

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.

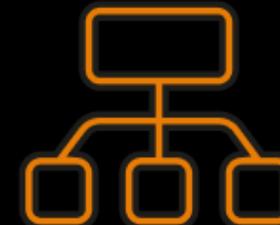
Экономим ваше время на настройке интернет-шлюза и отражения кибератак.



Более 4 000 компаний используют
Ideco UTM



180 человек в команде
S&M / R&D



Лидер по скорости разработки в
отрасли

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

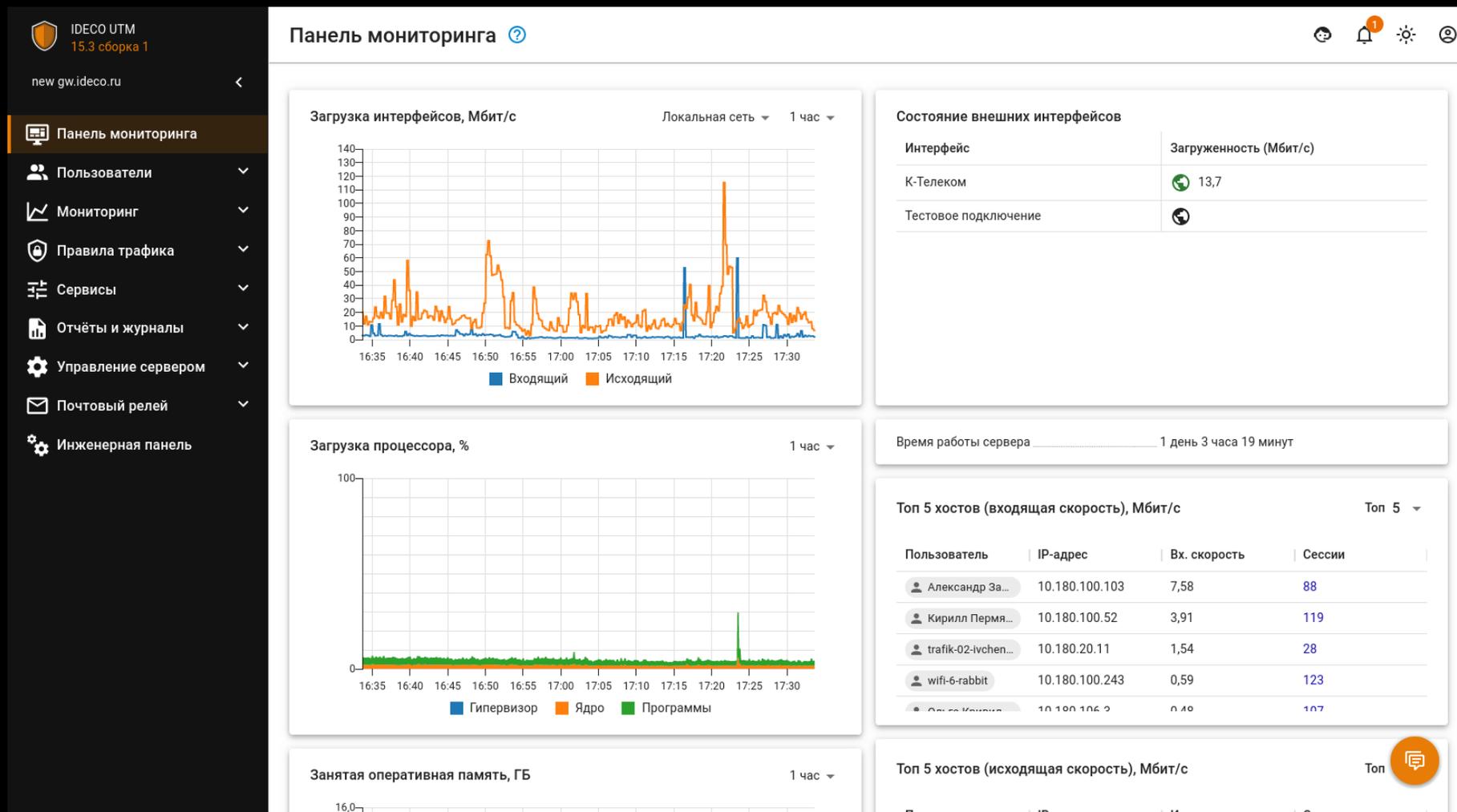
✓ Требования к СОВ

✓ 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)

