ideco

16.02.2023 11:15 МСК

ВЫБОР РОССИЙСКОГО NGFW

НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ ПРИ МИГРАЦИИ

Дмитрий Хомутов
Директор «Айдеко»

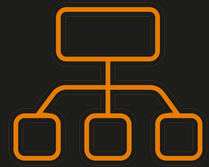
Айдеко

Помогаем клиентам защититься от современных угроз безопасности, средствами удобного межсетевого экрана Ideco UTM.

Экономим ваше время на настройке интернет-шлюза и отражения кибератак.

Более 3 000 компаний
используют Ideco UTM

120 человек в команде
S&M / R&D



Лидер по скорости
разработки в отрасли

* сертификат ФСТЭК А4/Б4, СОВ 4, УД 4, в реестре Минцифры


ideco

Ideco UTM

Фильтрация трафика L7
МЭ, СОВ, Контроль приложений,
Контент-фильтр

Сетевые службы
DNS, DHCP, NTP, балансировка и
резервирование канала, квоты,
шейпер трафика

Маршрутизация
Статическая
Динамическая OSPF, BGP

Управление
Веб-интерфейс, ssh,
центральная консоль

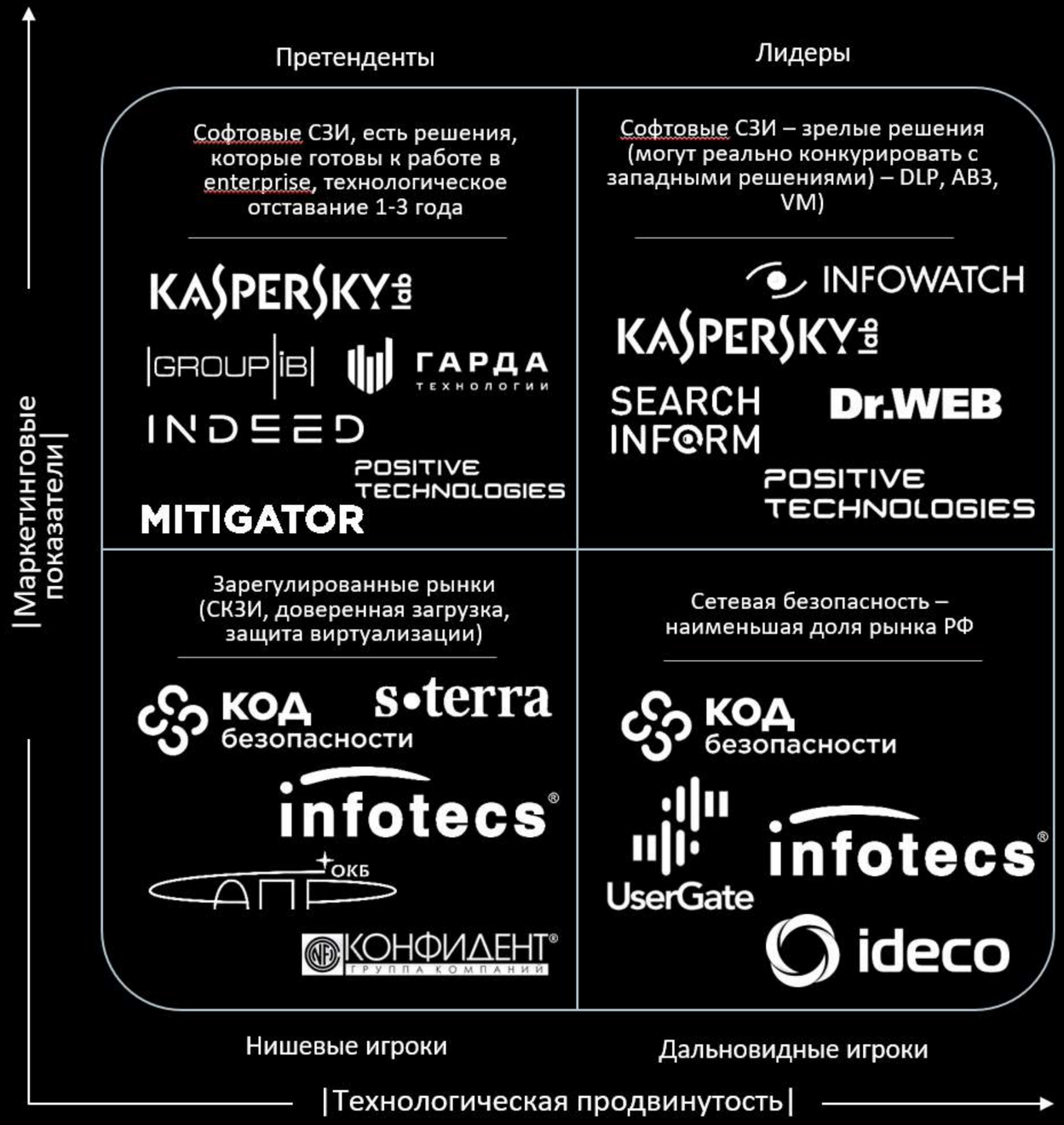
Мониторинг и отчетность
Телеграм бот, Zabbix Агент,
Syslog, SNMP, SIEM
Отчетность по пользователям

Пользователи
- Интеграция с LDAP
- Локальная база пользователей
- Авторизация (IP, MAC, Kerberos, Web, Агент, подсеть)
- Пользователи и группы как объекты в политиках фильтрации

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

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

ideco



Структура рынка. Гартнер по-русски

Сетевая безопасность

Наиболее проблемный, но в то же время наиболее востребованный сегмент СЗИ

Решение с «отсутствием» аналогов

NAC, безопасный Wi-Fi, MDM, безопасность в облаках, но есть рынки Латинской Америки, Индии, Китая

Главный тренд - резкое повышение спроса на ресурсы и компетенции интеграторов

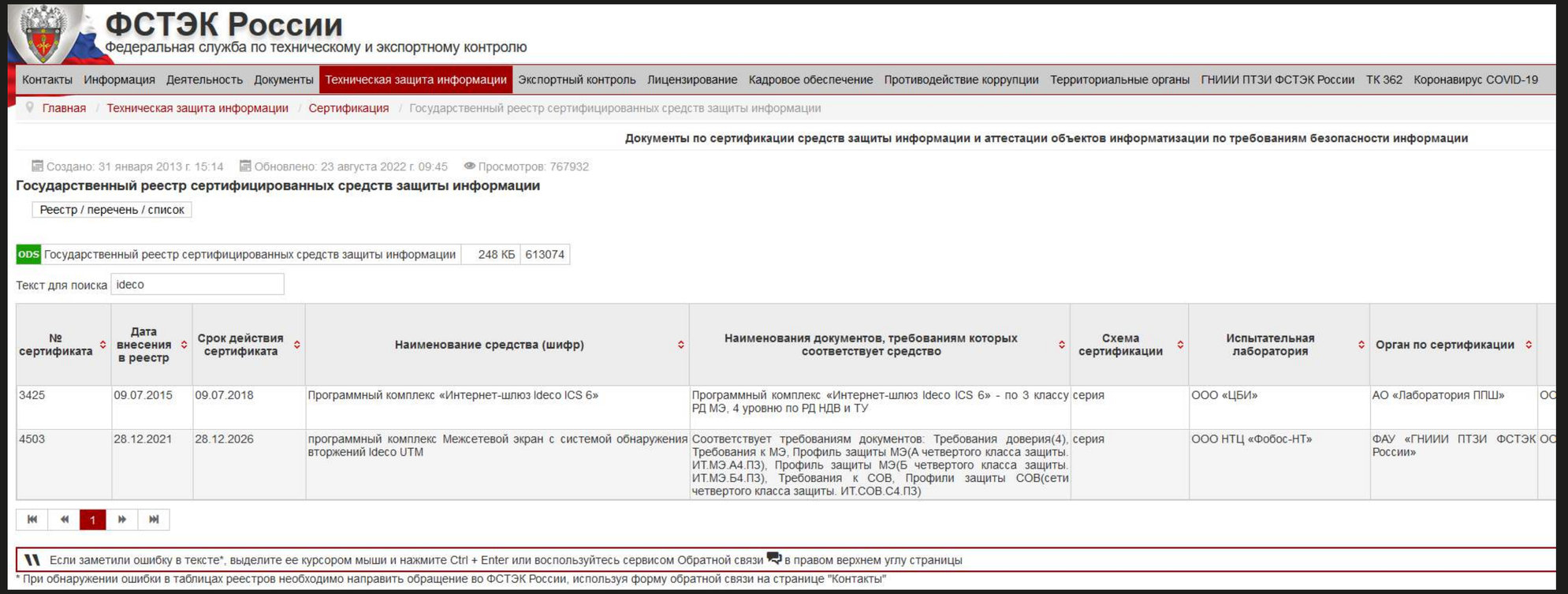
Критерии выбора NGFW

16 критериев выбора отечественных межсетевых экранов.

