servicepipe

Bot Protection

Облачная платформа тонкой фильтрации
трафика для защиты веб-ресурсов
от DDoS-атак, фулстек-ботов и целевых угроз

Bot Protectoin

servicepipe

Облачная платформа тонкой фильтрации трафика для высокоточной защиты веб-ресурсов от любой нежелательной автоматизации без потери пользователей

Принципы работы:

- Realtime-анализ 100+ метрик **каждого единичного запроса**
- Статистика — не основа для вынесения вердикта о блокировке
- Сигнатуры не являются статической частью конфигурации и генерируются автоматически
- Контроль дообучения командой аналитиков для повышения точности детекции

Режимы работы Bot Protection

servicepipe

Весь входящий трафик анализируется и передаётся клиенту (Threat Intelligence)

К запросам добавляется HTTP-заголовок X-Verdict

+

Блокировка автоматизированных запросов при обнаружении статистических аномалий в трафике

Статистический анализ трафика, в отсутствие атак запросы не блокируются

+

Блокировка всех нелегитимных запросов (даже единичных), включая DDoS-атаки

Фильтрация любой нежелательной автоматизации, включая низкочастотные атаки

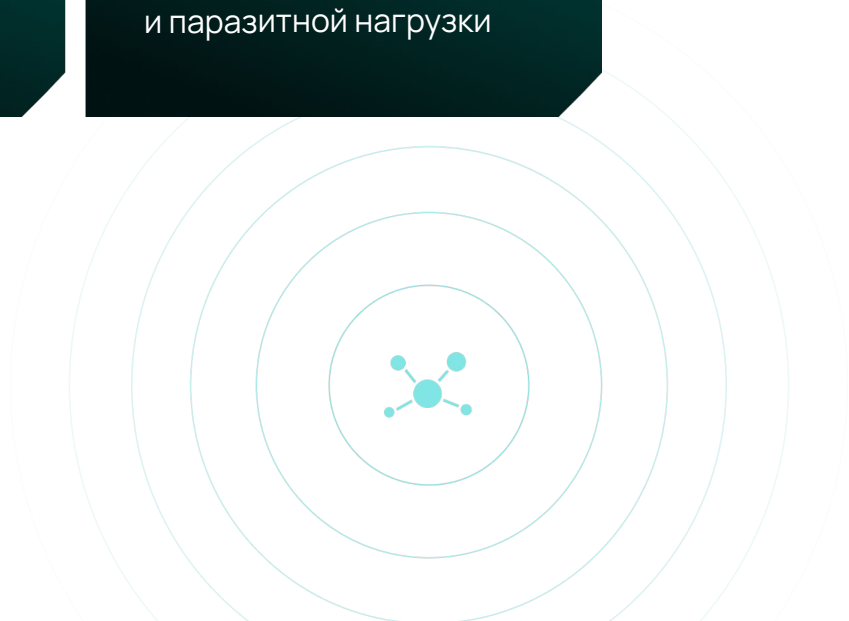
Области применения

servicepipe

Защита веб-ресурсов
от недоступности
и атак на бизнес-логику

Повышение точности
веб-аналитики
по защищаемым
ресурсам

Разгрузка WAF
и веб-серверов
от мусорной
и паразитной нагрузки



Преимущества Servicepipe Bot Protection

servicepipe

Защита без потери пользователей и влияния на SEO

Многофакторный анализ каждого запроса позволяет точно определить его источник (пользователь или бот), а также избежать задержек в срабатывании и влияния на SEO.

Удобство внедрения и эксплуатации

On-Prem, SaaS и гибридные инсталляции. API для интеграций. Подключение ~10 минут без сложных настроек, обучения и накопления статистики.

Соответствие требованиям законодательства и регуляторов

Поддержка ГОСТ-сертификатов и защита без раскрытия приватного ключа SSL для соответствия PCI DSS. Хранение персональных данных на территории РФ.

Оптимизация TCO (Total Cost of Ownership)

За счёт фильтрации паразитной нагрузки на приложения и IT-инфраструктуру.

