Отечественное решение для защиты сети и фильтрации трафика

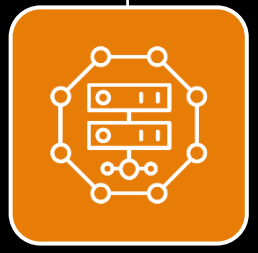
Александр Карманов

Presale-инженер «Айдеко»

Айдеко – российский разработчик решений для сетевой безопасности

фильтрация трафика

защита сети



развитие сетевых инфраструктур

Защищаем сети компаний межсетевым экраном Ideco UTM

с **2005** года на рынке ИБ

4 000 компаний используют Ideco UTM

40 000 человек используют VPN-подключения

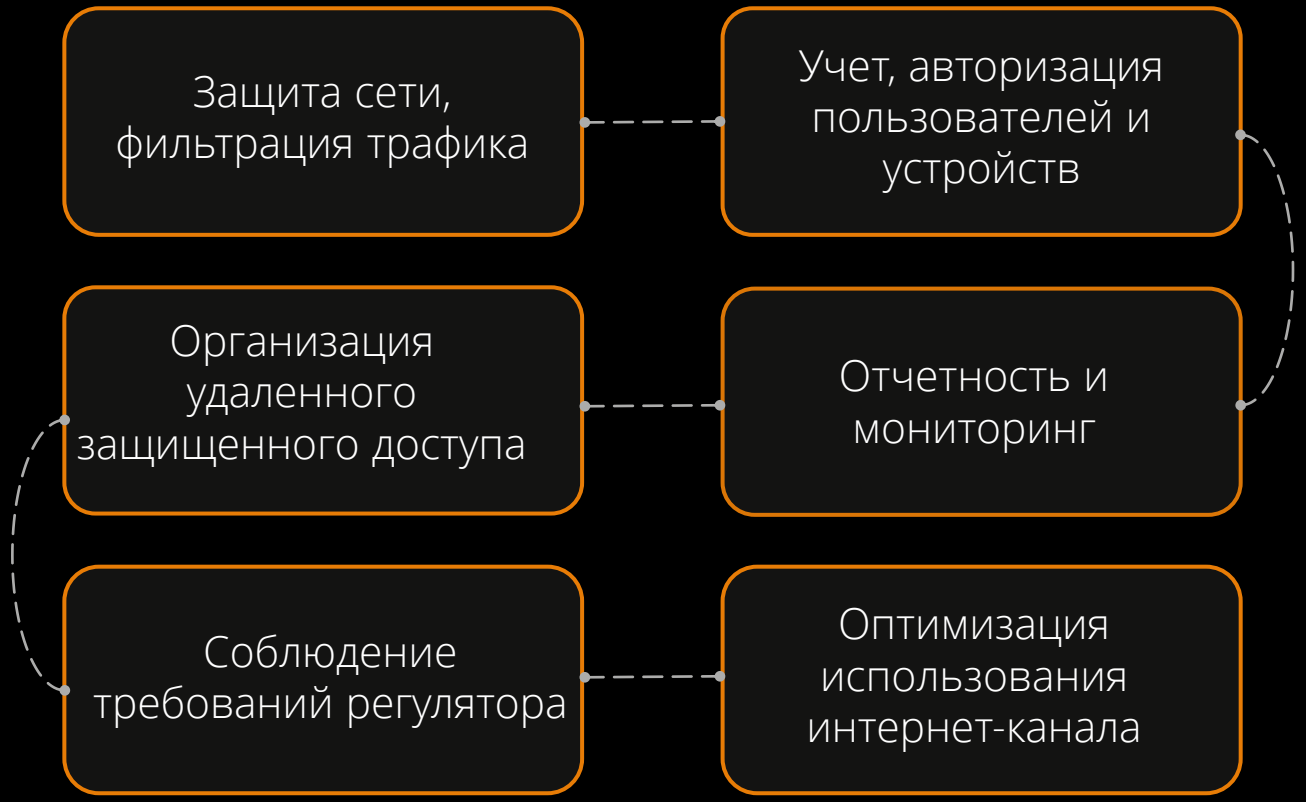
2 000 бесплатных лицензий для некоммерческого использования

с **2020** года сами работаем удаленно

ideco

Ideco UTM

Задачи:



DPI Фильтрация на 7 уровне модели OSI

15 млн доменов и IP-адресов C&C в нашем BlockList

500 млн URL в обновляемой базе данных

ideco

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021 г.

Решение входит в реестр российского ПО Минцифры РФ

- Требования доверия (4)
- Требования к МЭ
- Требования к СОВ
- Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ)
- Профили защиты СОВ (четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

ideco

IDECO UTM
14.2 сборка 155

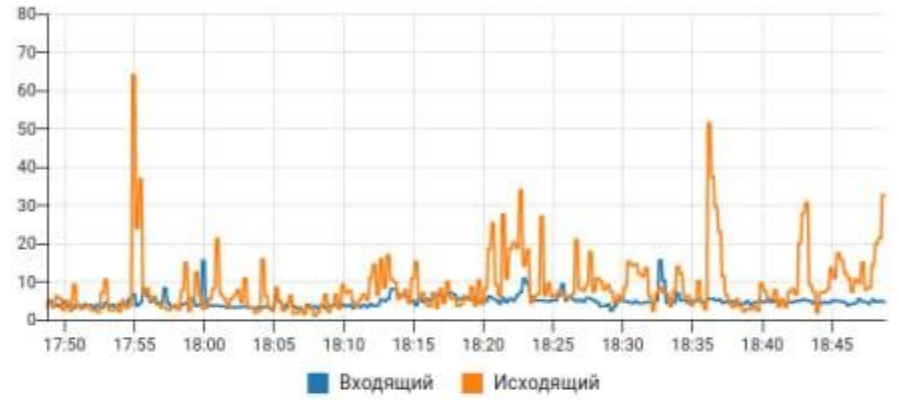
new gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты
- Управление сервером
- Почтовый релей

Панель мониторинга

Загрузка интерфейсов, Мбит/с

Локальная сеть · 1 час



Состояние внешних интерфейсов

Интерфейс	Загруженность (Мбит/с)
К-Телеком	45,0
Тестовое подключение	

Загрузка процессора, %

1 час

Время работы сервера 3 дня 7 часов 44 минуты

Топ 5 хостов (входящая скорость), Мбит/с

10.180.100.43	0,97
10.180.108.19	0,15
10.180.180.36	0,13
10.80.100.213	0,09
10.180.100.46	0,06

IPSec (исходящие)