Все, что есть в Ideco UTM.

синяя или оранжевая таблетка?

1. Комплаенс



ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Контакты | Информация | Деятельность | Документы | Техническая защита информации | Экспортный контроль | Лицензирование | Кадровое обеспечение | Противодействие коррупции | Территориальные органы | ГНИИИ ПТЗИ ФСТЭК России | ТК 362 | Коронавирус COVID-19

Главная / Техническая защита информации / Сертификация / Государственный реестр сертифицированных средств защиты информации

Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации

Создано: 31 января 2013 г. 15:14 Обновлено: 23 августа 2022 г. 09:45 Просмотров: 767932

Государственный реестр сертифицированных средств защиты информации

Реестр / перечень / список

ODS Государственный реестр сертифицированных средств защиты информации 248 КБ 613074

Текст для поиска ideco

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	
3425	09.07.2015	09.07.2018	Программный комплекс «Интернет-шлюз Ideco ICS 6»	Программный комплекс «Интернет-шлюз Ideco ICS 6» - по 3 классу РД МЭ, 4 уровню по РД НДВ и ТУ	серия	ООО «ЦБИ»	АО «Лаборатория ППШ»	ОС
4503	28.12.2021	28.12.2026	программный комплекс Межсетевой экран с системой обнаружения вторжений Ideco UTM	Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)	серия	ООО НТЦ «Фобос-НТ»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	ОС

1

Если заметили ошибку в тексте*, выделите ее курсором мыши и нажмите Ctrl + Enter или воспользуйтесь сервисом Обратной связи в правом верхнем углу страницы

* При обнаружении ошибки в таблицах реестров необходимо направить обращение во ФСТЭК России, используя форму обратной связи на странице "Контакты"

- продукты из реестра соотвествуют формальным требованиям к МЭ;
- в компании внедрена безопасная разработка (SDL);
- уровень зрелости компании и продукта.

Ideco UTM: сертификация ФСТЭК и Минцифры

- Сертификат ФСТЭК МЭ А4/Б4, СОВ 4, УД4;
- реестр программного обеспечения Минцифры: запись в реестре №329 от 08.04.2016;
- для защиты:

  ГИС: до 1 К3 (включительно),

  ИСПДн: до 1 У3 (включительно),

  АСУ: до К1 (включительно),

  Значимые объекты КИИ: до 1 класса (включительно),

  ИС ОП: II класс;
- соответствие требованиям:

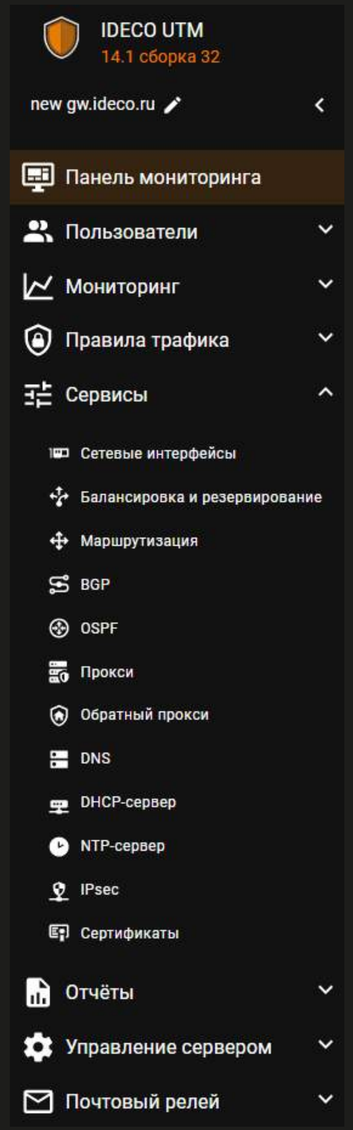
  187-ФЗ «О безопасности КИИ РФ»,

  152-ФЗ «О персональных данных»,

  139-ФЗ и 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

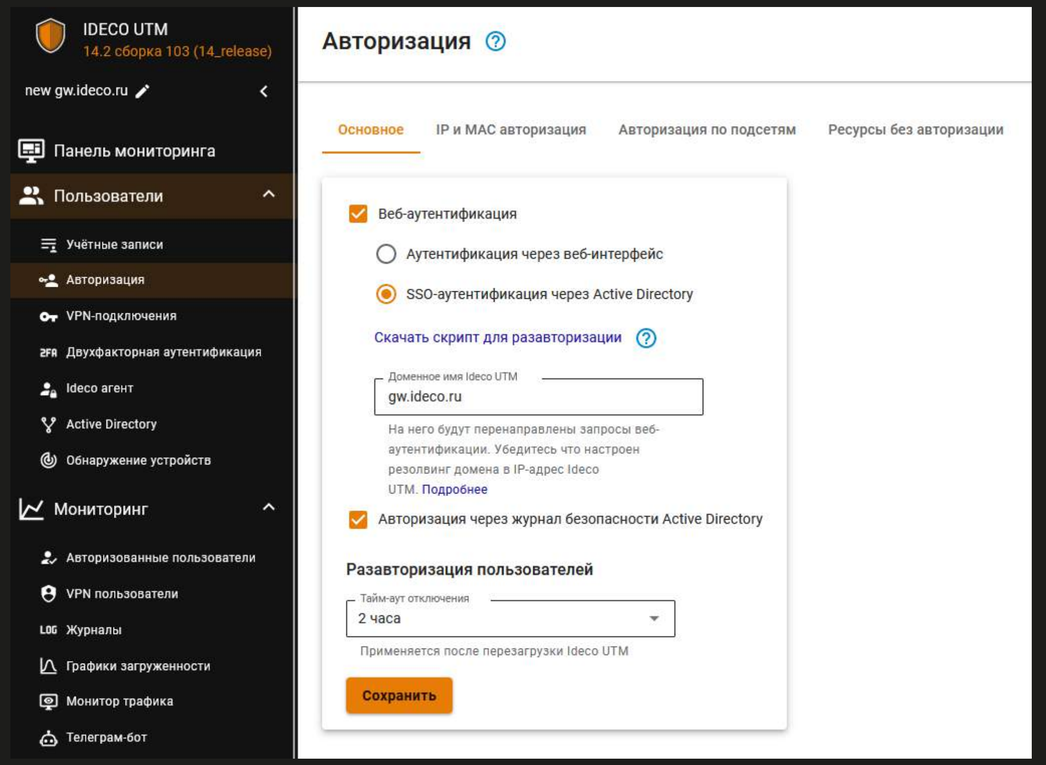
2. Сетевая и общая функциональность

- маршрутизация трафика (статическая, OSPF, BGP);
- сетевые сервисы (DNS, DDNS, NTP, DHCP, публикация ресурсов);
- балансировка, резервирование и агрегирование (LACP) каналов;
- кластеризация;
- централизованное управление.



3. Аутентификация пользователей

- интеграция с Microsoft Active Directory (несколькими доменами, Kerberos/NTLM, аутентификация по логам безопасности);
- интеграция с ALD PRO (апрель 2023);
- веб-авторизация;
- IP, IP+MAC для аутентификации устройств;
- авторизация подсетей (SIP-телефонов, камеры, Wi-Fi сети);
- автоматическая авторизация устройств и создание пользователей;
- VPN: PPTP, PPPoE, IKEv2/IPSec, L2TP/IPSec, SSTP;
- двухфакторная аутентификация (звонок, SMS, OTP-токен).



4. VPN-сервер

client-to-site

- IKEv2/IPSec;
- L2TP/IPSec’
- SSTP (SSL-VPN);
- Ideco agent (Wireguard).