Преимущества Servicepipe Bot Protection

servicepipe

Обнаружение даже единичных вредоносных запросов

Статистика — не основа принятия решений.

Моментальное реагирование, вердикт ‹1 мс

Полностью автоматический real-time анализ.

Защита от любых автоматизированных угроз

Сигнатуры не являются статической частью конфигурации, а генерируются автоматически на лету.

Высокоточная фильтрация, ‹0,01% false positive

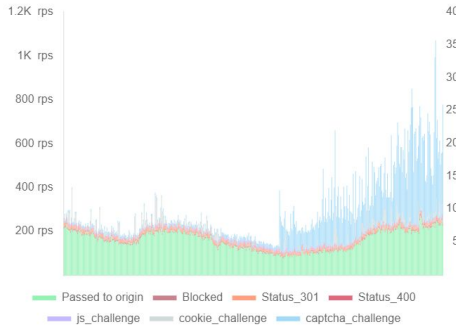
Machine Learning + контроль дообучения командой аналитиков.

Дашборд Application Protection

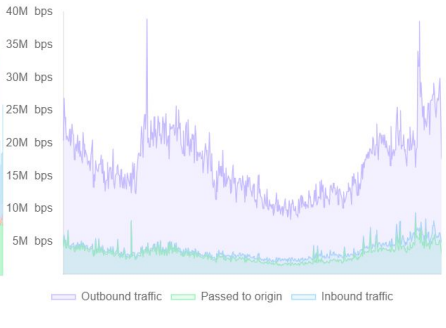
servicepipe

Принято на платформе	Пропущено на серверы оригинации	Заблокировано	Макс. скорость запросов принятых платформой	Макс. скорость пропущенных на ориджины запросов
21.1M req.	13.13M req.	202.85K req.	1.03K rps	270 rps

