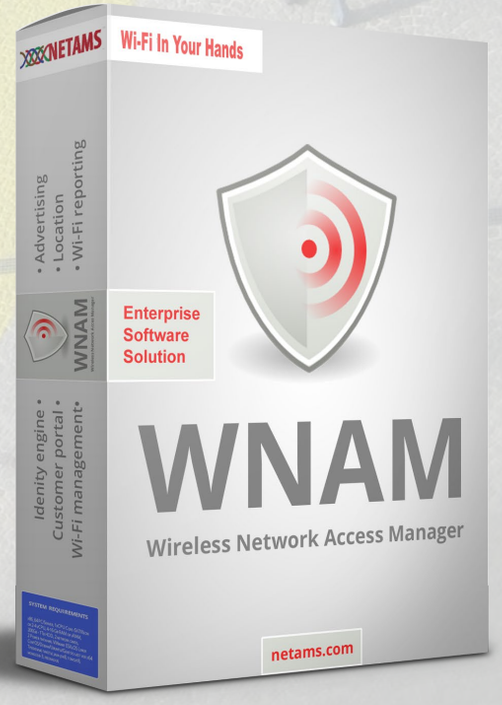
Корпоративная авторизация в проводных и беспроводных сетях

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 девяти 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

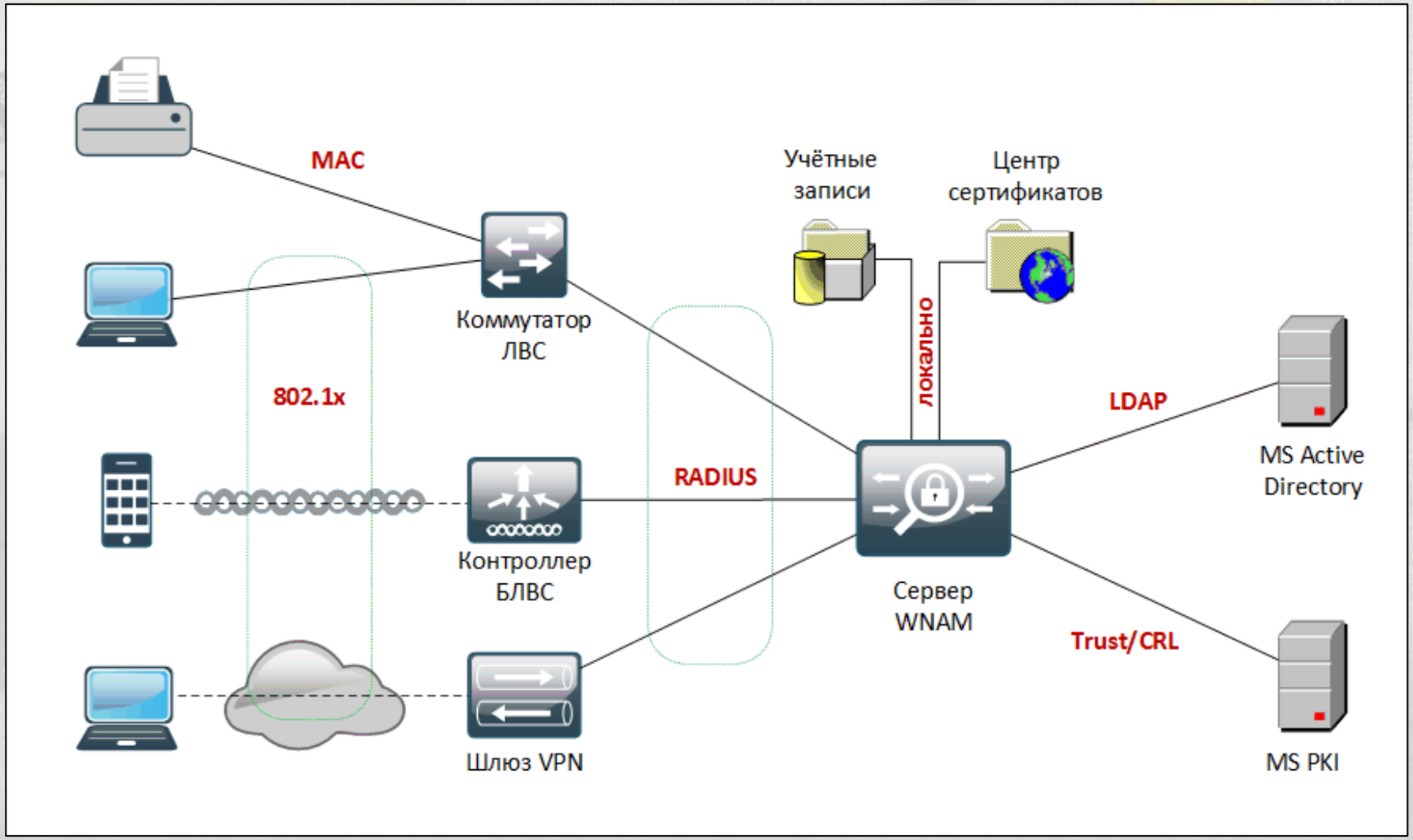
Собственные решения компании «Нетамс»

- Локальная разработка | ФИПС | Реестр Минцифры
- On-premises установка «без облаков»
- Бессрочная лицензия | Поддержка

1. Гостевой беспроводной доступ
   - ✓ WNAM (Wireless Network Access Manager)
2. Корпоративная авторизация
   - ✓ Дополнительный модуль для WNAM
3. Контроль качества Wi-Fi
   - ✓ WNAM Quality of Wireless
4. Контроллер беспроводных точек доступа Wi-Fi
   - ✓ WiCo

