

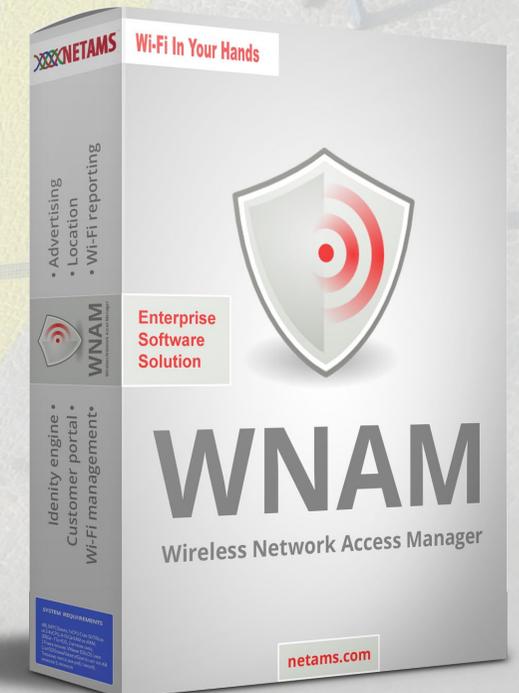
Корпоративная авторизация в проводных и беспроводных сетях

Ваша сеть

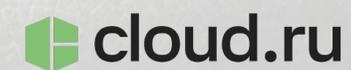
В ВАШИХ РУКАХ

О компании «Нетамс»

- Программное обеспечение и оборудование для сетей
- Работаем с 2008 года
- 11 лет опыта внедрения системы авторизации WNAM
- + три новых продукта за последние три года
- 250+ клиентов:
 - операторы связи
 - частный бизнес | банки | нефтяные компании | IT
 - государственные организации
- Служба технической поддержки
- Сеть партнеров



