

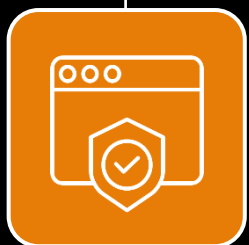
Отечественное решение для защиты сети и фильтрации трафика

Данила Анисимов

Presale-инженер «Айдеко»



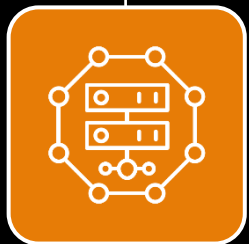
Айдеко – российский разработчик решений для сетевой безопасности



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 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

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 UTM
13.0 сборка 480

gw.ideco.ru

Панель мониторинга

Пользователи

Учётные записи

Авторизация

VPN-подключения

Двухфакторная аутентификация

Idesco агент

Active Directory

Обнаружение устройств

Мониторинг

Правила трафика

Сервисы

Отчёты

Управление сервером

Почтовый релей

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.

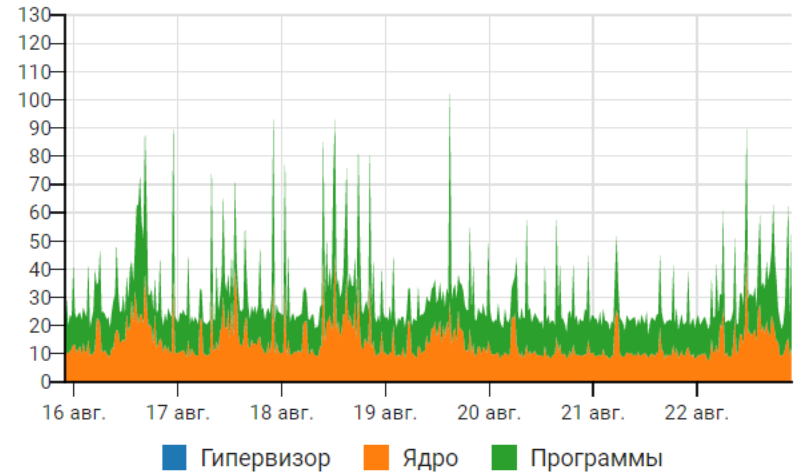
Количество пользователей 34 из 500

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



Поиск

- ▼ Все  
- > Non_AD   
- > **AD** Servers_AD 
- ▼ Users_AD   
- > **AD** Buhgalters 
- ▼ **AD** Developers 
- > **AD** Testing 
-  **AD** Алексей Дегтярев
-  **AD** Анастасия Тураева
-  **AD** Андрей Карелин
-  **AD** Андрей Мокрушин
-  **AD** Артем Щелкунов
-  **AD** Вадим Муравьев
-  **AD** Ваха Ирзаханов
-  **AD** Виктор Гуров
-  **AD** Владимир Ивченко
-  **AD** Владимир Папченко

Основное

Название

Все

Запретить

Разрешить

Сохранить

Пользователи

Авторизация

✓ IP, MAC, IP+MAC, подсеть

✓ WEB

✓ Интеграция с AD: Kerberos, NTLM, security log

✓ Агент

✓ Обнаружение устройств

The screenshot displays the IDECO UTM web interface. The left sidebar contains a navigation menu with the following items: Панель мониторинга, Пользователи (selected), Учётные записи, Авторизация, VPN-подключения, Двухфакторная аутентификация, Ideco агент, Active Directory, Обнаружение устройств, Мониторинг, Правила трафика, Сервисы, Отчёты, and Управление сервером. The main content area is titled 'Авторизация' and shows the 'IP и MAC авторизация' tab selected. A '+ Добавить' button is visible. Below it is a table with the following data:

IP-адрес	MAC-адрес	↑	Пользователь	Постоянная авторизация
10.180.105.8	-		work01	<input type="checkbox"/>
10.180.108.52	-		Руслан Никифоров	<input type="checkbox"/>
10.180.100.246	-		wifi-500-openspace	<input checked="" type="checkbox"/>
10.180.180.173	-		Антон Ковальчук	<input type="checkbox"/>
10.180.100.116	-		TV	<input checked="" type="checkbox"/>
10.180.180.174	-		Руслан Ханов	<input type="checkbox"/>
10.180.105.62	-		trafik-01-ivchenko	<input type="checkbox"/>
10.180.105.63	-		trafik-02-ivchenko	<input type="checkbox"/>
10.180.105.5	-		wintorm	<input type="checkbox"/>

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
L4 TCP	* Любой	IP 46.36.23.99	: 22176	DNAT	0	Для Марка 176	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	* Любой	IP 46.36.23.99	: 22175	DNAT	0	Для Марка 175	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	* Любой	IP 46.36.23.99	: 222	DNAT	0	Для Марка	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	IP Nebaluev-НО...	* Любой	: 5389	DNAT	0	ssh до window...	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	* Любой	* Любой	: 2262	DNAT	0	SSH на стенд D	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	* Любой	* Любой	: 2263	DNAT	0	SSH на стенд D	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 UDP	* Любой	IP 46.36.23.99	: 27015	DNAT	0	wireguard до се	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
L4 TCP	* Любой	IP 46.36.23.99	: 22443	DNAT	0	Проброс RDP д	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Контроль приложений

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

Сервисы

Контроль приложений Работает



+ Добавить Столбцы Фильтры Высота строки

Название	Применяется для	Протоколы	Действие	Управление
Разрешить тестировщикам то...	<ul style="list-style-type: none">Дмитрий ХомутовТимур НураевДмитрий МухаметовРуслан ХановАнтон КовальчукДмитрий ЮсовДмитрий Ахметов	Bittorrent Doh_dot	Разрешить	
разрешить TeamView	Андрей Моргунов	Teamviewer	Разрешить	
Правило для теста	Дмитрий Мухаметов	Bittorrent Teamviewer Sk	Разрешить	
Даниил	Даниил Овчинников	Rdp	Разрешить	
whatsapp	Все	Whatsapp Whatsappfiles	Разрешить	
Программы удаленного досту...	Все	Teamviewer Anydesk	Запретить	
TOR и торренты	Все	Bittorrent Tor Edonkey	Запретить	
Запрет шифрованных DNS-зап...	Все	Doh_dot Dnscrypt	Запретить	
Игры	Все	Steam Halflife2 Worldofk	Запретить	
Криптомайнеры	Все	Mining	Запретить	

Контент-фильтр

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

Сервисы

Отчёты

Управление сервером

Почтовый релей

Контент-фильтр

Расширенная база категорий

Обновление баз 6 дней назад

Статус Обновлений не требуется

Правила

Пользовательские категории

Настройки

URL для категоризации

Найти категории

+ Добавить

Отображать названия объектов

Строк на странице: 30

1-7 из 7

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 Зротика, 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

