

Отечественное решение для защиты сети и фильтрации трафика

Сергей Жужгов
Presale-инженер «Айдеко»



О компании

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

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



Более 4 000 компаний
используют Ideco UTM



180 человек в команде
S&M / R&D



Лидер по скорости
разработки в отрасли

Как мы работаем

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 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

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

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)

Панель мониторинга



IDECO UTM 15.1 сборка 104 Бета

new gw.ideco.ru

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

Панель мониторинга

Загрузка интерфейсов, Мбит/с Локальная сеть 1 час

■ Входящий ■ Исходящий

Состояние внешних интерфейсов

Интерфейс	Загруженность (Мбит/с)
К-Телеком	↑ 3,9
Тестовое подключение	↻

Время работы сервера 8 дней 18 часов 40 минут

Загрузка процессора, % 1 час

Топ 5 хостов (входящая скорость), Мбит/с Топ 5

Пользователь	IP-адрес	Вх. скорость	Сессии
Дмитрий Хо...	10.180.100.173	3,32	82
10.180.100.1...	10.180.100.140	2,09	3
Олег Пахомов	10.180.100.162	0,21	81
Владимир К...	10.180.100.84	0,11	12

Пользователи



IDECO UTM
15.1 сборка 104 Бета

new gw.ideco.ru

- Панель мониторинга
- Пользователи**
- Учётные записи
- Авторизация
- VPN-подключения
- 2FA Двухфакторная аутентификация
- Ideco агент
- Active Directory/Samba DC
- ★ ALD Pro
- Обнаружение устройств
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты и журналы
- Управление сервером
- Почтовый релей

Учётные записи

Поиск

- Все
- Non_AD
- AD Servers_AD
- Users_AD
 - AD Buhgalters
 - AD Developers
 - AD HR
 - AD Management
 - AD Marketing
 - AD Анастасия Деева
 - AD Анастасия Дубских
 - AD Анна Исакова
 - AD Георгий Чуб
 - AD Елизавета Туз
 - AD Марина Тябина
 - AD Ольга Полуянова
 - AD Outstaff
 - AD 1с специалист
 - AD Александр Лохнев
 - AD Любовь Нигматулина
 - AD Светлана Ясакова

Основное Квота

Название
Все

Дополнительные настройки

- Запретить доступ
- Разрешить удаленный доступ через VPN

Сохранить

Авторизация



The screenshot shows the 'Авторизация' (Authentication) configuration page in the IDECO UTM interface. The left sidebar contains a navigation menu with items like 'Панель мониторинга', 'Пользователи', 'Учётные записи', 'Авторизация', 'VPN-подключения', 'Двухфакторная аутентификация', 'Ideco агент', 'Active Directory/Samba DC', 'ALD Pro', 'Обнаружение устройств', 'Мониторинг', 'Правила трафика', 'Сервисы', 'Отчёты и журналы', 'Управление сервером', and 'Почтовый релей'. The main content area is titled 'Авторизация' and has three tabs: 'Основное' (selected), 'IP и MAC авторизация', and 'Авторизация по подсетям'. Under the 'Основное' tab, there are several settings: 'Веб-аутентификация' (checked), 'Аутентификация через веб-интерфейс' (unchecked), and 'SSO-аутентификация через Active Directory' (selected). Below these is a link to 'Скачать скрипт для разавторизации'. A text input field contains 'gw.ideco.ru' with a note: 'На него будут перенаправлены запросы веб-аутентификации. Убедитесь что настроен резолвинг домена в IP-адрес Ideco UTM. Подробнее'. Another checked option is 'Авторизация через журнал безопасности Active Directory'. Under the 'Разавторизация пользователей' section, there is a dropdown menu for 'Тайм-аут отключения' set to '2 часа' with a note: 'Применяется после перезагрузки Ideco UTM'. A 'Сохранить' button is at the bottom.

