

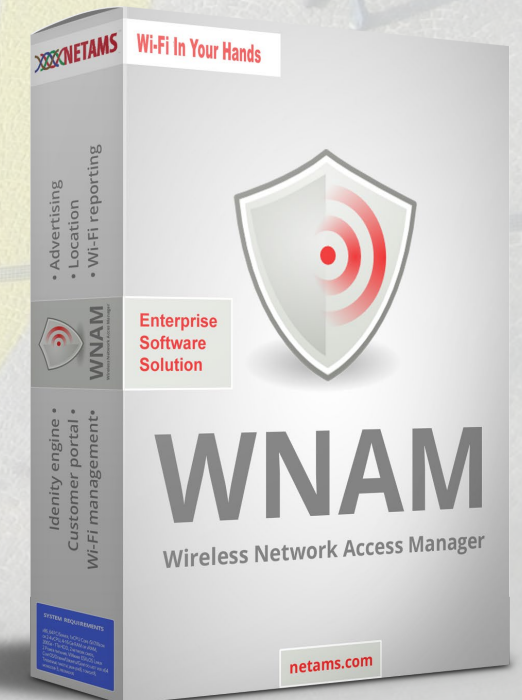
Корпоративная авторизация в проводных и беспроводных сетях

Ваша сеть

В ВАШИХ РУКАХ

О компании «Нетамс»

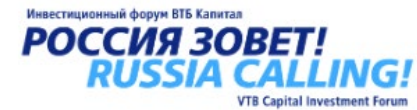
- Программное обеспечение и оборудование для сетей
- Работаем с 2008 года
- Более девяти лет опыта внедрения системы авторизации WNAM
- + три новых продукта за последние два года
- 200+ клиентов:
 - операторы связи
 - частный бизнес
 - государственные организации
- Служба техподдержки
- Сеть партнеров



Наши клиенты



ТТК



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

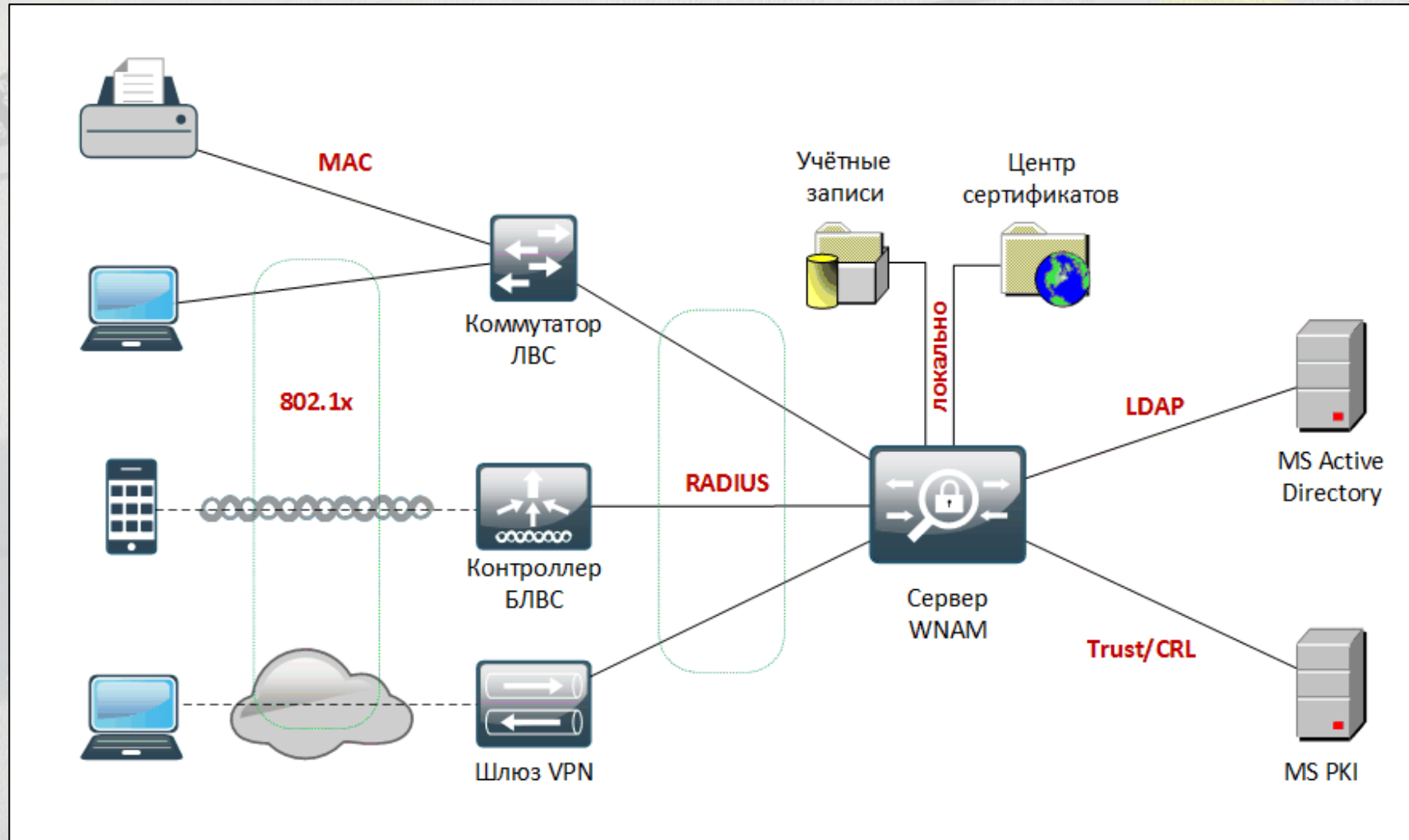
4. Контроллер беспроводных точек доступа Wi-Fi

