Отечественное решение для защиты сети и фильтрации трафика

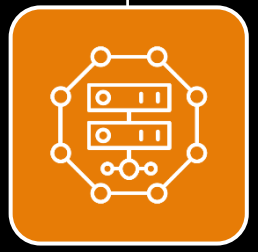
Данила Анисимов

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

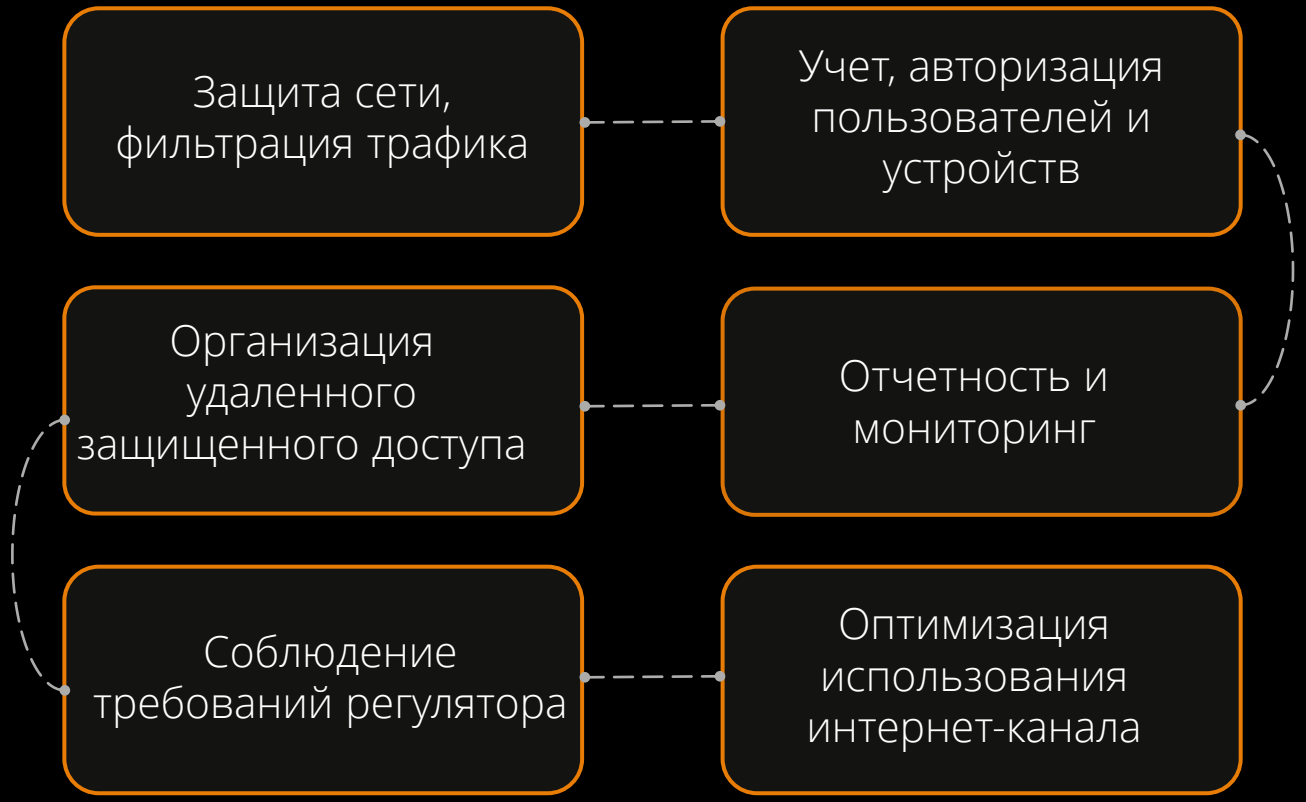
2 000 бесплатных лицензий для некоммерческого использования

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

Панель мониторинга

Время работы сервера ..... 14 минут

Управление модулями фильтрации

- Файрвол
- Контент-фильтр
- Контроль приложений
- Предотвращение вторжений
- Антивирусы веб-трафика
- Ограничение скорости

Лицензия

Номер лицензии UTM-1674589506

Окончание лицензии ..... через 20 лет

Окончание обновлений ..... через 7 месяцев, 24 марта 2023 г.

Окончание технической поддержки ..... через 7 месяцев, 24 марта 2023 г.

Количество пользователей ..... 34 из 500

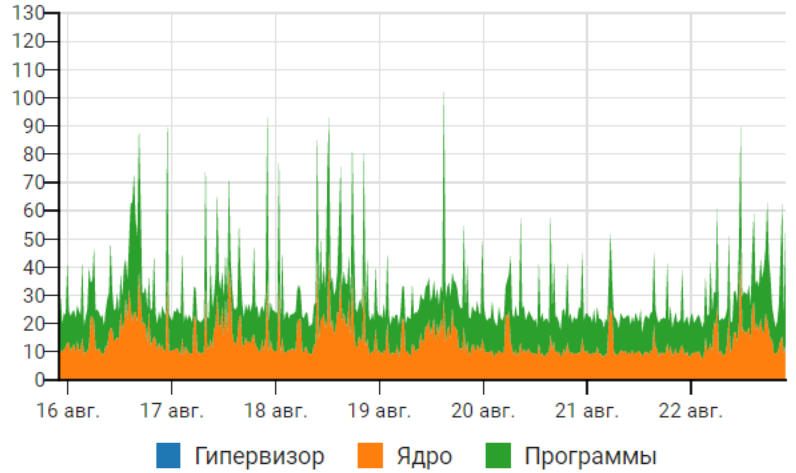
Информация о модулях:

Антивирус Касперского для веб- ..... 53 года назад (не используется)

Загрузка процессора, %

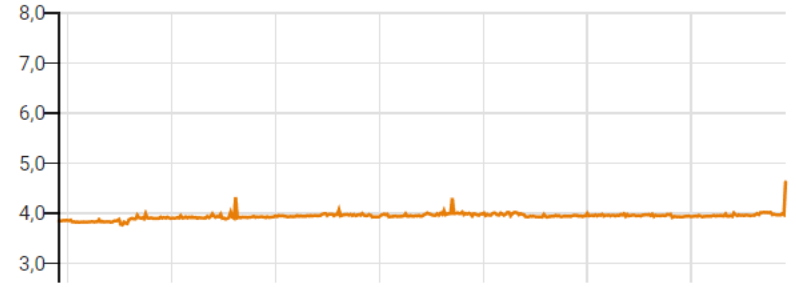
7 дней

Пиковое значение загрузки для одного ядра 100%. Например, при восьми ядрах максимальная загрузка 800%.