Наши клиенты



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

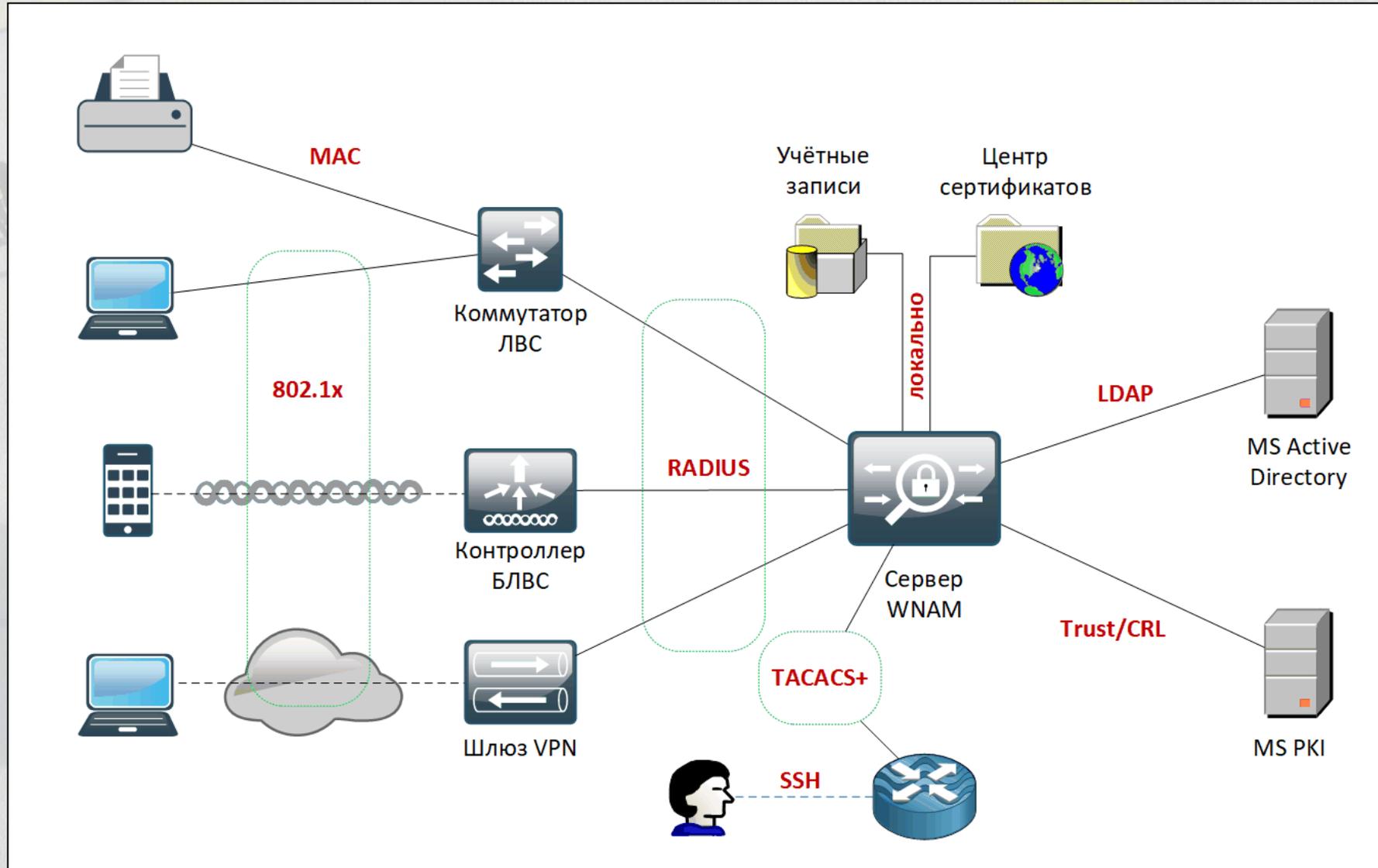
✓ **WNAM Quality of Wireless**

4. Контроллер беспроводных точек доступа Wi-Fi

✓ **WiCo (OEM)**

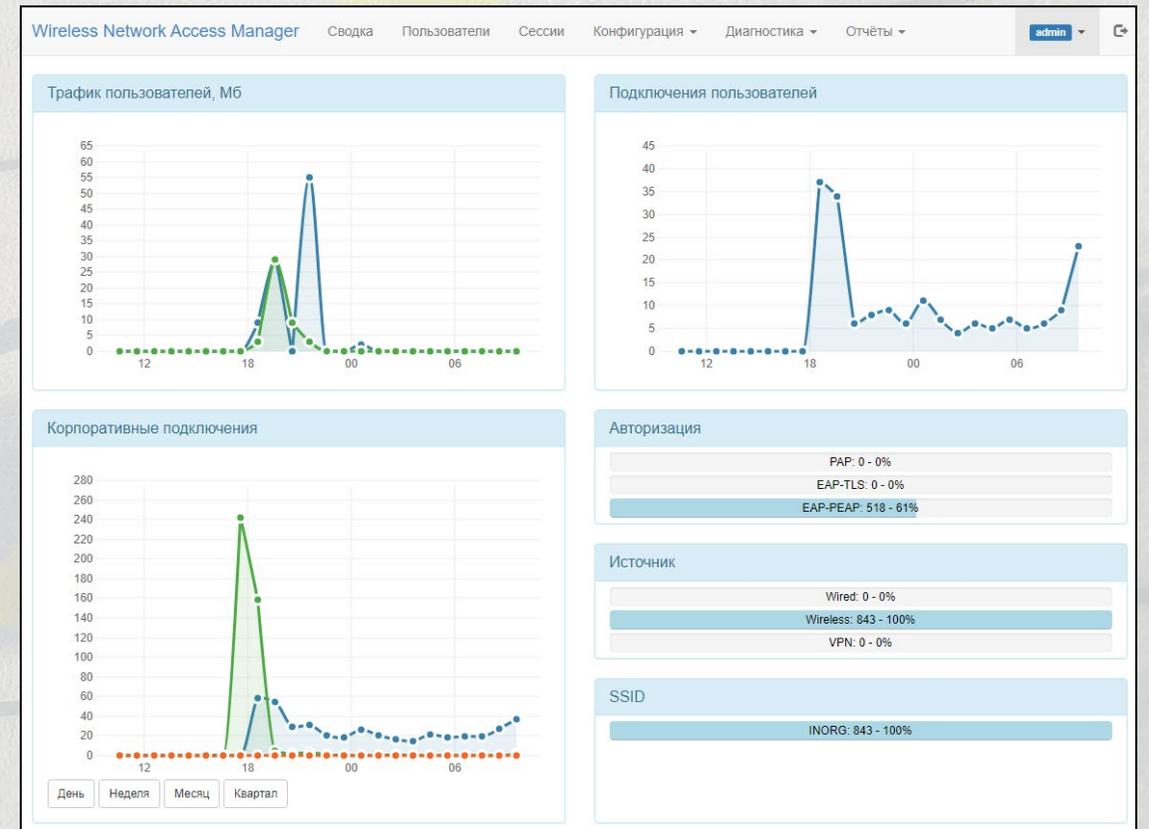


Архитектура корпоративной авторизации



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/ACS,
 Microsoft NPS, Aruba ClearPass, Ruckus Cloudpath
 Альтернатива опенсорсу FreeRADIUS/PacketFence

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
- Запрос второго фактора

Применяется наиболее подходящий профиль

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

Правило аутентификации

Отменить Клонировать Удалить

Включено Да

Наименование: EAP/AD сотрудники LAB

Приоритет: 100

Время:

- Любое
- Рабочие часы с: [] по: []

Источник запроса:

- Любой
- Подразделение: - любой -
- Сервер доступа: 10.241.200.6 e19800-2 WLAB
- Категории серверов доступа: [Выбрать]
- Совпадение в NAS Identity: []
- Совпадение в VLAN: [] Имя: [] Номер: []
- Проводный Беспроводный VPN Иной

SSID:

- Любой
- Имя сети: []
- WLAN ID: []