✓ IP, MAC, IP+MAC, подсеть

✓ WEB

✓ Интеграция с AD: Kerberos, NTLM, security log

✓ Агент

✓ Обнаружение устройств

Ideco Агент



Айдеко Аге... — □ ×

IDECO.AGENT

Редактирование профиля

Сохранить пароль

Подключаться автоматически

Айдеко Аге... — □ ×

IDECO.AGENT

Авторизация

Успешно разавторизован

Айдеко Аге... — □ ×

IDECO.AGENT

Авторизация

Успешно авторизован

Файрвол



IDECO UTM 15.1 сборка 104 Бета

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
- Сервисы
- Отчёты и журналы
- Управление сервером

Файрвол

Работает

FORWARD DNAT (перенаправление портов) INPUT SNAT Логирование

Транзитный трафик между интерфейсами

[+ Добавить](#) Отображать названия объектов Столбцы Фильтры Высота строки Счетчик срабатываний Поиск...

Протокол	Источник	Назначение	Порты назначения	Действие	Счетчик срабаты...	Комментарий	Управление
* Любой	ИП Атакующие а...	* Любой	* Любой	Запретить	0		
* Любой	* Любой	Украина	* Любой	Запретить	4 079		
* Любой	* Любой	Россия	* Любой	Разрешить			
* Любой	Management	e1.ru	* Любой	Запретить			
L4 TCP	Все	* Любой	: HTTP	Разрешить			
* Любой	Users_AD	* Любой	* Любой	Разрешить			
* Любой	Превышена ...	* Любой	* Любой	Запретить	0		
* Любой	Дмитрий Хо...	e1.ru	* Любой	Запретить			
* Любой	* Любой	* Любой	* Любой	Разрешить			

Строк на странице: 100 1-9 из 9

Контроль приложений



IDECO UTM 15.1 сборка 104 Бета

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
- Сервисы
- Отчёты и журналы
- Управление сервером

Контроль приложений

Работает

+ Добавить Столбцы Фильтры Высота строки

Поиск...

Название	Применяется для	Протоколы	Действие	Управление
Разрешить тестировщикам торренты	Андрей Карелин Тимур	Bittorrent Doh_dot Anydesk	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
разрешить TeamView	Андрей Моргунов	Teamviewer	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
whatsapp	* Любой	Whatsapp Whatsappfiles	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Программы удаленного доступа	* Любой	Teamviewer Anydesk	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
TOR и торренты	* Любой	Bittorrent Tor Edonkey	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Запрет шифрованных DNS-запросов	* Любой	Doh_dot Dnscrypt	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Игры	* Любой	Steam Halflife2 Worldofku	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Криптомайнеры	* Любой	Mining	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Мусорный трафик	* Любой	Adultcontent Ads_analytic_track	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️

Строк на странице: 100 1-9 из 9

Контент-фильтр



IDECO UTM 15.1 сборка 104 Бета

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
- Сервисы
- Отчёты и журналы
- Управление сервером

Контент-фильтр

Правила Пользовательские категории Настройки

URL для категоризации Найти категории

URL входит в категории:

+ Добавить Отображать названия объектов Столбцы Фильтры Высота строки Поиск...