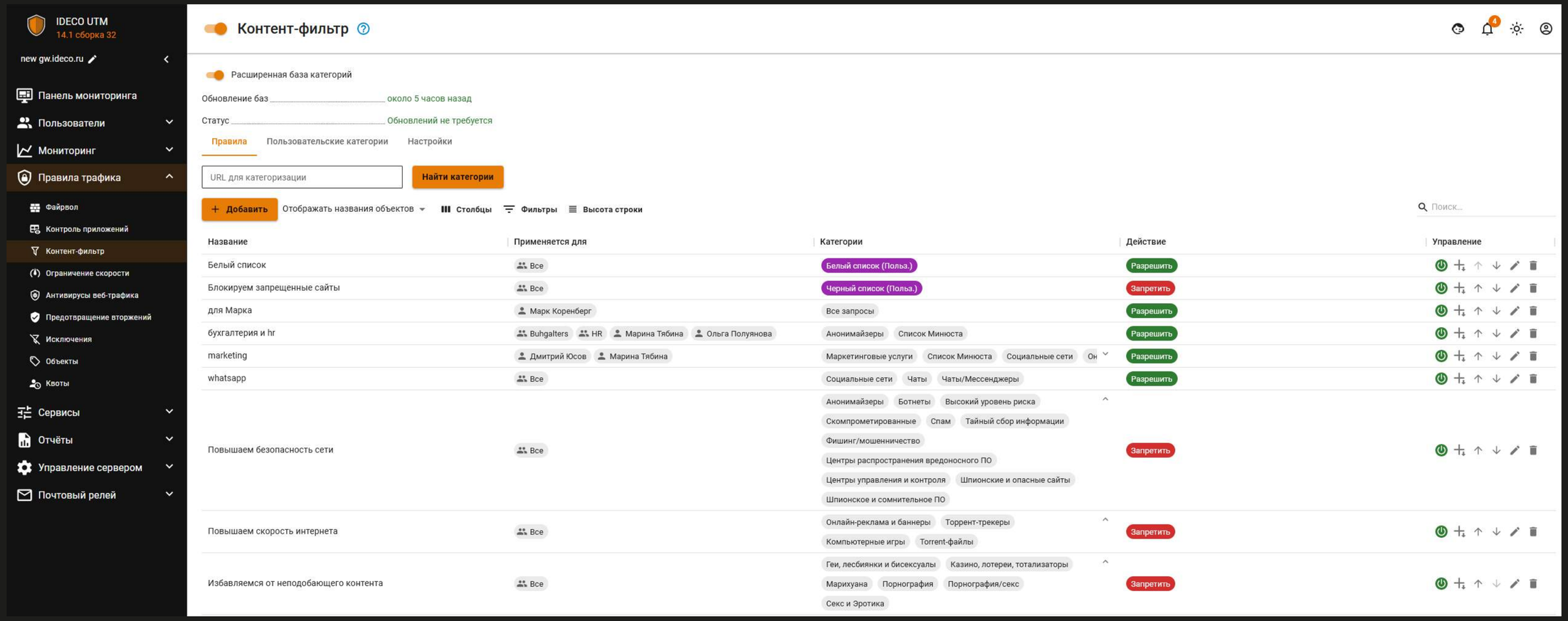
site-to-site

- IKEv2/IPSec.

5. Фильтрация трафика

функциональность NGFW/UTM

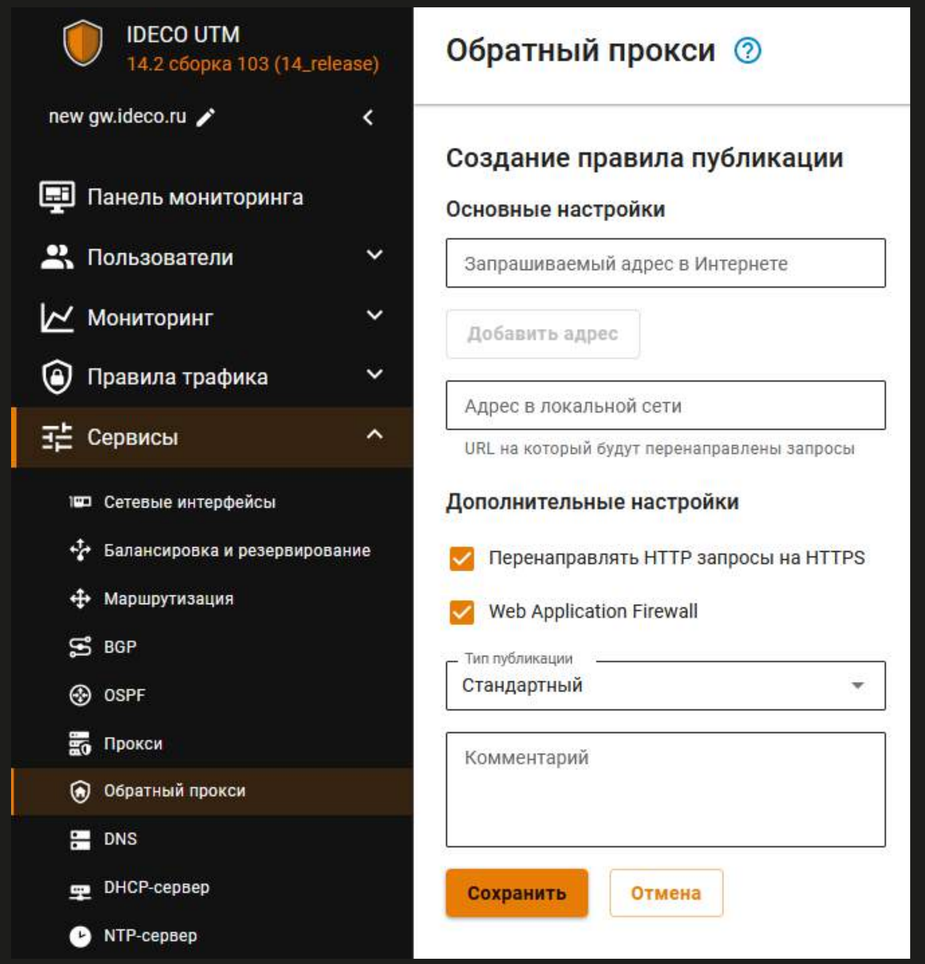
- модули анализа трафика до L7: FW, CF, AC, IPS, AV;
- правила по пользователям и группам, а не IP-адресам.



6. Публикация ресурсов

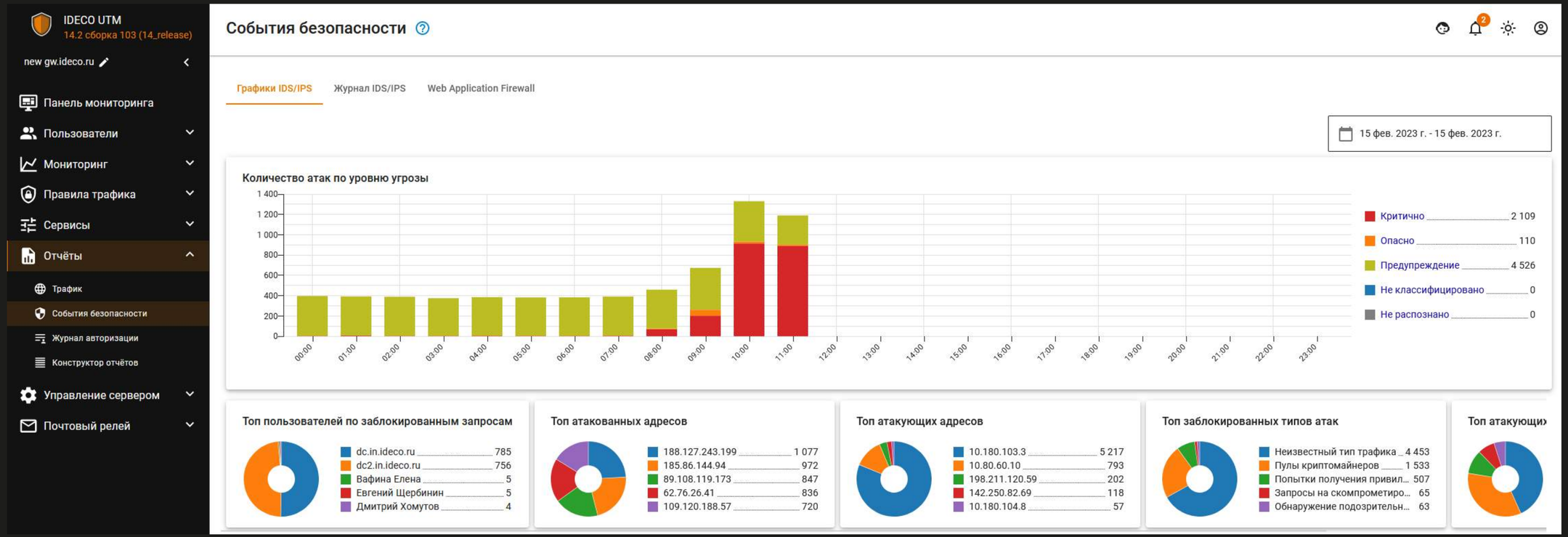
безопасная публикация

- обратный прокси-сервер с WAF для публикации веб-ресурсов;
- почтовый релей для публикации почтового сервера;
- защита опубликованных терминальных серверов (RDP).

