

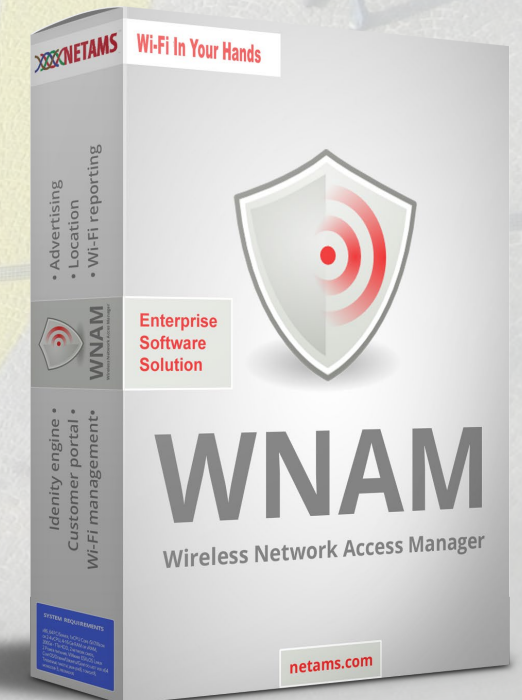
Корпоративная авторизация в проводных и Wi-Fi сетях

Ваша сеть

В ВАШИХ РУКАХ

О компании «Нетамс»

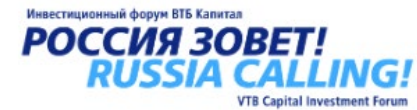
- Программное обеспечение и оборудование для сетей
- Работаем с 2008 года
- Более семи лет опыта внедрения системы авторизации WNAM
- + три новых продукта за последние два года
- 200+ клиентов:
 - операторы связи
 - частный бизнес
 - государственные организации
- Служба техподдержки
- Сеть партнеров