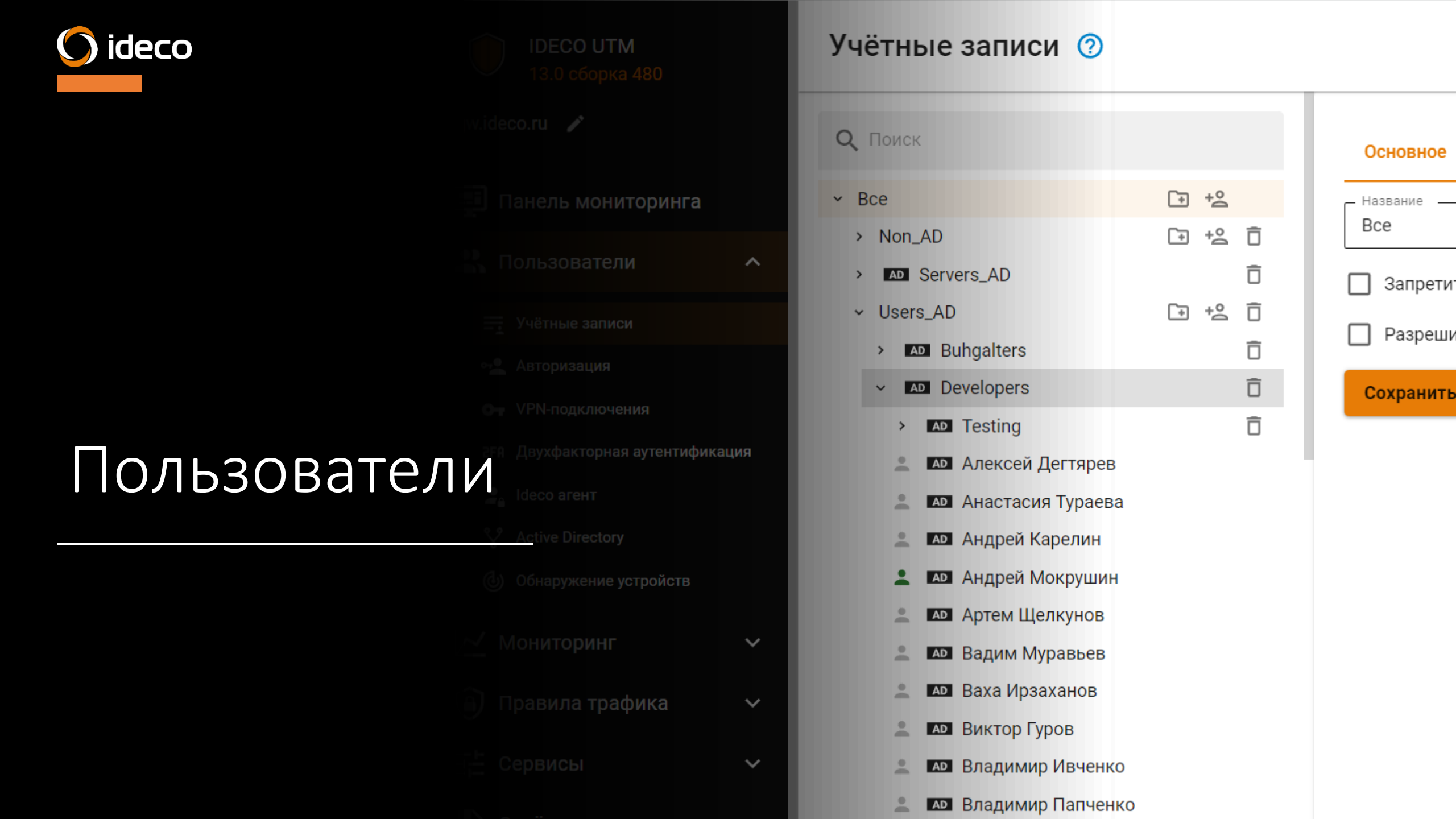
Занятая оперативная память, ГБ

7 дней



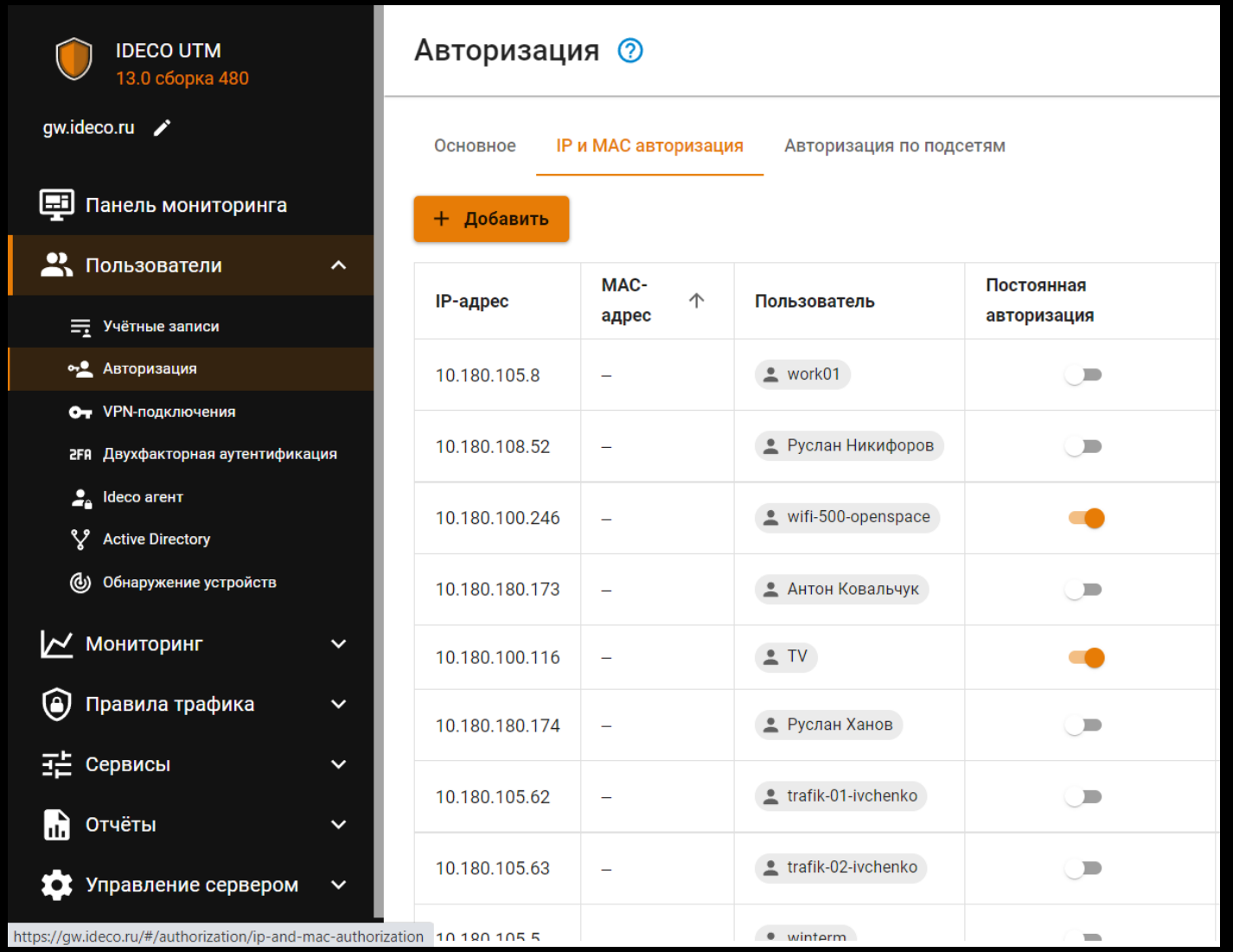
ideco

Пользователи

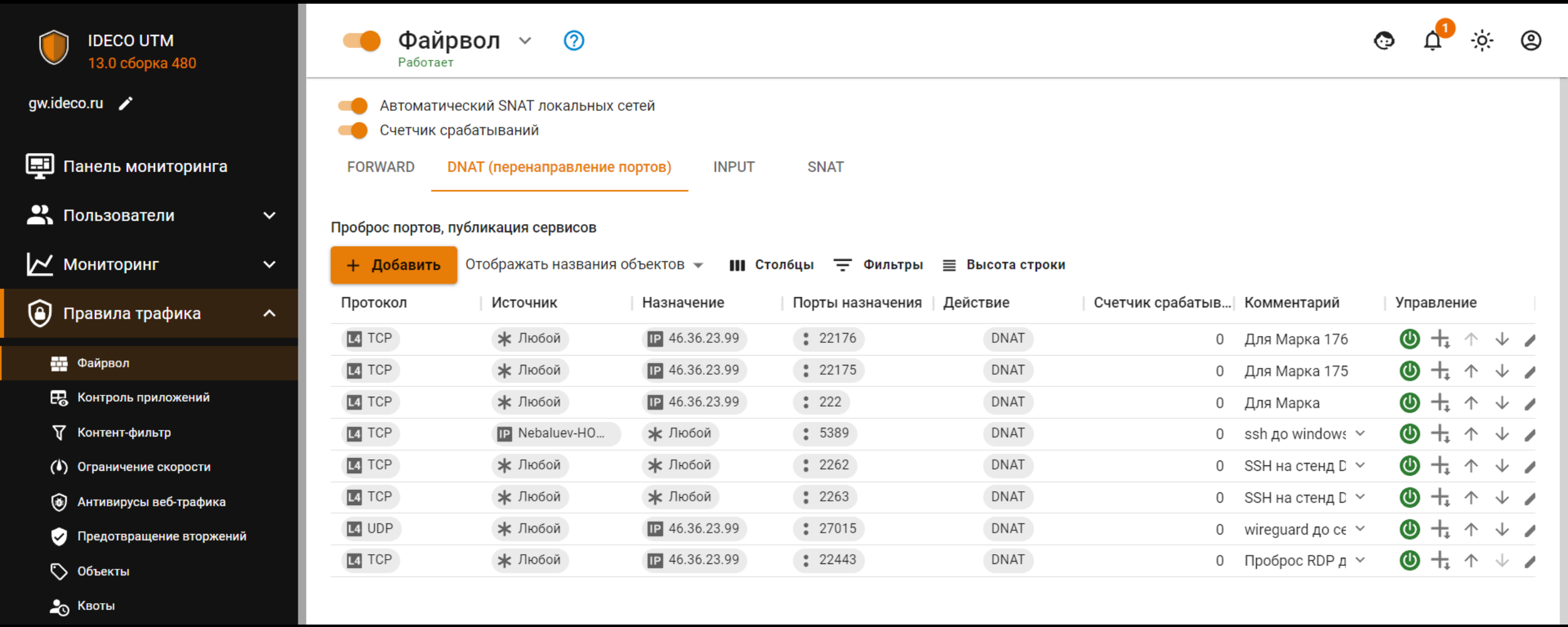