Данные отсутствуют

Занятая оперативная память, ГБ

1 час

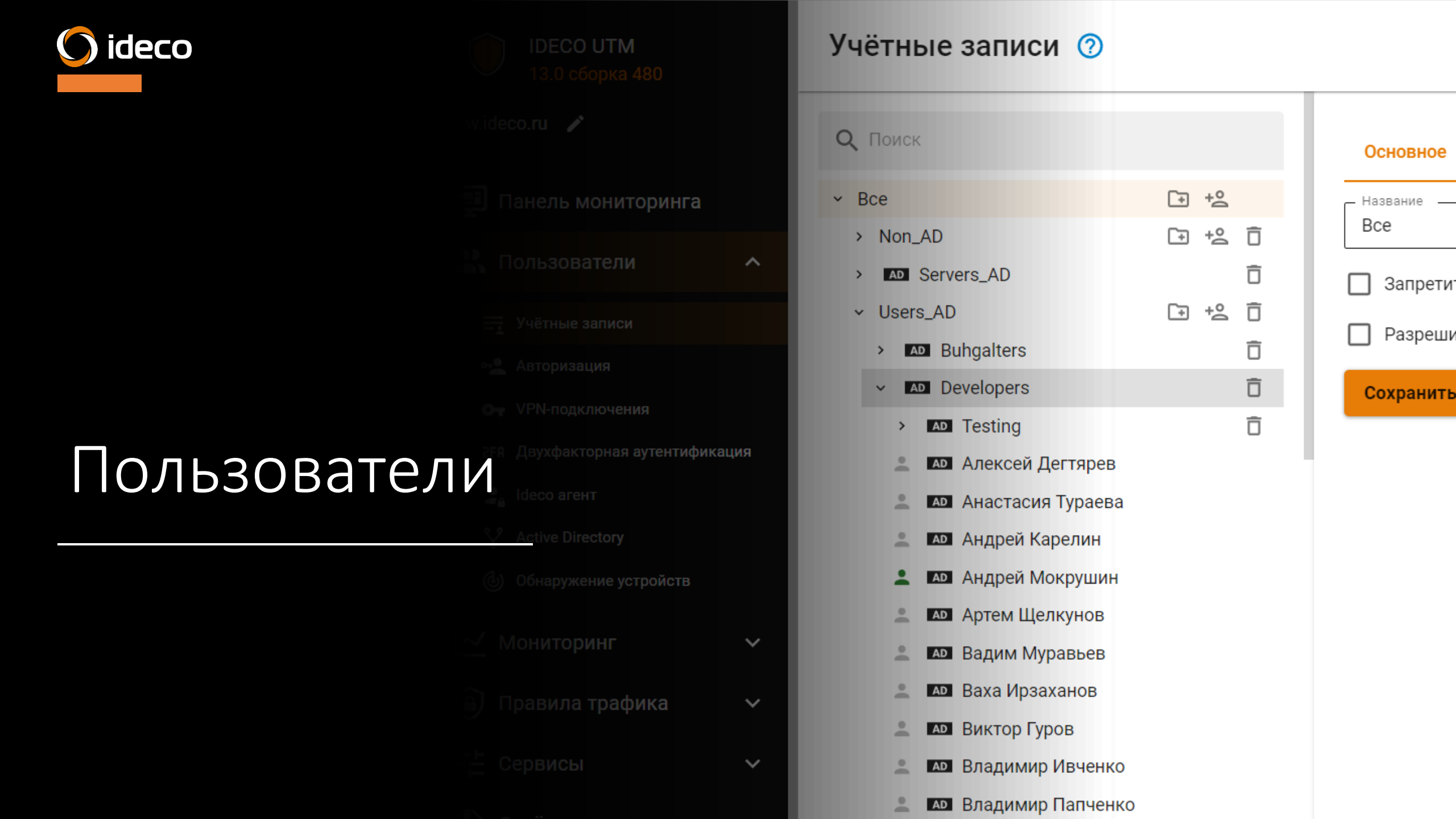
Топ 5 хостов (исходящая скорость), Мбит/с

IPSec (входящие)