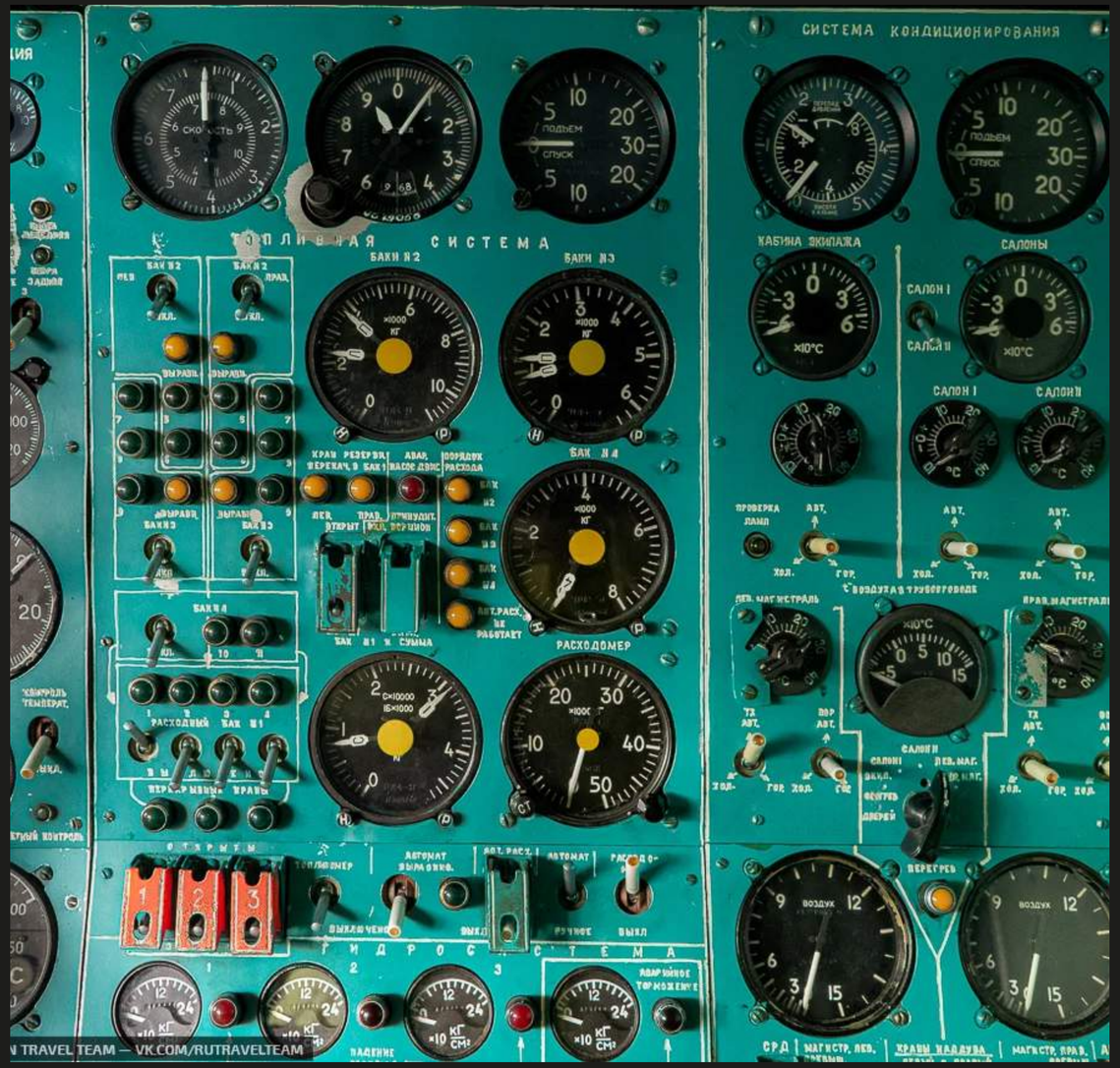


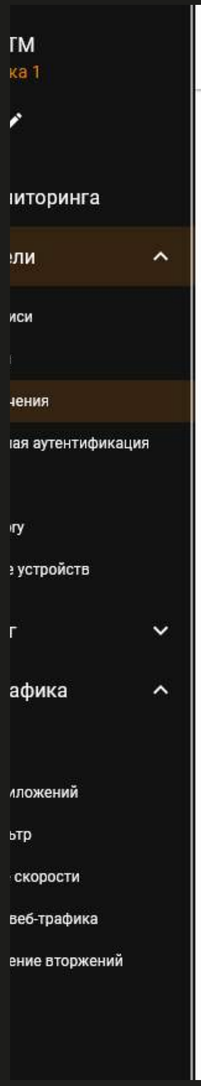
7. Мониторинг, отчеты, журналирование

- интеграции с внешними системами: syslog (с SIEM), SNMP, Zabbix-агент, ICAP (DLP);
- отчеты по трафику (общий трафик, приложения, веб-трафик по категориям);
- мониторинг (пользователи, трафик, трафик приложений);
- нагрузка на сервер (процессор, память, LA), сетевые интерфейсы, диск;
- события безопасности;
- журналы системы (в веб-интерфейсе с версии 14.2).



8. Простой и удобный UX/UI





VPN-подключения

Работает

Основное | Фиксированные IP-адреса VPN

Основные настройки

Сеть для VPN-подключений: 10.180.99.0/24

- [x] Подключение по PPTP
- [ ] Подключение по PPPoE
- [x] Подключение по IKEv2/IPSec
  - Домен: irina.7kingdoms.ru
  - PowerShell - скрипт для настройки подключений
- [x] Подключение по SSTP
  - Домен: irina.7kingdoms.ru
  - Порт: 4443
  - PowerShell - скрипт для настройки подключений
- [x] Подключение по L2TP/IPSec
  - PSK: ••••••••••••••••••••••••••••••••
  - PowerShell - скрипт для настройки подключений