Профилирование:

- Не важно
- Ещё нет профиля
- Логический профиль: Cameras
- Политики и правила: [Выбрать]
- Группа MAC адресов: GL-inet (94:83:C4)

Источник проверки учётных данных:

- Не применимо
- Пароль в существующем эндпоинте
- Администратор WNAM
- Локальный администратор оборудования
- Служба каталога: lab.wnam.ru
- Группа: Test Group 88
- Строка в имени группы: []

Метод:

- Эндпоинт: любой машинный предварительно машинно-авторизованный
- PAP
 - 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
 - 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 APM («Сакура»)
- Протоколирование события авторизации (+SIEM)

Применяется наиболее подходящий профиль

- По умолчанию: отказ в доступе

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

Ограничения
 Политику КИБ "Сакура"
 Длительность сессии Реавторизация по завершении
 Скорость Up Скорость Down
 Объем трафика Up Объем трафика Down

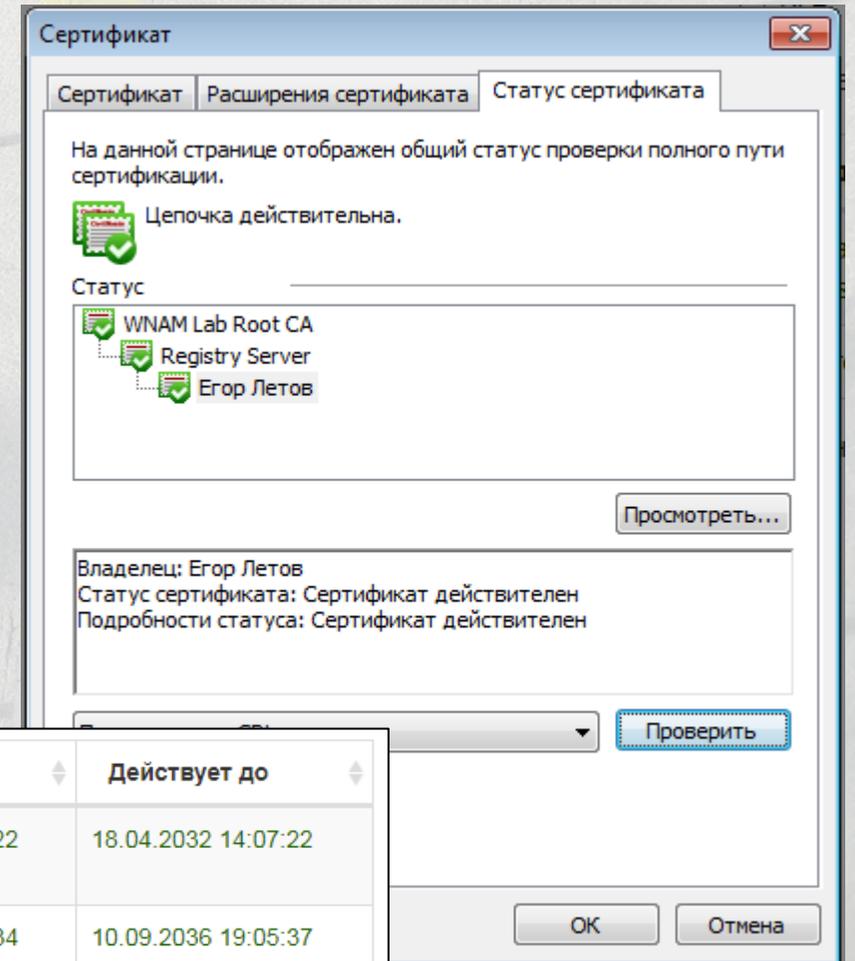
Эндпоинт
 Лимит числа MAC на сертификат/логин:
 Действие по превышении лимита: Заблокировать самый старый Запретить новый
 Не создавать эндпоинт