Предотвращение вторжений

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

Сервисы

Отчёты

Управление сервером

Почтовый релей

Предотвращение вторжений
Работает



Журнал Правила Исключения Настройки

Остановить

Фильтры

Скачать CSV

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	104.16.249.249:443



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

Сервисы



Мониторинг трафика

IDECO UTM
13.0 сборка 480

gw.ideco.ru

Панель мониторинга

Пользователи

Мониторинг

Авторизованные пользователи

VPN пользователи

Журналы

Графики загрузки

Монитор трафика

Telegram-бот

SNMP

Syslog

Zabbix агент

Правила трафика

Сервисы

Отчёты

Монитор трафика



По узлам локальной сети По приложениям

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

IDECO UTM
13.0 сборка 480

gw.ideco.ru

Панель мониторинга

Пользователи

Мониторинг

Правила трафика

Сервисы

Отчёты

Трафик

События безопасности

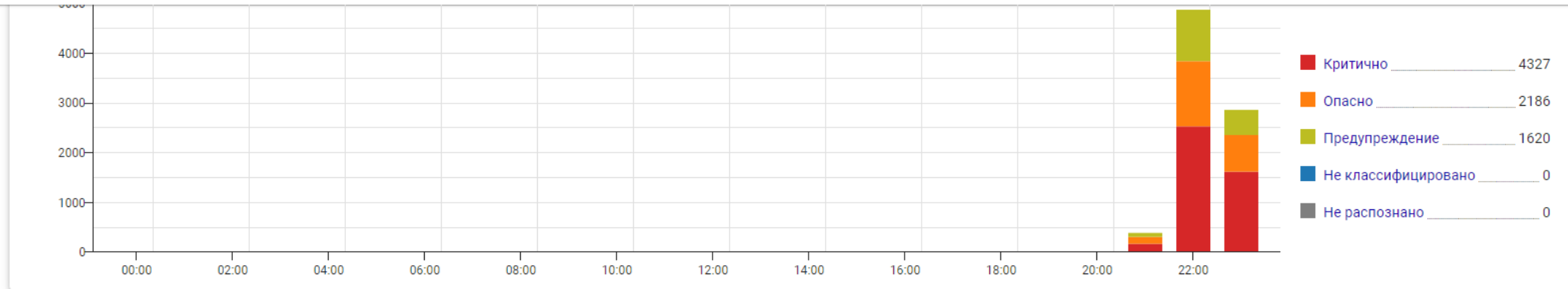
Журнал авторизации

Конструктор отчётов

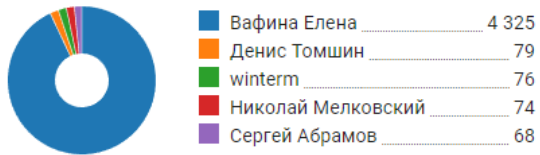
Управление сервером

Почтовый релей

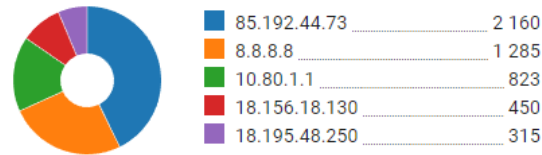
События безопасности



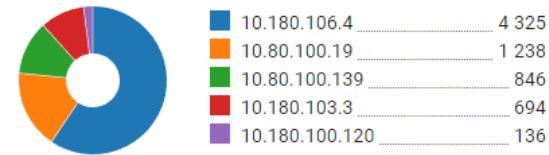
Топ пользователей по заблокированным запросам



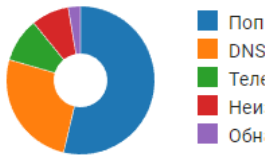
Топ атакованных адресов



Топ атакующих адресов



Топ заблокированных типов



Скачать CSV



Столбцы



Фильтры



Высота строки

Дата и время	Результат анализ	Уровень угрозы	Наименование правила	Событие безоп...	ID	Протокол	Источник	Пользователь (...)	Назначение	Местоположен...
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000082	UDP	10.80.100.19:3368		8.8.8.8:53	США
22 авг. 2022 г. ...	allowed	Предупреждение	ET JA3 Hash - [Abuse.ch] Possible ToFse	Неизвестный тип	2028807	TCP	10.180.103.3:5646	dc2.in.ideco.ru	185.241.193.245:4	Россия
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000010	UDP	10.80.100.139:535		10.80.1.1:53	
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000010	UDP	10.80.100.19:3309		8.8.8.8:53	США
22 авг. 2022 г. ...	allowed	Предупреждение	ET JA3 Hash - [Abuse.ch] Possible ToFse	Неизвестный тип	2028807	TCP	10.180.103.3:5646	dc2.in.ideco.ru	185.241.193.245:4	Россия
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000010	UDP	10.80.100.19:4157		8.8.8.8:53	США
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000010	UDP	10.80.100.19:6092		8.8.8.8:53	США
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000082	UDP	10.80.100.19:5408		8.8.8.8:53	США
22 авг. 2022 г. ...	blocked	Опасно	DNSoverHTTPS	DNS поверх HTTP	1000082	UDP	10.80.100.19:4973		8.8.8.8:53	США