Сохранить

Передача маршрутов

Локальные маршруты для передачи по VPN только

- (•) Отправлять все локальные сети
- ( ) Не отправлять

Будут отправляться только маршруты до подсетей Ideo

- ( ) Отправлять только указанные

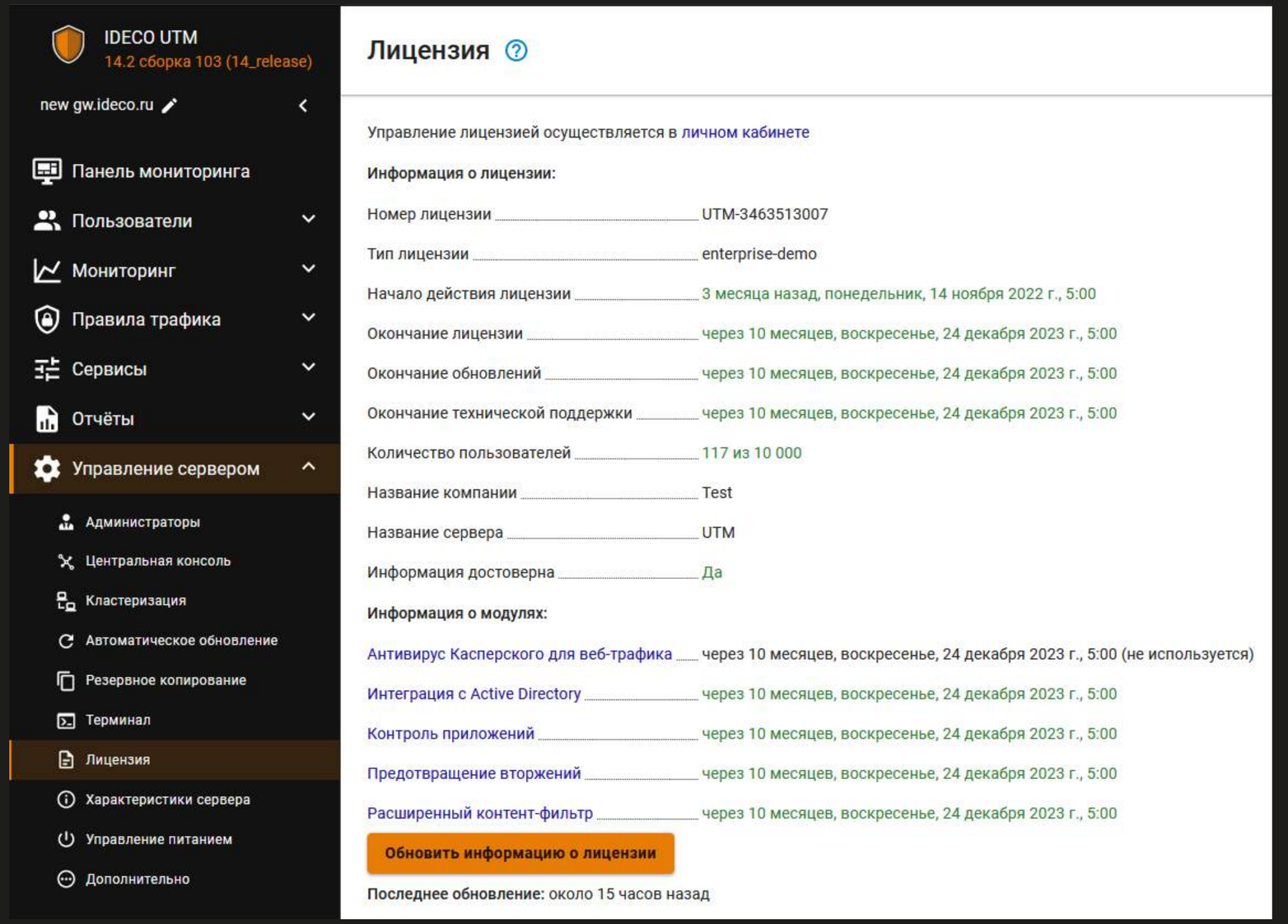
Маршруты

Выберите сеть

Сохранить

9. Лицензирование

- количество пользователей одновременно выходящих в интернет (каждый пользователь может авторизовать до 5 устройств);
- безлимитные по количеству пользователей лицензии возможны для ПАК-ов;
- лицензия бессрочная;
- в Security Update входит:
  - переход на новые версии;
  - расширенные базы КФ;
  - работа и базы IPS;
  - работа и базы АС;
  - антивирус/антиспам Касперского;
  - тех. поддержка.



10. Производительность и сайзинг

как подобрать ПАК или мощность гиперизора

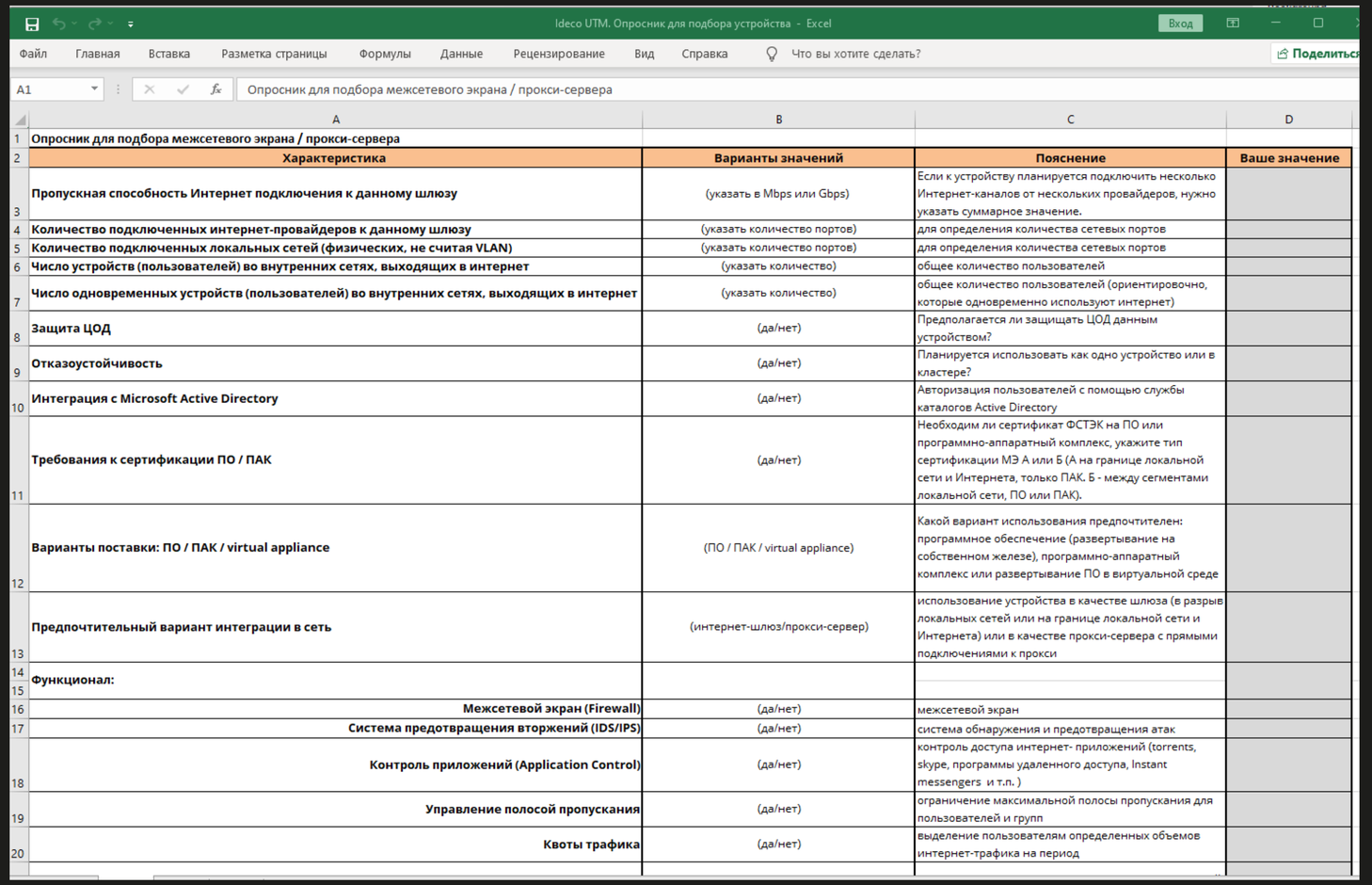
Основные параметры

- ФСТЭК/НЕ ФСТЭК;
- ПАК/ПО;
- количество пользователей;
- скорость трафика (для внешних интерфейсов).

Наибольшее влияние на производительность:

- IPS;
- антивирус веб-трафика.

Обращайтесь к нашим партнерам или на sales@ideco.ru



Ideco UTM. Опросник для подбора устройства - Excel

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид Справка Что вы хотите сделать?

A1: Опросник для подбора межсетевого экрана / прокси-сервера

	A	B	C	D
1	**Опросник для подбора межсетевого экрана / прокси-сервера**			
2	**Характеристика**	**Варианты значений**	**Пояснение**	**Ваше значение**
3	**Пропускная способность Интернет подключения к данному шлюзу**	(указать в Mbps или Gbps)	Если к устройству планируется подключить несколько Интернет-каналов от нескольких провайдеров, нужно указать суммарное значение.	
4	**Количество подключенных интернет-провайдеров к данному шлюзу**	(указать количество портов)	для определения количества сетевых портов	
5	**Количество подключенных локальных сетей (физических, не считая VLAN)**	(указать количество портов)	для определения количества сетевых портов	
6	**Число устройств (пользователей) во внутренних сетях, выходящих в интернет**	(указать количество)	общее количество пользователей	
7	**Число одновременных устройств (пользователей) во внутренних сетях, выходящих в интернет**	(указать количество)	общее количество пользователей (ориентировочно, которые одновременно используют интернет)	
8	**Защита ЦОД**	(да/нет)	Предполагается ли защищать ЦОД данным устройством?	
9	**Отказоустойчивость**	(да/нет)	Планируется использовать как одно устройство или в кластере?	
10	**Интеграция с Microsoft Active Directory**	(да/нет)	Авторизация пользователей с помощью службы каталогов Active Directory	
11	**Требования к сертификации ПО / ПАК**	(да/нет)	Необходим ли сертификат ФСТЭК на ПО или программно-аппаратный комплекс, укажите тип сертификации МЭ А или Б (А на границе локальной сети и Интернета, только ПАК. Б - между сегментами локальной сети, ПО или ПАК).	
12	**Варианты поставки: ПО / ПАК / virtual appliance**	(ПО / ПАК / virtual appliance)	Какой вариант использования предпочтителен: программное обеспечение (развертывание на собственном железе), программно-аппаратный комплекс или развертывание ПО в виртуальной среде	
13	**Предпочтительный вариант интеграции в сеть**	(интернет-шлюз/прокси-сервер)	использование устройства в качестве шлюза (в разрыв локальных сетей или на границе локальной сети и Интернета) или в качестве прокси-сервера с прямыми подключениями к прокси	
14	**Функционал:**			
15				
16	**Межсетевой экран (Firewall)**	(да/нет)	межсетевой экран	
17	**Система предотвращения вторжений (IDS/IPS)**	(да/нет)	система обнаружения и предотвращения атак	
18	**Контроль приложений (Application Control)**	(да/нет)	контроль доступа интернет- приложений (torrents, skype, программы удаленного доступа, Instant messengers и т.п.)	
19	**Управление полосой пропускания**	(да/нет)	ограничение максимальной полосы пропускания для пользователей и групп	
20	**Квоты трафика**	(да/нет)	выделение пользователям определенных объемов интернет-трафика на период	