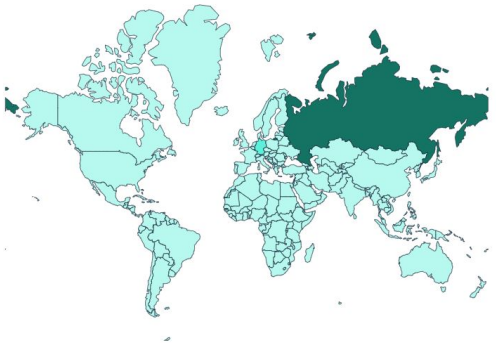
Статистика по запросам, rps / rpm



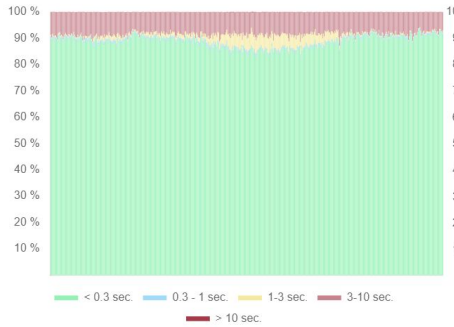
Статистика по полосе трафика, bps / bpm



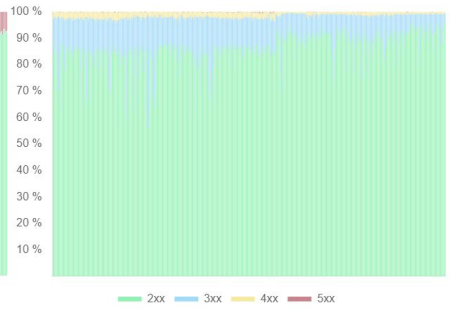
География запросов



Время ответа серверов ориг., %



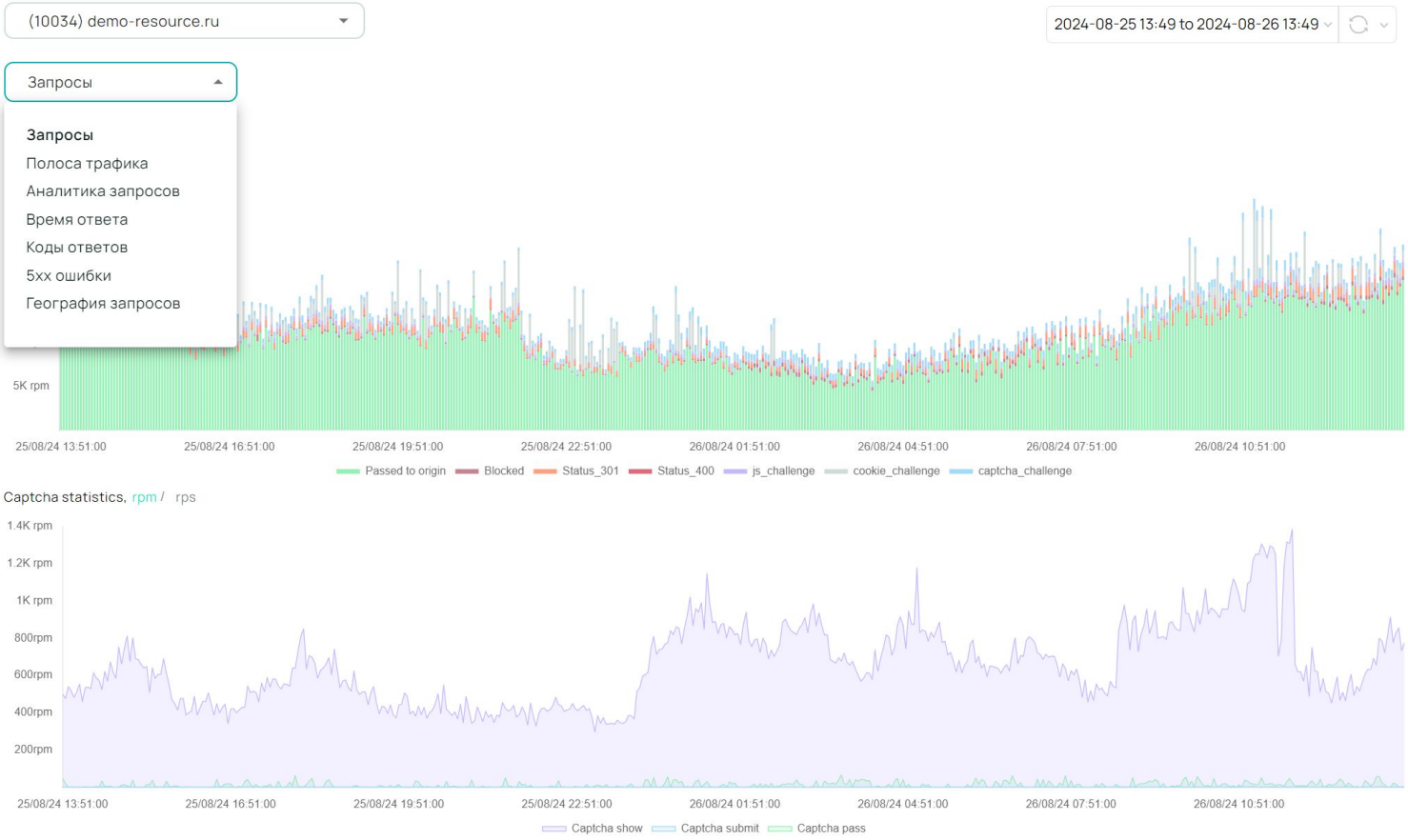
Коды ответов серверов ориг., %



Топ 5 стран	Запросы	%
Russian Federation	2985802	67.73 %
Germany	736592	16.71 %
Singapore	257261	5.84 %
United States of America	74438	1.69 %
Indonesia	37963	0.86 %