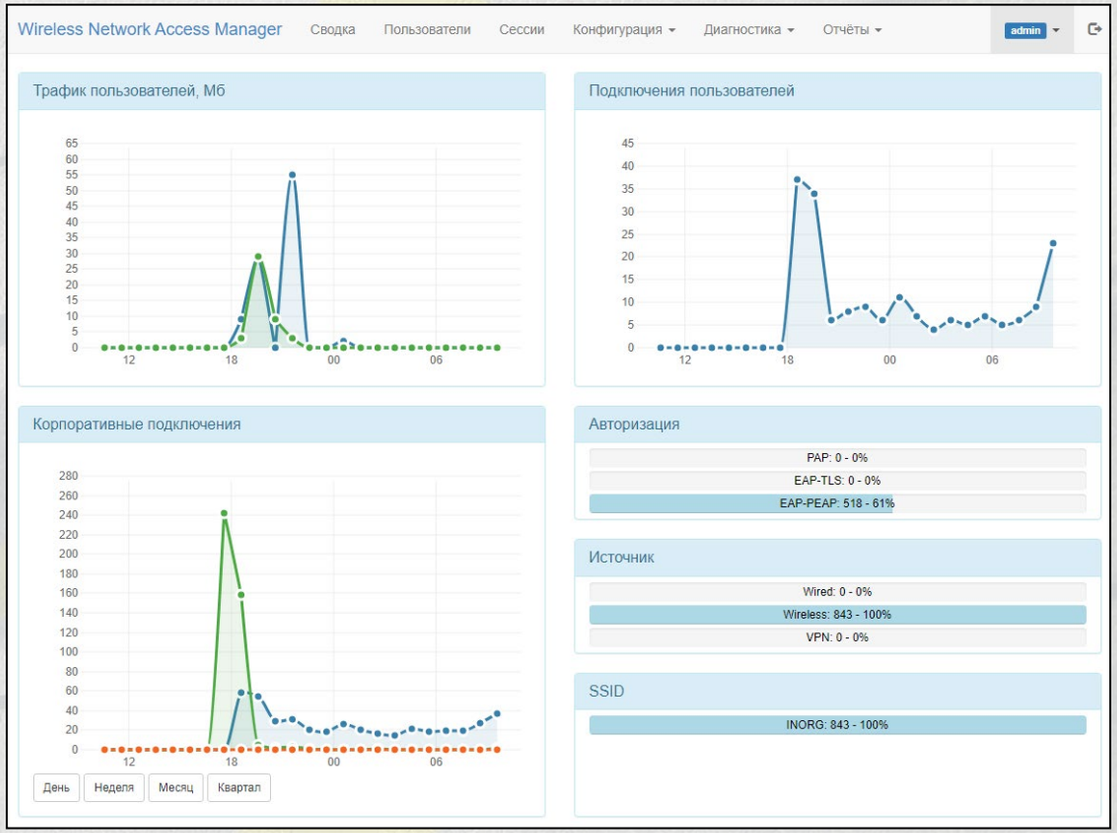
Архитектура корпоративной авторизации

WNAM – сервер контроля доступа пользователей к сети



Корпоративная авторизация WNAM

- Контроль доступа
  - В закрытых сетях Wi-Fi
  - Проводных подключений к ЛВС
  - VPN подключений
  - Администраторов к оборудованию
- Собственный RADIUS-сервер
  - Поддержка MAC bypass (MAB)
  - Поддержка EAP-TLS и EAP-PEAP/MSCHAPv2
- Гибкая система конфигурации через браузер
- Отказоустойчивость и кластеризация
- Диагностика и траблшутинг
- Российское ПО для Linux