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
- 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 (ALD Pro)
- 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
<input type="checkbox"/>	Exchange Servers	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=main,DC=lab,DC=wnam,DC=ru
<input type="checkbox"/>	Users	CN=Users,CN=Builtin,DC=main,DC=lab,DC=wnam,DC=ru
<input checked="" type="checkbox"/>	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, помещение в карантин

1000+ встроенных правил, можно создавать свои

Профиль ✕

Наименование:

Тип: Встроенный

Включен:

Описание:

Родитель:

Минимум:

Политики:

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

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

Совпадение в EAP Identity

List1 ▼

- GL-Inet (94:83:C4)
- List1**
- MyButters
- MyButtersV
- Randomized MAC

Контроль защищенности АРМ

- Проверка наличия антивируса, обновлений, процессов
- Замена Cisco Anyconnect Posture
- КИБ «Сакура» от IT Expertise. Win, Mac, Linux
- Сервер «Сакура» контролирует агентов.
- Изменение статуса агента направляется на WNAM.
- Статус защищенности эндпоинта (IP, MAC).
- Отправка команды переавторизации порта. RADIUS CoA.
- Назначение карантинных VLAN, ACL, dACL
- «Излечение эндпоинта» - повторение процесса. Целевой VLAN.

Общие
Ограничения
Категории
Оплата
Профили устройства
Лог

Пользователь-100

Выбрать категории

Машинная авторизация	09.09.2023, 18:24:18	<input checked="" type="checkbox"/> активна
Контроль защищенности	09.09.2023, 18:24:17	Статус: нет нарушений

Интеграция с сервером КИБ "Сакура" ^

Если нет информации об установленности агента, то вернуть:

- Accept
 - VLAN ID
 - ACL ID
 - User Role (Aruba)
 - Загружаемый ACL
- Reject
- Quarantine

Если уровень ниже или равен Compliant , то вернуть:

- Accept
 - VLAN ID
 - ACL ID
 - User Role (Aruba)
 - Загружаемый ACL
- Reject
- Quarantine

Длительность кэширования статуса агента, мин.:

Траблшутинг

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

Параметры записи о сессии

MAC	5A:42:9F:04:97:39	Время начала	19.04.2022, 20:05:39
Идентификатор	79101234567@wnam.c	Имя	Василий Пупкин
IP адрес	IP адрес	Метод	EAP_TLS
SSID	Corporate Wi-Fi	Фреймов	10
Площадка	FNM В 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 - a1profiles candidates: 4, a2profiles candidates: 8
2: filterForA1Identity - a1profiles candidates: 3 for source access server / bclient
3: filterForWLAN - a1profiles candidates: 3 for wlan 'Corporate Wi-Fi' (ID=2)
4: newRadiusFrame - Frame type: EAP_IDENTITY, Frame ID: 2, RADIUS EAP State: null
5: filterForA1Identity - a1profiles 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 - a1profiles 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 - a1profiles candidates: 1 for method EAP_TLS
12: radius - send RADIUS CHALLENGE with 6 attributes

```

Корпоративные подключения

- Все площадки - - Все сервера доступа -

Показывать: записей на странице

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

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	Уровень	15
Идентификатор сессии	489d22cc	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

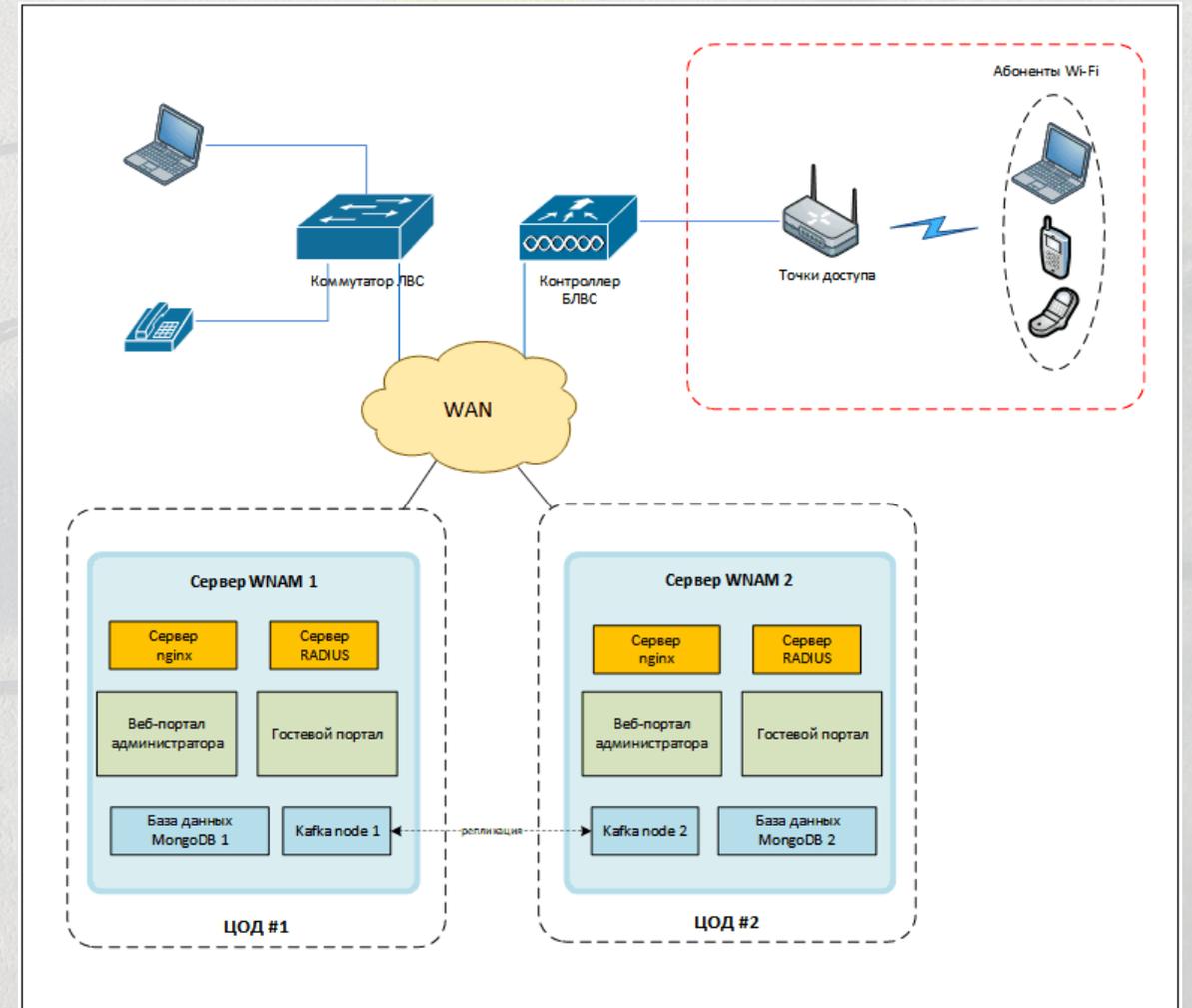
- Поддержка кластерной конфигурации
- Репликация базы данных
- Поддержка гео-распределенной конфигурации

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

Поддерживается виртуализация

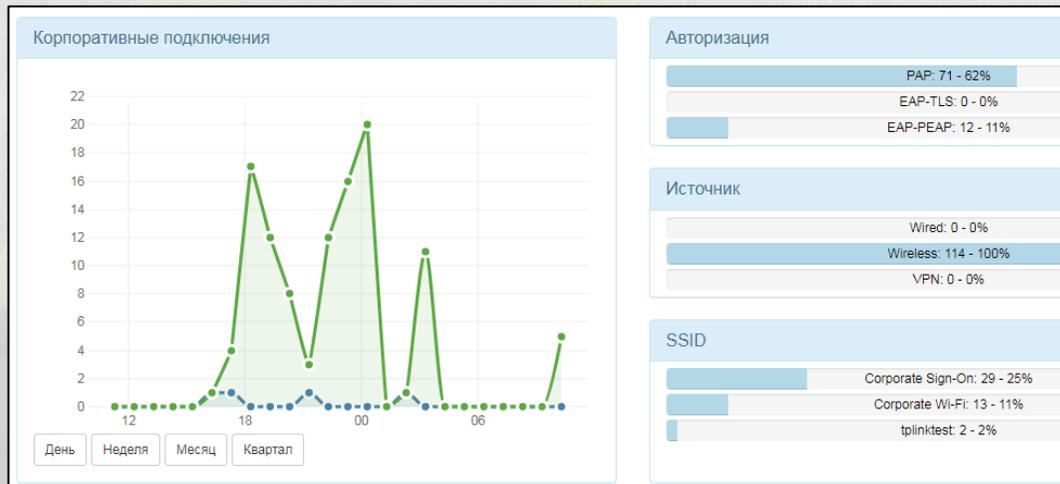
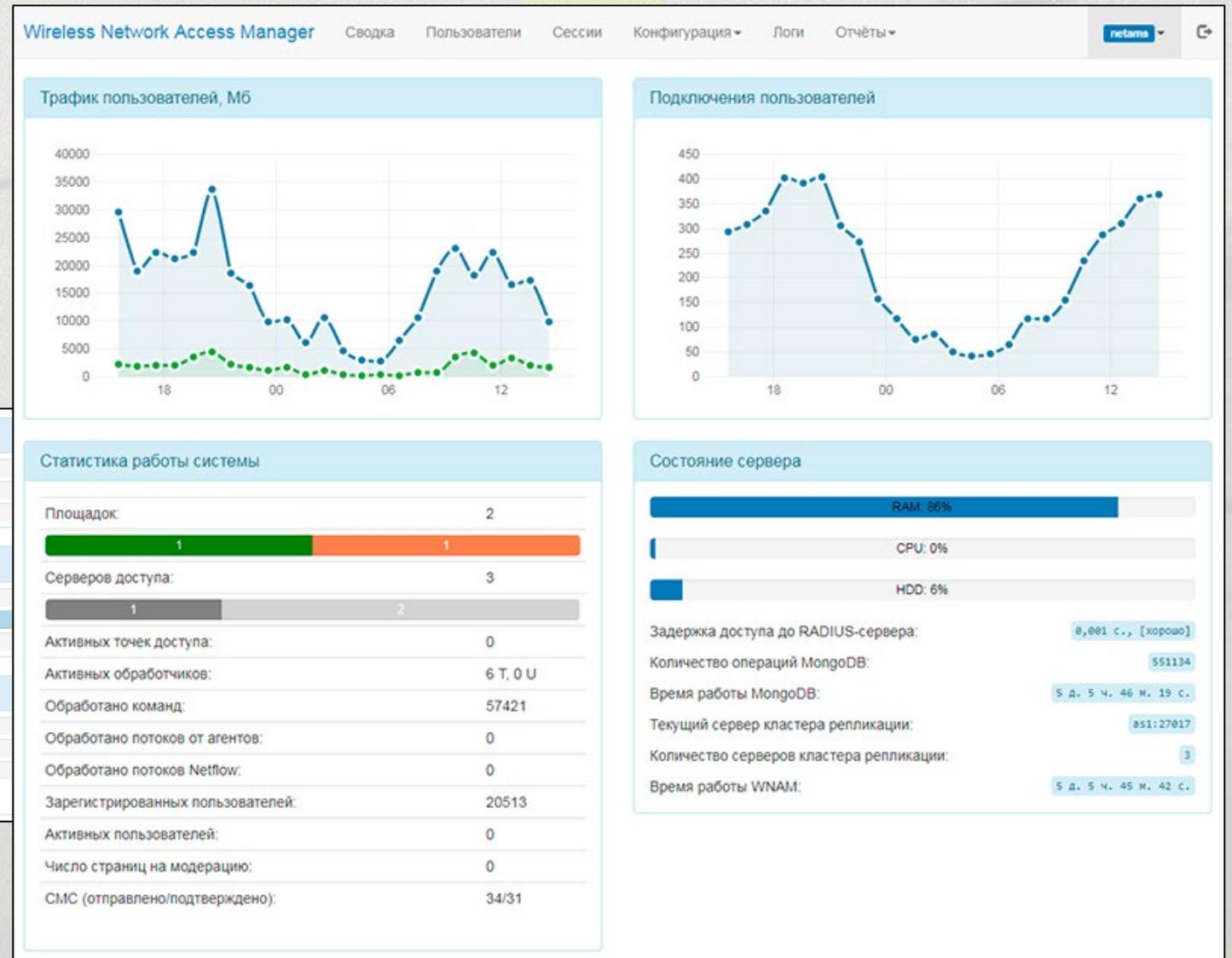
Поставляется в виде:

- 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



Сравнение с аналогами

Cisco ISE

Чего у нас нет:

- SGT метки, TrustSEC
- FIPS Mode
- EAP-TEAP, TLS v1.3
- Posturing (средствами AnyConnect)
- MDM

Что у нас есть:

- Поддержка значительного числа Wi-Fi контроллеров (гостевая авторизация)
- Большие возможности по гостевой авторизации (звонок, Госуслуги, конструктор страниц, ...)
- Проверенный 802.1X/TACACS+ с отечественными вендорами
- Контроль защищенности APM через интеграцию с КИБ «Сакура»
- Поддержка 2FA (в т.ч. Telegram, отечественные решения, своё приложение, + доступ в UI)
- Расширенные опции карантина
- SNMP опрос оборудования + контроля статуса портов ЛВС