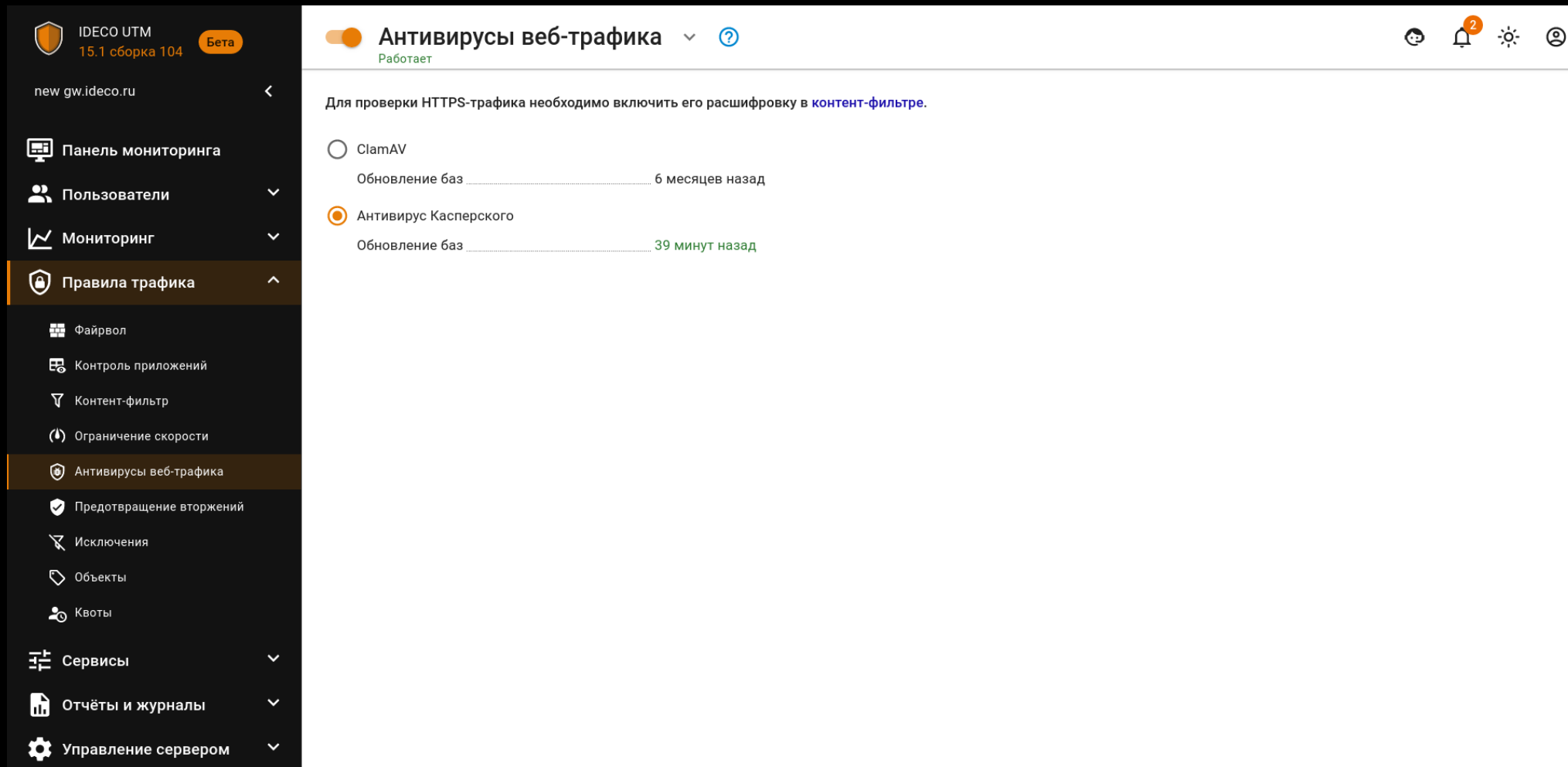
Название	Применяется для	Категории	Действие	Управление
Белый список	Все	Белый список (Польз.)	Разрешить	🔌 + ↑ ↓ ✎ 🗑️
Блокируем запрещенные сайты	Все	Черный список (Польз.)	Запретить	🔌 + ↑ ↓ ✎ 🗑️
для Марка	Марк Коренберг	Все запросы	Разрешить	🔌 + ↑ ↓ ✎ 🗑️
бухгалтерия и hr	Buhgalters HR Мг	Анонимайзеры Список Мини	Разрешить	🔌 + ↑ ↓ ✎ 🗑️
test2	Все Андрей Карелин	e1.ru (Польз.)	Расшифровать	🔌 + ↑ ↓ ✎ 🗑️
test	Андрей Карелин	e1.ru (Польз.)	Запретить	🔌 + ↑ ↓ ✎ 🗑️
Для Хомутова (тест блокировки)	Дмитрий Хомутов	e1.ru (Польз.)	Запретить	🔌 + ↑ ↓ ✎ 🗑️
marketing	Марина Тябина	Маркетинговые услуги Спис	Разрешить	🔌 + ↑ ↓ ✎ 🗑️
whatsapp	Все	Социальные сети Чаты	Разрешить	🔌 + ↑ ↓ ✎ 🗑️
Повышаем безопасность сети	Все	Анонимайзеры Ботнеты	Запретить	🔌 + ↑ ↓ ✎ 🗑️

Строк на странице: 100 1-12 из 12

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
- ✓ Блокировка quic/http3
- ✓ Гибкая настройка политик
- ✓ Обновление сигнатур 2 раза в день с серверов в РФ

Антивирусы веб-трафика



The screenshot shows the IDECO UTM web interface. The left sidebar contains a navigation menu with the following items: IDECO UTM 15.1 сборка 104 (Beta), new gw.ideco.ru, Панель мониторинга, Пользователи, Мониторинг, Правила трафика (highlighted), Файрвол, Контроль приложений, Контент-фильтр, Ограничение скорости, Антивирусы веб-трафика (highlighted), Предотвращение вторжений, Исключения, Объекты, Квоты, Сервисы, Отчёты и журналы, and Управление сервером. The main content area is titled 'Антивирусы веб-трафика' and shows a status of 'Работает'. A message states: 'Для проверки HTTPS-трафика необходимо включить его расшифровку в контент-фильтре.' Below this, two antivirus options are listed: ClamAV (update 6 months ago) and Антивирус Касперского (update 39 minutes ago).