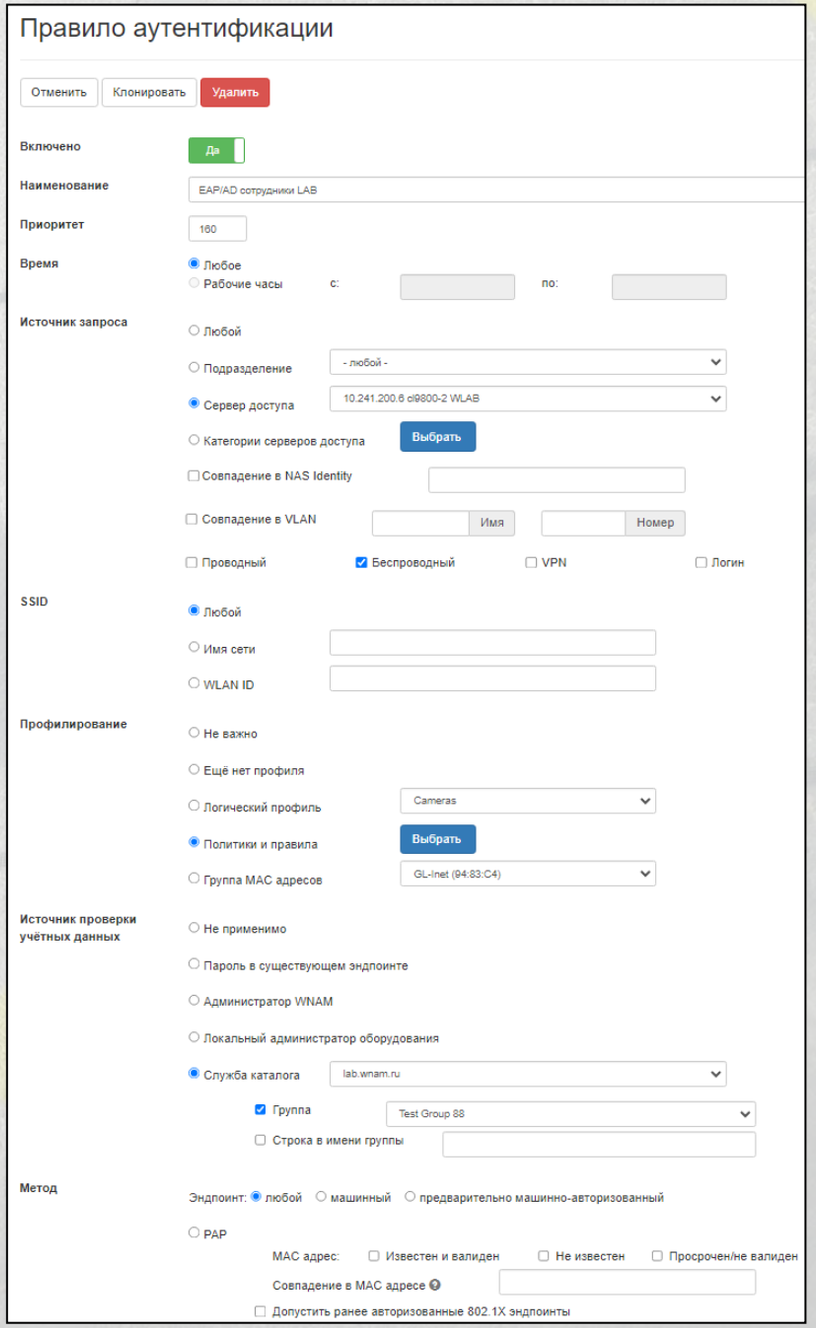
Альтернатива проприетарным Cisco ISE, Cisco ACS, Microsoft NPS, Aruba ClearPass, Ruckus Cloudpath
Альтернатива опенсорсу FreeRADIUS

Модель правил аутентификации

- Проверка источника и типа подключения
- Проверка «личности» подключающегося:
  - Локальная база данных
  - Взаимодействие с PKI
    - Проверка валидности сертификата
    - Проверка полей в сертификате
  - Взаимодействие со службами каталога
    - Проверка хэша пароля
    - Членство в группах
    - LDAP-атрибуты
- Проверка результатов профилирования
- Гибкие фильтры и критерии запроса

Применяется наиболее подходящий профиль

- Быстрое принятие решения (пустить или нет)
- Переход на правила авторизации (что вернуть)