Статус	Название

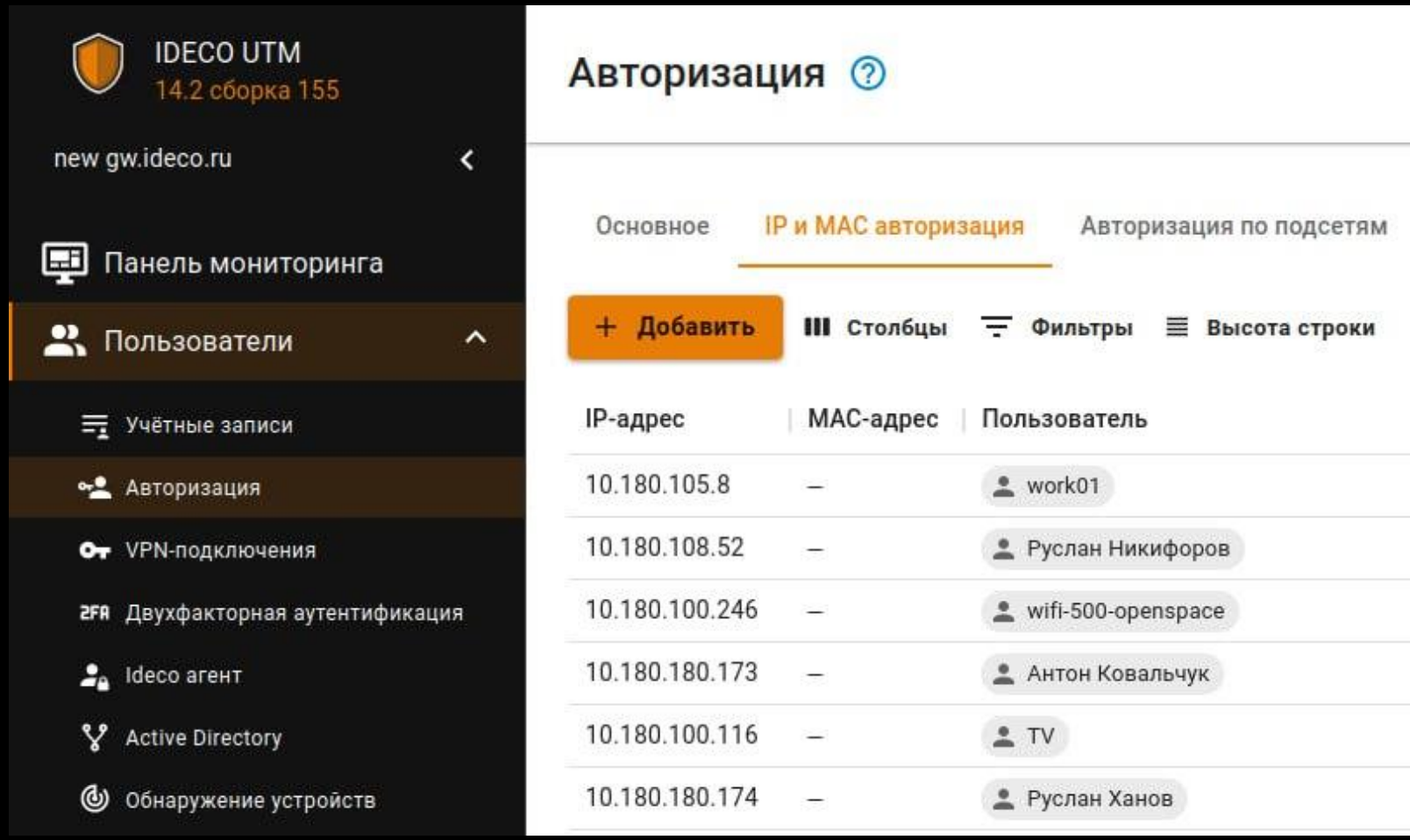
ideco

Пользователи

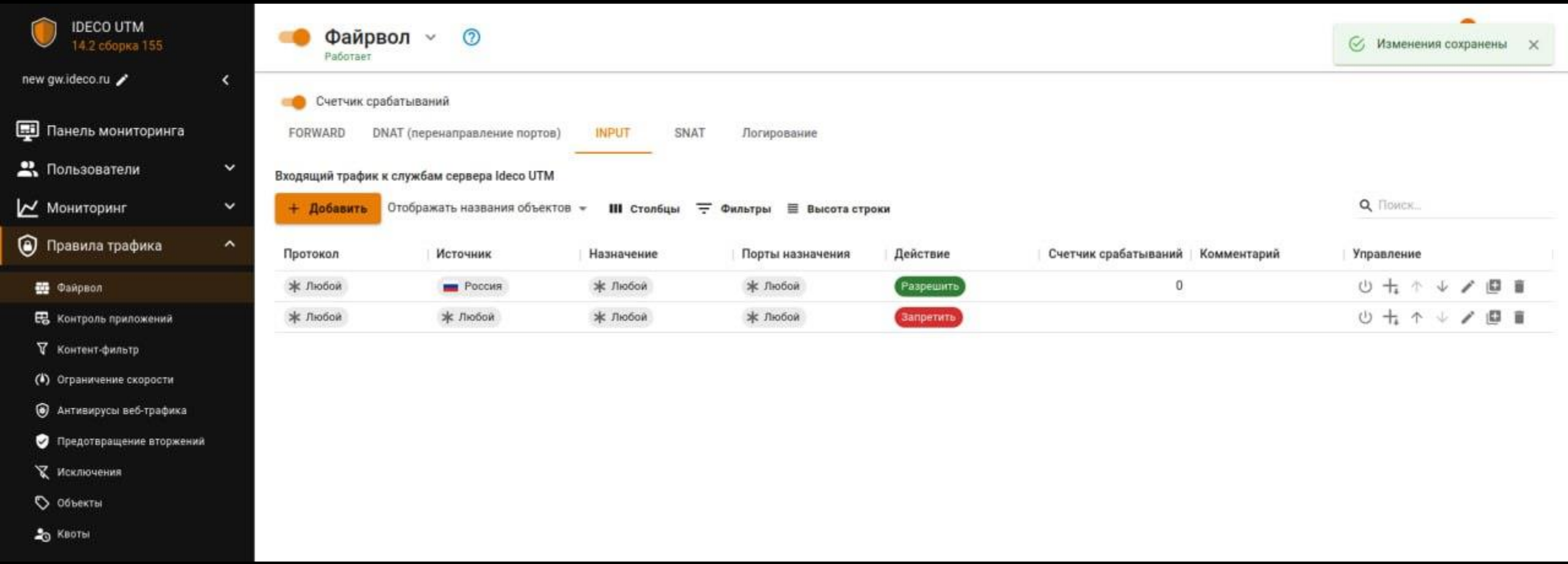


Авторизация

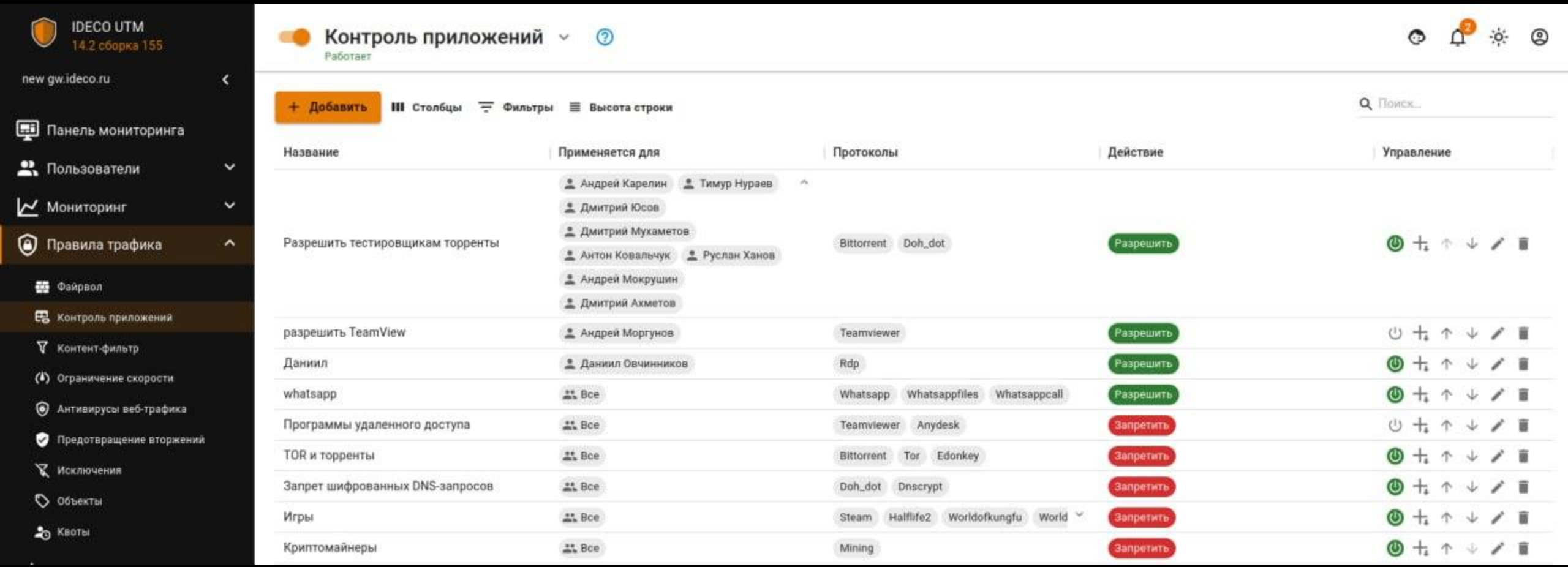
- IP, MAC, IP+MAC, подсеть
- WEB
- Интеграция с AD: Kerberos, NTLM, security log
- Агент
- Обнаружение устройств