✓ WiCo



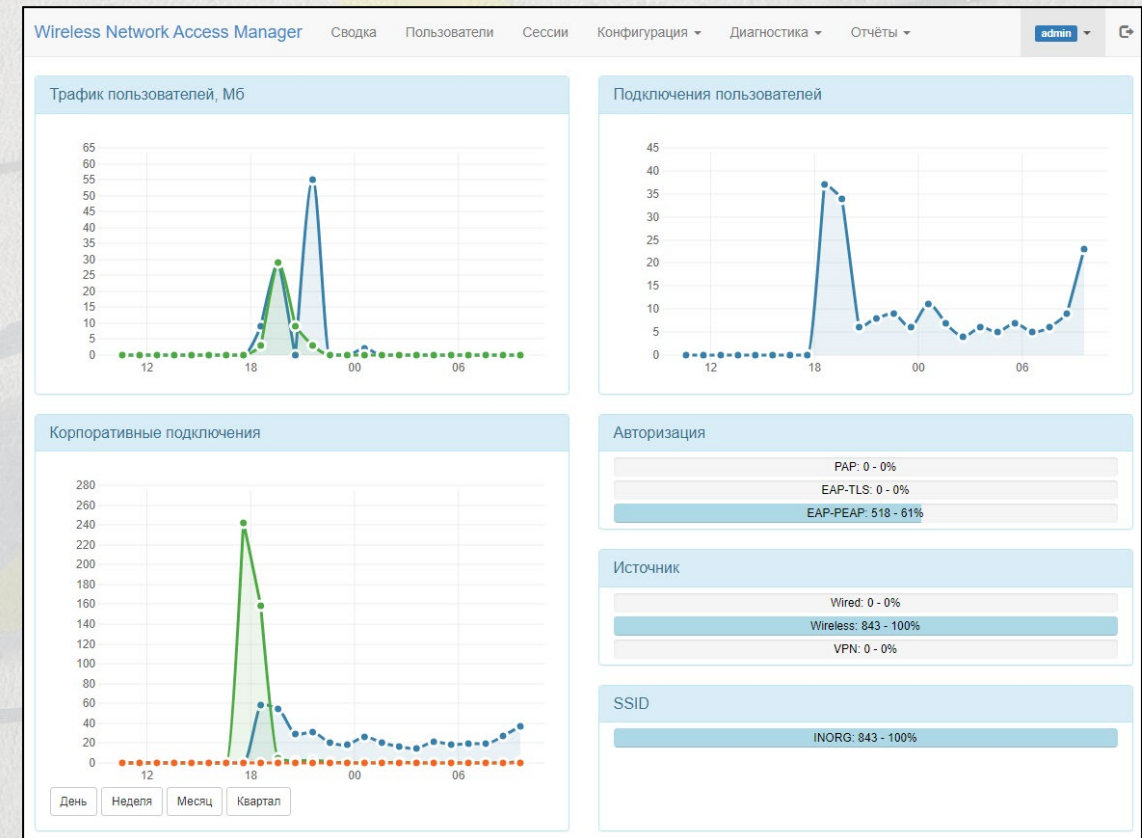
Архитектура корпоративной авторизации

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 openсору 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
- Выбирается наиболее подходящий профиль
 - Быстрое принятие решения (пустить/нет)
 - Переход на правила авторизации

