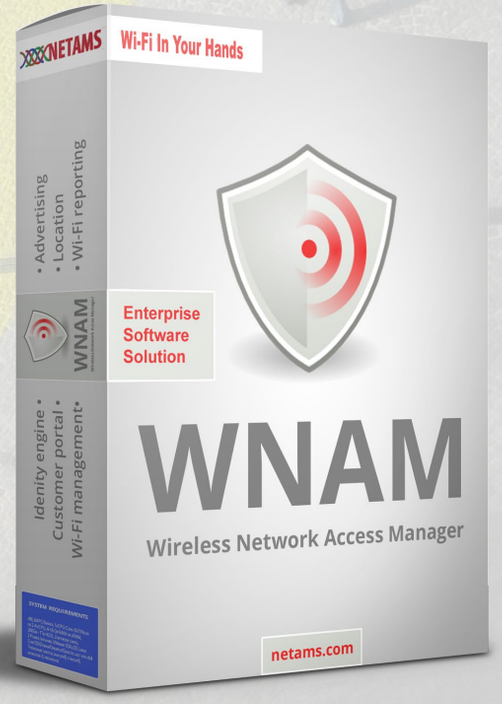
Корпоративная авторизация в проводных и Wi-Fi сетях

Ваша сеть В ВАШИХ РУКАХ

www.netams.com info@netams.com +7 (499) 346-76-60

О компании «Нетамс»

- Программное обеспечение и оборудование для сетей
- Работаем с 2008 года
- Более семи лет опыта внедрения системы авторизации WNAM
- + три новых продукта за последние два года
- 200+ клиентов:
  - операторы связи
  - частный бизнес
  - государственные организации
- Служба техподдержки
- Сеть партнеров



NETAMS

Наши клиенты

Ростелеком

ТТК

orange Business Services

UZTELECOM

ГЭС-2

ВДНХ

FIFA WORLD CUP RUSSIA 2018

KRASNOYARSK 2019
29TH WINTER UNIVERSIADE

Инвестиционный форум ВТБ Капитал
РОССИЯ ЗОВЕТ!
RUSSIA CALLING!
VTB Capital Investment Forum

Sk Сколково

МегаФон

Hoff

ТАТТЕЛЕКОМ

И
SINCE 2014
Имеретинский
КУРОРТНЫЙ РАЙОН

NAUMEN

Для вашей сети

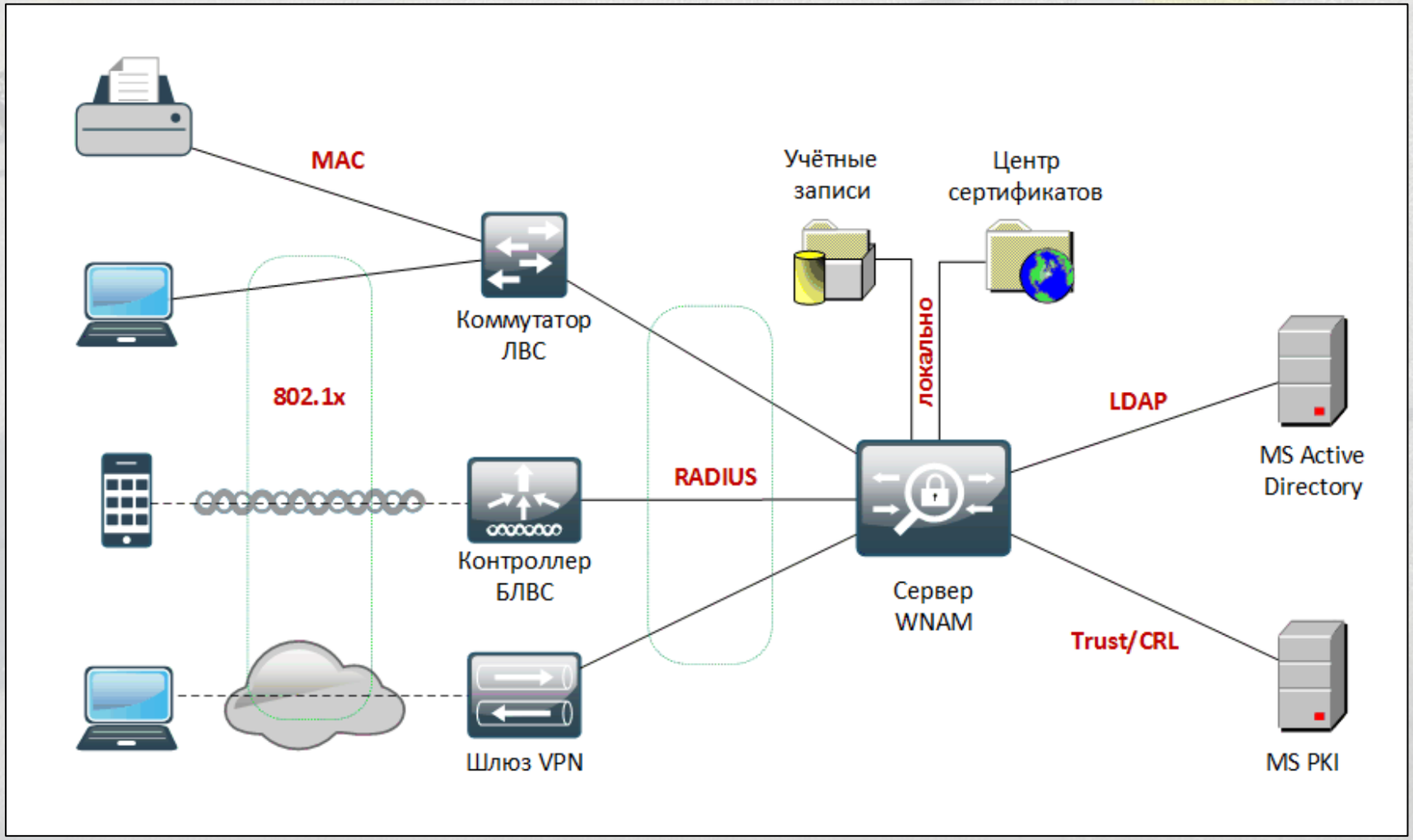
Собственные решения компании «Нетамс»

