нажать на кнопку сортировки, после чего будут доступны графики сброшенного трафика по включенным контрмерам

WEB-интерфейс MITIGATOR

Графики сброшенного трафика

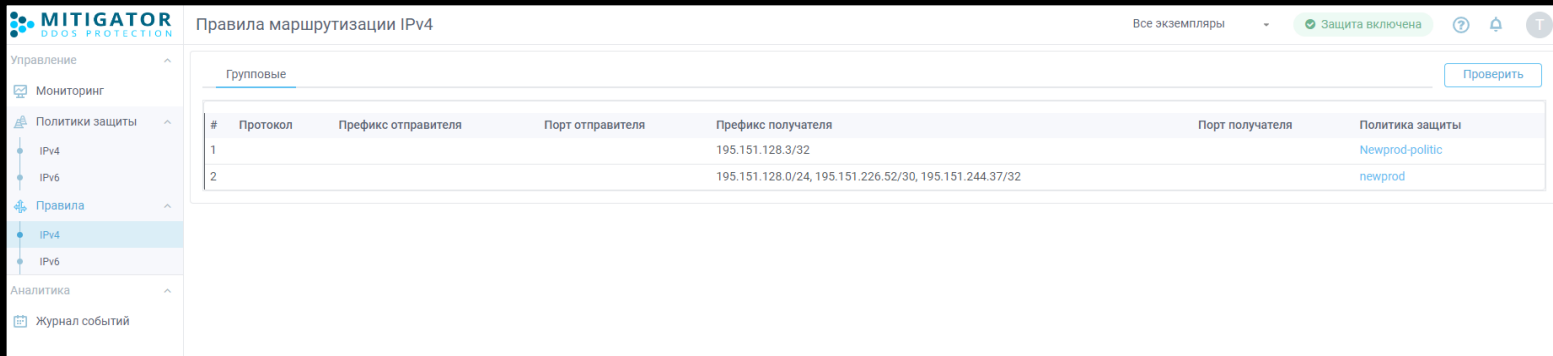
- При наведении курсора на график сброшенного в контрмере трафика появляется табличка с информацией о том, какой трафик сбрасывается, также указываются значения bps и rps трафика



WEB-интерфейс MITIGATOR

Правила маршрутизации для префиксов

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



The screenshot shows the MITIGATOR web interface. The left sidebar contains navigation links: Управление, Мониторинг, Политики защиты, Правила, and Аналитика. The 'Правила' section is expanded, showing 'IPv4' and 'IPv6' sub-sections. The main content area is titled 'Правила маршрутизации IPv4' and displays a table of routing rules. The table has columns for #, Protocol, Sender Prefix, Sender Port, Receiver Prefix, Receiver Port, and Protection Policy. Two rules are listed: Rule 1 for protocol 195.151.128.3/32 with policy 'Newprod-politic', and Rule 2 for protocol 195.151.128.0/24, 195.151.226.52/30, 195.151.244.37/32 with policy 'newprod'. A 'Проверить' button is visible in the top right corner of the table area.

#	Протокол	Префикс отправителя	Порт отправителя	Префикс получателя	Порт получателя	Политика защиты
1				195.151.128.3/32		Newprod-politic
2				195.151.128.0/24, 195.151.226.52/30, 195.151.244.37/32		newprod

- 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!



Business