Правило аутентификации

Отменить

Клонировать

Удалить

Включено

Да

Наименование

EAP/AD сотрудники LAB

Приоритет

100

Время

Любое

Рабочие часы

с:

по:

Источник запроса

Любой

Подразделение

Сервер доступа

Категории серверов доступа

Совпадение в NAS Identity

Совпадение в VLAN

Проводной

Беспроводной

VPN

Логин

SSID

Любой

Имя сети

WLAN ID

Профилирование

Не важно

Ещё нет профиля

Логический профиль

Политики и правила

Группа MAC адресов

Источник проверки учётных данных

Не применимо

Пароль в существующем эндпоинте

Администратор WNAME

Локальный администратор оборудования

Служба каталога

Метод

Эндпоинт: Любой

машинный

предварительно машинно-авторизованный

RAP

MAC адрес:

Известен и валиден

Не известен

Просрочен/не валиден

Совпадение в MAC адресе

Допустить ранее авторизованные 802.1X эндпоинты

Модель правил авторизации

- Проверка результата аутентификации
 - Правило или тэг
- Вернуть оборудованию
 - Номер VLAN
 - Фильтр
 - Загружаемый ACL
 - Ограничения
 - Редирект на портал самообслуживания
 - Произвольные RADIUS-атрибуты
- Работа с эндпоинтами
- Проверка защищенности APM («Сакура»)
- Протоколирование события
- Выбирается наиболее подходящий профиль

Правило авторизации

Отменить

Клонировать

Удалить

Включено

Да

Наименование

Wired - apply dACL

Приоритет

90

Условие

Результат аутентификации:

☒ Allow
 ☐ Deny

☐ Совпадение тэга

☒ Совпадение правила

wired local

Применить

☐ VLAN ID

☐ Voice Domain

☐ ACL ID

☒ Загружаемый ACL

acl-deny-1.1.1.1

☐ RADIUS атрибуты

☐ Политику КИБ "Сакура"

Ограничения

☐ Длительность сессии
 ☐ Реавторизация по завершении

☐ Скорость Up
 ☐ Скорость Down

☐ Объем трафика Up
 ☐ Объем трафика Down

Эндпоинт

Лимит числа MAC на сертификат/логин:

Действие по превышении лимита:

☒ Заблокировать самый старый
 ☐ Запретить новый

☐ Не создавать эндпоинт

Добавить

☐ Тэг или категорию в запись пользователя

☒ Имя правила авторизации
 ☐ Имя правила аутентификации
 ☐ Метку

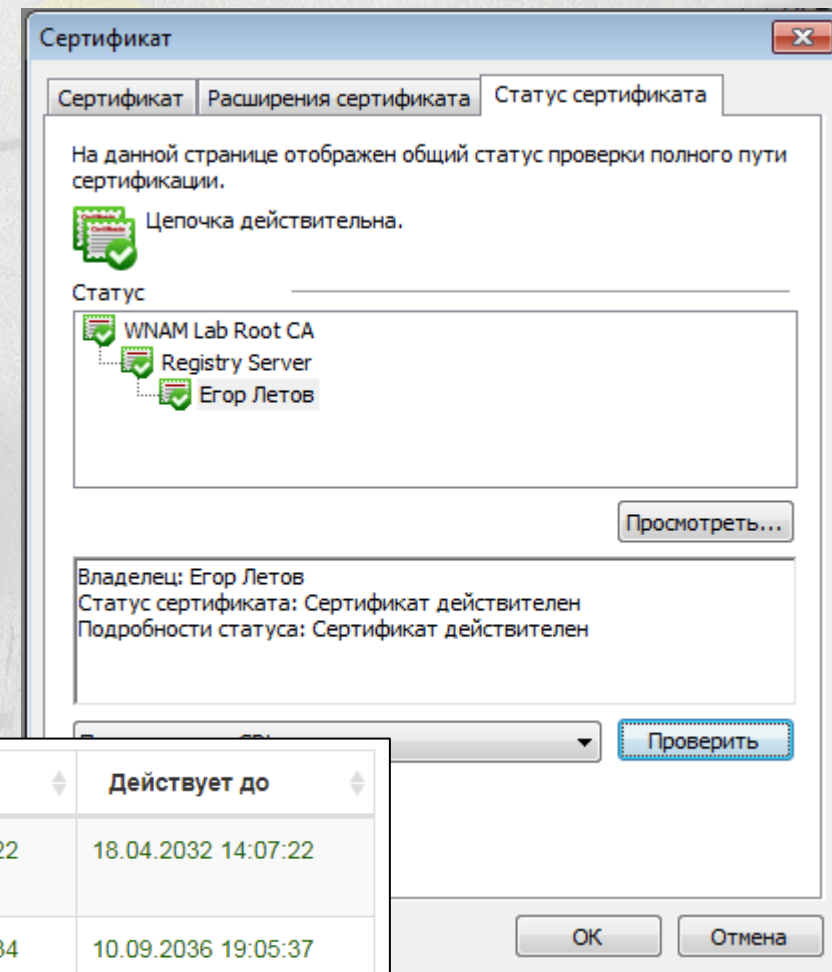
☐ Признак VIP в запись пользователя

Вернуть

☒ Accept
 ☐ Reject

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
- 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
- Мультидомен
- 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,DC=lab,DC=wnam,DC=ru
☐	Users	CN=Users,CN=Builtin,DC=main,DC=lab,DC=wnam,DC=ru
☒	Domain Users	CN=Domain Users,CN=Users,DC=main,DC=lab,DC=wnam,DC=ru

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, карантин

1000+ встроенных правил

Профиль

Наименование

Cisco-IP-Phone-7861

Тип

Встроенный

Включен

☒

Описание

Политика для Cisco-IP-Phone-7861

Родитель

Cisco-IP-Phone

Минимум

70

Политики

Отфильтровать по названию

Cisco-IP-Phone-7841Rule12

Cisco-IP-Phone-6961Rule22

Xerox-WorkCentre-7345-DHC

Android-Samsung-Galaxy-Ph

Android-Samsung-Galaxy-Ph

Cisco-IP-Phone-7841Rule11

Xerox-WorkCentre-5755_Rul

Android-Samsung-Galaxy-Ph

→

←

≡

Cisco-IP-Phone-7861Rule3

Cisco-IP-Phone-7861Rule11

Cisco-IP-Phone-7861Rule22

{ "updateTime": 0, "name": "Cisco-IP-Phone-7861-Rule1-Check1", "description": "Условие для Cisco-IP-Phone-7861, основано на DHCP:dhcp-class-identifier", "attributeName": "dhcp-class-identifier", "attributeValue": "7861", "operator": "CONTAINS", "type": "DHCP", "userVisible": true }

Метод

☒ PAP

MAC адрес:

☒ Известен и валиден
 ☒ Не известен
 ☒ Просрочен/не валиден

Совпадение в MAC адресе ?

☒ Профиль устройства

List1

GL-Inet (94:83:C4)

List1

MyButters

MyButtersV

Randomized MAC

☐ Совпадение в EAP Identity

Траблшутинг

- Детальный лог подключения
- Совпавшие правила и профили
- Примененные атрибуты ACL, VLAN
- Аккаунтинг трафика
- Причина отказа в подключении

Корпоративные подключения

- Все площадки -

- Все сервера доступа -

Показывать: 10 записей на странице

Время	MAC	Идентификатор	Площадка	NAS	Профиль авторизации	Статус
19.04.2022 20:05:39	5A:42:9F:04:97:39	79101234567@wnam.dev.netams.com	FNM B CWA	FNM LAB IOS XE 93.180.6.168	Все пользователи в VLAN 100	
19.04.2022 19:33:38	5A:42:9F:04:97:39	79101234567@wnam.dev.netams.com	FNM B CWA	FNM LAB IOS XE 93.180.6.168	По сертификату (TLS) Все пользователи в VLAN 100	✓