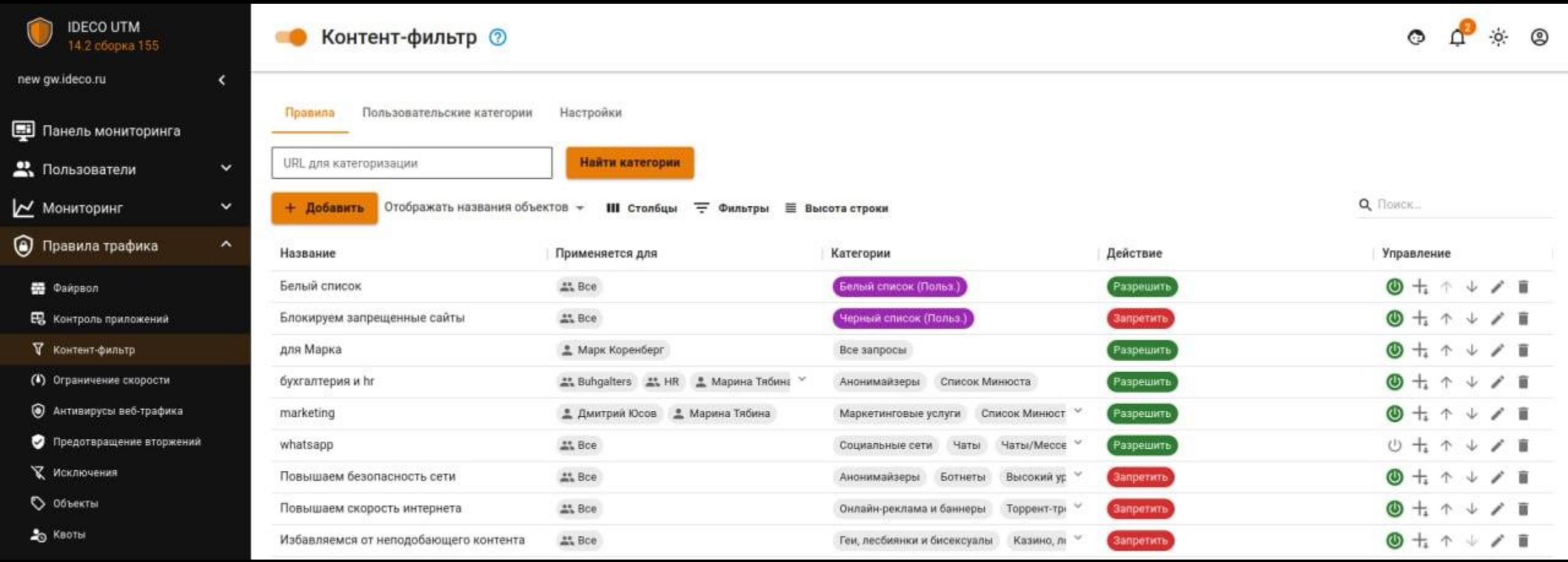
Файрвол


IDECO UTM
14.2 сборка 155
new gw.ideco.ru
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Файрвол
Контроль приложений
Контент-фильтр
Ограничение скорости
Антивирусы веб-трафика
Предотвращение вторжений
Исключения
Объекты
Квоты
Файрвол
Работает
Изменения сохранены
Счетчик срабатываний
FORWARD
DNAT (перенаправление портов)
INPUT
SNAT
Логирование
Входящий трафик к службам сервера Ideco UTM
Добавить
Отображать названия объектов
Столбцы
Фильтры
Высота строки
Поиск...
Протокол
Источник
Назначение
Порты назначения
Действие
Счетчик срабатываний
Комментарий
Управление
Любой
Россия
Любой
Любой
Разрешить
0
Любой
Любой
Любой
Любой
Запретить