Ideco SX+

до 75 пользователей

Ideco SX+

Решения для малого бизнеса

Предназначен для небольших организаций, численностью до 75 активных пользователей интернет. Позволяет ввести ограничения по трафику для каждого из сотрудников или отдельных групп, защитить периметр сети, сегментировать сеть и использовать несколько интернет-провайдеров (благодаря 6 сетевым интерфейсам), а также предоставить возможность удаленной работы сотрудников по VPN.

Характеристики

Процессор	Intel Core i5-10210U (1.6GHz, 6M, 4-Cores)
Память	16GB SO-DIMM DDR4
Хранилище	mSATA 256GB
Сетевой адаптер	6 x i210/i211

Производительность (трафик EMIX)

Межсетевой экран	до 5 Гб/сек
Контентная фильтрация	до 2 Гб/сек
Контроль приложений	до 1 Гб/сек
Предотвращение вторжений	до 0,4 Гб/сек
Режим NGFW	до 0,4 Гб/сек

Ideco MX и LX

1U-сервера. MX 50-350 пользователей, LX до 1000

Ideco MX и LX

Решения для малого и среднего бизнеса

Серверы этой линейки обладают повышенным уровнем надёжности, производительности и управляемости в сочетании с возможностью наращивания ресурсов вычислительной системы. Всё это обеспечивает непрерывность бизнес-процессов как малых, так и средних предприятий.

Позволяют защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все основные потребности сетевой инфраструктуры.

Характеристики

	MX	LX
Процессор	Intel Xeon E-2234 (3.6GHz, 8M, 4-Cores)	Intel® Xeon® E-22xx (8 ядер, 16Mb, 8 GT/s)
Память	16Gb DDR4-2133 ECC	32Gb DDR4-2133 ECC
Хранилище	240Gb SATA SSD	240Gb SATA SSD
Сетевой адаптер	4x Gigabit LAN ports	4x Gigabit LAN ports

Производительность (трафик EMIX)

	MX	LX
Межсетевой экран	до 8 Гб/сек	до 11,5 Гб/сек
Контентная фильтрация	до 5 Гб/сек	до 8,1 Гб/сек
Контроль приложений	до 2,2 Гб/сек	до 3,5 Гб/сек
Предотвращение вторжений	до 1,2 Гб/сек	до 1,8 Гб/сек
Режим NGFW *	до 1,2 Гб/сек	до 1,8 Гб/сек

Ideco LX+ и EX

2U сервера. LX+ до 3000 пользователей, EX до 10000

Ideco LX+ и EX

Решения для среднего и крупного бизнеса

Серверы этой линейки обладают повышенным уровнем надёжности, производительности и управляемости в сочетании с возможностью наращивания ресурсов вычислительной системы. Всё это обеспечивает непрерывность бизнес-процессов предприятий любого размера.

Позволяют защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все основные потребности сетевой инфраструктуры.

Характеристики

	LX+	EX
Процессор	Intel Xeon Silver 4214R 12 ядер, 24 потока	Intel Xeon Gold 6238R 28 ядра, 56 потока
Память	64Gb DDR4 ECC REG	64Gb DDR4-2133 ECC
Хранилище	480Gb SATA SSD	480Gb SATA SSD
Сетевой адаптер	4x Gigabit LAN ports, 4×10 Gb SFP+	4x Gigabit LAN ports, 4×10 Gb SFP+
Источник питания	2x Блока питания 800 Вт (2*800 Вт)	2x Блока питания 800 Вт (2*800 Вт)

Производительность (трафик EMIX)

	LX+	EX
Межсетевой экран	до 19,6 Гб/сек	до 42 Гб/сек
Контентная фильтрация	до 10,2 Гб/сек	до 25 Гб/сек
Контроль приложений	до 4 Гб/сек	до 8,8 Гб/сек
Предотвращение вторжений	до 2 Гб/сек	до 5 Гб/сек
Режим NGFW *	до 2 Гб/сек	до 5 Гб/сек

Ideco MX и MX+ Cert

сертифицированные ФСТЭК, в апреле 2023 будет в наличии новая модель на Xeon

Ideco MX и MX+ Cert

Сертифицировано ФСТЭК

Сертифицирован по требованиям к межсетевым экранам типа А, Б 4-го класса и системам обнаружения вторжений. Сертификат №4503 от 28.12.2021.

Сертифицированная аппаратная платформа MX для организаций от 100 до 350 пользователей, MX+ от 300 до 700. Позволяет защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все потребности сетевой инфраструктуры.Соответствие требованиям ФСТЭК, решение широкого круга задач и возможность интеграции с AD/LDAP позволяет линейке Ideco MX обеспечить потребности компаний малого и среднего бизнеса.

Характеристики

	MX Cert	MX + Cert
Процессор	Intel Atom C-3758 (8 ядер, 2,2 ГГц)	Intel® Atom C-3958 (16 ядер, 2,0 ГГц)
Память	16GB DDR4	32Gb DDR4
Хранилище	240Gb SATA SSD	240Gb SATA SSD
Сетевой адаптер	8×1Gb Lan	8×1Gb Lan

Производительность (трафик EMIX)

	MX Cert	MX + Cert
Межсетевой экран	до 3 Гб/сек	до 6 Гб/сек
Контентная фильтрация	до 1,7 Гб/сек	до 3,2 Гб/сек
Контроль приложений	до 0,7 Гб/сек	до 1,3 Гб/сек
Предотвращение вторжений	до 0,3 Гб/сек	до 0,6 Гб/сек
Режим NGFW *	до 0,3 Гб/сек	до 0,6 Гб/сек

Минимальные аппаратные требования актуальной версии

Платформа	Обязательная поддержка UEFI
Процессор*	Intel Pentium G/i3/i5/i7/Xeon E3/Xeon E5 с поддержкой SSE 4.2
Оперативная память*	8 Гб (16 Гб при количестве пользователей более 75)
Накопитель	Жесткий диск или SSD, объемом 64 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe или совместимый аппаратный RAID. Дополнительный жесткий диск или SSD при использовании почтового сервера.
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel, Broadcom. Поддерживаются Realtek, D-Link и другие.
Гипервизоры	VMware, Microsoft Hyper-V (2-го поколения), VirtualBox, KVM, Citrix XenServer.
Дополнительно	Монитор и клавиатура
Замечания	Обязательная поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер жесткого диска.

11. Техническая поддержка

На этапе тестирования

- подключение presale-инженера для презентации по ВКС;
- подключение presale-инженера в сделках более 150 пользователей для проведения пилотного проекта;
- чат в TG для быстрых ответов в пилотном проекте.