Наши клиенты



ТТК



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

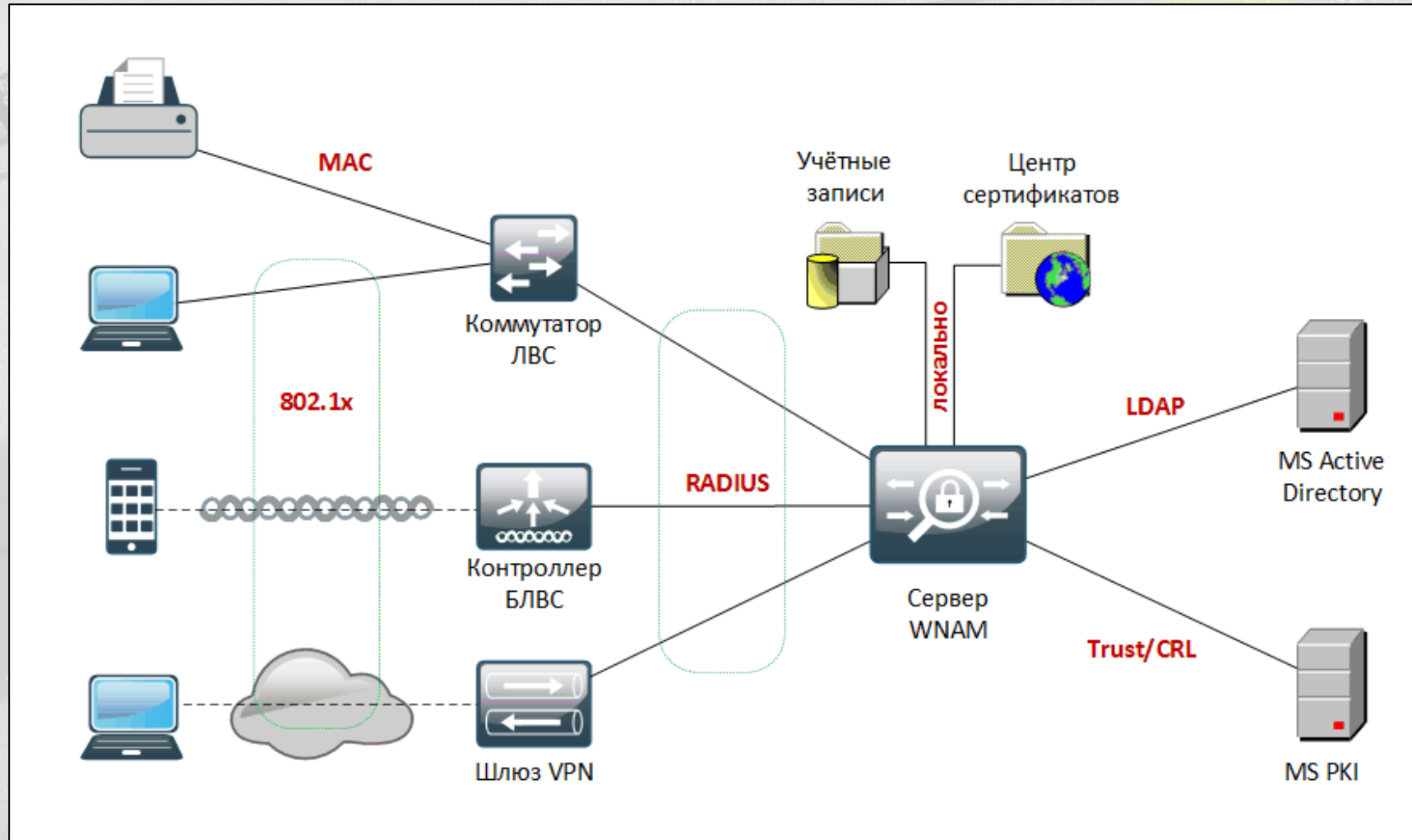
4. Управление оборудованием Wi-Fi

✓ WNAM Devices Controller



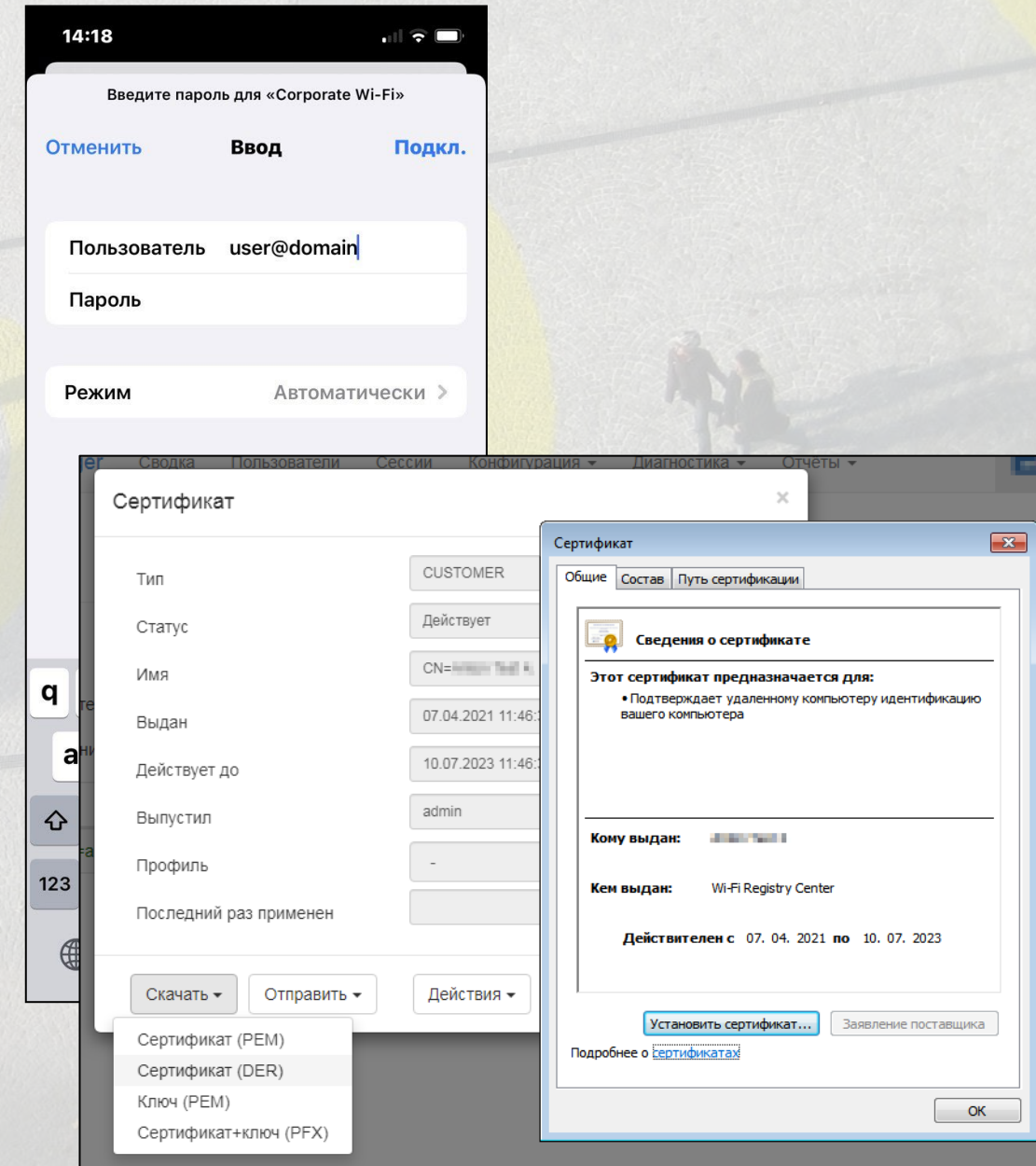