Контроль приложений



Контент-фильтр

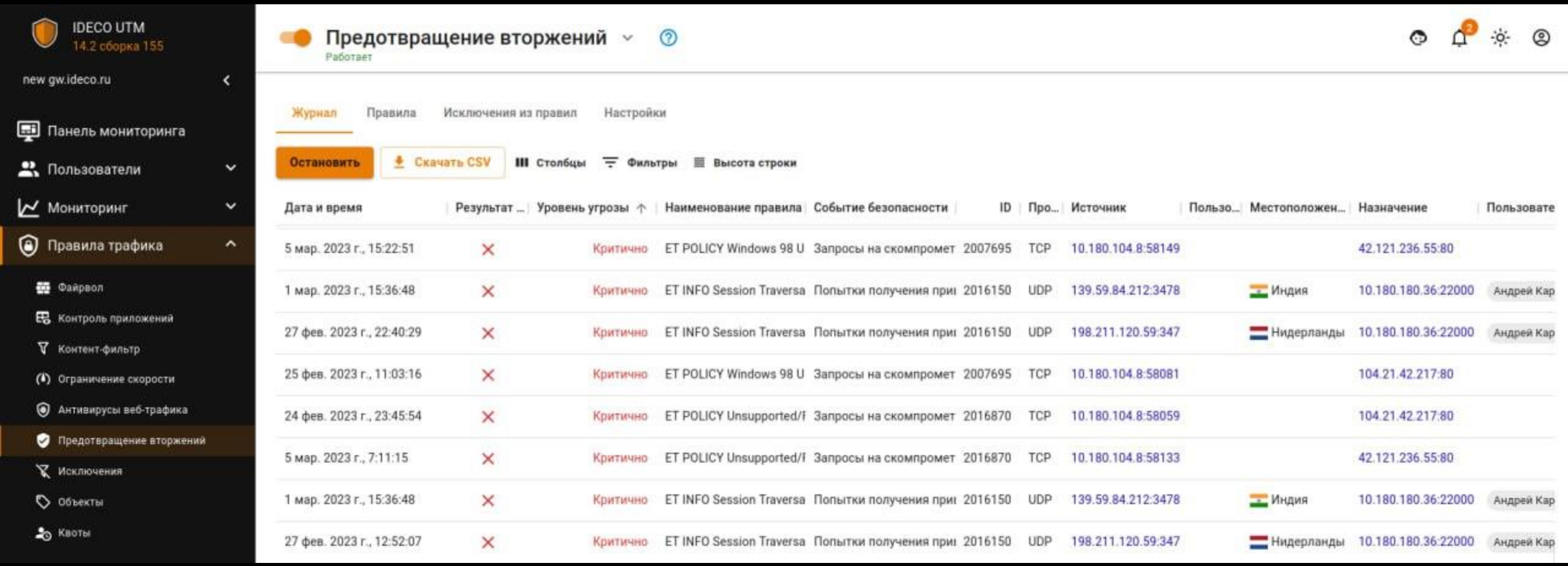


Контент-фильтр

- Технологический партнер: российская компания SkyDNS
- Более 100 миллионов доменов и 500 миллионов URL в базе
- SNI / SSL BUMP
- Возможность создания своих списков
- Возможность блокировки приложений (80 и 443)
- Безопасный поиск
- Антивирусная проверка WEB трафика
- Блокировка quic/http3
- Гибкая настройка политик
- Обновление сигнатур 2 раза в день с серверов в РФ

ideco

Предотвращение вторжений



ideco

Предотвращение вторжений

- 25 000 сигнатур в 60 категориях правил