Статистика по трафику

servicepipe



Расширенная аналитика и отчёты по ботам

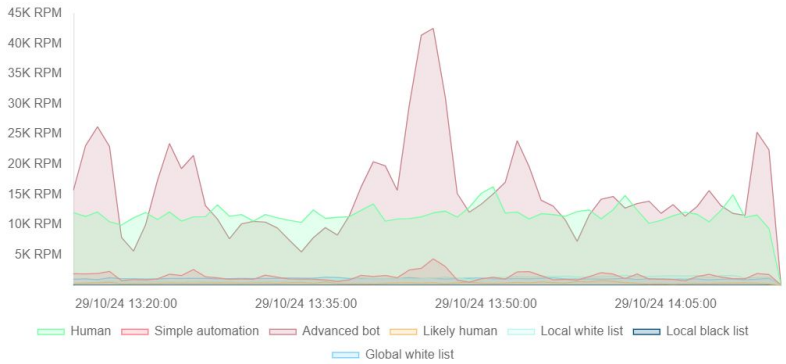
servicepipe

(10034) demo-resource.ru

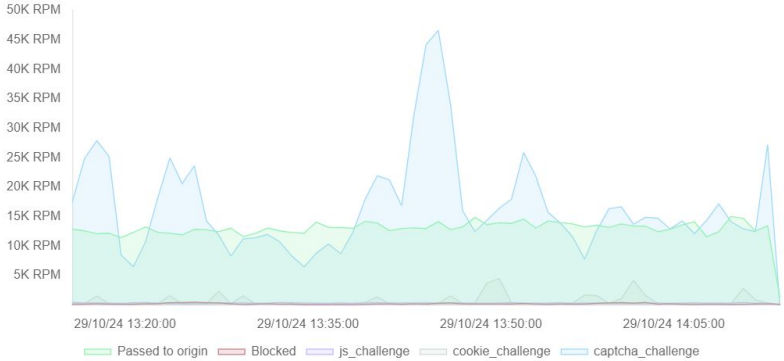
Intra-day

now-1h to now

Requests by sources rpm / rps



Requests by actions rpm / rps



TOP source IP adresses

#	IP	Subnet	Netname	Requests count
1	165.225.72.150	165.225.72.0/23	Zscaler Switzerland GmbH	120289
2	165.225.72.149	165.225.72.0/23	Zscaler Switzerland GmbH	96972
3	165.225.72.151	165.225.72.0/23	Zscaler Switzerland GmbH	94075
4	165.225.72.156	165.225.72.0/23	Zscaler Switzerland GmbH	43267
5	178.176.81.132	178.176.0.0/14	PJSC MegaFon	4

Download PDF

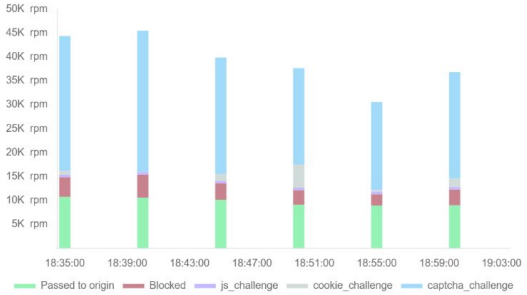
Отчёты по аномалиям

servicepipe

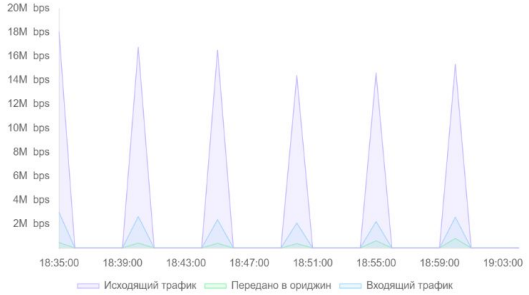
Anomaly ID 32434

Start: 16/04/24 18:41:00 Stop: 16/04/24 18:50:00	Resource name demo-resource.ru	Max blocked requests rate 109 rpm	Total blocked requests 44588