Авторизация

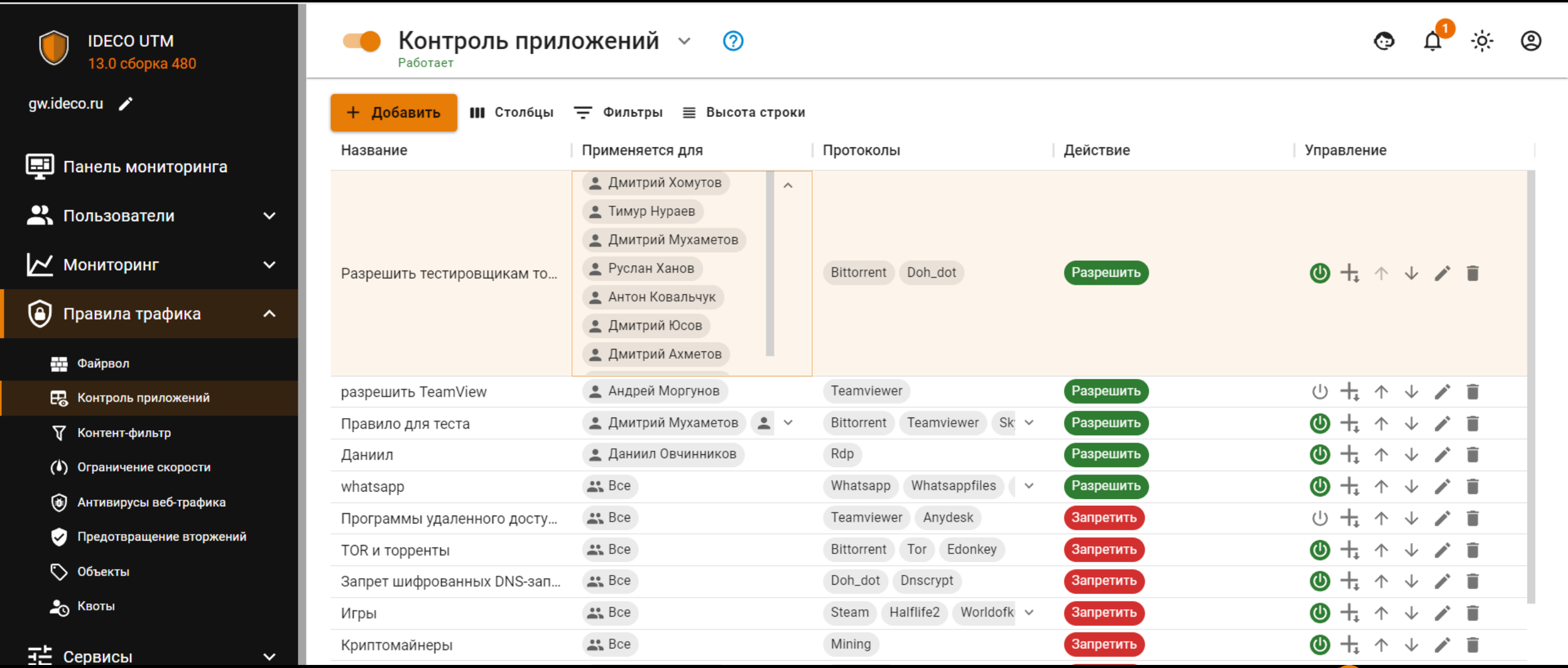
- IP, MAC, IP+MAC, подсеть
- WEB
- Интеграция с AD: Kerberos, NTLM, security log
- Агент
- Обнаружение устройств