- Локальная разработка | ФИПС | РПО
- On-premises установка «без облаков»
- Бессрочная лицензия | поддержка

1. Гостевой беспроводной доступ
   - ✓ WNAM (Wireless Network Access Manager)
2. Корпоративная авторизация
   - ✓ Дополнительный модуль WNAM X
3. Контроль качества Wi-Fi
   - ✓ WNAM Quality of Wireless
4. Управление оборудованием Wi-Fi
   - ✓ WNAM Devices Controller

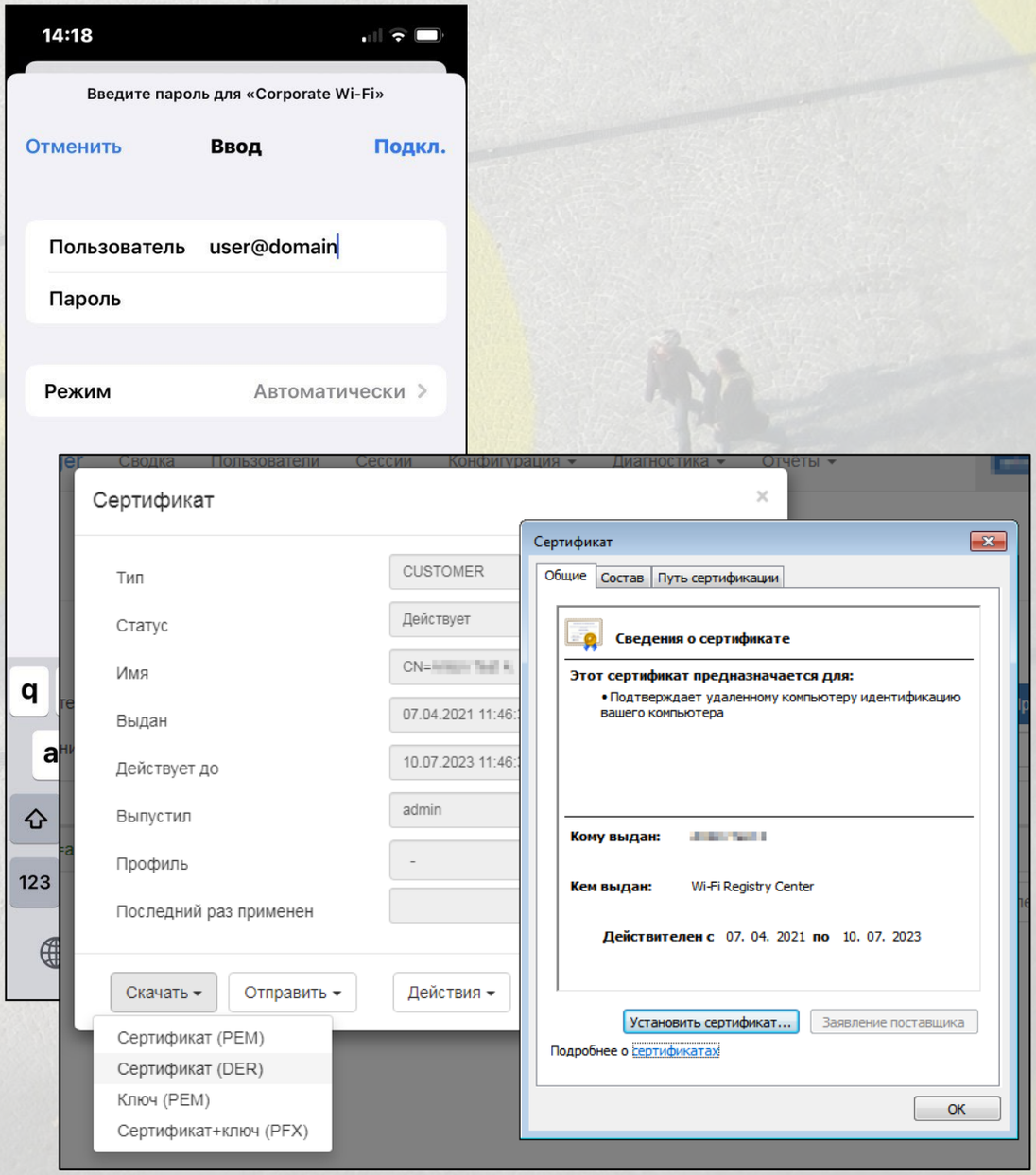
Архитектура решения корпоративной авторизации