Параметры записи о сессии

MAC

5A:42:9F:04:97:39

Время начала

19.04.2022, 20:05:39

Идентификатор

79101234567@wnam.dev.netams.com

Имя

Василий Пупкин

IP адрес

IP адрес

Метод

📶 EAP_TLS

SSID

Corporate Wi-Fi

Фреймов

10

Площадка

FNM B CWA

Сервер доступа

FNM LAB IOS XE

Профиль аутентификации

По сертификату (TLS)

Тэг

tls

✓

Профиль авторизации

Все пользователи в VLAN 100

Тэг

✓

Лог подключения:

1: findOrCreate - alprofiles candidates: 4, a2profiles candidates: 8

2: filterForA1Identity - alprofiles candidates: 3 for source access server / bclient

3: filterForWLAN - alprofiles candidates: 3 for wlan 'Corporate Wi-Fi' (ID=2)

4: newRadiusFrame - Frame type: EAP_IDENTITY, Frame ID: 2, RADIUS EAP State: null

5: filterForA1Identity - alprofiles candidates: 3 for identity 79101234567@wnam.dev.netams.com

6: radius - send RADIUS CHALLENGE with 3 attributes

7: newRadiusFrame - Frame type: EAP_TLS, Frame ID: 3, RADIUS EAP State: 0x2b686c67795223295c5d285938202351

8: filterForA1Method - alprofiles candidates: 1 for method EAP_TLS

9: radius - send RADIUS CHALLENGE with 6 attributes

10: newRadiusFrame - Frame type: EAP_TLS, Frame ID: 4, RADIUS EAP State: 0x2b686c67795223295c5d285938202351

11: filterForA1Method - alprofiles candidates: 1 for method EAP_TLS

12: radius - send RADIUS CHALLENGE with 6 attributes

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 доступ			
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

Уровень

15

Фреймов

6

Идентификатор сессии

489d22cc

NAS

172.16.130.38

tty1

Сервер доступа

R20 LAB SW

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

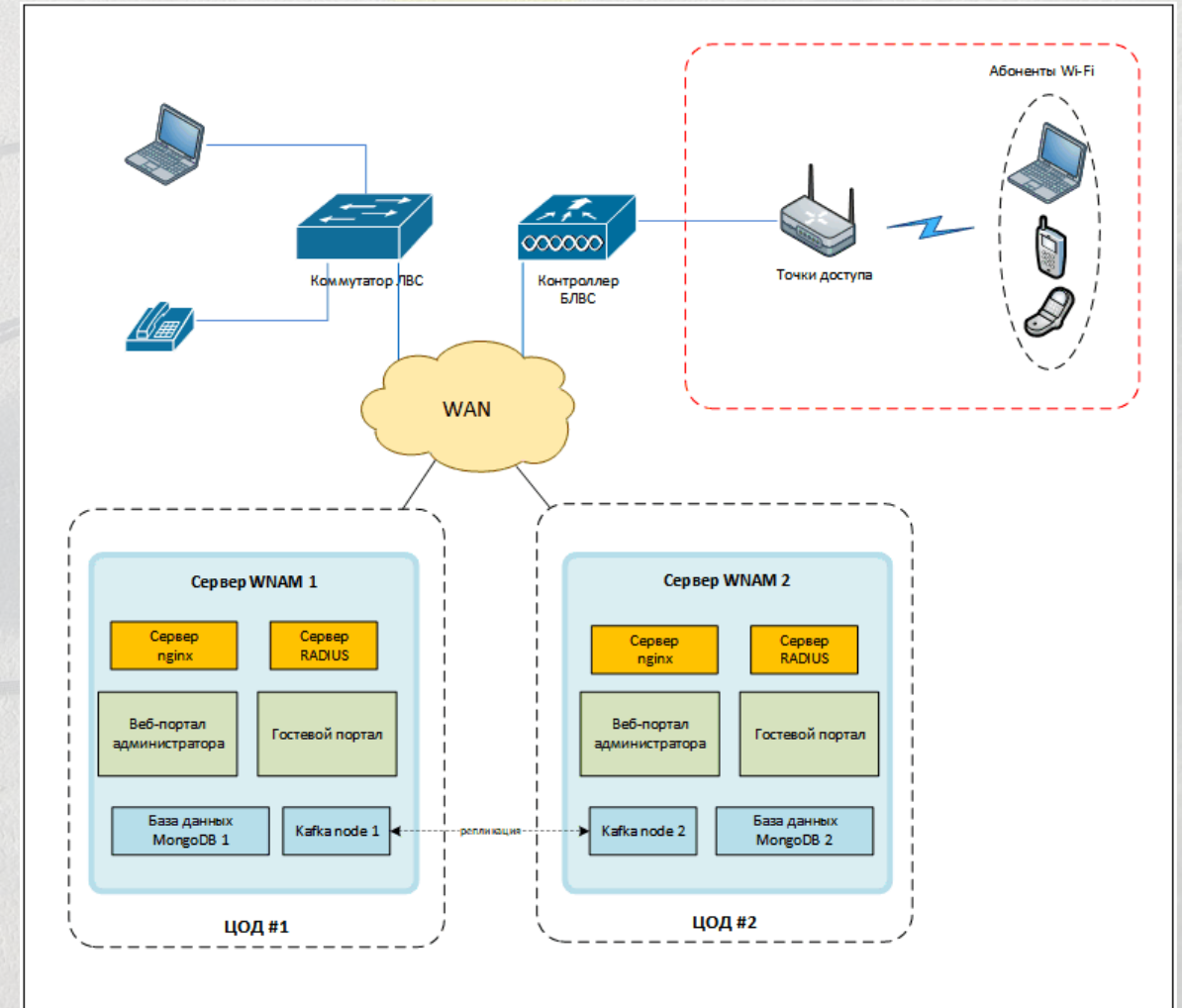
- Поддержка кластерной конфигурации
- Репликация базы данных
- Поддержка гео-распределенной конфигурации