IDECO UTM 15.1 сборка 104 Бета

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
- Сервисы
- Отчёты и журналы
- Управление сервером

Антивирусы веб-трафика Работает

Для проверки HTTPS-трафика необходимо включить его расшифровку в [контент-фильтре](#).

- ClamAV
Обновление баз 6 месяцев назад
- Антивирус Касперского
Обновление баз 39 минут назад

Антивирусы веб-трафика



ВНИМАНИЕ обнаружен вирус!

При попытке перейти по запрошенному вами адресу
Антивирус Касперского обнаружил вредоносный объект

Предотвращение вторжений



IDECO UTM 15.1 сборка 104 Бета

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
- Сервисы
- Отчёты и журналы
- Управление сервером

Предотвращение вторжений

Работает

Журнал Правила Исключения из правил Настройки

Столбцы Фильтры Высота строки Скачать CSV

Дата и время	Результат ...	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	IP источн
28 сент. 2023 г., 14:46:46	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.80.60.1
28 сент. 2023 г., 14:46:46	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	213.180.2
28 сент. 2023 г., 14:46:46	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	37.140.16
28 сент. 2023 г., 14:46:46	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	93.158.16
28 сент. 2023 г., 14:46:44	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.180.10
28 сент. 2023 г., 14:46:42	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.80.60.1
28 сент. 2023 г., 14:46:39	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.180.10
28 сент. 2023 г., 14:46:39	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.80.60.1
28 сент. 2023 г., 14:46:36	✘	Опасно	(o)DoH Query for mask-api.icloud.com	DNS поверх HTTPS	27992010	UDP	10.180.10
28 сент. 2023 г., 14:46:36	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	213.180.2
28 сент. 2023 г., 14:46:36	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	37.140.16
28 сент. 2023 г., 14:46:36	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	93.158.16
28 сент. 2023 г., 14:46:36	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	213.180.2
28 сент. 2023 г., 14:46:26	⚠	Предупреждение	ET INFO Session Traversal Utilities for NAT	Обнаружение подозрительной сс	2016150	UDP	213.180.2

Всего строк: 31 из 1108010

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

Мониторинг трафика



IDECO UTM 15.1 сборка 104 Бета

new gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг**
- Авторизованные пользователи
- VPN пользователи
- Графики загрузки
- Монитор трафика**
- Проверка IP/домена
- Telegram-бот
- SNMP
- Zabbix агент
- Правила трафика
- Сервисы
- Отчёты и журналы
- Управление сервером
- Почтовый релей

Монитор трафика

По узлам локальной сети **По приложениям**

☰ Столбцы ☰ Высота строки

Приложение	Сессии	Вх. скорость Мбит/с	Исх. скорость Мбит/с	Вх. пакеты Mpps	Исх. пакеты Mpps
TLS	706	4,53	0,10	0,00	0,00
WireGuard	1	0,54	0,05	0,00	0,00
STUN	279	0,12	1,01	0,00	0,00
Неизвестно	221	0,12	0,03	0,00	0,00
RTP	2	0,09	0,09	0,00	0,00
HTTP	306	0,07	0,10	0,00	0,00
TLS.Telegram	415	0,07	0,04	0,00	0,00
Discord	5	0,04	0,12	0,00	0,00
RPC	3	0,02	0,00	0,00	0,00
TLS.Google	123	0,02	0,00	0,00	0,00
TLS.Discord	80	0,01	0,00	0,00	0,00
TLS.WhatsApp	12	0,00	0,00	0,00	0,00
TLS.Yandex	218	0,00	0,01	0,00	0,00