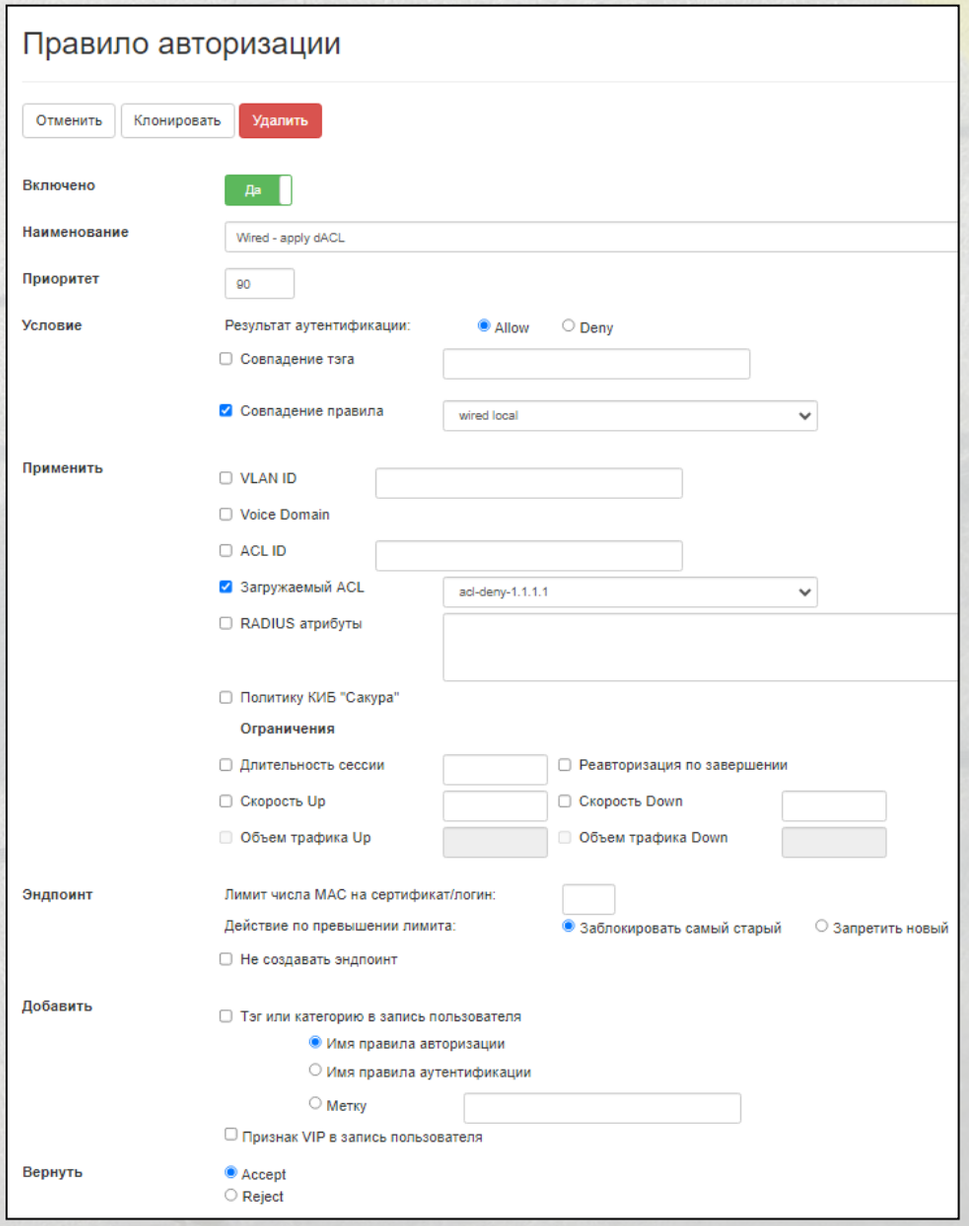


Модель правил авторизации

- Проверка результата аутентификации
  - Какое совпало правило
- Вернуть сетевому оборудованию:
  - Номер VLAN
  - Фильтр
  - Загружаемый ACL
  - Ограничения доступа
  - Редирект на портал самообслуживания
  - Произвольные RADIUS-атрибуты
- Формирование профиля эндпоинта
- Проверка защищенности АРМ («Сакура»)
- Протоколирование события авторизации (+SIEM)

Применяется наиболее подходящий профиль

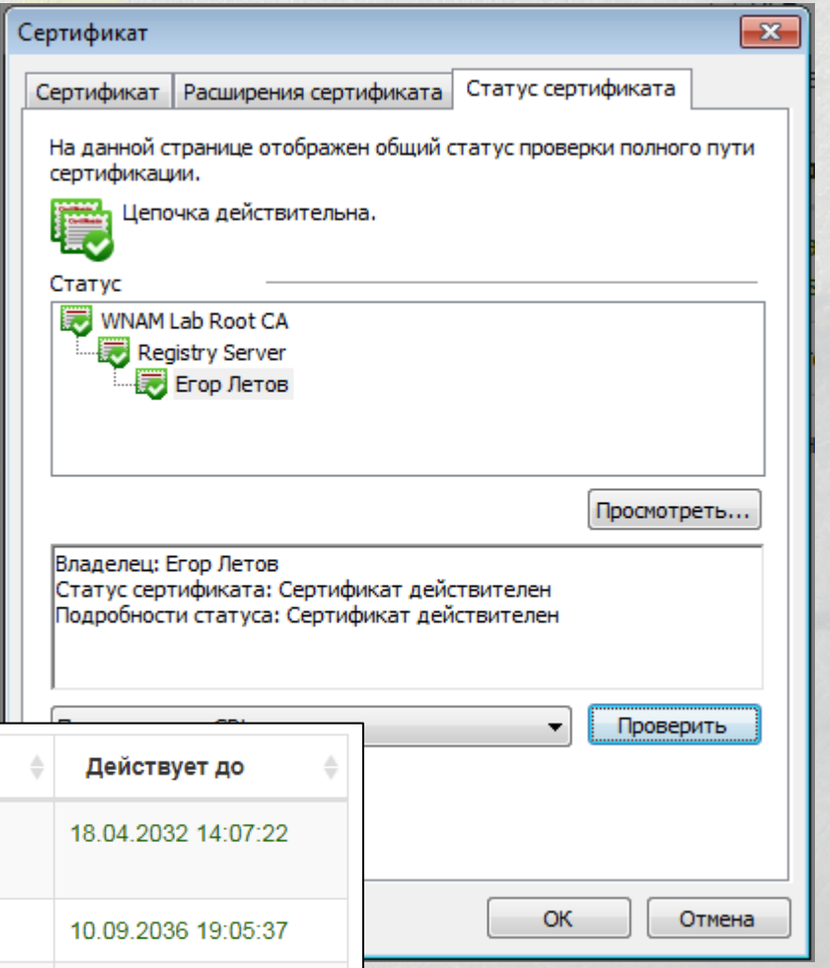
- По умолчанию: отказ в доступе



Работа с сертификатами

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

- Для работы RADIUS-сервера WNAM
- Формирование клиентских сертификатов доступа
- Портал самообслуживания. Поддержка SCEP для BYOD
- Авторизация по EAP-TLS



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 со службами каталога

- MS Active Directory и FreeIPA
- Получение списка доменных групп и важных атрибутов
- Проверка групп и атрибутов пользователя в момент его авторизации
- EAP-PEAP/MSCHAPv2
- NTLM-проверка пароля
- Мульти-домен
- Кластерная конфигурация