Работает под управлением ОС Linux, в том числе Astra Linux

Поддерживается виртуализация

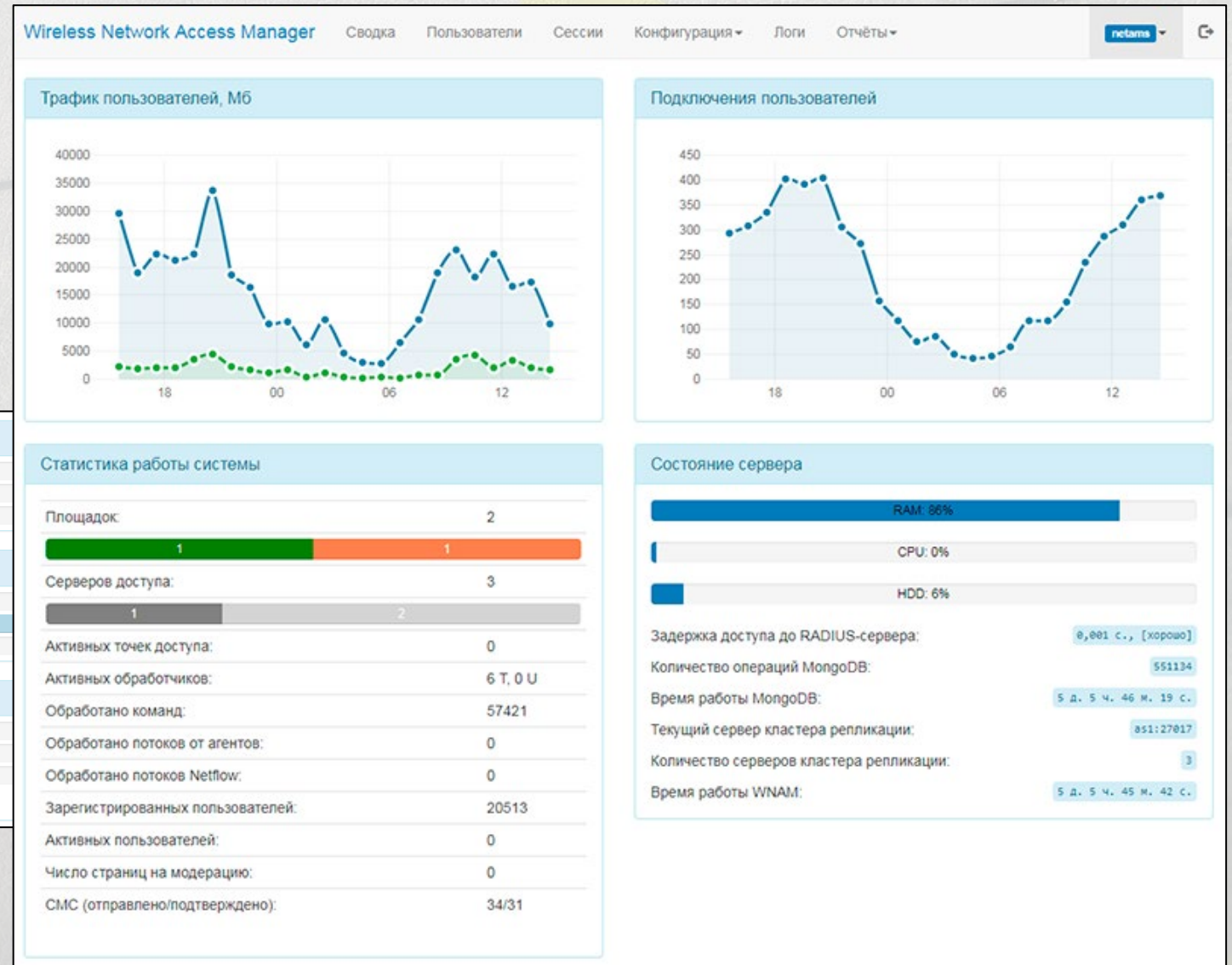
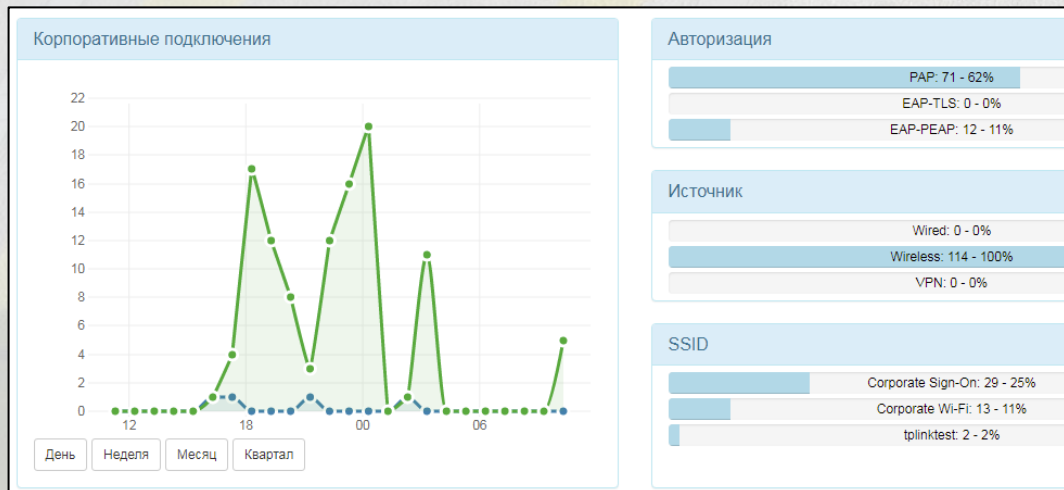
Поставляется в виде:

- 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 (онбординга) 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

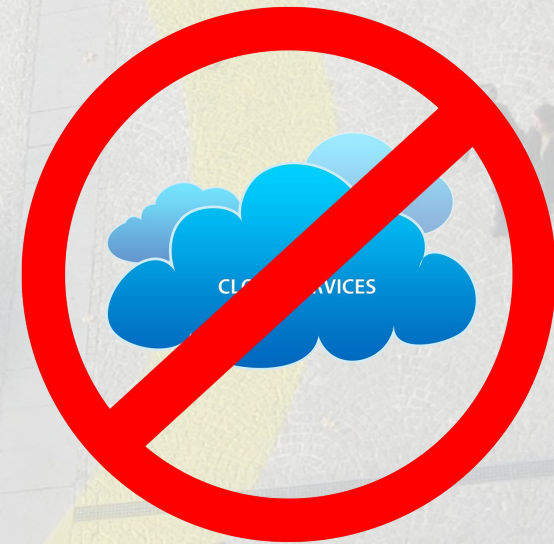
Доработки

- 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 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»



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