Всего строк: 50

Мониторинг трафика



IDECO UTM
15.3 сборка 1

new gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг**
- Авторизованные пользователи
- VPN пользователи
- Графики загрузки
- Монитор трафика**
- Проверка IP/домена
- Телеграм-бот
- SNMP
- Zabbix агент
- Правила трафика
- Сервисы
- Отчёты и журналы
- Управление сервером
- Почтовый релей

Монитор трафика

По узлам локальной сети | По приложениям

← Сессии nikiforov-stand 10.80.20.37 Столбцы Высота строки

Протокол/по...	Назначение (I...	Назначение (...)	Приложение	Протокол/По...	Вх. скорость ↓	Исх. скорость	Вх. пакеты M	Исх. пакеты M	Длительность	Интерфейс
TCP/39788	178.79.227.128	—	HTTP.Winc	TCP/80	0,01	0,00	0,00	0,00	6 часов 43 мину	сеть 10...
TCP/38750	34.104.35.123	—	HTTP.Google	TCP/80	0,01	0,00	0,00	0,00	2 часа 47 минут	сеть 10...
ICMP	1.1.1.1	—	Неизвестно	ICMP	0,00	0,00	0,00	0,00	2 дня 9 часов 4	сеть 10...
ICMP	8.8.8.8	—	Неизвестно	ICMP	0,00	0,00	0,00	0,00	2 дня 9 часов 4	сеть 10...
ICMP	77.88.8.8	—	Неизвестно	ICMP	0,00	0,00	0,00	0,00	2 дня 9 часов 4	сеть 10...
TCP/50808	208.115.231.21	—	TLS.AnyDesk	TCP/6568	0,00	0,00	0,00	0,00	2 дня 8 часов 5	сеть 10...
UDP/50247	194.190.168.1	—	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	сеть 10...
TCP/49108	172.65.32.248	—	TLS	TCP/443	0,00	0,00	0,00	0,00	0 минут	сеть 10...
UDP/35328	162.159.200.1	—	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	сеть 10...
TCP/49096	172.65.32.248	—	TLS	TCP/443	0,00	0,00	0,00	0,00	0 минут	сеть 10...
TCP/54914	172.65.32.248	—	TLS	TCP/443	0,00	0,00	0,00	0,00	0 минут	сеть 10...
TCP/54904	172.65.32.248	—	TLS	TCP/443	0,00	0,00	0,00	0,00	0 минут	сеть 10...
UDP/58462	83.143.51.50	—	NTP	UDP/123	0,00	0,00	0,00	0,00	0 минут	сеть 10...

Всего строк: 19

События безопасности



- Авторизованные пользователи
- VPN пользователи
- Графики загрузки
- Монитор трафика
- Проверка IP/домена
- Telegram-бот
- SNMP
- Zabbix агент
- Правила трафика
- Сервисы
- Отчёты и журналы**
- Трафик
- Журнал событий
- События безопасности**
- Действия администраторов
- Журнал авторизации
- Конструктор отчётов
- Syslog
- Управление сервером
- Почтовый релей

События безопасности

Графики IDS/IPS | Журнал IDS/IPS | Web Application Firewall

28 сент. 2023 г. - 28 сент. 2023 г.