- Обновление раз в 4 часа с серверов в РФ
- Блокировка по Geo-IP
- Блокировка обновлений ПО и устаревшего ПО
- Экспорт журнала в CSV

ideco

Сервисы

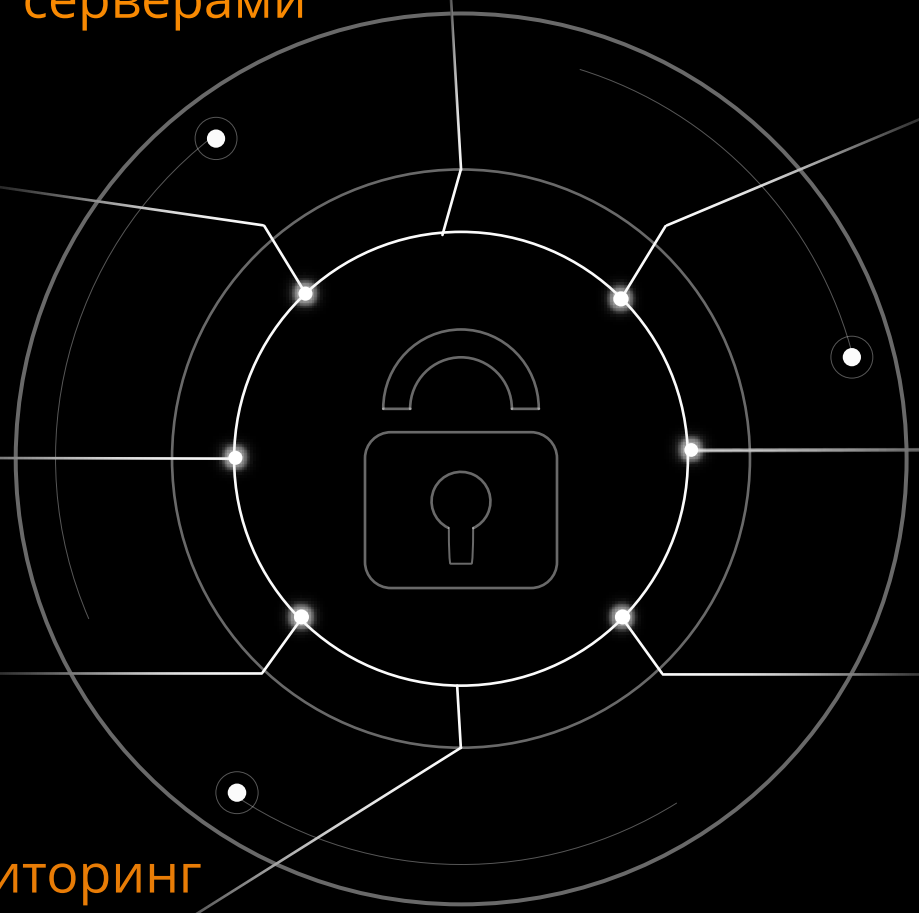
Центральная консоль управления несколькими серверами

Трафик
Балансировка канала
Резервирование канала
Квоты
Шейпинг

Маршрутизация
Статическая
Динамическая OSPF, BGP

DNS, DHCP, NTP

Мониторинг
Телеграм бот
Zabbix Агент
Syslog, SNMP



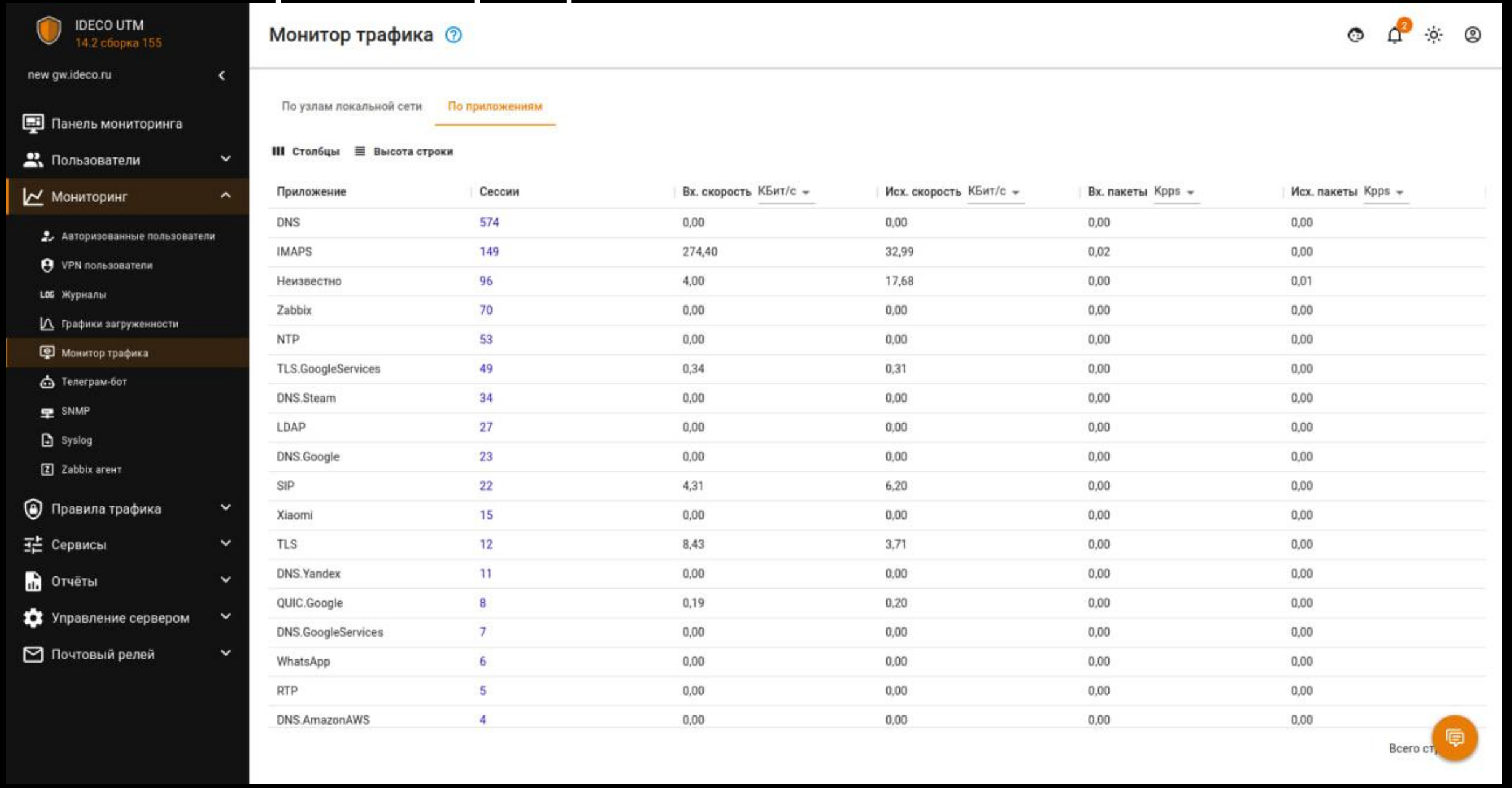
VPN
- Site-To-Site IPsec
- IKEv2
- SSTP
- Wireguard (клиент)
- L2TP/IPSec