Архитектура решения корпоративной авторизации

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

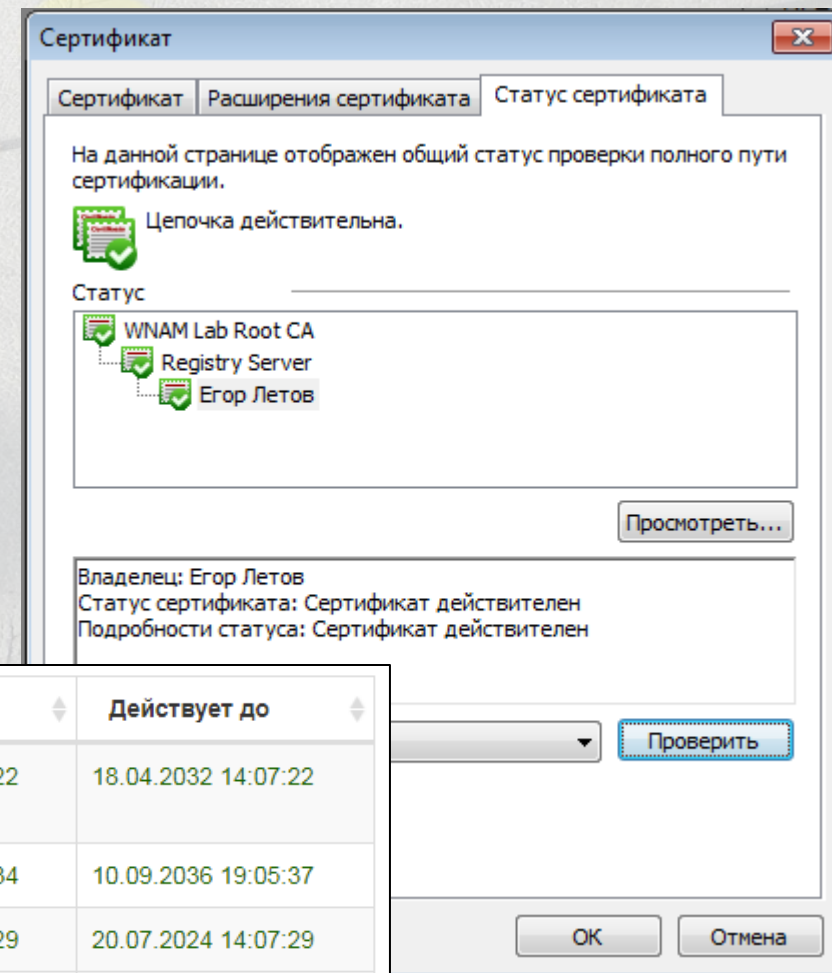
Назначаемый VLAN или ACL
 RADIUS-атрибуты (+редактор)
 URL редиректа на портал:
 CMC-авторизация
 самообслуживание (сертификат)
 Параметры сессии:
 длительность, скорость, объем
 Правила проверок:
 учетных записей и сертификатов
 MAC адресов
 членство в группах AD