Количество атак по уровню угрозы

Уровень угрозы	Количество
Критично	63
Опасно	1 845
Предупреждение	1 285

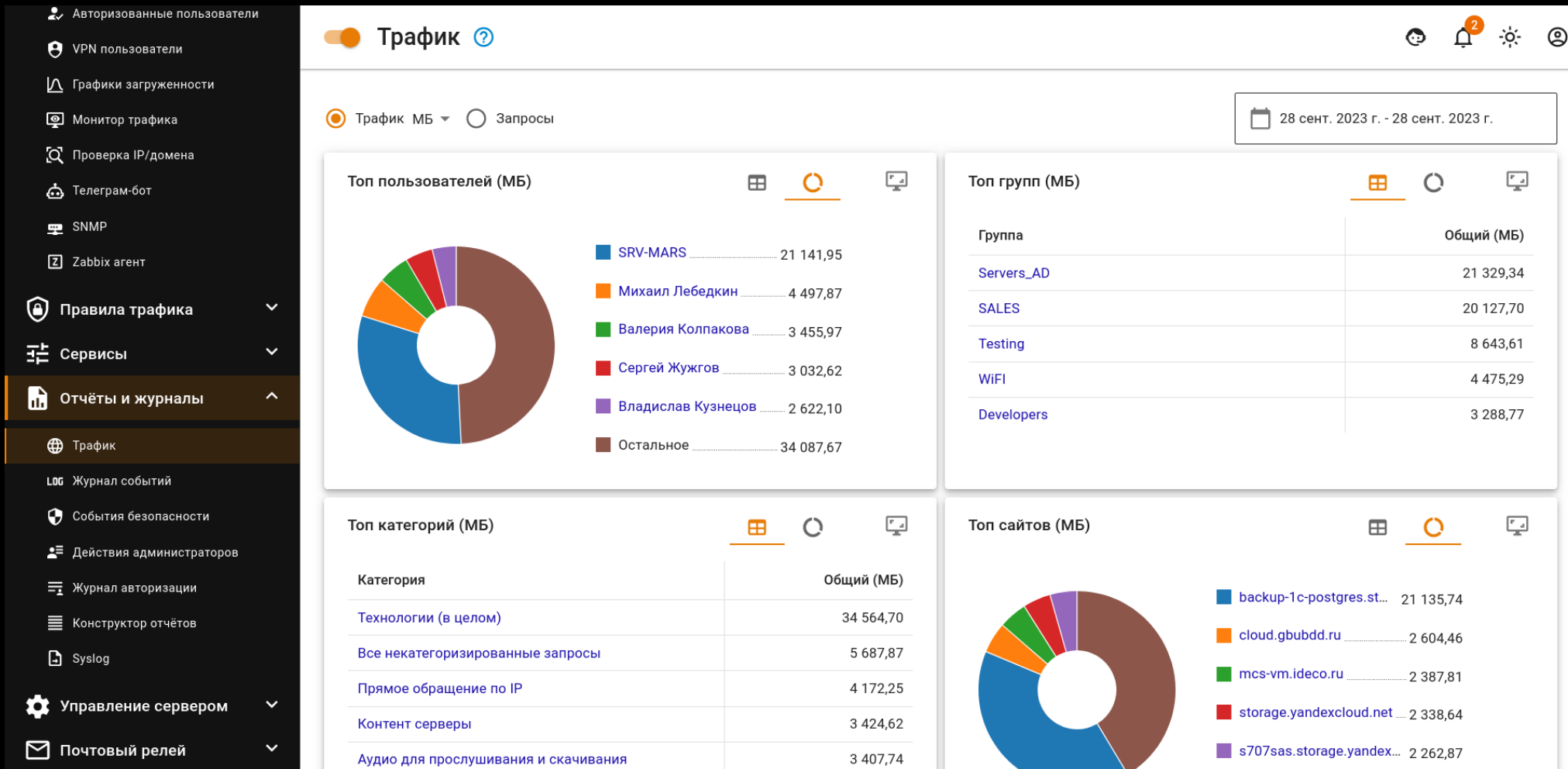
Топ атакованных адресов

Адрес	Количество
10.80.100.254	675
10.180.100.162	177
10.180.100.58	173
10.180.100.96	157
10.180.108.40	9

Топ заблокированных типов атак

Тип атаки	Количество
DNS поверх HTTPS	1 338
Обнаружение подозрител...	1 278
Пулы криптомайнеров	250
Потенциально опасный тра...	218
Запросы на скомпрометиро...	59

Детализированная отчётность по трафику



Аудит действий администраторов



- Авторизованные пользователи
- VPN пользователи
- Графики загруженности
- Монитор трафика
- Проверка IP/домена
- Telegram-бот
- SNMP
- Zabbix агент
- Правила трафика
- Сервисы
- Отчёты и журналы**
- Трафик
- Журнал событий
- События безопасности
- Действия администраторов**
- Журнал авторизации
- Конструктор отчётов
- Syslog
- Управление сервером
- Почтовый релей

Действия администраторов

Перенос строк в сообщениях | Столбцы | Фильтры | Скачать CSV

Поиск...