WNAM – сервер контроля доступа пользователей через сетевое оборудование



Корпоративная авторизация

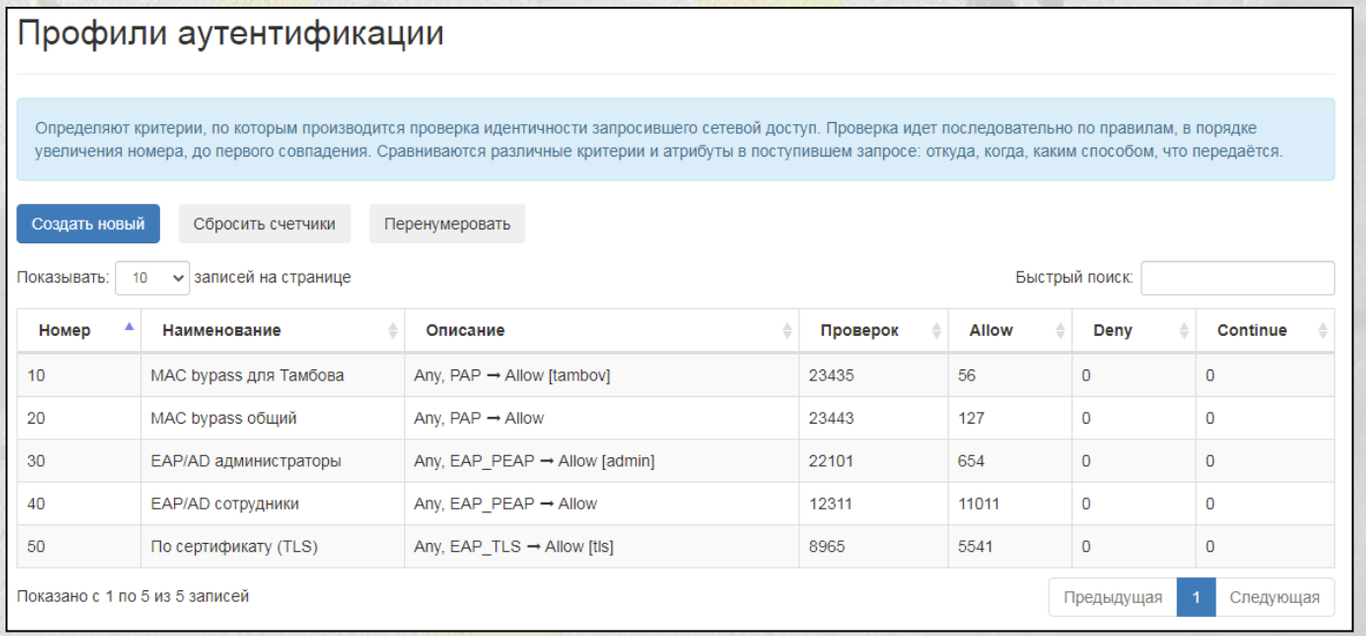
- Авторизация в закрытых 🔒 сетях Wi-Fi
- Авторизация проводных подключений к ЛВС
- Собственный RADIUS-сервер
  - Поддержка MAC bypass
  - Поддержка EAP-TLS и EAP-PEAP/MSCHAPv2
- Встроенный центр сертификатов
- Поддержка сторонних центров сертификатов
- Поддержка Active Directory
- Профилирование конечных устройств
- Поддержка TACACS+
- Логирование запросов / траблшутинг
- Отказоустойчивость
- Отчёты



Модель профилей

- Аутентификация (идентичность подключающегося)
- Авторизации (что позволено)
- Применяется наиболее подходящий профиль

Назначаемый VLAN или ACL
RADIUS-атрибуты (+редактор)
URL редиректа на портал:
    CMC-авторизация
    самообслуживание (сертификат)
Параметры сессии:
    длительность, скорость, объем
Правила проверок:
    учетных записей и сертификатов
    MAC адресов
    членство в группах AD

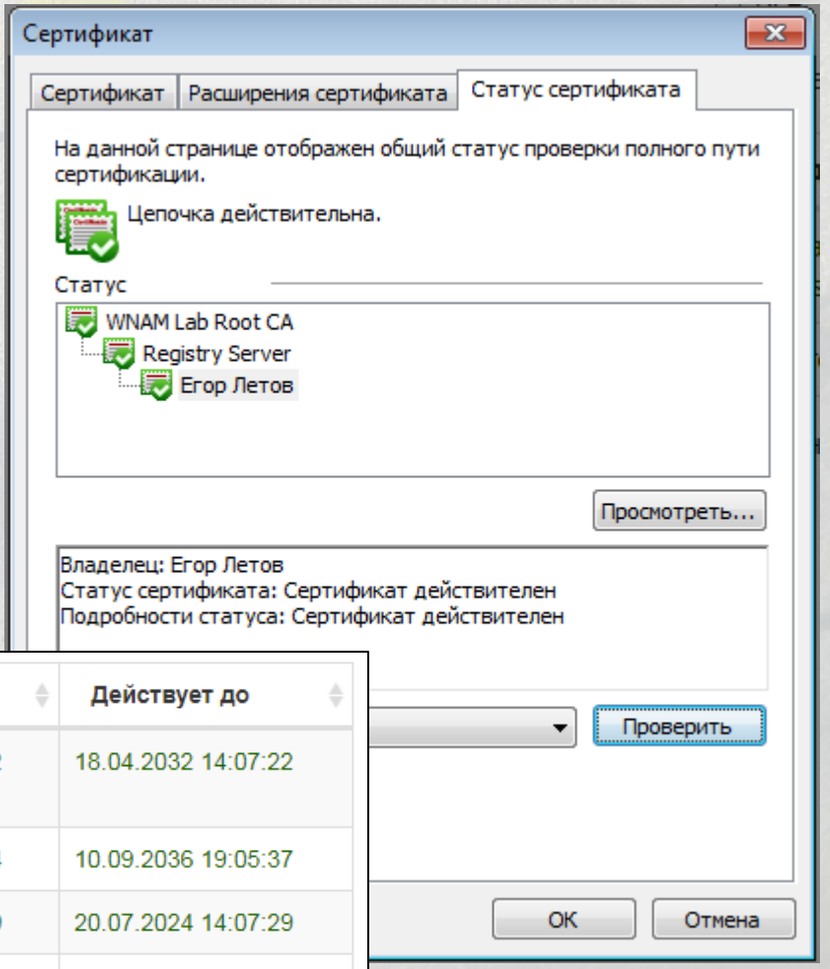


Альтернатива проприетарным Cisco ISE, Cisco ACS, Microsoft NPS, Aruba ClearPass, Ruckus Cloudpath
Альтернатива сложному в настройке и неудобному в эксплуатации опенсорсу FreeRADIUS

Работа с сертификатами

- Встроенный корневой УЦ
- Подчиненные сертификаты от УЦ вашего предприятия
- Запрос на подпись сертификата CSR в вашем УЦ
- Проверка списков отзыва