Отказоустойчивость:
- Кластеризация Active/Passive
- Резервное копирование
- Программный Watchdog

Обратный прокси
- Публикация WEB приложений
- Публикация OWA Exchange
- WAF

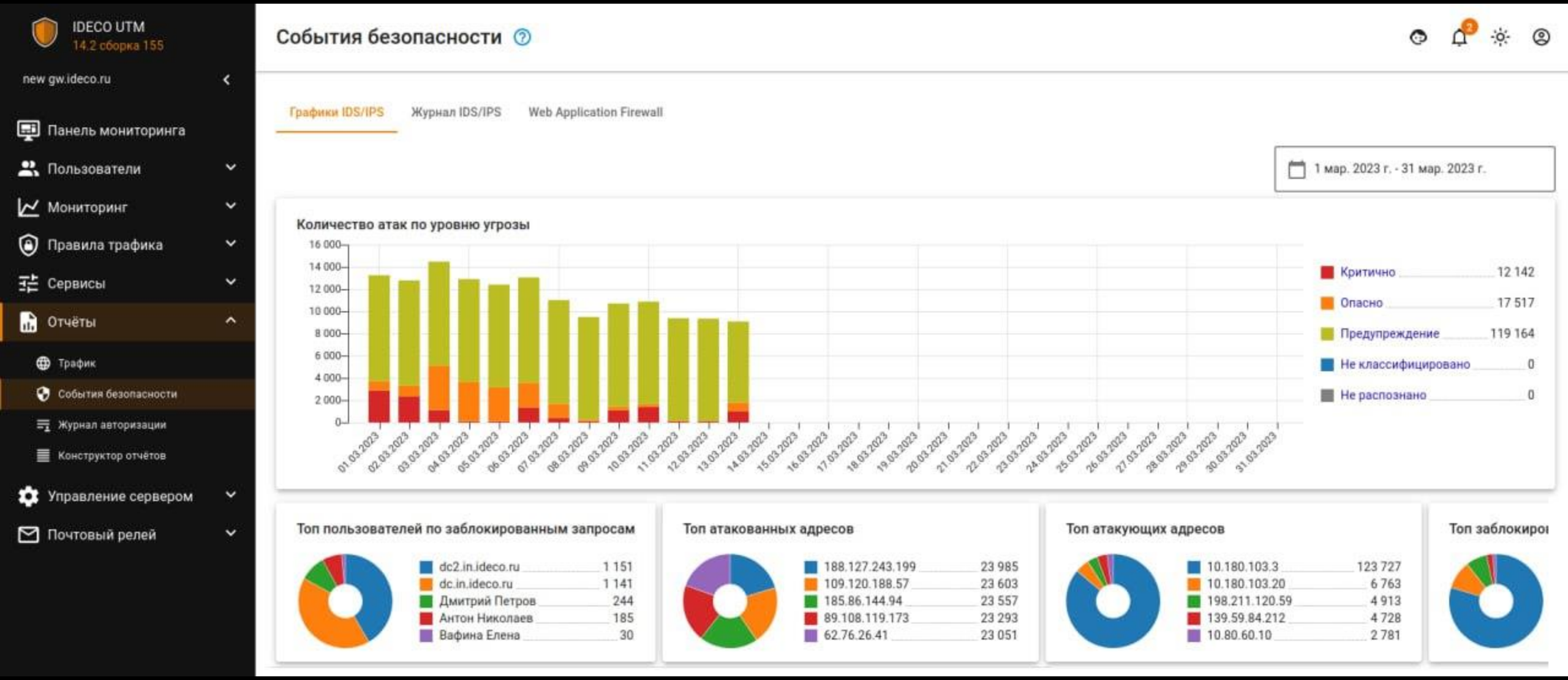
ideco

Мониторинг трафика

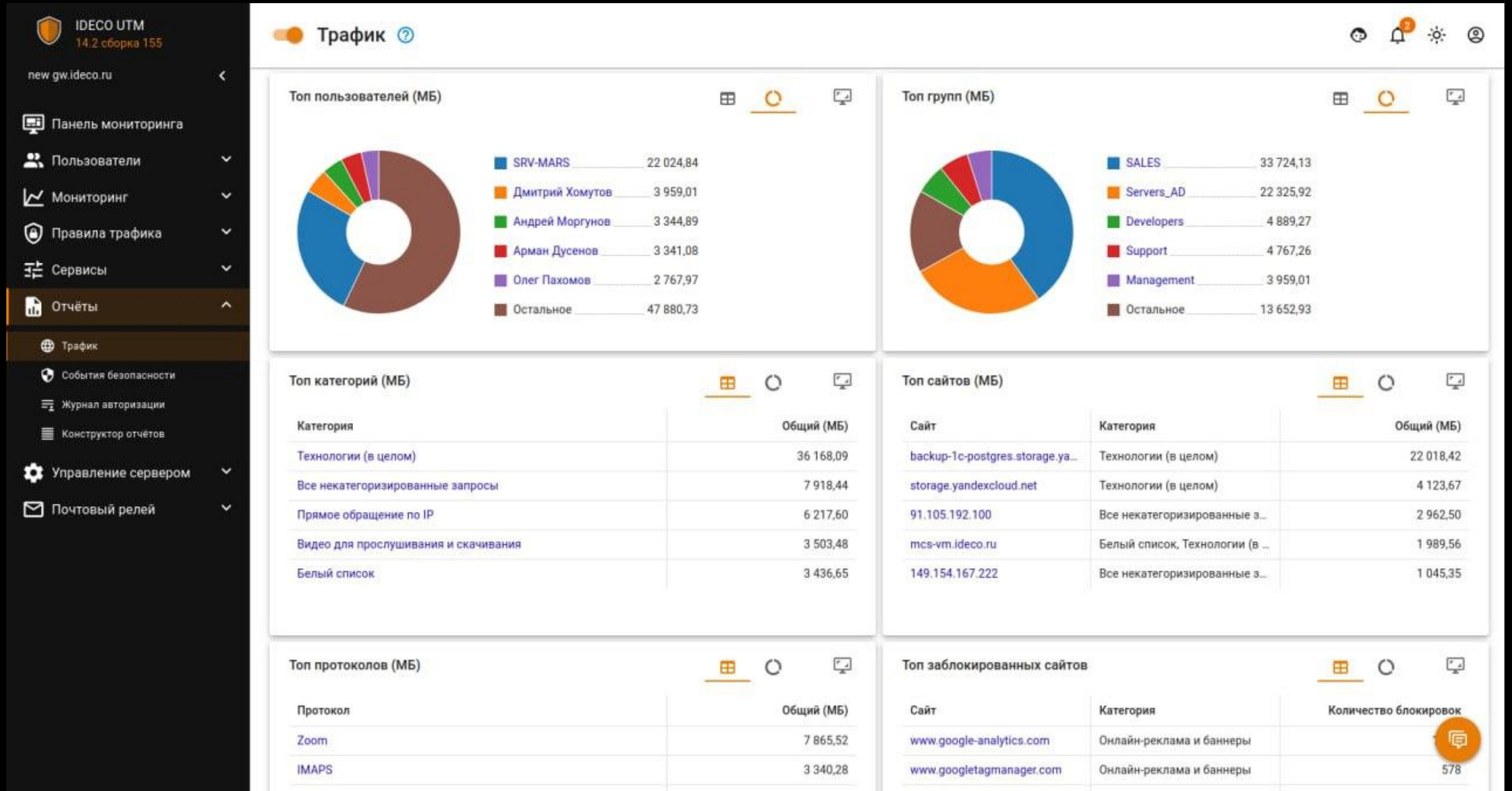


Приложение	Сессии	Вх. скорость КБит/с	Исх. скорость КБит/с	Вх. пакеты Kpps	Исх. пакеты Kpps
DNS	574	0,00	0,00	0,00	0,00
IMAPS	149	274,40	32,99	0,02	0,00
Неизвестно	96	4,00	17,68	0,00	0,01
Zabbix	70	0,00	0,00	0,00	0,00
NTP	53	0,00	0,00	0,00	0,00
TLS.GoogleServices	49	0,34	0,31	0,00	0,00
DNS.Steam	34	0,00	0,00	0,00	0,00
LDAP	27	0,00	0,00	0,00	0,00
DNS.Google	23	0,00	0,00	0,00	0,00
SIP	22	4,31	6,20	0,00	0,00
Xiaomi	15	0,00	0,00	0,00	0,00
TLS	12	8,43	3,71	0,00	0,00
DNS.Yandex	11	0,00	0,00	0,00	0,00
QUIC.Google	8	0,19	0,20	0,00	0,00
DNS.GoogleServices	7	0,00	0,00	0,00	0,00
WhatsApp	6	0,00	0,00	0,00	0,00
RTP	5	0,00	0,00	0,00	0,00
DNS.AmazonAWS	4	0,00	0,00	0,00	0,00