Дата и время	Логин	Действие	Модуль	Сообщение	Статус	Описание
28.09.2023, 14:40:15	s.zhuzhgov	Добавление	web-backend	Сделал POST-запрос	Успешно	-
28.09.2023, 14:36:13	s.zhuzhgov	Добавление	web-backend	Сделал POST-запрос	Успешно	-
28.09.2023, 14:08:05	v.ivchenko	Редактирование	dns-backend	Сделал PUT-запрос	Успешно	-
28.09.2023, 13:59:52	v.ivchenko	Добавление	dns-backend	Сделал POST-запрос	Успешно	-
28.09.2023, 13:37:38	homutov	Редактирование	system-backend	Сделал PATCH-запрос	Успешно	-
28.09.2023, 13:34:20	homutov	Редактирование	routing-rest-backend	Сделал PUT-запрос	Успешно	-
28.09.2023, 13:34:13	homutov	Редактирование	routing-rest-backend	Сделал PUT-запрос	Успешно	-
28.09.2023, 13:24:41	m.panin	Добавление	web-backend	Сделал POST-запрос	Успешно	-
28.09.2023, 12:19:55	v.ivchenko	Редактирование	dns-backend	Сделал PUT-запрос	Успешно	-
28.09.2023, 12:19:41	v.ivchenko	Добавление	web-backend	Сделал POST-запрос	Успешно	-
28.09.2023, 11:42:31	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:29	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:26	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:23	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:20	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:11	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:09	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:42:00	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:58	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:56	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:54	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:43	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:36	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:32	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 11:41:29	homutov	Удаление	proxy-backend	Сделал DELETE-запрос	Успешно	-
28.09.2023, 9:39:05	homutov	Добавление	suricata-backend	Сделал POST-запрос	Успешно	-

Всего строк: 50 из 66

Почтовый сервер/ релей



IDECO UTM 15.1 сборка 104 Бета

new gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты и журналы
- Управление сервером
- Почтовый релей**
- Основные настройки
- Расширенные настройки
- Антиспам
- Правила
- Почтовая очередь

Основные настройки Остановлен

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 STARTTLS, 993 SSL)

POP3(S) (110 STARTTLS, 995 SSL)

Web-почта

Диск для хранения почты

Для хранения почтовых ящиков нужен отдельный жесткий диск

Подключить

Сервисы



Трафик

- Балансировка канала
- Резервирование канала
- Квоты
- Шейпинг

Маршрутизация

- Статическая
- Динамическая OSPF, BGP

DNS, DHCP, NTP

Мониторинг

- Телеграм бот
- Zabbix Агент
- Syslog, SNMP

Центральная консоль

- Управление несколькими серверами

VPN

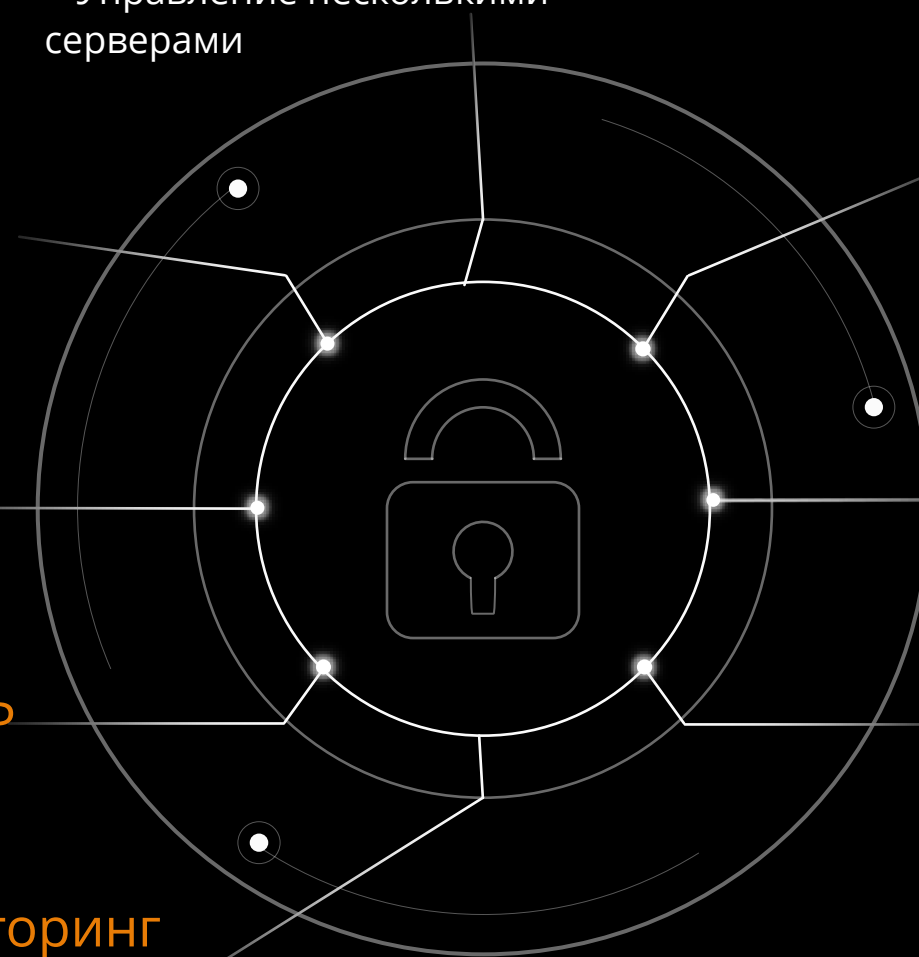
- Site-To-Site IPsec
- IKEv2
- SSTP
- Wireguard (клиент)
- L2TP/IPSec