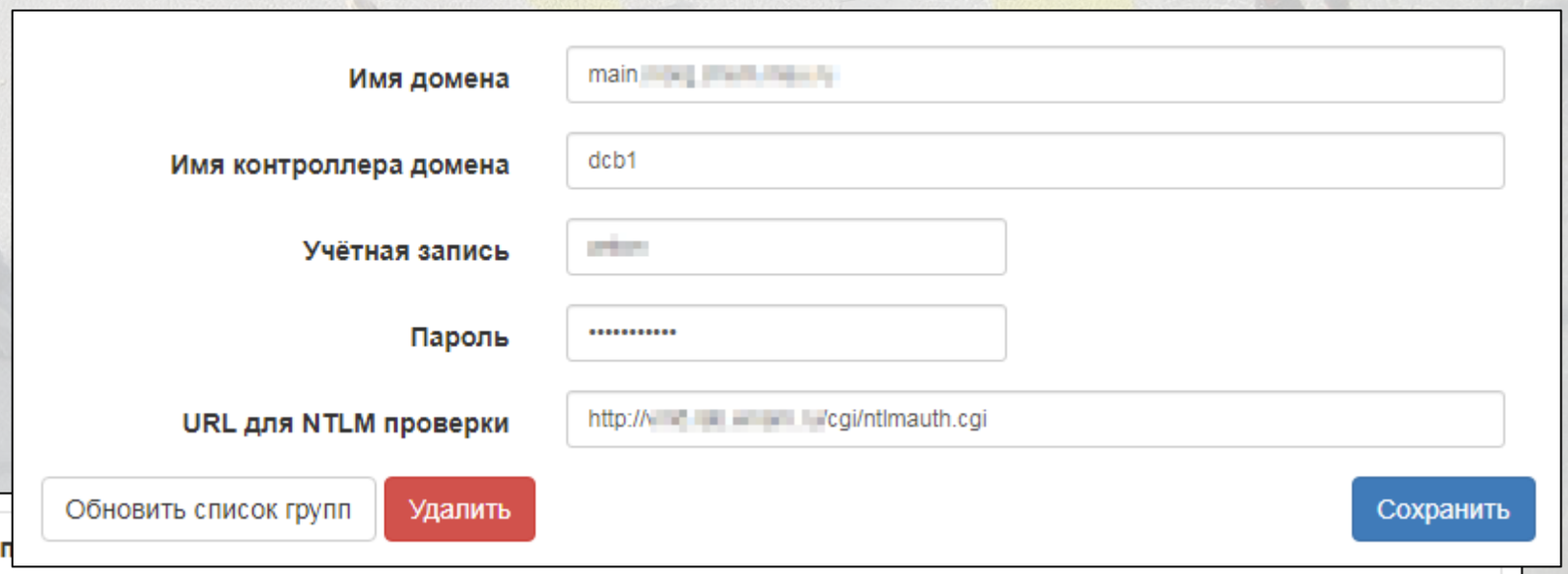
- Для работы RADIUS-сервера WNAM
- Формирование клиентских сертификатов доступа



Тип	Имя	Действует с	Действует до
CA	CN=WNAM Lab Root CA, O=Netams. LLC, OU=Development, L=Moscow, E=support@netams.com	18.04.2022 14:07:22	18.04.2032 14:07:22
CA	CN=MAIN2 domain root, DC=main	10.09.2016 19:00:34	10.09.2036 19:05:37
REGCENTER	CN=Registry Server, O=Netams. LLC, OU=Development, L=Moscow, E=support@netams.com	18.04.2022 14:07:29	20.07.2024 14:07:29
SERVER	CN=Auth Server, O=Netams. LLC, OU=Development, L=Moscow, E=support@netams.com	18.04.2022 14:07:25	20.07.2024 14:07:25
SERVER	CN=acs	11.09.2021 11:15:28	10.09.2026 11:15:28

Взаимодействие с Active Directory

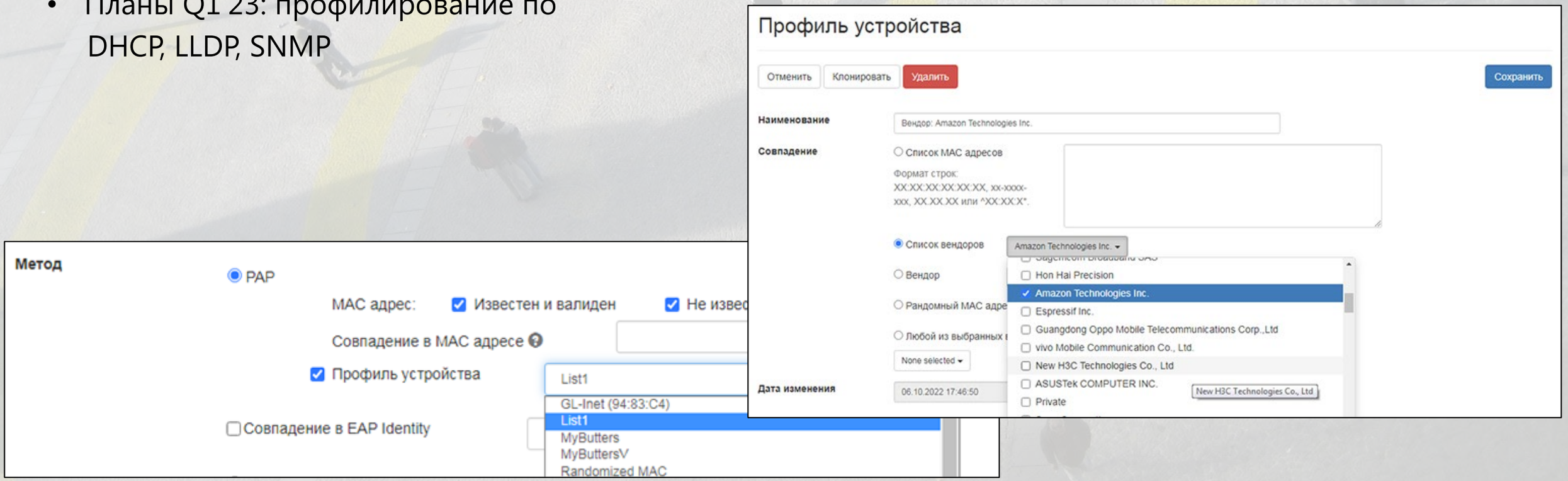
- Получение списка доменных групп для проверок по ним
- Получение групп и атрибутов пользователя в момент авторизации
- NTLM-проверка пароля для EAP-PEAP/MSCHAPv2
- Поддержка нескольких доменов