Профили аутентификации						
Определяют критерии, по которым производится проверка идентичности запросившего сетевой доступ. Проверка идет последовательно по правилам, в порядке увеличения номера, до первого совпадения. Сравниваются различные критерии и атрибуты в поступившем запросе: откуда, когда, каким способом, что передается.						
Создать новый Сбросить счетчики Перенумеровать Показывать: 10 записей на странице Быстрый поиск:						
Номер	Наименование	Описание	Проверок	Allow	Deny	Continue
10	MAC bypass для Тамбова	Any, PAP → Allow [tambov]	23435	56	0	0
20	MAC bypass общий	Any, PAP → Allow	23443	127	0	0
30	EAP/AD администраторы	Any, EAP_PEAP → Allow [admin]	22101	654	0	0
40	EAP/AD сотрудники	Any, EAP_PEAP → Allow	12311	11011	0	0
50	По сертификату (TLS)	Any, EAP_TLS → Allow [tls]	8965	5541	0	0
Показано с 1 по 5 из 5 записей						Предыдущая 1 Следующая

Альтернатива проприетарным Cisco ISE, Cisco ACS, Microsoft NPS, Aruba ClearPass, Ruckus Cloudpath
 Альтернатива сложному в настройке и неудобному в эксплуатации openсopcy 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, O=Netams. LLC, OU=Development, L=Moscow, E=support@netams.com	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, O=Netams. LLC, OU=Development, L=Moscow, E=support@netams.com	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 домена

main

Имя контроллера домена

dcb1

Учётная запись

Пароль

URL для NTLM проверки

http://.../cgi/ntlmauth.cgi

Обновить список групп

Удалить

Сохранить

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

Профилирование устройств

- Ведения списков оборудования по вендорам, таблицам MAC 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

Метод

☒ PAP

MAC адрес: ☒ Известен и валиден ☒ Не известен

Совпадение в MAC адресе ?

☒ Профиль устройства

☐ Совпадение в EAP Identity

List1

GL-Inet (94:83:C4)

List1

MyButters

MyButtersV

Randomized MAC

Профиль устройства

Наименование

Совпадение

☐ Список MAC адресов

Формат строк:
XX:XX:XX:XX:XX:XX, xx-xxxx-
xxx, XX.XX.XX или *XX:XX:X*.