Отчетность в различных разрезах

IDECO UTM
13.0 сборка 480

gw.ideco.ru

Панель мониторинга

Пользователи

Мониторинг

Правила трафика

Сервисы

Отчёты

Трафик

События безопасности

Журнал авторизации

Конструктор отчётов

Управление сервером

Почтовый релей

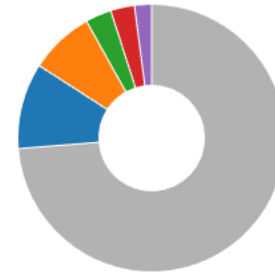
Трафик

Топ категорий (МБ)



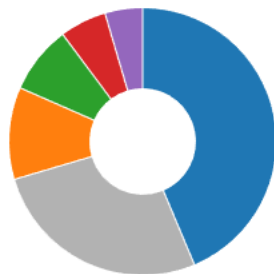
Все некатегоризиро...	110 528,75
Технологии (в целом)	91 044,62
Видео для прослушив...	75 897,68
Прямое обращение п...	53 894,29
Контент серверы	27 381,97
Остальное	154 130,19

Топ сайтов (МБ)



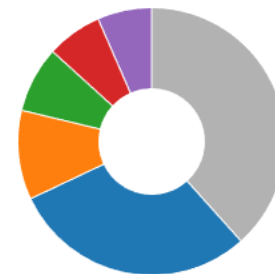
91.105.192.100	35 304,75
storage.yandexcloud.net	26 410,65
rr3--sn-3uxaxjvh-n8mz...	10 353,73
rr2--sn-3uxaxjvh-n8mz.g...	9 439,38
rr1--sn-3uxaxjvh-n8mz.g...	6 572,85
Остальное	254 540,20

Топ протоколов (МБ)



Zoom	58 635,63
IMAPS	14 799,16
Unknown	10 876,49
RTP	7 401,24
IPSec	5 919,40
Остальное	35 868,11

Топ заблокированных сайтов



www.google-analytics.com	7 544
www.googletagmanager.co...	2 721
counter.yadro.ru	2 005
top-fwz1.mail.ru	1 677
yt3.ggpht.com	1 637
Остальное	9 782

Топ заблокированных категорий



Онлайн-реклама и банне...	22 265
Ссылки Microsoft	1 040

Топ заблокированных протоколов



DoH DoT	221 025
---------	---------

Пример детализации по протоколу

gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты
- Трафик**
- События безопасности
- Журнал авторизации
- Конструктор отчётов
- Управление сервером
- Почтовый релей

Трафик

Трафик / [Топ протоколов](#) / [Zoom](#)

Трафик МБ Запросы

24 июл. 2022 г. - 22 авг. 2022 г.

Количество трафика (МБ)

Дата	Входящий (МБ)	Исходящий (МБ)
24.07	1500	4500
25.07	4000	14000
26.07	1000	2500
27.07	1500	3500
28.07	2500	7000
29.07	1000	3000
30.07	1000	3000
01.08	1000	2000
02.08	3000	12000
03.08	1000	1500
04.08	1000	1000

Топ пользователей (МБ)

Пользователь	Общий (МБ)
Дмитрий Хомутов	6 868,20
Руслан Никифоров	5 158,40
Олег Пахомов	5 067,04
Анна Байдосова	3 679,97
Марк Коренберг	3 175,52