#	Имя группы	Путь групп
☐	Exchange Servers	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=main,
☐	Users	CN=Users,CN=Builtin,DC=main,DC=
☑	Domain Users	CN=Domain Users,CN=Users,DC=

Профилирование устройств

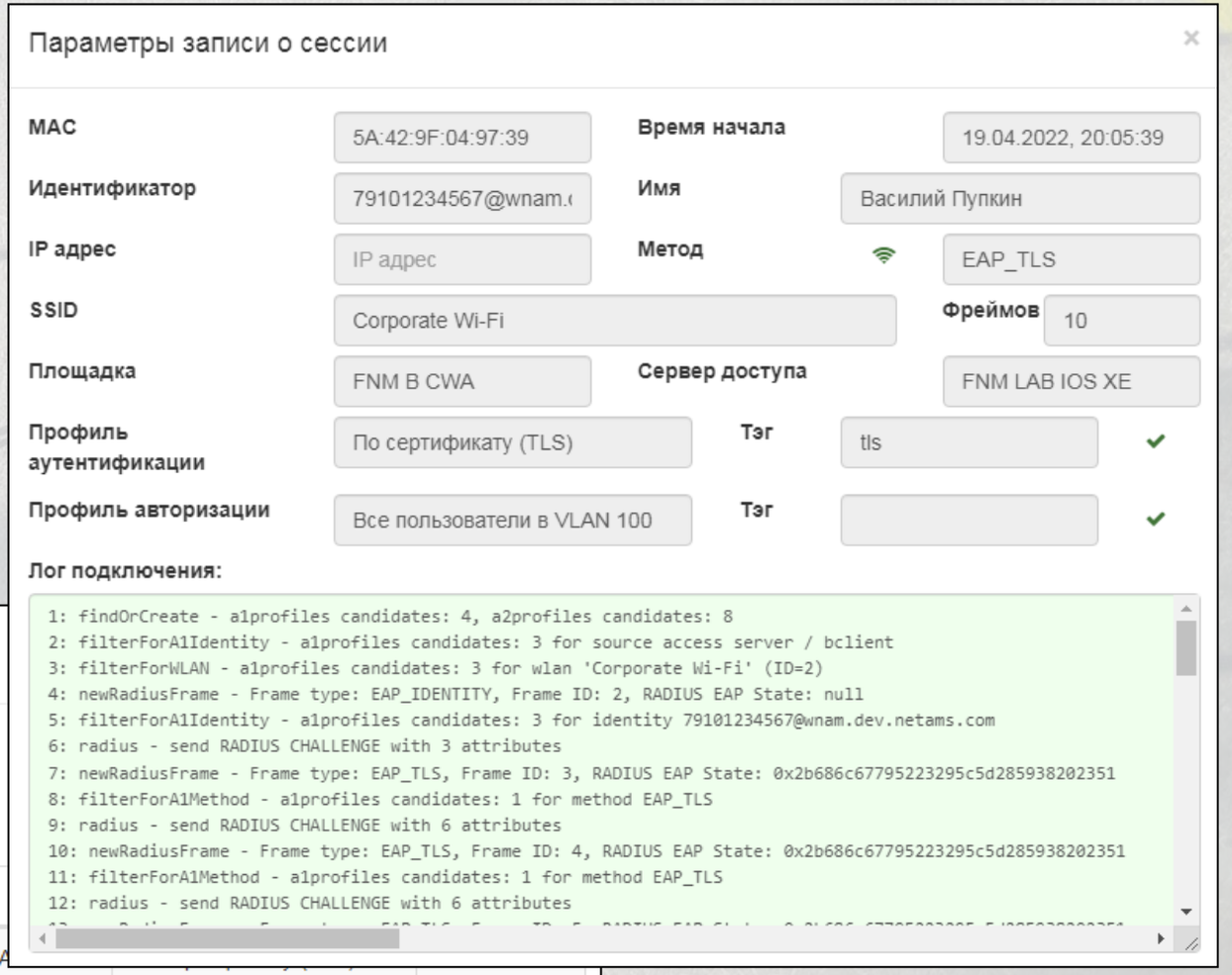
- Ведения списков оборудования по вендорам, таблицам MC адресов
- Работает при MAC-авторизации (MAC Bypass) для тех, кто не поддерживает EAP-TLS/EAP-PEAP
- Привязка к профилям аутентификации
- Назначение политик (VLAN, ACL) оконечному оборудованию на основе MAC-адреса
- Планы Q1’23: профилирование по
  DHCP, LLDP, SNMP