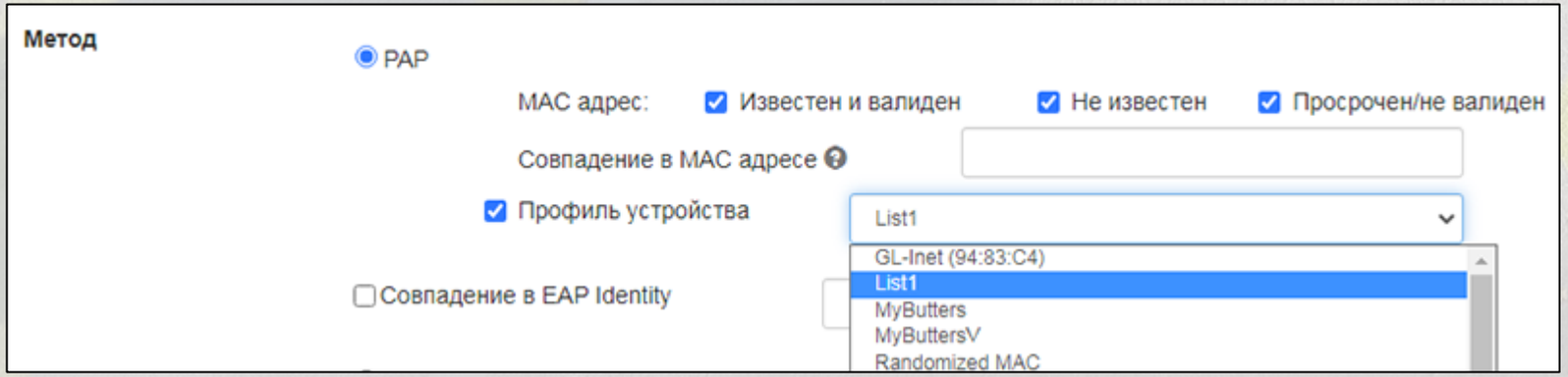
Домен	Статус
lab.wnam.ru	Важных групп: 3, Важных атрибутов:3 TEST-WNAM1 LDAPS NTLM win.lab.wnam.ru 24.10.2023 09:55:33 TEST-WNAM2 LDAPS NTLM win.lab.wnam.ru 24.10.2023 09:47:51
main.inorg.chem.msu.ru	Важных групп: 0, Важных атрибутов:0 TEST-WNAM1 LDAPS NTLM 10.241.144.75 24.10.2023 09:55:33 TEST-WNAM2 LDAPS NTLM dcb1.main.inorg.chem.msu.ru 24.10.2023 09:47:51
otherdom.wnam.ru	Важных групп: 1, Важных атрибутов:2 TEST-WNAM1 LDAPS dc.otherdom.wnam.ru 24.10.2023 09:55:33

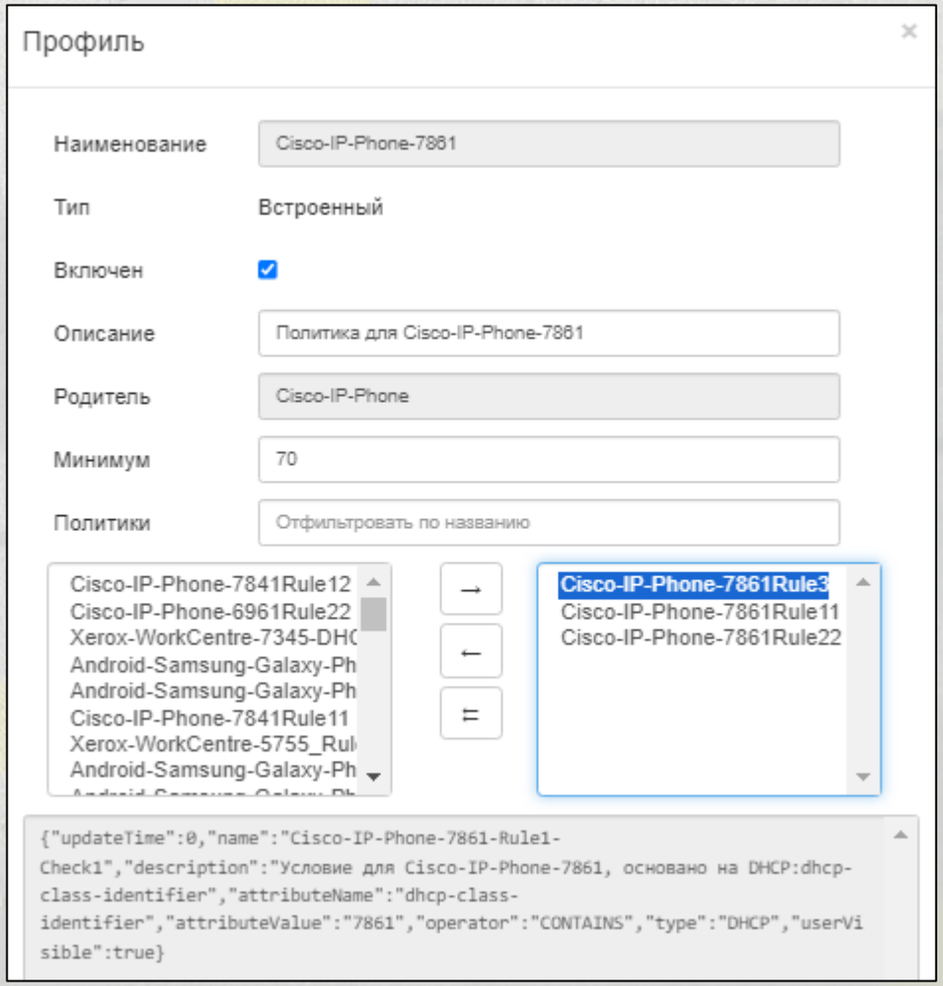
#	Имя группы	Путь группы в AD
☐	Exchange Servers	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=main,[redacted]
☐	Users	CN=Users,CN=Builtin,DC=main,DC=[redacted]
☑	Domain Users	CN=Domain Users,CN=Users,DC=[redacted]

Профилирование устройств

- Работает при MAC-авторизации (MAB)
- Применяется в правилах аутентификации
- Источники данных:
  - По вендорам, по таблицам MAC адресов
  - DHCP, CDP, LLDP данные от Cisco Device Sensor
  - SNMP опрос коммутаторов
  - Анализ DHCP пакетов Linux-агентом
- CoA (сброс порта) при смене профиля, помещение в карантин