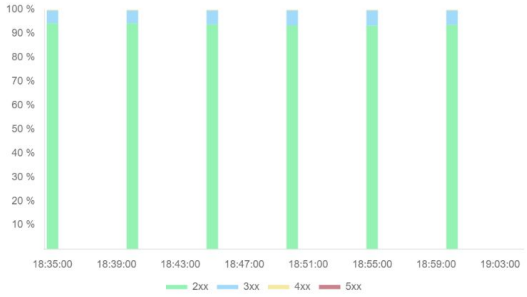
Request statistics, rpm / rps



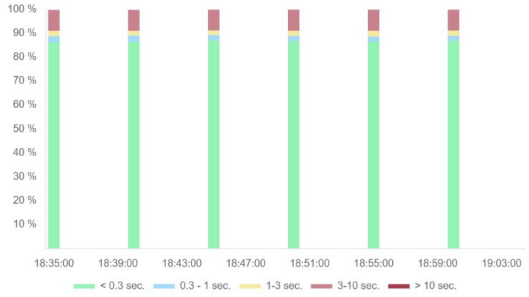
Bandwidth statistics, bps



Origin's response code statistics, % rpm / rps



Origin's response time statistics, % rpm / rps

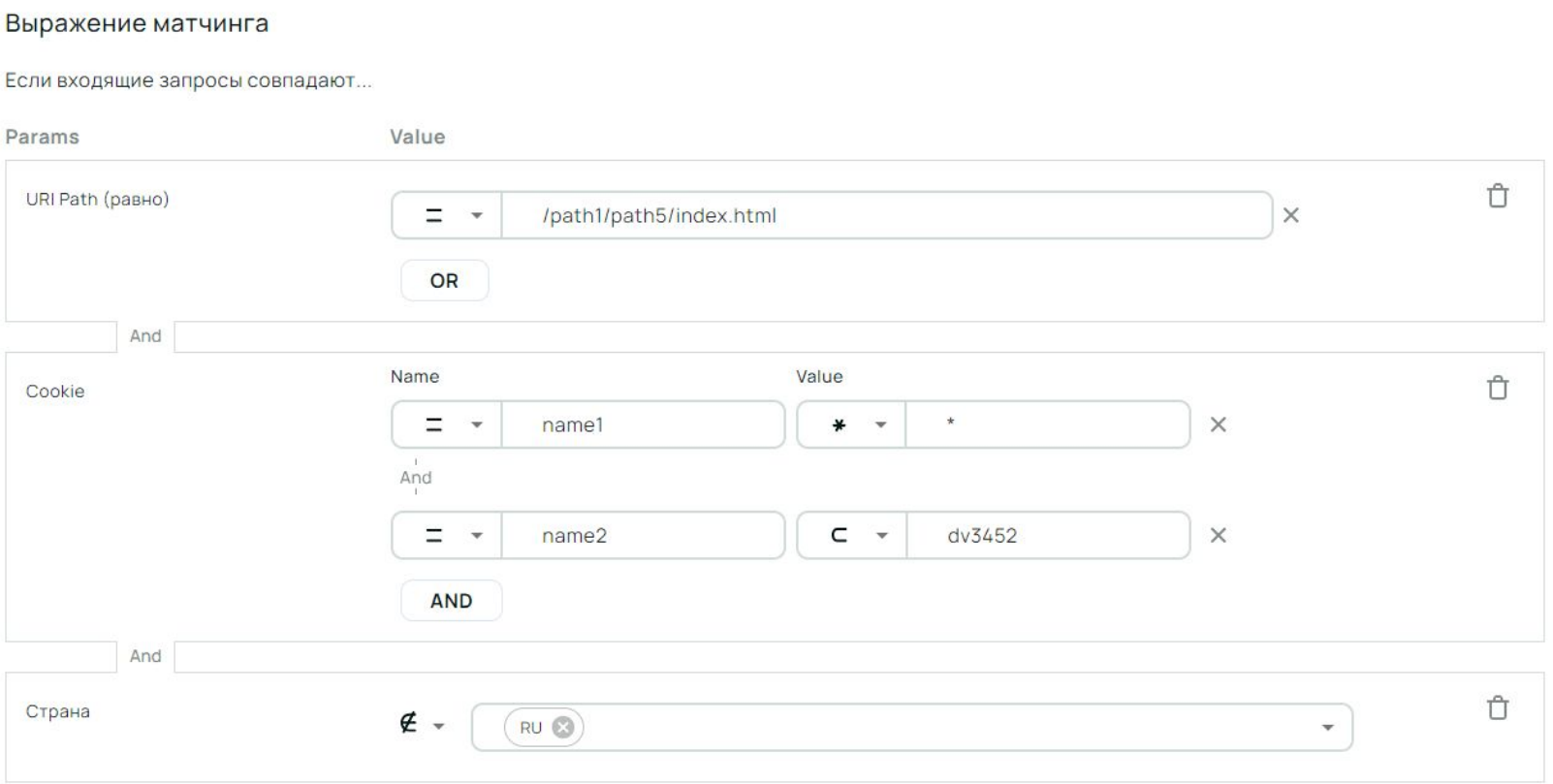


All resources

ID ↓	Start	Stop	(id) Resource name	Max blocked
34397	30/04/24 12:07:00	30/04/24 12:08:00	(10034) demo-resource.ru	58
34392	30/04/24 11:47:00	30/04/24 11:48:00	(10034) demo-resource.ru	48
34055	27/04/24 10:31:00	27/04/24 10:32:00	(10034) demo-resource.ru	59
34053	27/04/24 10:29:00	27/04/24 10:31:00	(10034) demo-resource.ru	51
34012	27/04/24 08:00:00	27/04/24 08:01:00	(10034) demo-resource.ru	54
33958	26/04/24 21:33:00	26/04/24 21:37:00	(10034) demo-resource.ru	63
33519	25/04/24 01:28:00	25/04/24 01:29:00	(10034) demo-resource.ru	47
33012	21/04/24 11:46:00	21/04/24 11:47:00	(10034) demo-resource.ru	64
32864	19/04/24 19:32:00	19/04/24 19:33:00	(10034) demo-resource.ru	30
32797	19/04/24 10:01:00	19/04/24 10:05:00	(10034) demo-resource.ru	48
32794	19/04/24 09:51:00	19/04/24 10:00:00	(10034) demo-resource.ru	46
32791	19/04/24 09:46:00	19/04/24 09:55:00	(10034) demo-resource.ru	47
32787	19/04/24 09:36:00	19/04/24 09:46:00	(10034) demo-resource.ru	43
32784	19/04/24 09:34:00	19/04/24 09:40:00	(10034) demo-resource.ru	42