Топ блокировок

Данные отсутствуют



Почтовый сервер/релей

Основной почтовый домен
dkim-mx.test.ideco.dev

Имя хоста почтового сервера
dkim-mx.test.ideco.dev

Используется как HELO почтового сервера

Дополнительные почтовые домены

Добавить домен

Relay-домены
dkim.test.ideco.dev|10.180.180.229

Почтовые домены в локальной сети, для которых будут пересылаться письма извне. Формат:
domain.name|192.168.1.1 или domain.name|relay.domain

Добавить Relay-домен

Сохранить

- IMAP(S) (143 STARTT
- POP3(S) (110 STARTT
- Web-почта

Диск для хранения почты

Для хранения почтовых ящи
отдельный жесткий диск

Подключить

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

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

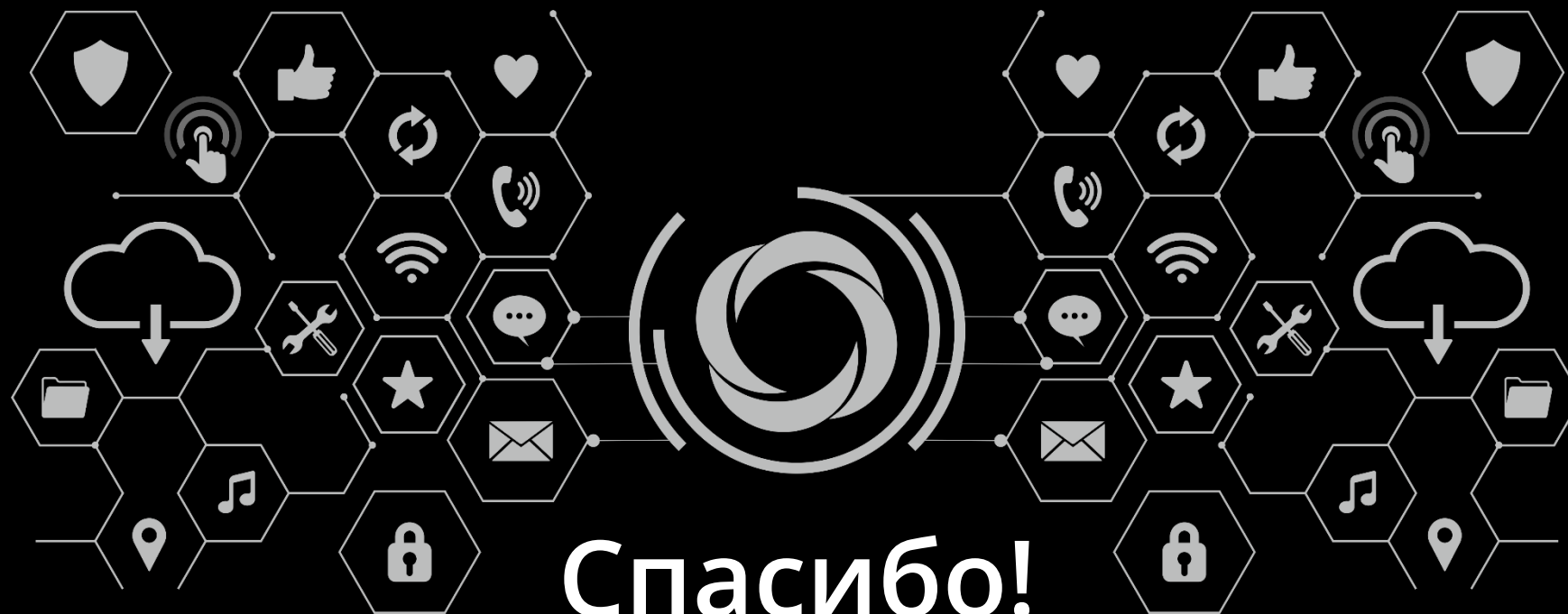
- портал поддержки help.ideco.ru
- электронная почта
- телефон
- Telegram
- чат в продукте

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



 @Dvanisimov

 d.anisimov@ideco.ru



 t.me/idecoutm

 @ideco