1000+ встроенных правил, можно создавать свои

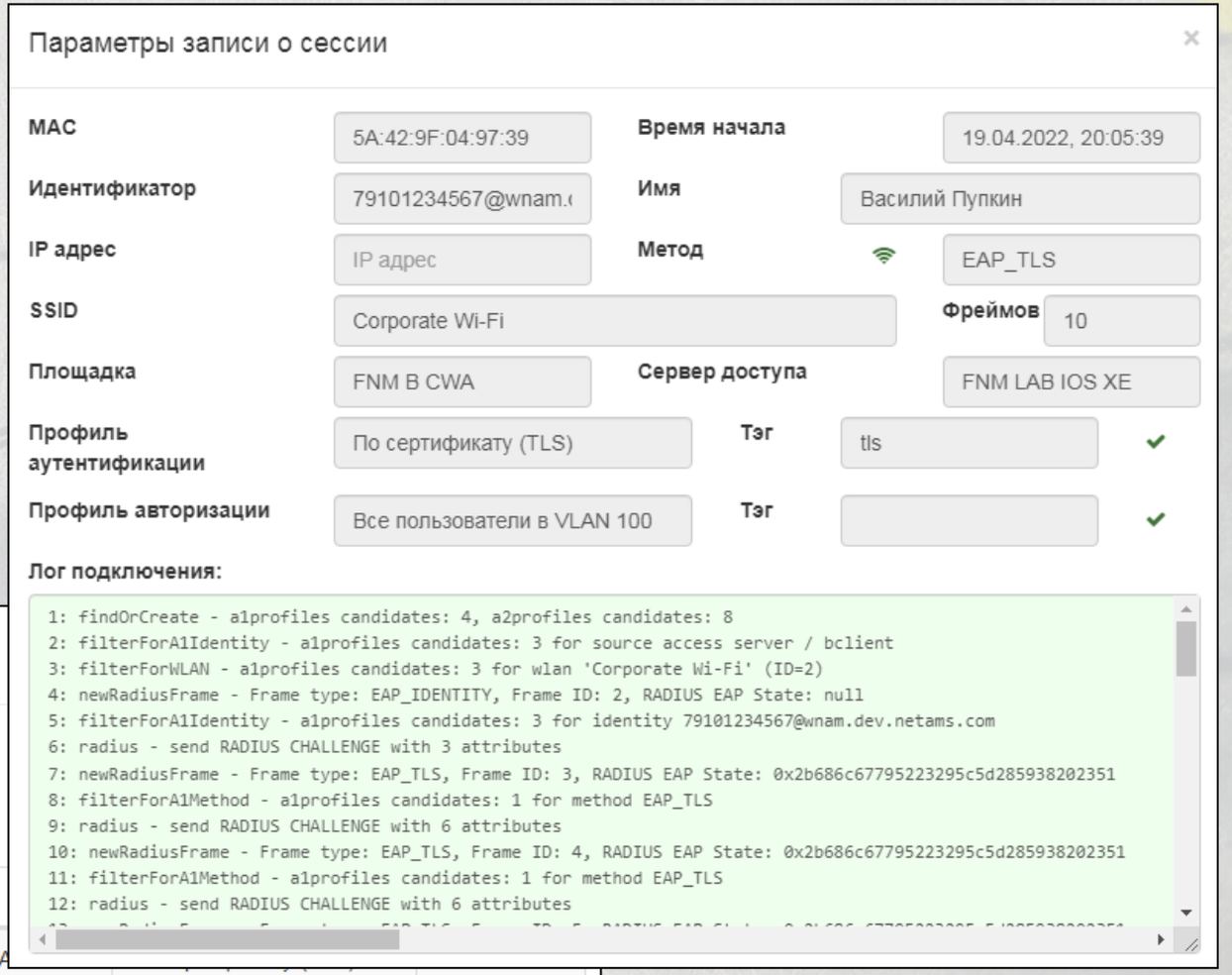


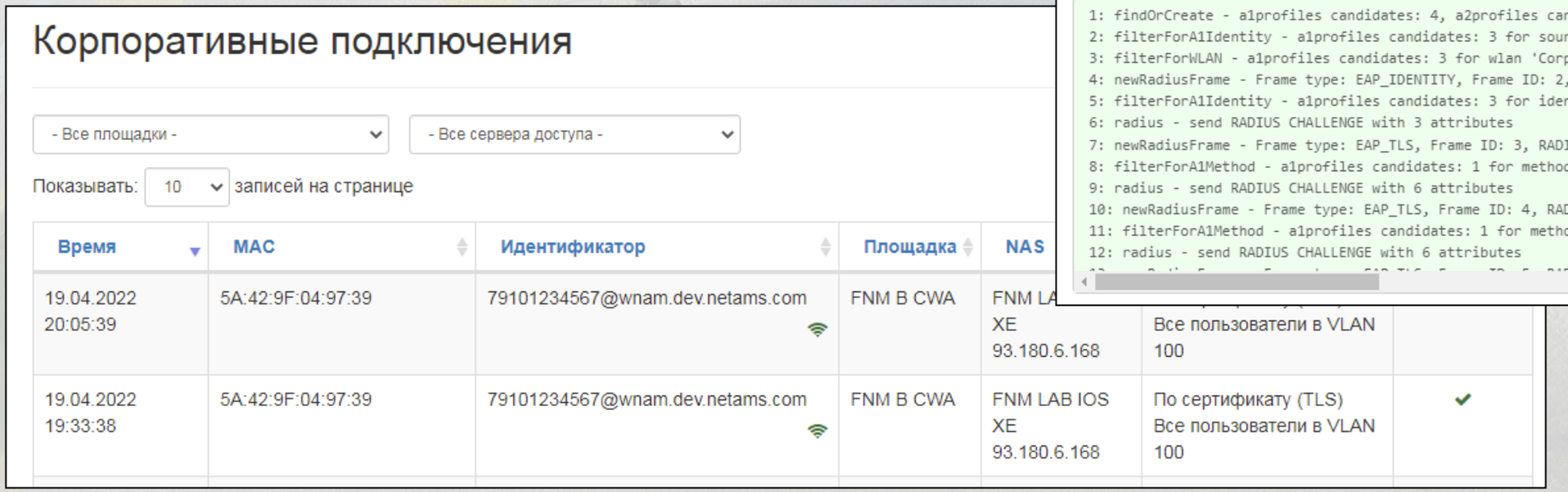


Траблшутинг

- 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 пользователи служб каталога