Пользовательские правила фильтрации

servicepipe



Логи запросов

servicepipe

Гибкий фильтр

4 суток — глубина хранения

24 часа — период отображения

Выгрузка дампов трафика на почту

	28/10 14:25:18	block client_non_ddos	54.86.50.139 US	simple_automatization	PostmanRuntime/7.42.0	GET /	script	my.servicepipe.ru
	28/10 14:20:56	block client_non_ddos	104.47.26.126 SG	simple_automatization		HEAD /	script	my.servicepipe.ru
	28/10 14:19:57	block client_non_ddos	95.87.68.239 KG	simple_automatization	curl/8.10.1	HEAD /	script	my.servicepipe.ru
	28/10 13:03:00	block client_non_ddos	85.142.162.99 RU	simple_automatization	Links (2.22; Linux X86_64; GNU C; text)	GET /favicon.ico	static	my.servicepipe.ru
	28/10 13:03:00	block client_non_ddos	85.142.162.99 RU	simple_automatization	Links (2.22; Linux X86_64; GNU C; text)	GET /favicon.ico	static	my.servicepipe.ru http://my.servicepipe.ru/favicon.ico
	28/10 13:03:00	block client_non_ddos	85.142.162.99 RU	simple_automatization	Links (2.22; Linux X86_64; GNU C; text)	GET /apple-touch-icon.png	static	my.servicepipe.ru
	28/10 13:03:00							
	28/10 13:02:59							
	28/10 13:02:59							
	28/10 08:00:18							
	28/10 00:00:12							
	27/10 22:20:32	client_non_ddos	US		Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible; OAI-SearchBot/1.0; +https://openai.com/searchbot	/robots.txt		