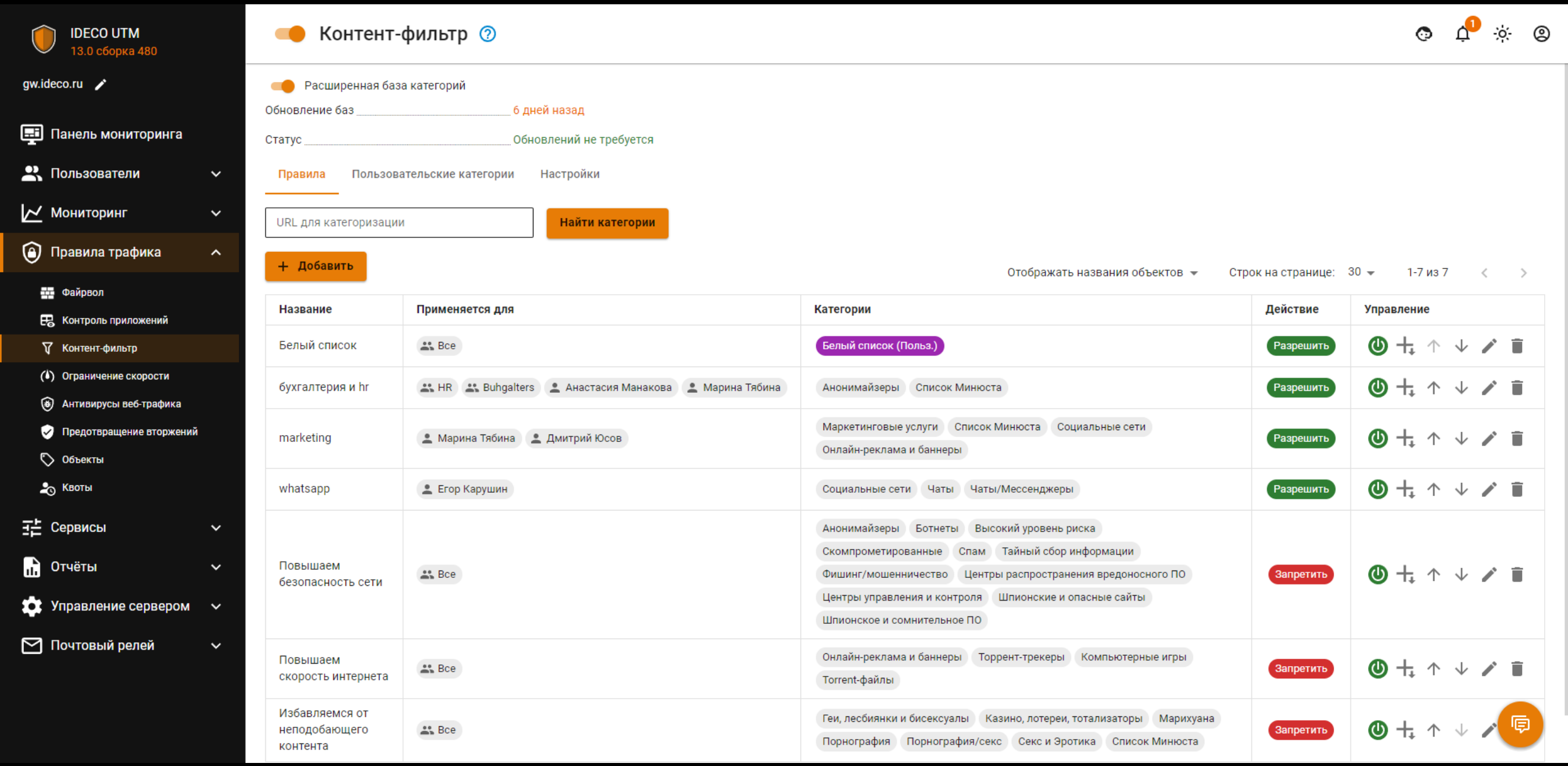
Файрвол


IDECO UTM
13.0 сборка 480
gw.ideco.ru
Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Файрвол
Контроль приложений
Контент-фильтр
Ограничение скорости
Антивирусы веб-трафика
Предотвращение вторжений
Объекты
Квоты
Файрвол
Работает
Автоматический SNAT локальных сетей
Счетчик срабатываний
FORWARD
DNAT (перенаправление портов)
INPUT
SNAT
Проброс портов, публикация сервисов
Добавить
Отображать названия объектов
Столбцы
Фильтры
Высота строки
Протокол
Источник
Назначение
Порты назначения
Действие
Счетчик срабатыв...
Комментарий
Управление
TCP Любой 46.36.23.99 22176 DNAT 0 Для Марка 176
TCP Любой 46.36.23.99 22175 DNAT 0 Для Марка 175
TCP Любой 46.36.23.99 222 DNAT 0 Для Марка
TCP Nebaluev-HO... Любой 5389 DNAT 0 ssh до windows
TCP Любой Любой 2262 DNAT 0 SSH на стенд D
TCP Любой Любой 2263 DNAT 0 SSH на стенд D
UDP Любой 46.36.23.99 27015 DNAT 0 wireguard до се
TCP Любой 46.36.23.99 22443 DNAT 0 Проброс RDP д