- 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

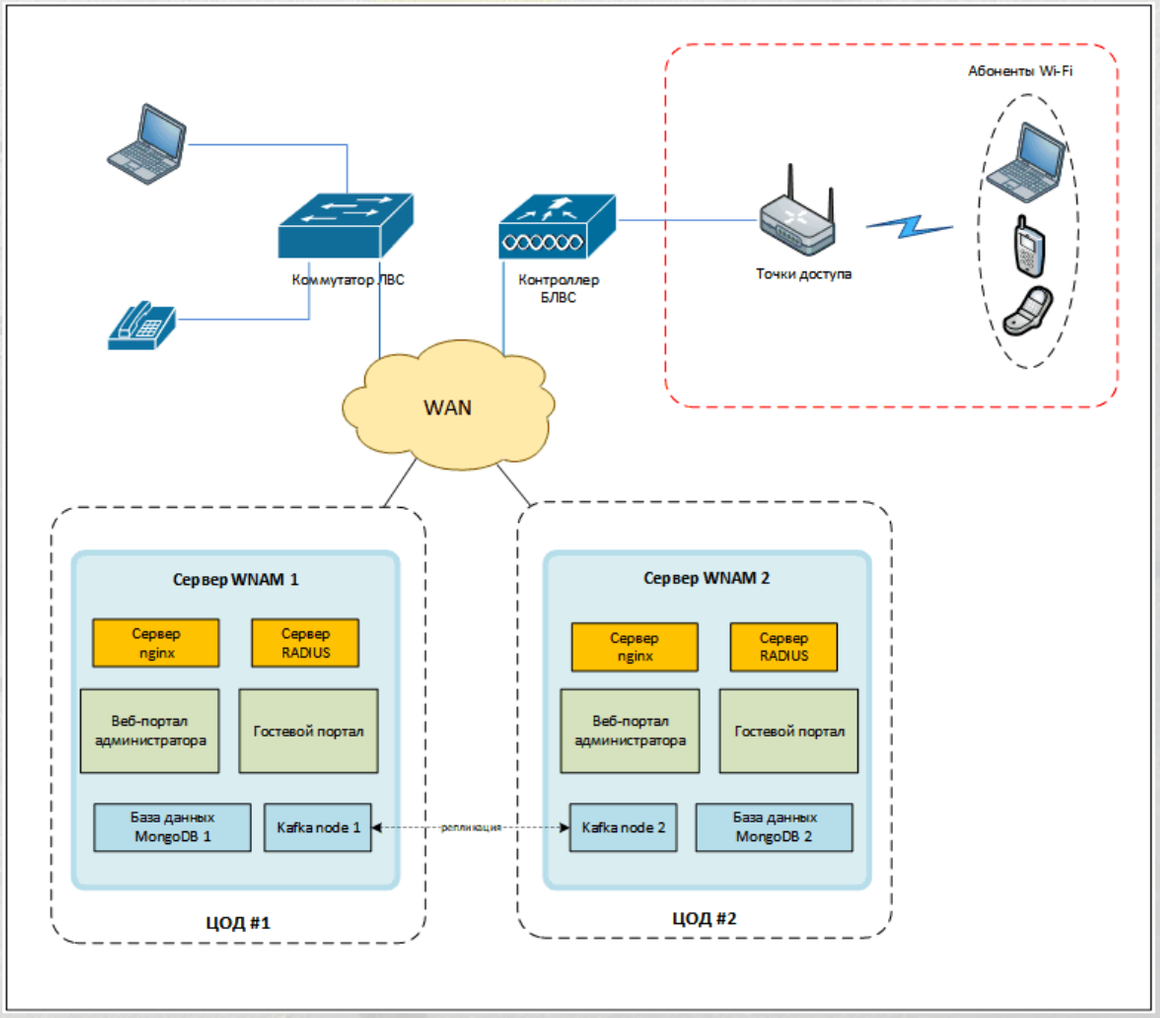
- Поддержка кластерной конфигурации
- Репликация базы данных
- Поддержка гео-распределенной конфигурации