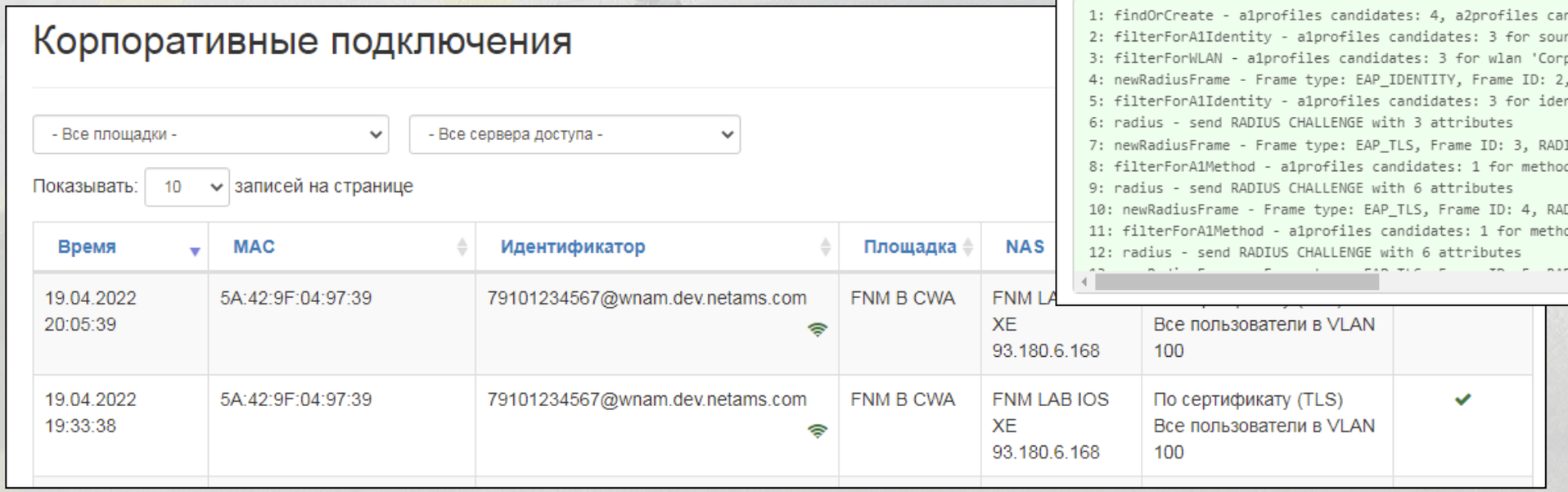


Траблшутинг

- Детальный лог подключения
- Совпавшие правила и профили
- Примененные атрибуты ACL, VLAN
- Аккаунтинг трафика

- Причина отказа в подключении





TACACS+

- Авторизация доступа администраторов к сетевому оборудованию
- Локальная база учётных записей, групп, или Active Directory
- Примененные атрибуты и ограничения
- Разрешенные и запрещенные команды
- Лог набранных администратором команд

- Поиск «кто это сделал?»

Время	Логин	Откуда	Сервер доступа			
20.05.2022 17:33:21	testuser	172.16.130.5	R20 LAB SW 172.16.130.38			
20.05.2022 12:21:03	anton	172.16.130.5	R20 LAB SW 172.16.130.38			
20.05.2022 12:20:44	nouser	172.16.130.5	R20 LAB SW 172.16.130.38			
20.05.2022 12:20:33	testuser	172.16.130.5	R20 LAB SW 172.16.130.38	0	3	⊘
19.05.2022 18:36:20	testuser	172.16.130.5	R20 LAB SW 172.16.130.38	15	5	✔

Параметры записи о сессии

Логин	testuser	Результат аутентификации	✔
Время начала	20.05.2022, 17:33:21	Время завершения	20.05.2022, 17:33:29
Удалённый адрес	172.16.130.5		
Идентификатор сессии	489d22cc	Уровень 15	Фреймов 6
Сервер доступа	R20 LAB SW	NAS 172.16.130.38	tty1

Лог подключения:

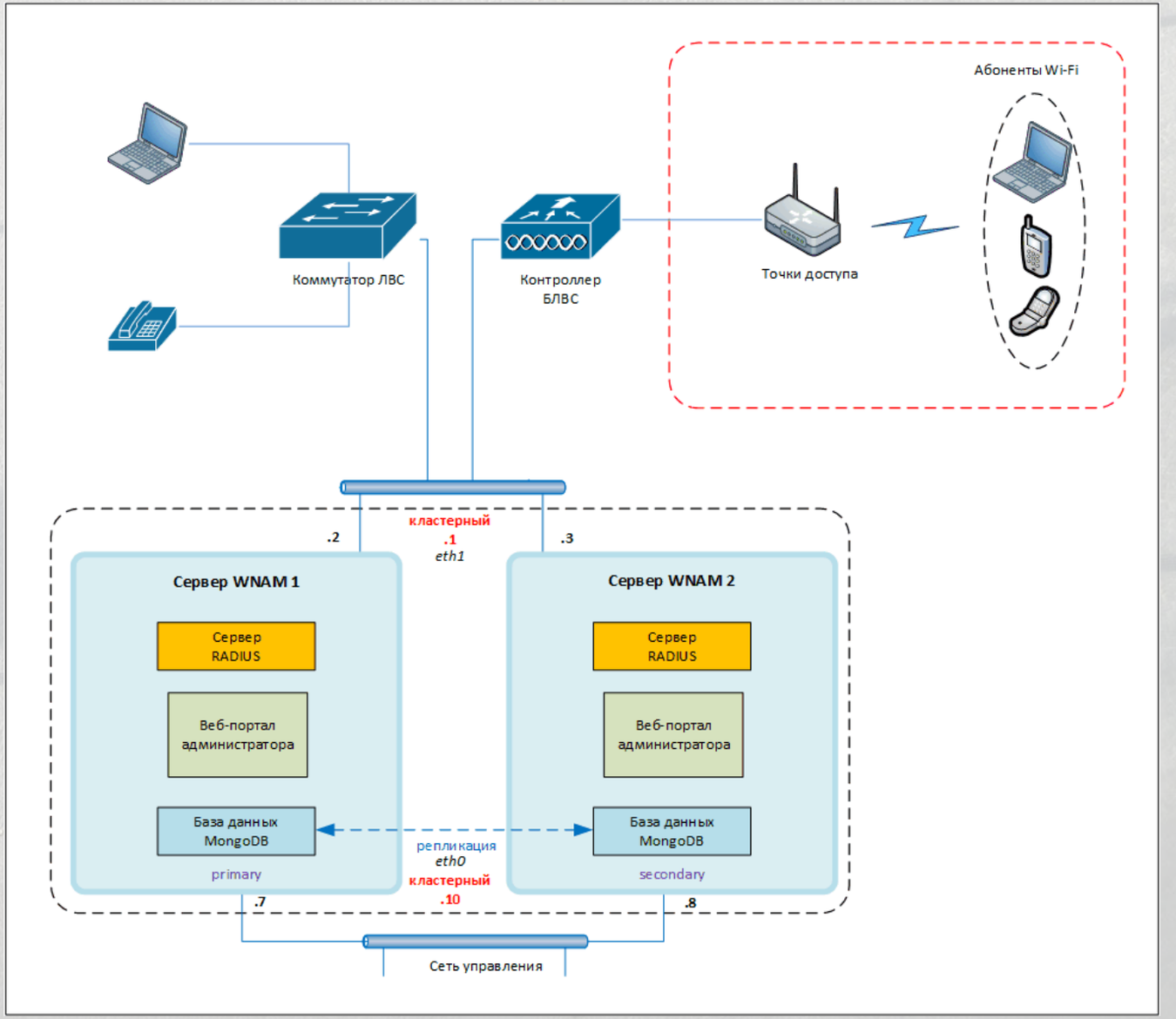
```
20.05.2022, 17:33:21 [1] authentication ASCII - request password
20.05.2022, 17:33:23 [2] authentication ASCII - success
20.05.2022, 17:33:23 [3] authorization action - [service=shell, cmd*]
20.05.2022, 17:33:23 [4] accounting started - [task_id=113, timezone=UTC, service=shell]
20.05.2022, 17:33:26 [5] authorization command - show version
20.05.2022, 17:33:29 [6] authorization command - exit
20.05.2022, 17:33:29 [7] accounting stopped - [task_id=113, timezone=UTC, service=shell, disc-cause=1, disc-cause-
```