Контроль приложений



Контент-фильтр



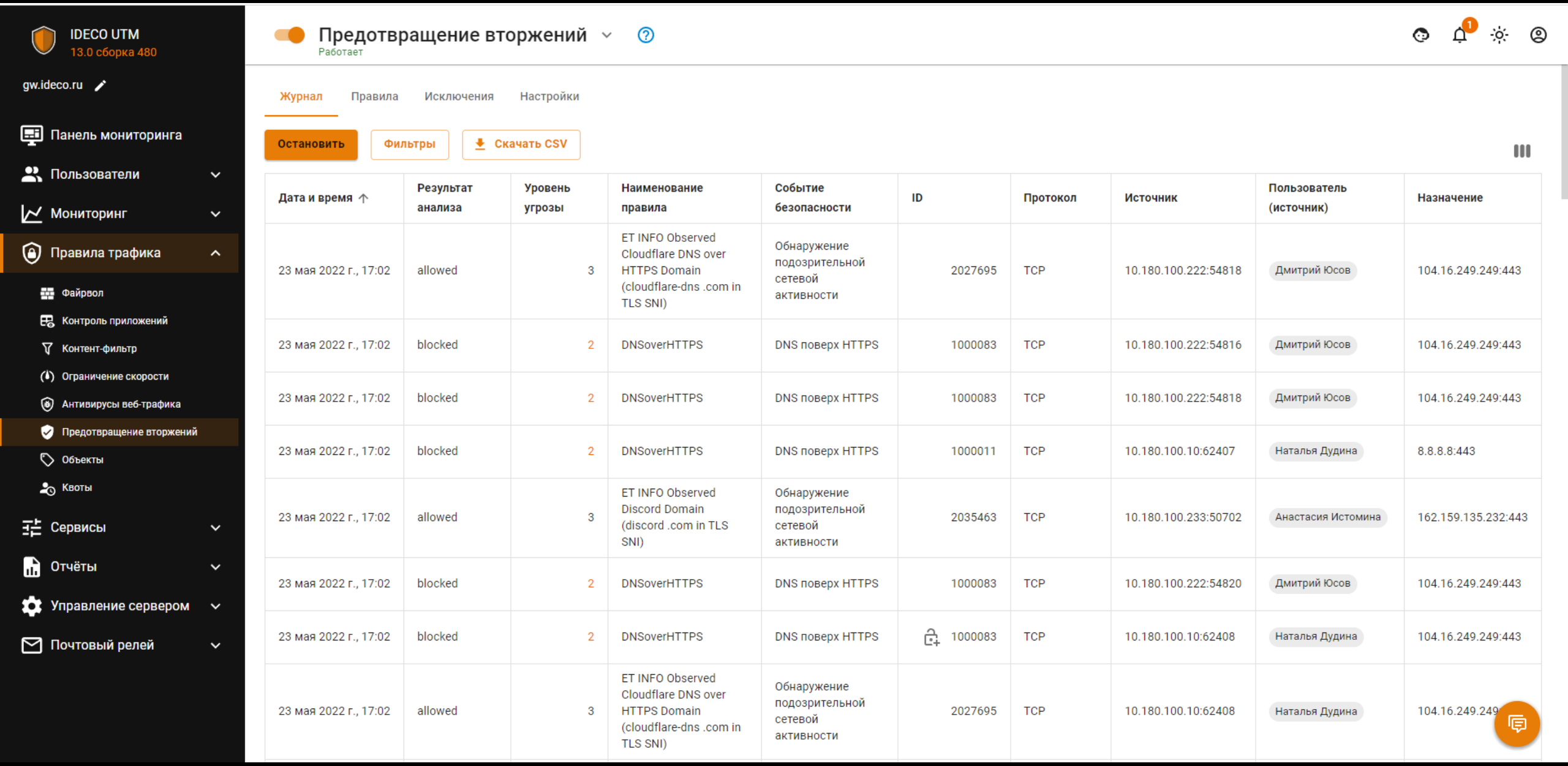
Название	Применяется для	Категории	Действие	Управление
Белый список	Все	Белый список (Польз.)	Разрешить	
бухгалтерия и hr	HR, Buhgalters, Анастасия Манакова, Марина Тябина	Анонимайзеры, Список Минюста	Разрешить	
marketing	Марина Тябина, Дмитрий Юсов	Маркетинговые услуги, Список Минюста, Социальные сети, Онлайн-реклама и баннеры	Разрешить	
whatsapp	Егор Карушин	Социальные сети, Чаты, Чаты/Мессенджеры	Разрешить	
Повышаем безопасность сети	Все	Анонимайзеры, Ботнеты, Высокий уровень риска, Скомпрометированные, Спам, Тайный сбор информации, Фишинг/мошенничество, Центры распространения вредоносного ПО, Центры управления и контроля, Шпионские и опасные сайты, Шпионское и сомнительное ПО	Запретить	
Повышаем скорость интернета	Все	Онлайн-реклама и баннеры, Торрент-трекеры, Компьютерные игры, Torrent-файлы	Запретить	
Избавляемся от неподобающего контента	Все	Геи, лесбиянки и бисексуалы, Казино, лотереи, тотализаторы, Марихуана, Порнография, Порнография/секс, Секс и Эротика, Список Минюста	Запретить	

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



Дата и время	Результат анализа	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	Источник	Пользователь (источник)	Назначение
23 мая 2022 г., 17:02	allowed	3	ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)	Обнаружение подозрительной сетевой активности	2027695	TCP	10.180.100.222:54818	Дмитрий Юсов	104.16.249.249:443
23 мая 2022 г., 17:02	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000083	TCP	10.180.100.222:54816	Дмитрий Юсов	104.16.249.249:443
23 мая 2022 г., 17:02	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000083	TCP	10.180.100.222:54818	Дмитрий Юсов	104.16.249.249:443
23 мая 2022 г., 17:02	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000011	TCP	10.180.100.10:62407	Наталья Дудина	8.8.8.8:443
23 мая 2022 г., 17:02	allowed	3	ET INFO Observed Discord Domain (discord .com in TLS SNI)	Обнаружение подозрительной сетевой активности	2035463	TCP	10.180.100.233:50702	Анастасия Истомина	162.159.135.232:443
23 мая 2022 г., 17:02	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000083	TCP	10.180.100.222:54820	Дмитрий Юсов	104.16.249.249:443
23 мая 2022 г., 17:02	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000083	TCP	10.180.100.10:62408	Наталья Дудина	104.16.249.249:443
23 мая 2022 г., 17:02	allowed	3	ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)	Обнаружение подозрительной сетевой активности	2027695	TCP	10.180.100.10:62408	Наталья Дудина	104.16.249.249