☒ Список вендоров

☐ Вендор

☐ Рандомный MAC адрес

☐ Любой из выбранных

None selected

Дата изменения

Amazon Technologies Inc. ▼

- ☐ Ubiquiti Broadband
- ☐ Hon Hai Precision
- ☒ Amazon Technologies Inc.
- ☐ Espressif Inc.
- ☐ Guangdong Oppo Mobile Telecommunications Corp., Ltd.
- ☐ vivo Mobile Communication Co., Ltd.
- ☐ New H3C Technologies Co., Ltd.
- ☐ ASUSTek COMPUTER INC.
- ☐ Private

New H3C Technologies Co., Ltd

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		
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

MAC5A:42:9F:04:97:39

Идентификатор79101234567@wnam.dev.netams.com

IP адресIP адрес

SSIDCorporate Wi-Fi

ПлощадкаFNM B CWA

Профиль аутентификацииПо сертификату (TLS)

Профиль авторизацииВсе пользователи в VLAN 100

Время начала19.04.2022, 20:05:39

ИмяВасилий Пупкин

МетодEAP_TLS

Фреймов10

Сервер доступаFNM LAB IOS XE

Тэгtls✓

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 Active Directory
- 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

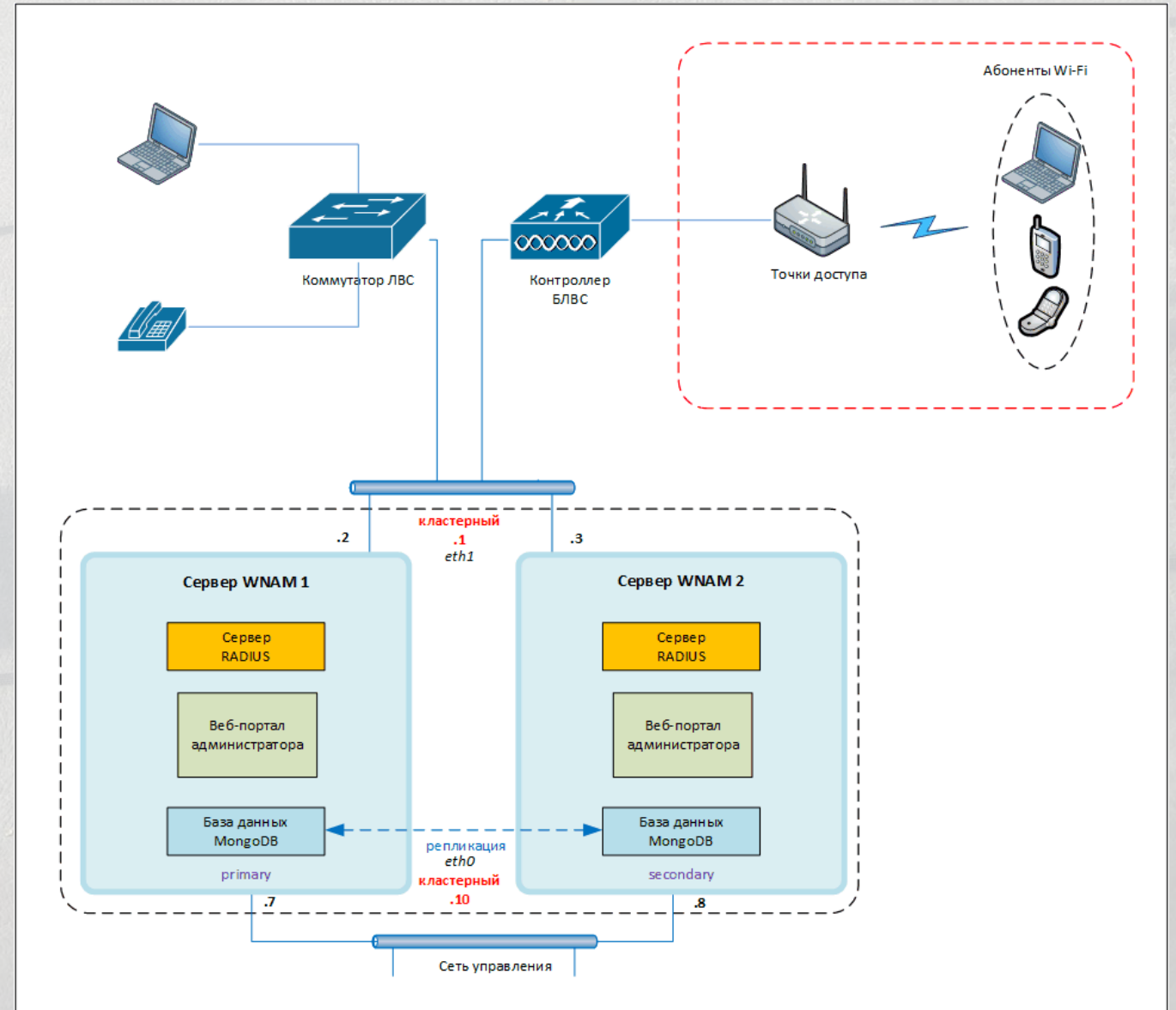
20.05.2022, 17:33:29 [7] accounting stopped - [task_id=113, timezone=UTC, service=shell, disc-cause=1, disc-cause=...