Отказоустойчивость

- Кластеризация Active/Passive
- Резервное копирование

Обратный прокси

- Публикация WEB приложений
- Публикация OWA Exchange
- WAF



Возможности Ideco UTM 15



- ✓ Обновленная платформа на базе ядра Linux 6.1.18
- ✓ Возможность использования расширенной базы правил предотвращения вторжений от Лаборатории Касперского
- ✓ Балансировка трафика на несколько серверов обратным прокси-сервером
- ✓ Интеграция с сервисом "Мультифактор" для 2FA
- ✓ Интеграция с Samba DC, ALD PRO
- ✓ IGMP Proxy (пропуск мультикаст-трафика)
- ✓ Аудит действий администраторов
- ✓ Перехват NTP-запросов к внешним серверам (в настройках NTP-сервера)
- ✓ Выгрузка отчетов из раздела "Трафик" в формате csv
- ✓ В Контроль приложений добавлены протоколы: ADSAnalytic, AdultContent, SRTP. Улучшено определение приложений

Будущее Ideco UTM

- ✓ Развиваем агент
 - NAC
 - Linux, macOS
- ✓ Увеличиваем скорость обработки трафика, переходим на свою кодовую базу
- ✓ VRR/DPDK
- ✓ Добавляем создание профилей IPS, AC, Контент-фильтр
- ✓ Добавляем различные способы авторизации
 - Отечественные КД
 - Radius
- ✓ Шифрование
- ✓ Развиваем централизованное управление
- ✓ Добавляем сетевые функции
 - GRE
 - Зеркалирование трафика
 - IPv6

Возможности тестирования



MY . IDECO

Компания: Ideco

- NGFW
- Monitoring Bot
- Security
- Личные данные
- Компании

NGFW

s.zhuzhgov@ideco.ru

Лицензирование **Скачать** Online-демо

Межсетевой экран Ideco UTM 15

Межсетевой экран следующего поколения, система предотвращения вторжений, контент-фильтр, межсетевой экран веб-приложений, контроль приложений, VPN-сервер и многое другое.

Пробная версия после регистрации работает в полнофункциональном режиме 40 дней.

Внимание! Для установки Ideco UTM требуется отдельный сервер или виртуальная машина!

[Инструкция](#) по созданию загрузочного USB-диска для установки на сервер.

[Примечания к релизу 15](#)

[Присоединяйтесь](#) к обсуждению в нашей группе в Telegram.

Скачать

Размер файла:
996 МБ
Версия:
15.3
Build:
1
Дата выпуска:
10 октября 2023 г.
MD5:
9911a929b712857c8fbf5cca46315135

Высокопроизводительный межсетевой экран Ideco UTM VPP на новом сетевом стеке

Высокоскоростной межсетевой экран следующего поколения на технологиях DPDK/VPP. Рекомендуется для пилотных проектов крупного enterprise-сегмента.

Межсетевой экран следующего поколения, система предотвращения вторжений, контроль приложений.

Пробная версия после регистрации работает в полнофункциональном режиме 40 дней.

Скачать

Размер файла:
1.20 ГБ
Версия:
15
Build:
0



Спасибо!



 @blackzeshi

 s.zhuzhgov@ideco.ru

 t.me/idecoutm

 @ideco