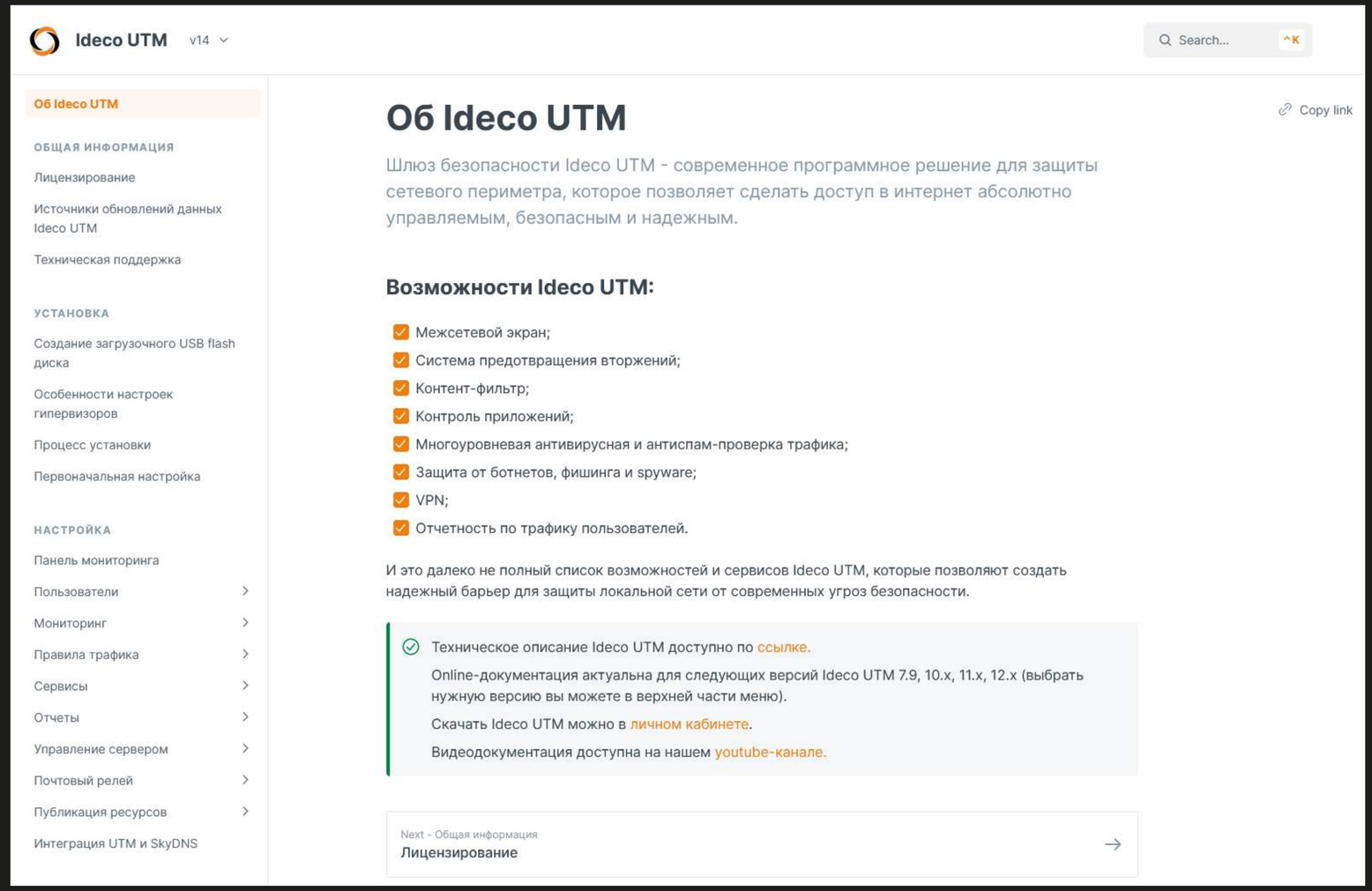
Техническая поддержка

- каналы обращения: телефон, емейл, tg-бот, портал поддержки, чат в интерфейсе;
- стандартная поддержка 12x5+8 часов суббота;
- расширенная поддержка 24x7x365;
- SLA первого ответа 4 часа;
- 3 линии тех. поддержки.

12. Документация

docs.ideco.dev

- версионирование;
- частое обновление;
- документирование REST-API.



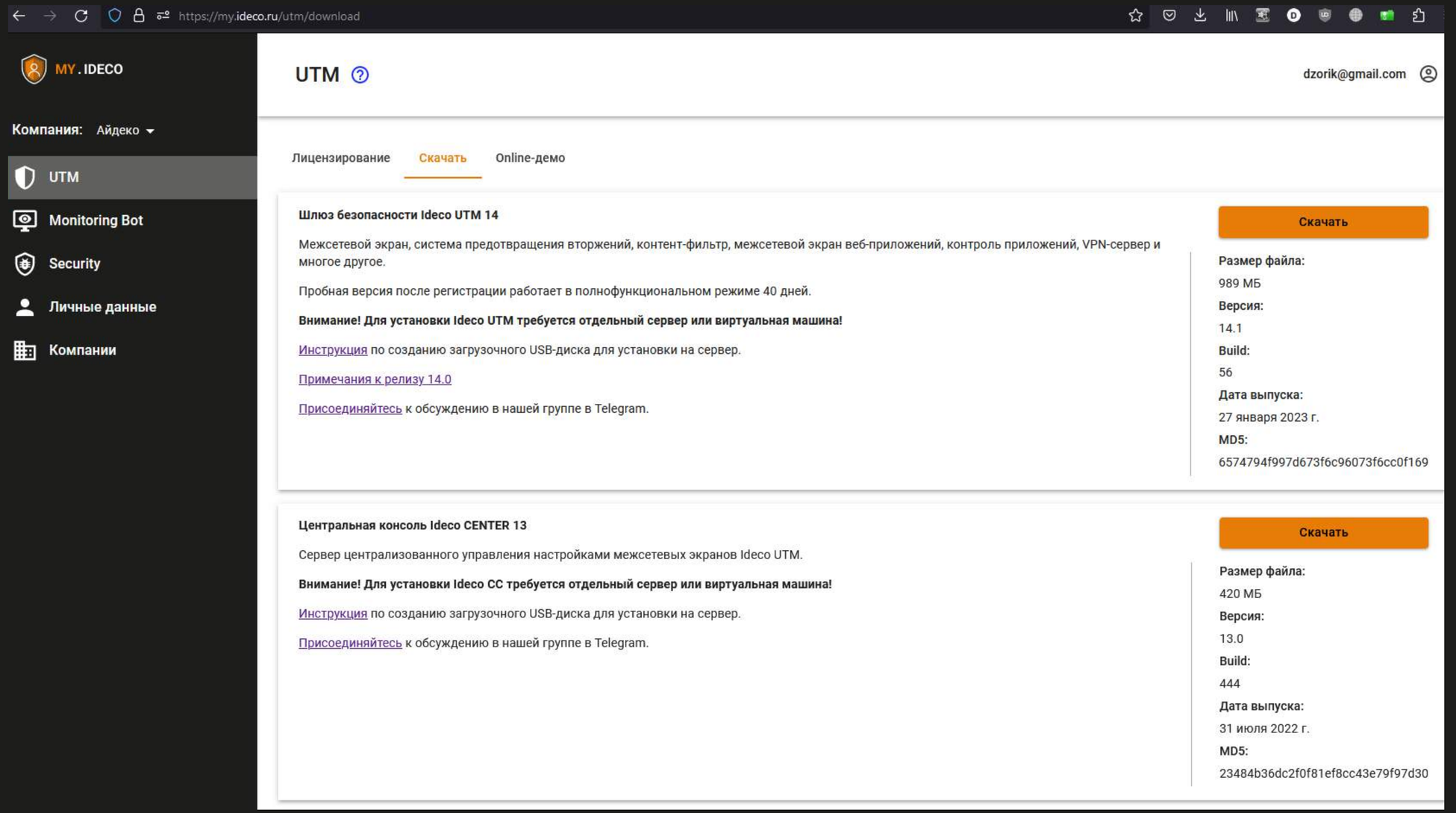
13. Сообщество и обратная связь

ideco

Ideco UTM: создаём вместе
1 054 участника

t.me/idecoutm

14. Тестирование



15. Преимущества Ideco UTM

ideco

Защита сразу «из коробки»