Веб-интерфейс



Сервисы



Файрвол

- ✓ FORWARD/ INPUT
- ✓ DNAT/ SNAT
- ✓ Логирование



Контроль приложений

- ✓ Более 300 протоколов



Контентная фильтрация

- ✓ SNI/ SSL Bumping
- ✓ Более 500 тыс. URL



Обратный прокси

- ✓ Балансировка
- ✓ WAF
- ✓ Let's Encrypt



Предотвращение вторжений

- ✓ 30000 сигнатур
- ✓ Обновления 1 раз в 4 часа



Потоковый антивирус веб-трафика

- ✓ ClamAV
- ✓ Антивирус Касперского

Сервисы



Различные способы авторизации

- ✓ IP/ MAC/ Подсеть
- ✓ Web
- ✓ Kerberos/ NTLM/ Security logs
- ✓ Агент



VPN-сервер

- ✓ S2S-туннели
- ✓ IKEv2/ SSTP/ PPTP/ L2TP
- ✓ Wireguard
- ✓ 2FA



Быстрое внедрение

- ✓ AD
- ✓ Samba DC
- ✓ ALD Pro



Детализированная отчётность

- ✓ Отчётность по трафику
- ✓ События безопасности
- ✓ Аудит действий администраторов

Сервисы

Настройка сети

- ✓ Маршрутизация
- ✓ DNS
- ✓ DHCP
- ✓ NTP

Мониторинг устройства

- ✓ Загрузка ядра и интерфейсов
- ✓ Количество трафика
- ✓ Телеграм-бот/ Zabbix агент
- ✓ Syslog
- ✓ SNMP

Отказоустойчивость

- ✓ Кластеризация Active/Passive
- ✓ Резервное копирование

Почтовый сервер/релей

- ✓ Антиспам

Оптимизация использования интернет-канала

- ✓ Резервирование
- ✓ Балансировка
- ✓ Агрегация интерфейсов по LACP
- ✓ Шейпинг

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

Клиентский сервис

- 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



Возможности Ideco UTM 15

- ✓ Обновленная платформа на базе ядра Linux 6.1.18
- ✓ Расширенная база 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 Proxu (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.

Ideco NGFW 16: возможности

- ✓ Обновленное ядро Linux 6.3
- ✓ Zone Based Firewall
- ✓ Импорт пользователей из ALD PRO
- ✓ Защита от DOS в обратном прокси
- ✓ Улучшенная настройка VPN-авторизации пользователей
- ✓ Возможность создания маршрутов для IPSec-подключений
- ✓ Расширенные возможности DHCP
- ✓ Overlayfs и использование всего дискового пространства
- ✓ Авторизация пользователей доверенных доменов Active Directory
- ✓ Возможность включить/выключить модуль подсчета квот трафика
- ✓ Увеличена производительность модулей глубокого анализа трафика

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

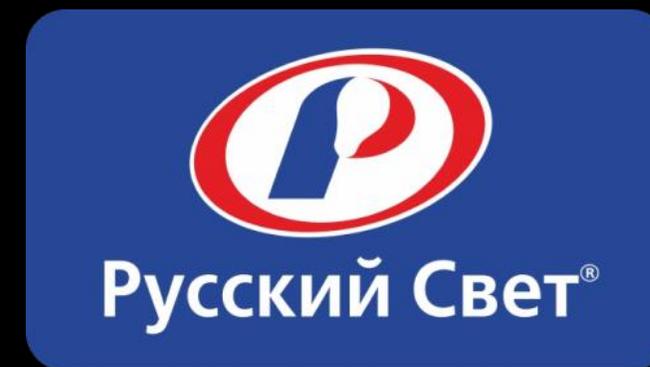
Русский свет

Запрос: замена CISCO и open source, круглосуточная ТП и выделенный канал связи, установка на своё железо, централизованное управление и мониторинг

Количество пользователей: 4000

По каким критериям выбирали Айдеко: поддержка вендора с гарантированным SLA, уверенность в присутствии на российском рынке, возможность базовой настройки продукта специалистами не экспертного уровня, резервирование каналов Интернет

Способ интеграции: межсетевой экран, прокси-сервер



АО «Арселор Миттал Темиртау»

Запрос: миграция с Microsoft TMG

Количество пользователей: 4500

По каким критериям выбирали Айдеко: техподдержка, русскоязычный интерфейс, лёгкость настройки

Способ интеграции: межсетевой экран, прокси-сервер, VPN-сервер



Компания, входящая в ОПК

Запрос:

импортозамещение

Способ интеграции:

межсетевой экран

прокси-сервер

VPN-сервер

почтовый сервер



Спасибо!



 @blackzeshi

 s.zhuzhgov@ideco.ru

 t.me/idecoutm

 @ideco