Отказоустойчивость

- Поддержка кластерной конфигурации
- Репликация базы данных
- Поддержка гео-распределенной конфигурации

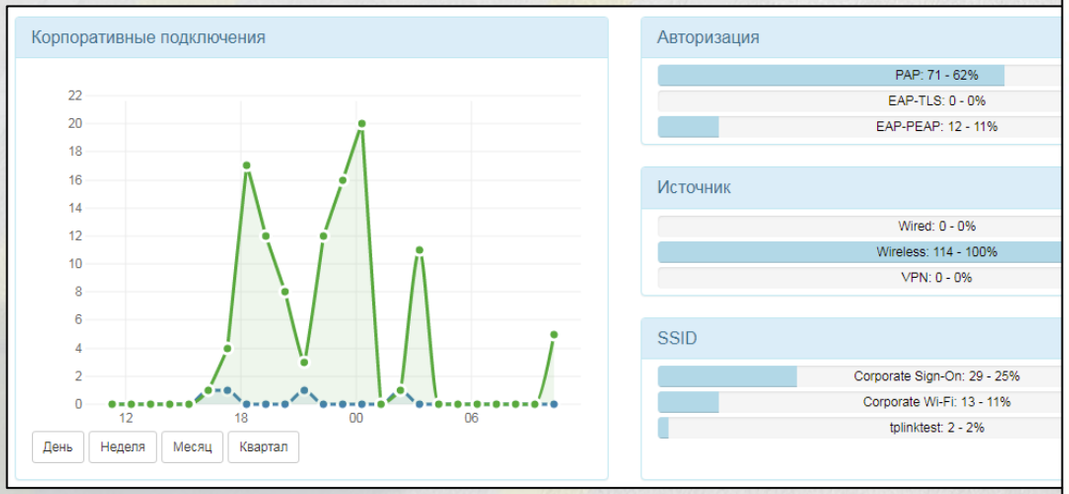
Работает под управлением ОС Linux, в том числе российских