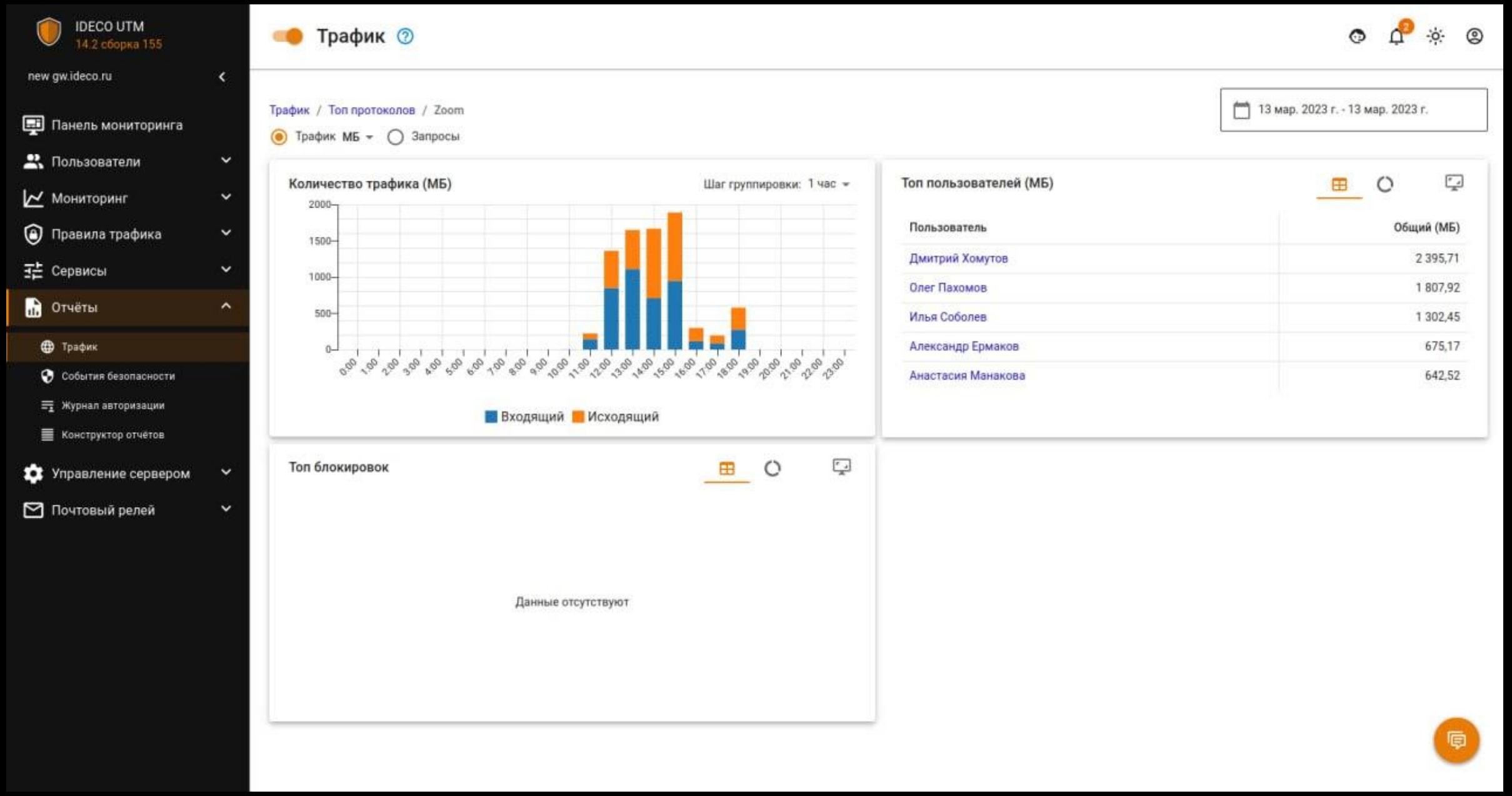
События безопасности



Отчетность в различных разрезах

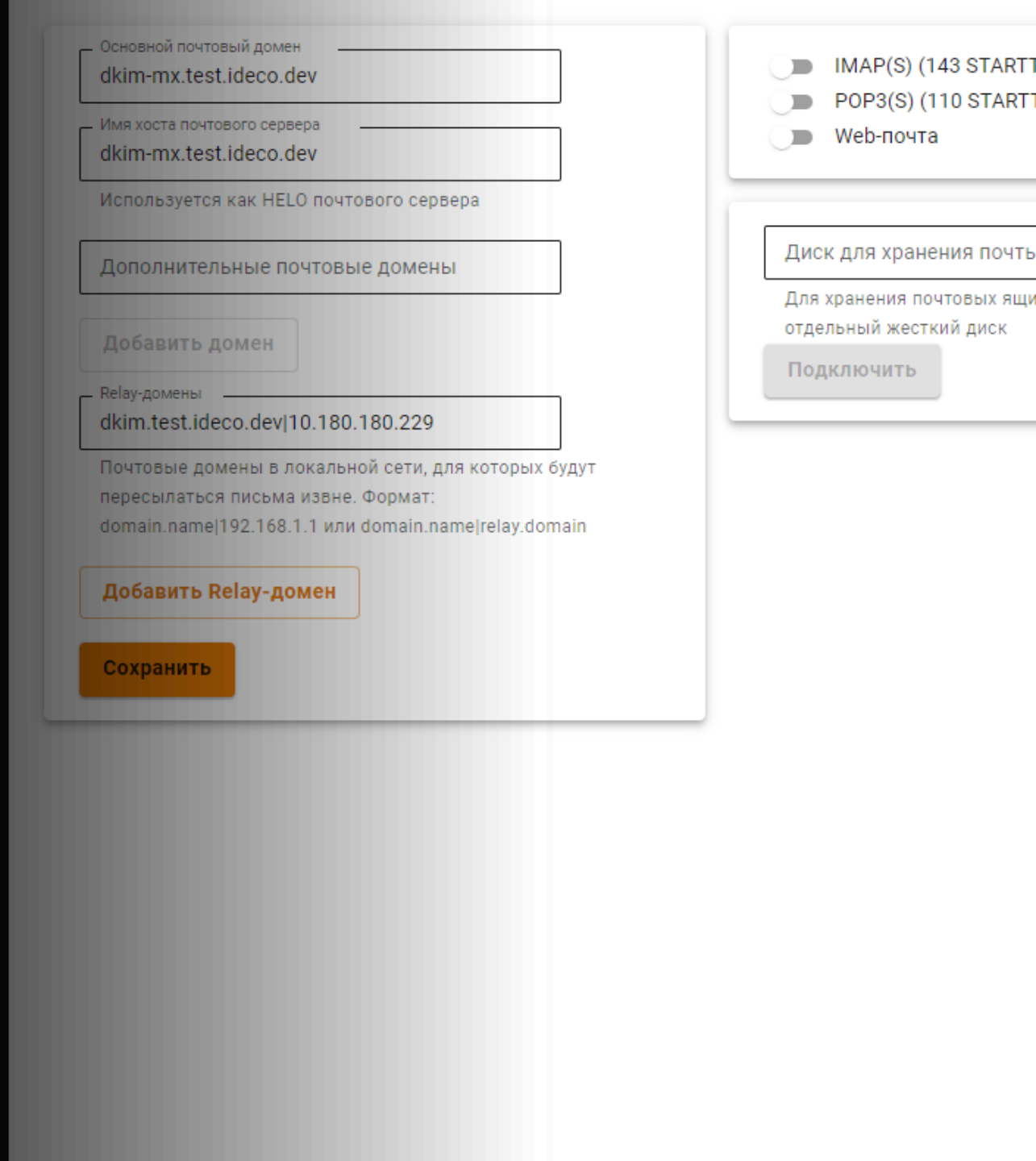


Пример детализации по протоколу



ideco

Почтовый сервер/релей



Переход с конкурентных решений

- Kerio Control
- Устаревшие решения под Windows: Microsoft ISA/TMG, UG Proxy and Firewall, Traffic Inspector
- Различные российские решения
- L3 FW
- Cisco ASA/WSA, Checkpoint, Fortinet – здесь сложнее, но активно догоняем
- Переход с самописных шлюзовых и прокси решений на Linux/FreeBSD

ideco

Customer success

Гибкая разработка

Моментальная реакция на новые вызовы и угрозы
Road-map по задачам пользователей

Защита сети «из коробки»

Преднастроенные правила фильтрации, IPS, FW

Шай-тек (Shy-tech)

Умные технологии для интуитивно понятных решений

Многоканальная техподдержка

-портал поддержки help.ideco.ru
-электронная почта
-телефон
-Telegram
-чат в продукте

Customer success

Выделенный менеджер для каждого
Фокус на долгосрочное партнерство
CustDev и проблемные интервью
Близко к community

Presale

Поддержка и консультации на этапе тестирования и внедрения
Решения для нестандартных кейсов

ideco

ideco

Спасибо!

@rasmusowlson

a.karmanov@ideco.ru

t.me/idecoutm

@ideco