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

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

Трафик
Балансировка канала
Резервирование канала
Квоты
Шейпинг

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

Маршрутизация
Статическая
Динамическая OSPF, BGP

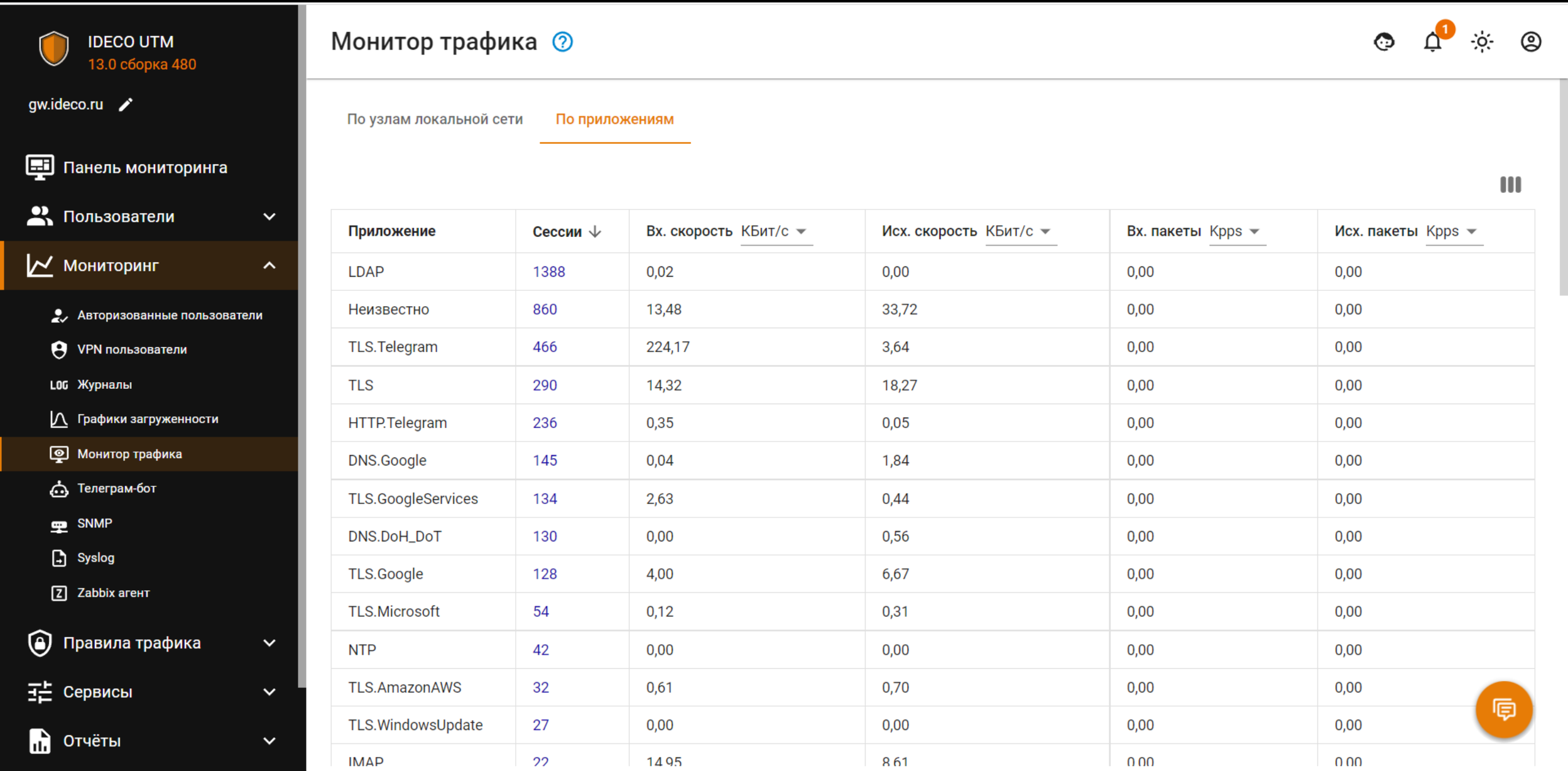
DNS, DHCP, NTP

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

Мониторинг
Телеграм бот
Zabbix Агент
Syslog, SNMP

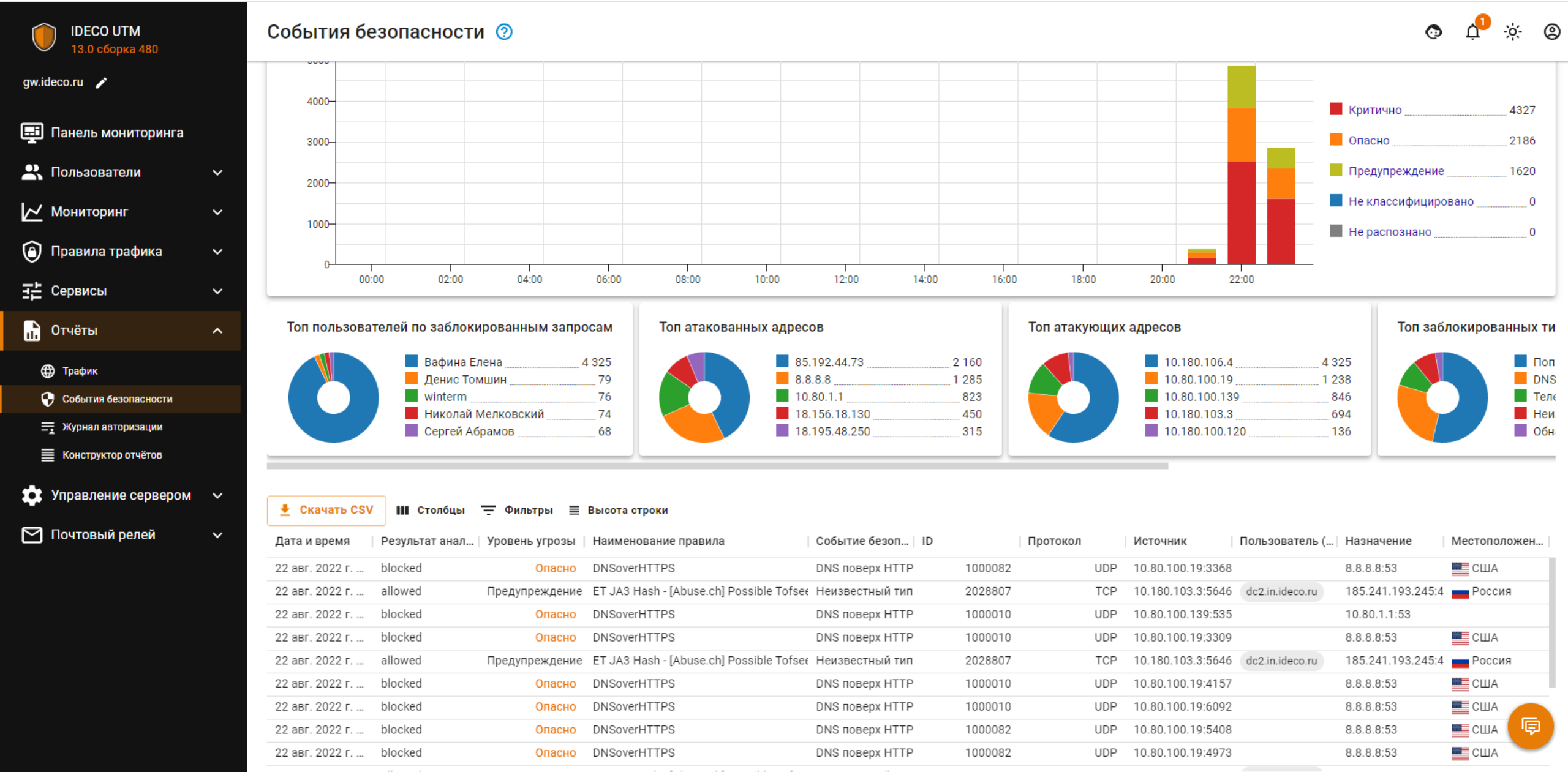
ideco

Мониторинг трафика

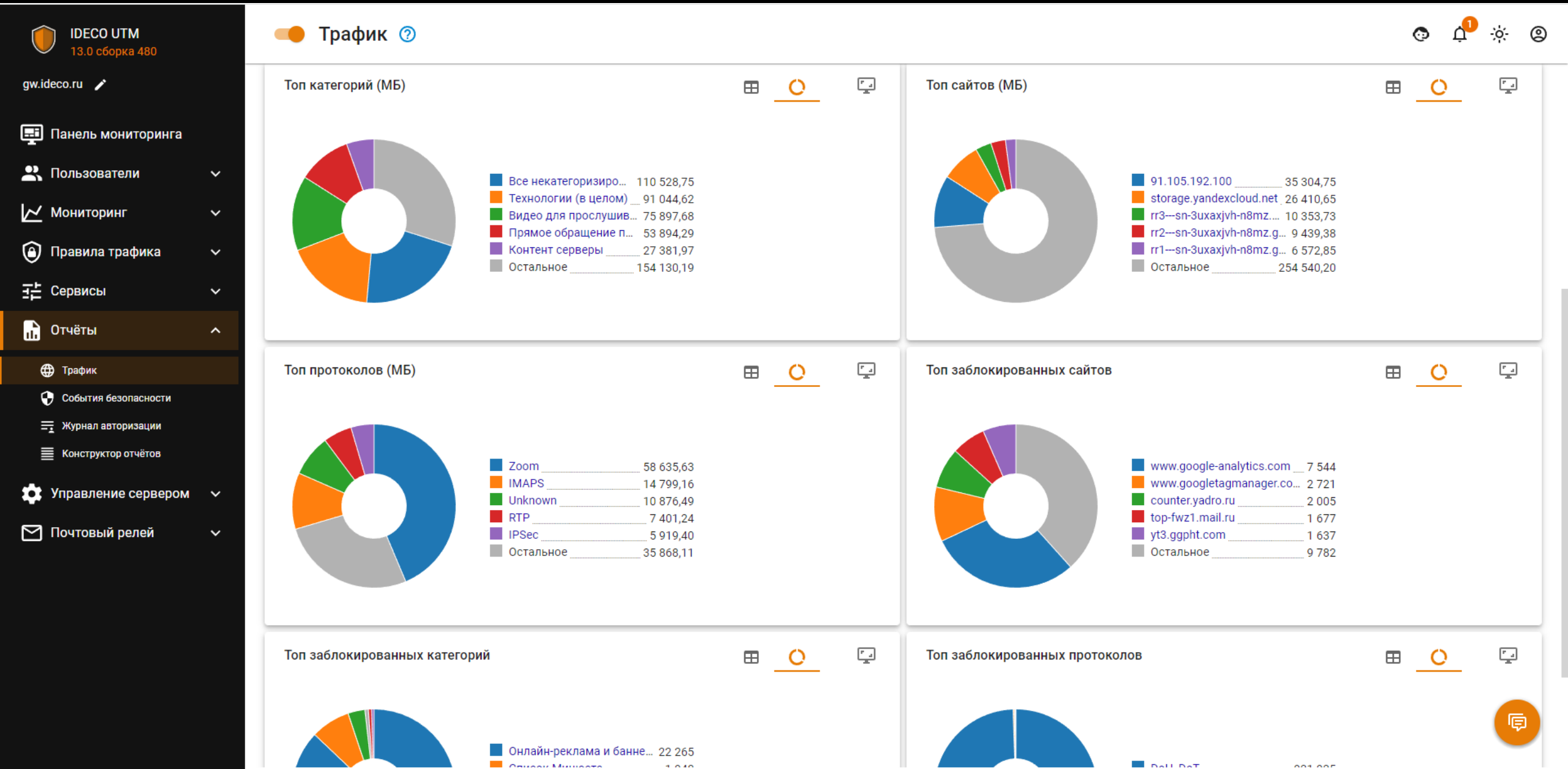


Приложение	Сессии	Вх. скорость КБит/с	Исх. скорость КБит/с	Вх. пакеты Kpps	Исх. пакеты Kpps
LDAP	1388	0,02	0,00	0,00	0,00
Неизвестно	860	13,48	33,72	0,00	0,00
TLS.Telegram	466	224,17	3,64	0,00	0,00
TLS	290	14,32	18,27	0,00	0,00
HTTP.Telegram	236	0,35	0,05	0,00	0,00
DNS.Google	145	0,04	1,84	0,00	0,00
TLS.GoogleServices	134	2,63	0,44	0,00	0,00
DNS.DoH_DoT	130	0,00	0,56	0,00	0,00
TLS.Google	128	4,00	6,67	0,00	0,00
TLS.Microsoft	54	0,12	0,31	0,00	0,00
NTP	42	0,00	0,00	0,00	0,00
TLS.AmazonAWS	32	0,61	0,70	0,00	0,00
TLS.WindowsUpdate	27	0,00	0,00	0,00	0,00
IMAP	22	14,95	8,61	0,00	0,00