- Возможность напрямую обратиться к вендору, а не отправить «тикет-в-индию»

Сравнение с аналогами

Microsoft NPS

Чего у нас нет:

- Нативной поддержки взаимодействия с AD

Что у нас есть:

- Нормальные средства диагностики, статистики и отчетов
- Профайлер для MAB методов
- Гостевая авторизация
- BYOD
- TACACS+
- Кластерная конфигурация

Сравнение с аналогами

FreeRADIUS

Чего у нас нет:

- Бесплатной версии

Что у нас есть:

- Web GUI
- Нормальные средства диагностики, статистики и отчетов
- Профайлер для MAB методов
- Гостевая авторизация
- BYOD
- TACACS+
- Кластерная конфигурация
- Мульти-доменное подключение к AD
- Техническая поддержка

Сравнение с аналогами

ГазИнформСервис «Efros Defense Operations»

- + Сертификат ФСТЭК
- Сложно запустить, не всегда это получается

Deck.Auth

- Меньше функций
- Проблемы кластеризации
- Подписочная модель

AxelNAS

- Сырой продукт на основе opensource

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

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

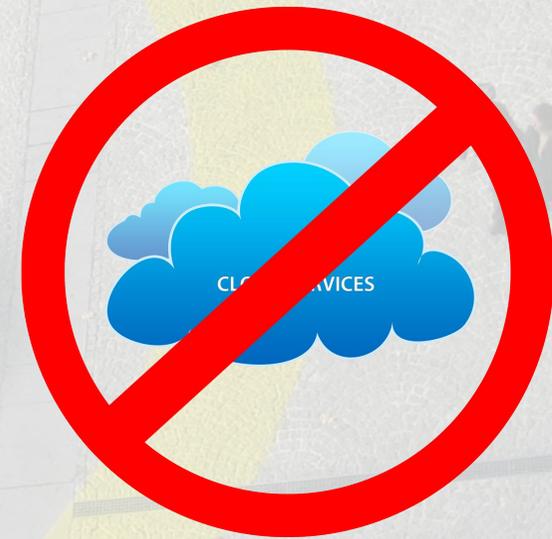
Доработки

- 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