Работает под управлением ОС Linux, в том числе Astra Linux и RedOS

Поддерживается виртуализация

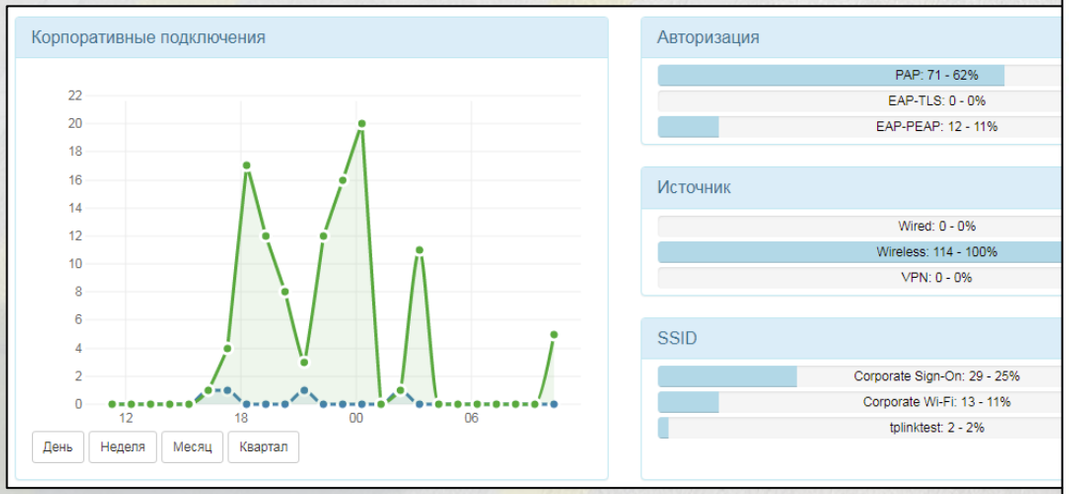
Поставляется в виде:

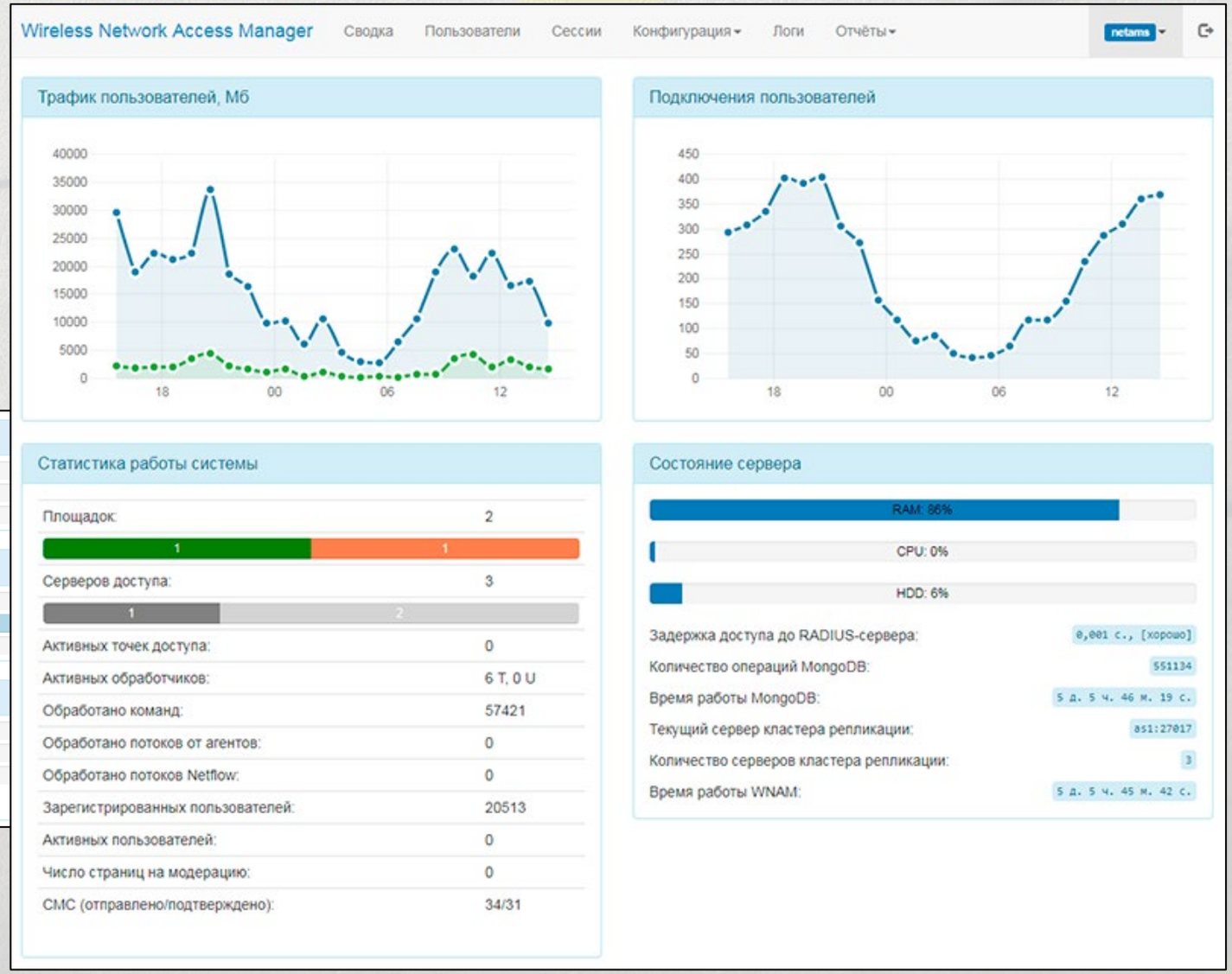
- Образ VM
- Онлайн-установщик



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
Профилирование по DHCP, CDP, LLDP, SNMP
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
Поддержка авторизации через второй фактор (RADIUS, Telegram, Anyconnect/TOTP)
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 и MAB доступ на основе политик
- Сенсор качества Wi-Fi – WNAM Quality of Wireless
  - Проактивный мониторинг и контроль SLA
  - Инструменты для инженеров
- Управление точками доступа – Контроллер «WiCo»

На все продукты – бессрочная лицензия!

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