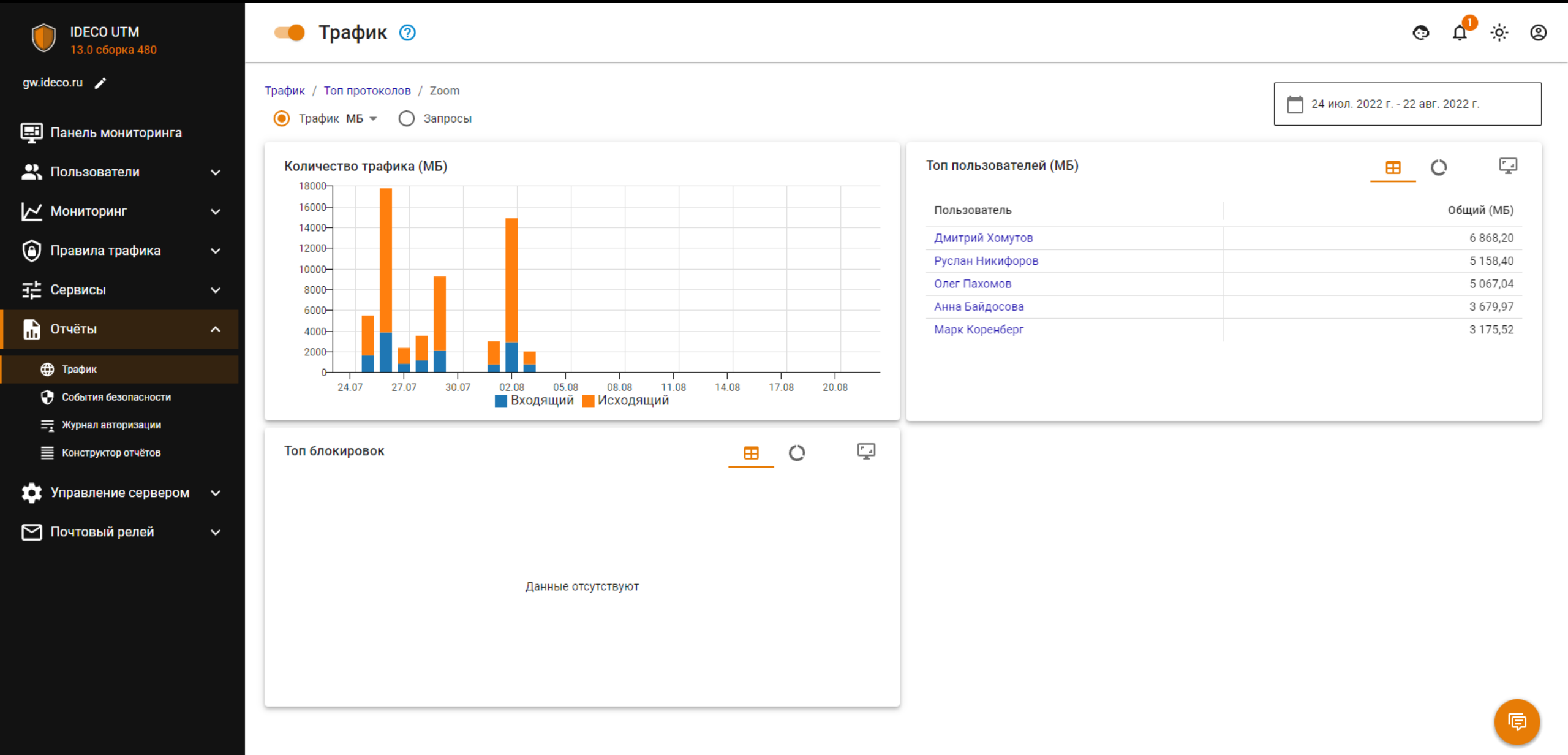
События безопасности



Отчетность в различных разрезах

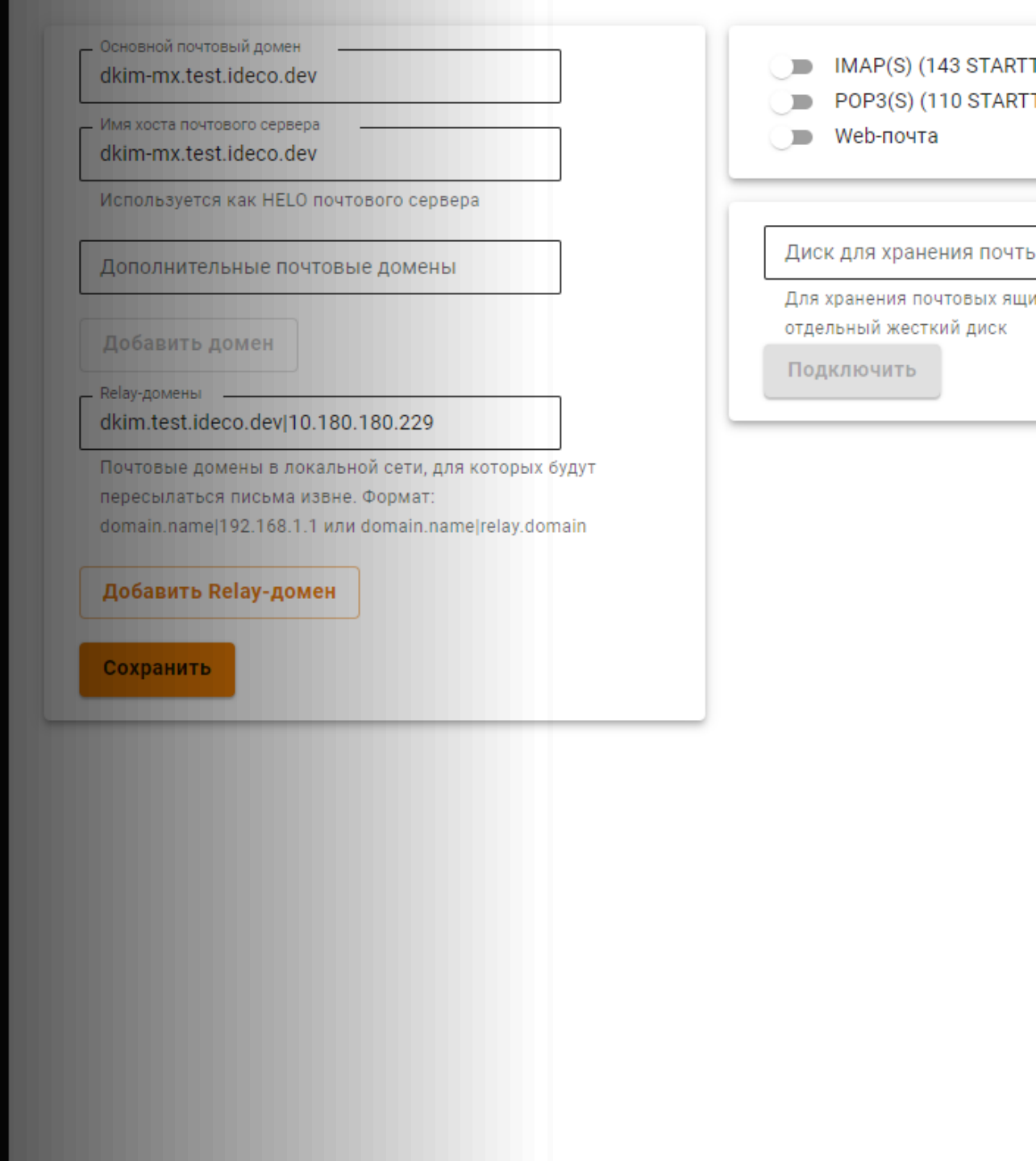


Пример детализации по протоколу



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!

@Dvanisimov

d.anisimov@ideco.ru

t.me/idecoutm

@ideco