	28/10 18:58:52	pass client_non_ddos	45.85.105.171 LT	human	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0	GET /users/login	script	my.servicepipe.ru
	28/10 18:58:52	pass client_non_ddos	45.85.105.171 LT	human	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0	GET /fonts/pfdindisplaypro-light-webfont.woff2	static	my.servicepipe.ru https://my.servicepipe.ru/fonts/stylesheet.css
	28/10 18:58:51	pass client_non_ddos	45.85.105.171 LT	human	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0	GET /	script	my.servicepipe.ru
	28/10 18:58:47	pass client_non_ddos	45.85.105.171 LT	human	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0	GET /etc/passwd	script	my.servicepipe.ru

servicepipe

Варианты интеграции

Облачный с проксированием трафика

с раскрытием SSL и сменой A-записи DNS

Гибрид с модулем NGINX

без раскрытия SSL (при подключении Антибота)

TCP-стрим + NGINX-модуль

без раскрытия SSL (подключение без Защищённого IP-транзита)

Бесшовная интеграция с WAF от технологических партнёров

Вебмониторэкс
защита веб-приложений

positive technologies

solidlab

Защита веб-приложений с раскрытием SSL

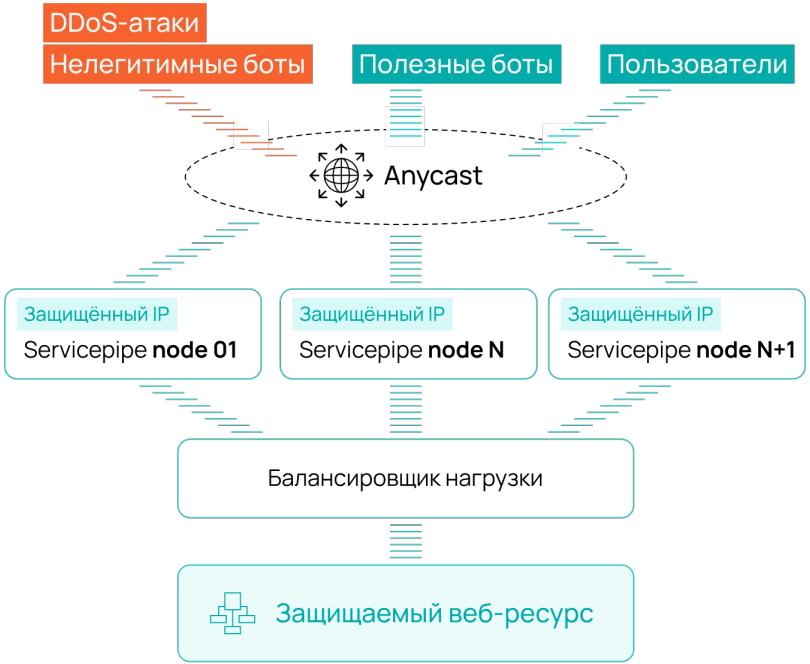
servicepipe

Облачный вариант интеграции

Стандартная схема с проксированием трафика через платформу фильтрации Servicepipe (Cloud Protection)

Это рекомендуемый и самый распространённый вариант подключения защиты, при котором реакция на атакую происходит мгновенно. Позволяет защитить веб-приложение от большинства известных угроз.

Дополнительно возможна оптимизация скорости работы приложения, распределенное кеширование и доставка статического контента приложений средствами CDN.



Защита веб-приложений без раскрытия SSL

servicepipe

Гибридная интеграция с NGINX-модулем

Гибридная схема с модулем актуальна тем, кому необходима защита без раскрытия SSL-сертификатов (например, финансовый сектор)

Схема позволяет блокировать любые, даже единичные запросы ботов ещё до момента их обработки. Это исключает риск, вывода из строя приложения внезапной объемной атакой, а также вероятность достижения своих целей продвинутыми ботами.

Модуль может быть развернут без проксирования трафика через сеть Servicepipe. Это позволит сохранить под своим контролем и управлением сетевые маршруты, по которым к защищаемому ресурсу обращаются пользователи.

Эшелонированная защита веб-ресурсов

servicepipe