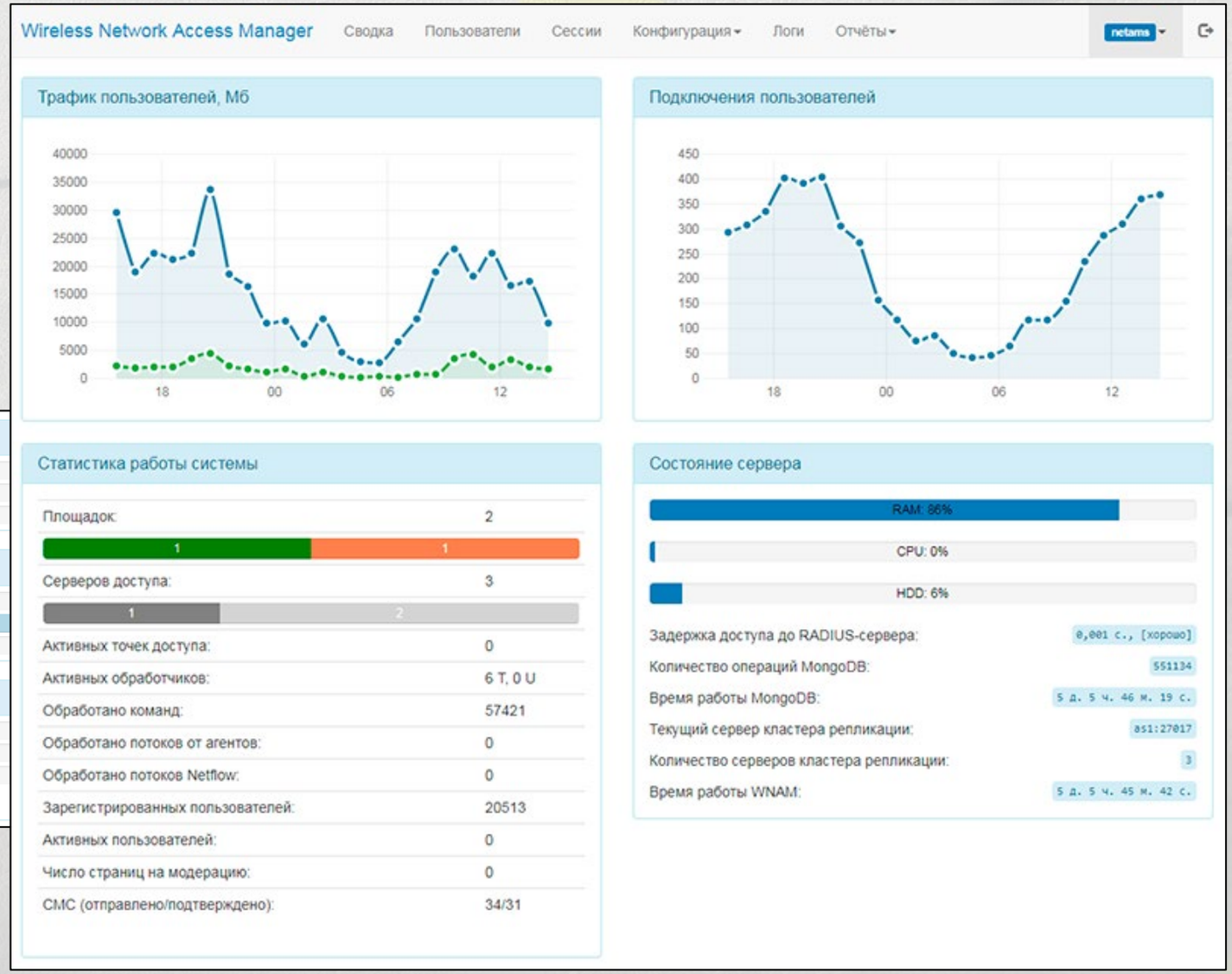
Поддерживается виртуализация



Интерфейс

- Ролевая модель доступа в UI
- Дашборды и отчеты по типам авторизации, правилам и т.п.
- Аккаунтинг сессий и трафика
- Экспорт данных CSV, PDF
- Экспорт данных по API





Список функций

Модуля корпоративной авторизации WNAM (без учёта гостевой Wi-Fi авторизации)

Собственный RADIUS сервер с поддержкой TLSv1, TLSv1.1, TLSv1.2
Поддержка матчинга по источнику NAS, группе NAS, типу подключения, имени SSID
Поддержка MAB (RADIUS PAP)
Проверка MAC-адреса в подсистеме профилирования устройств
Профили устройств на основе MAC, маски MAC, группы MAC, вендора, вложенных профилей
Проверка совпадения по EAP Identity (регулярное выражение)
Поддержка EAP-PEAP
Мульти-домен с обращением по LDAP
Проверка NTLM-пароля в контроллере домена
Проверка членства учетной записи в группе домена (выбрана или по подстроке)
Поддержка EAP-TLS
Встроенный удостоверяющий центр
Интеграция с удостоверяющим центром предприятия (CSR, Trust)
Доверенное формирование пользовательских сертификатов
Портал самообслуживания (онбоардинга) EAP-TLS с предварительной CMC- или AD-авторизацией
Проверка валидности сертификата клиента

Список функций

Модуля корпоративной авторизации WNAM (без учёта гостевой Wi-Fi авторизации)

Проверка по полям DN, SAN, Issuer сертификата
Проверка наличия учетной записи из поля сертификата в Active Directory
Поддержка machine+user идентификации
Множественные политики аутентификации на основе визуально настраиваемых критериев
Множественные политики авторизации на основе визуально настраиваемых критериев
Матчинг по совпадению тэга или совпавшего правила аутентификации
Справочник и редактор RADIUS-атрибутов
Назначение VLAN, Voice domain, ACL ID, произвольных RADIUS атрибутов
Формирование загружаемых ACL, назначение профилям
Ограничения по длительности, скорости трафика и объема данных в сессиях
Лимитирование создания новых эндпоинтов
Логгирование попыток AAA подключений, диагностика неисправностей

Учётные записи и группы пользователей TACACS+
Парольная политика учетных записей TACACS+
Редактор политик подключений с ограничениями по командам и атрибутам
Логгирование попыток TACACS+ подключения, набранных команд, диагностика неисправностей

Поддержка продаж

ведется с привлечением авторизованных системных интеграторов

Проектирование

- Помощь с разработкой архитектуры решения (лицензии, сайзинг, инфраструктура, …)
- Демо-лицензии

Внедрение

- Пуско-наладочные работы силами обученных специалистов
- Помощь в настройке взаимодействия с системами заказчика
- Настройка правил авторизации в соответствии и бизнес-требованиями
- Обучение специалистов заказчика

Техническая поддержка

- Работа по регламенту в соответствии с согласованным SLA

Доработки

- Оперативное устранение выявленных замечаний
- Расширение функционала системы по запросу заказчика

Оборудование и программное обеспечение WNAM

Дополняет вашу сеть полезными сервисами

- Гостевая авторизация WNAM (Wireless Network Access Manager)
  - Полное соответствие требованиям законодательства
  - Реклама, статистика, опросы
- Корпоративная авторизация WNAM
  - 802.1x доступ на основе политик
- Сенсор качества Wi-Fi – WNAM Quality of Wireless
  - Проактивный мониторинг и контроль SLA
  - Инструменты для инженеров
- Управление точками доступа - WNAM Devices Controller

Всё запускается на ваших серверах, без облаков!

Узнать больше:

https://www.netams.com/corp_auth/

Запросить условия:

info@netams.com

+7 (499) 346-76-60