Отказоустойчивость

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

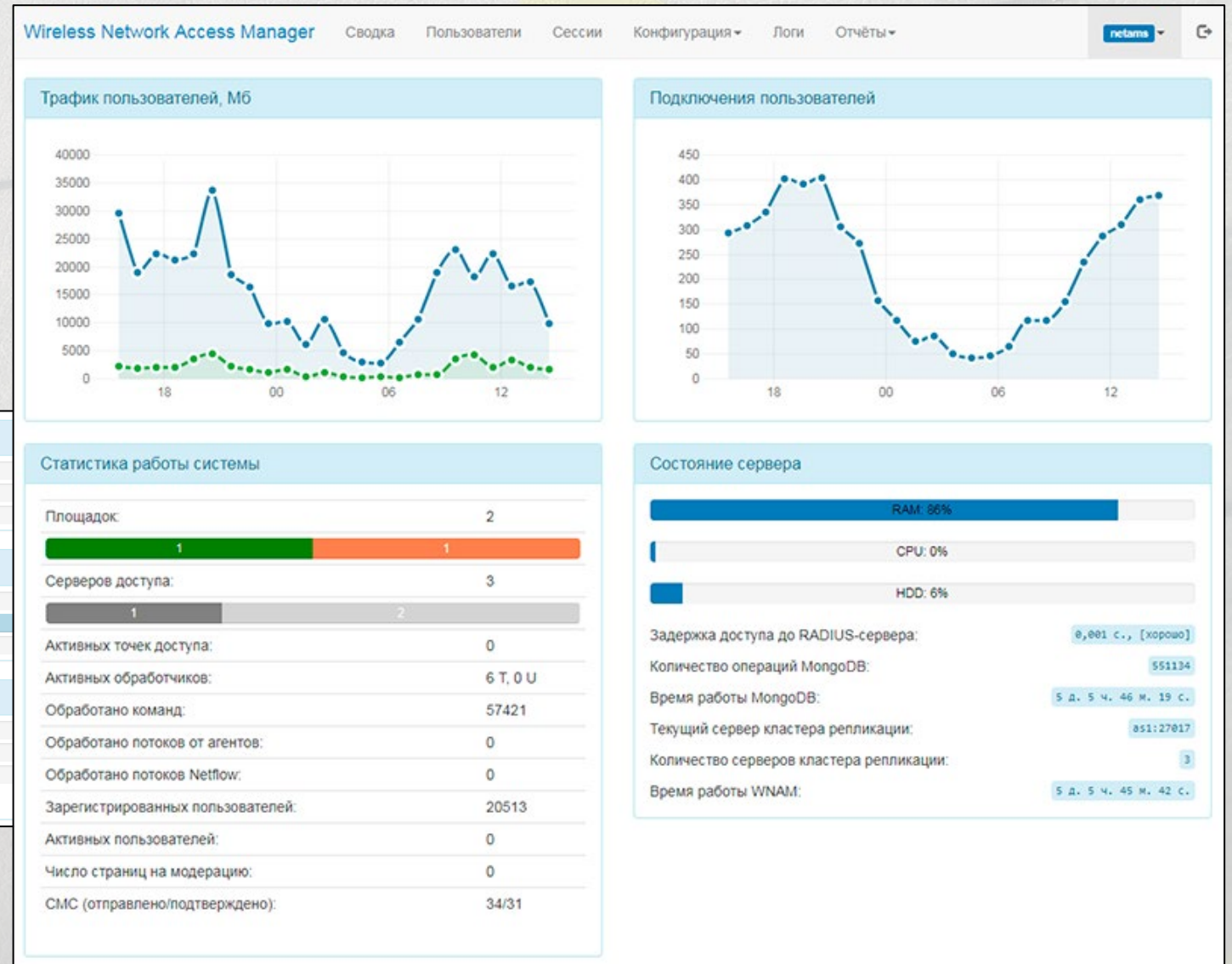
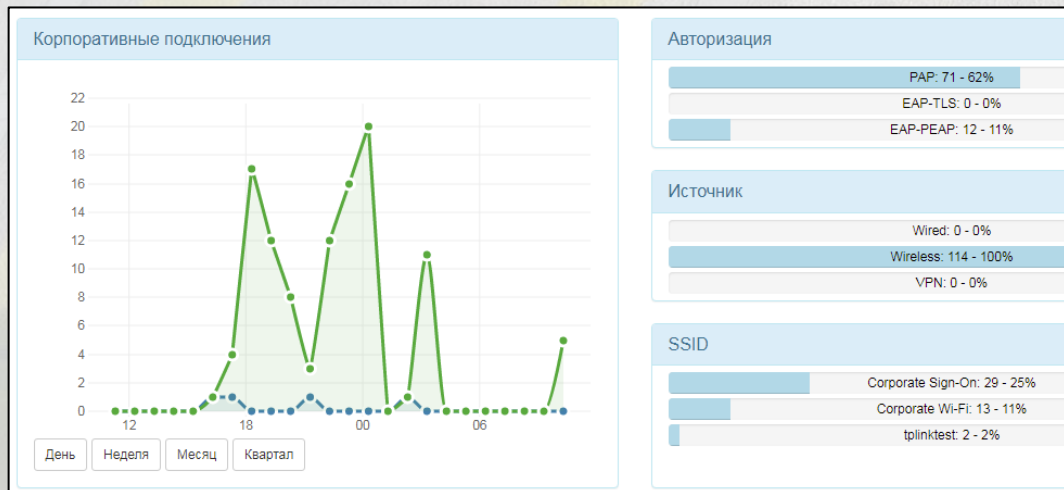
Работает под управлением ОС Linux, в том числе российских

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 (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

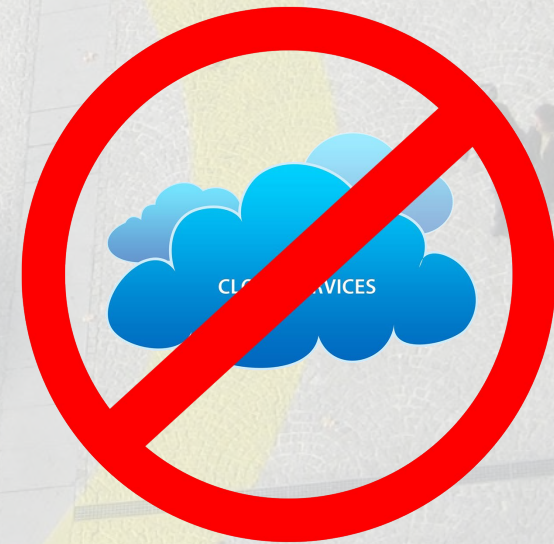
Доработки

- 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 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