Готовность к ответу на вызовы 2023

Реактивные технологии

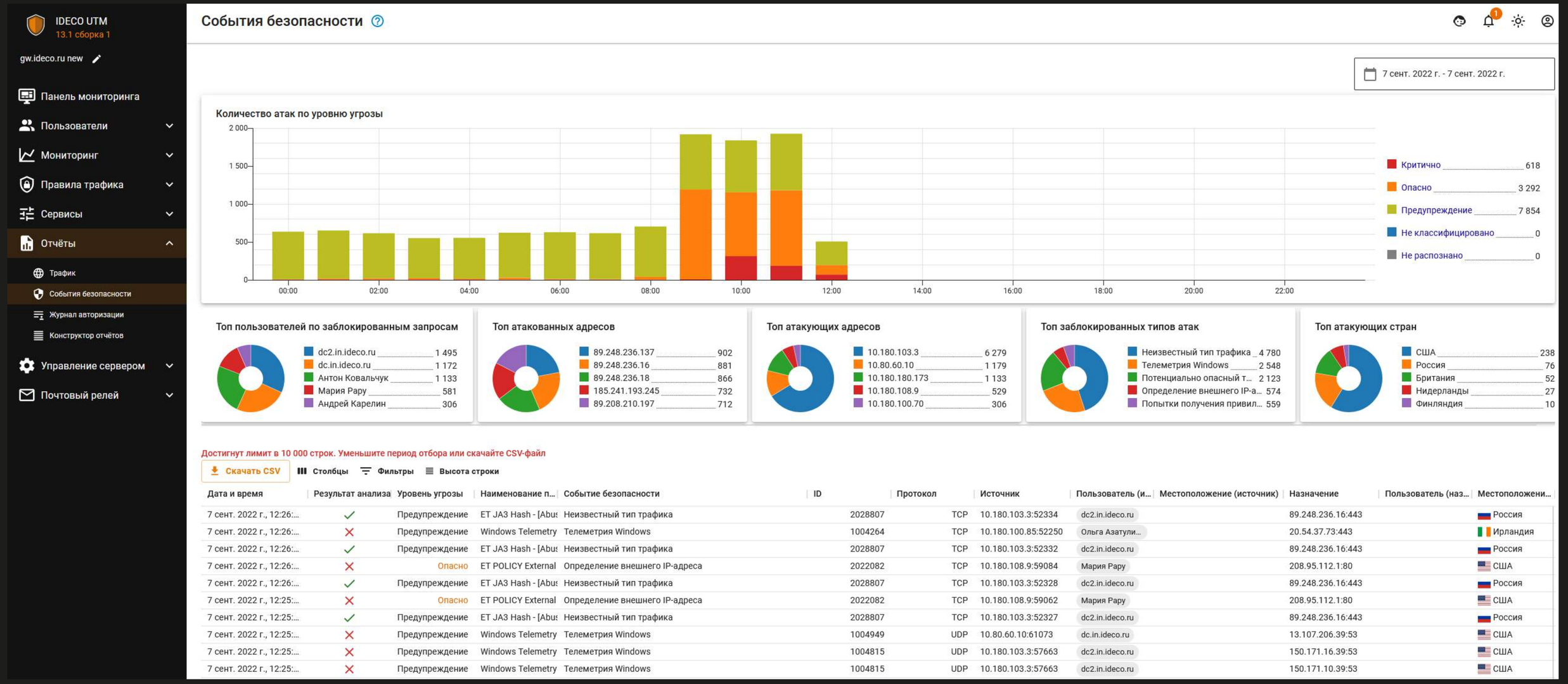
Сервис поддержки on-line

«Шай-тек» (shy-tech) «скромные технологии»

Чемпион по скорости разработки

Интересный факт: среднее время ответа технической поддержки в чат - 45 секунд.

Ideco UTM 14: защита “из коробки”



Killer Feature

ideco

Продукт

- VPN-агент/агент аутентификации;
- аутентификация по логам безопасности контроллеров домена Active Directory;
- нативные VPN-протоколы IKEv2 и SSTP;
- полный доступ к системе через терминал.

Поддержка

- чат в веб-интерфейсе, среднее время ответа - 45 секунд;
- общение с разработчиками в сообществе в tg-группе;
- быстрое развитие продукта.

Коммерческие условия

- цена ниже многих конкурентов;
- кластер отказоустойчивости входит в базовую лицензию;
- центральная консоль управления входит в базовую лицензию;
- нет привязки лицензии к “железу”.

16. RoadMap

ideco

Муравей на ходу делает больше, чем дремлющий бык.

R&D

- dataplane;
- frontend;
- backend;
- devops;
- ручное тестирование;
- автоматизированное тестирование;
- документация;
- ФСТЭК.

8 development teams

2023 год

Ideco UTM 15. Апрель 2023 года

- пропуск мультикаст-трафика;
- адаптивность веб-интерфейса под мобильные устройства;
- балансировка трафика обратным прокси-сервером;
- интеграция с ALD PRO;
- аудит действий администраторов;
- авторизация пользователей терминальных серверов.

Будущее: Ideco ~~UTM~~ NGFW 16

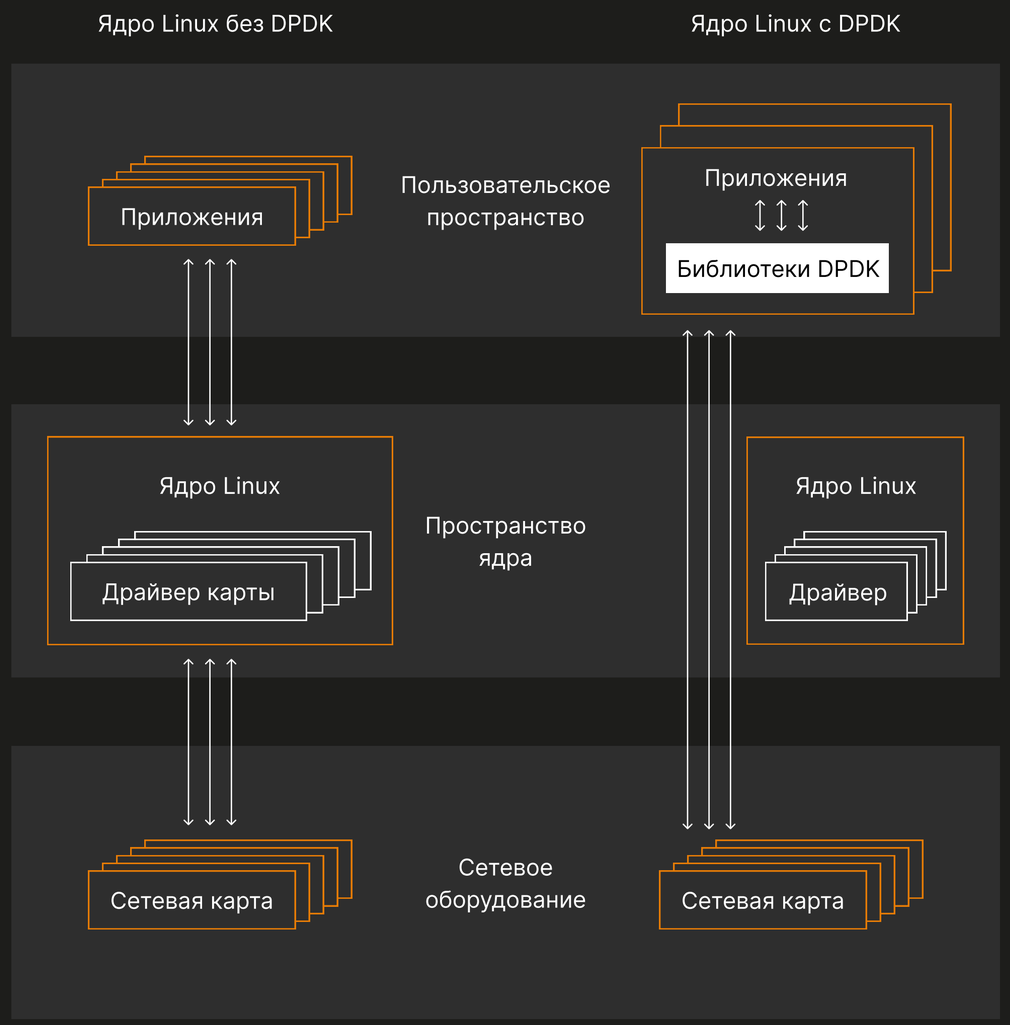
Релиз август 2023 года.

- x10 скорость обработки трафика, полностью «свой» стек обработки трафика, общие правила firewall/DPI/IPS;
- x2 скорость обработки веб-трафика, новейший модуль прокси-сервера (от Айдеко);
- высокоскоростной NGFW и технологическое лидерство среди отечественных решений.

Архитектура Ideco UTM

- Linux 5.18;
- сила opensource-модулей;
- микросервисы vs монолит;
- kernel vs userspace (DPDK).

Оптимальный фундамент для быстрого развития enterprise-продукта.



Уникальный календарь Айдеко

Интересный факт: это уже 12-ый календарь от компании Айдеко.

ideco

СОЗДАЕМ ВМЕСТЕ

t.me/idecoutm - группа
t.me/ideco - канал
my.ideco.ru - скачать