

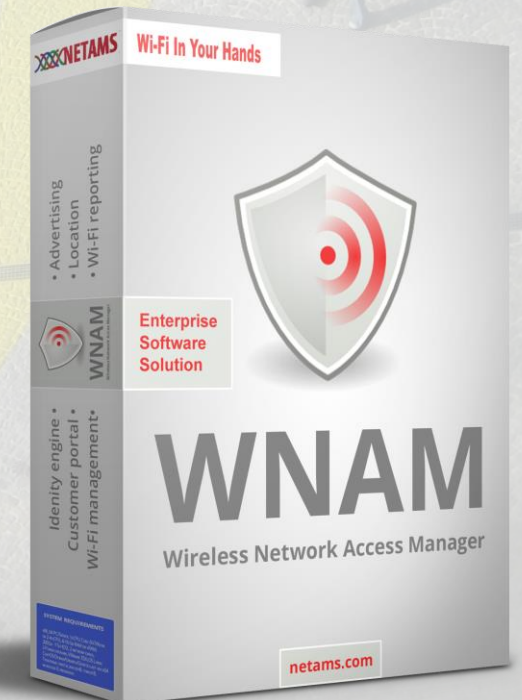
# Корпоративная авторизация в проводных и Wi-Fi сетях

Ваша сеть

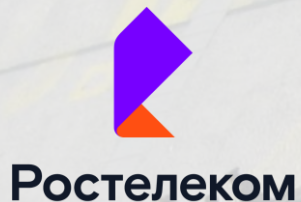
**В ВАШИХ РУКАХ**

## 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

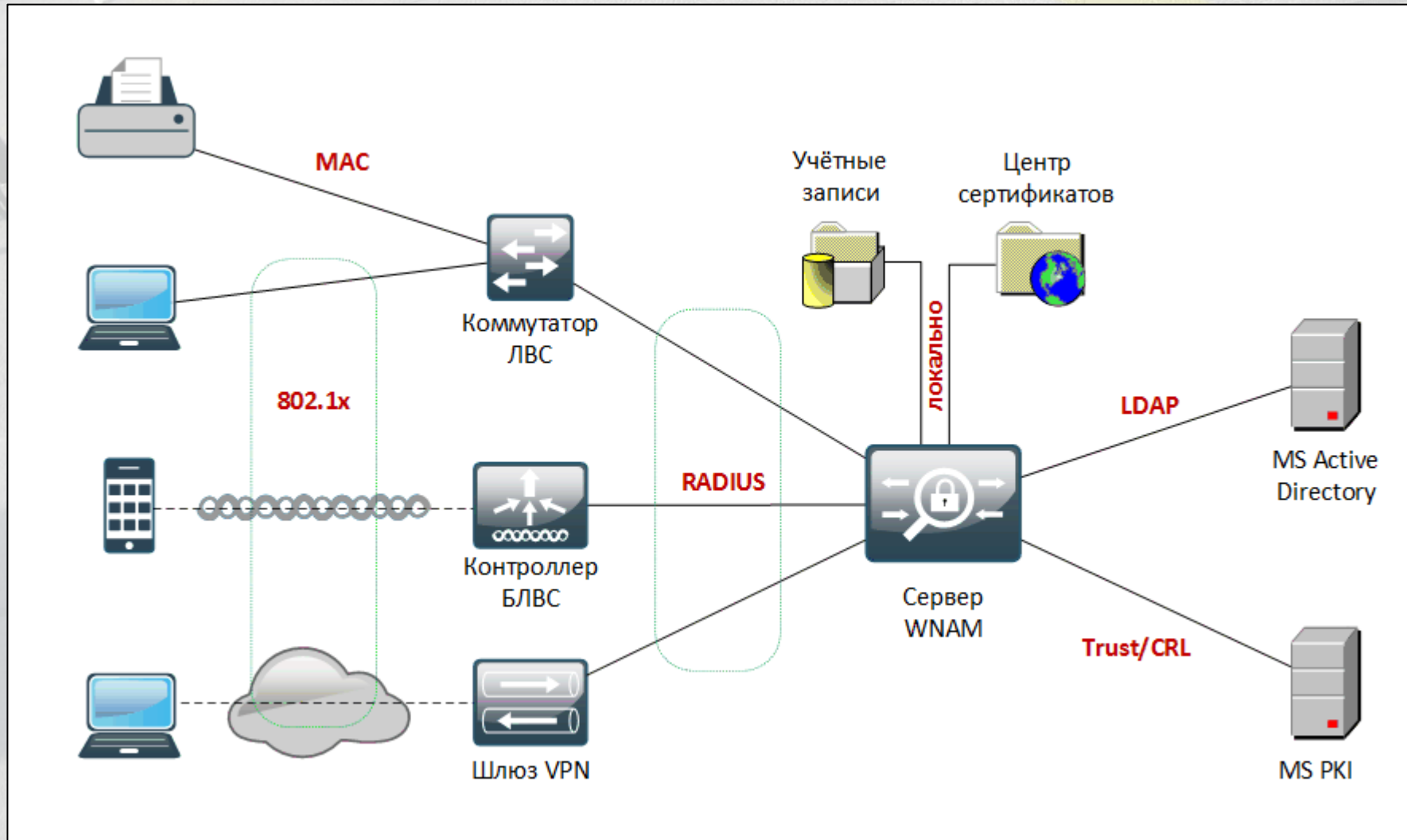
✓ **WNAM Quality of Wireless**

#### 4. Управление оборудованием Wi-Fi


✓ **WNAM Devices Controller**

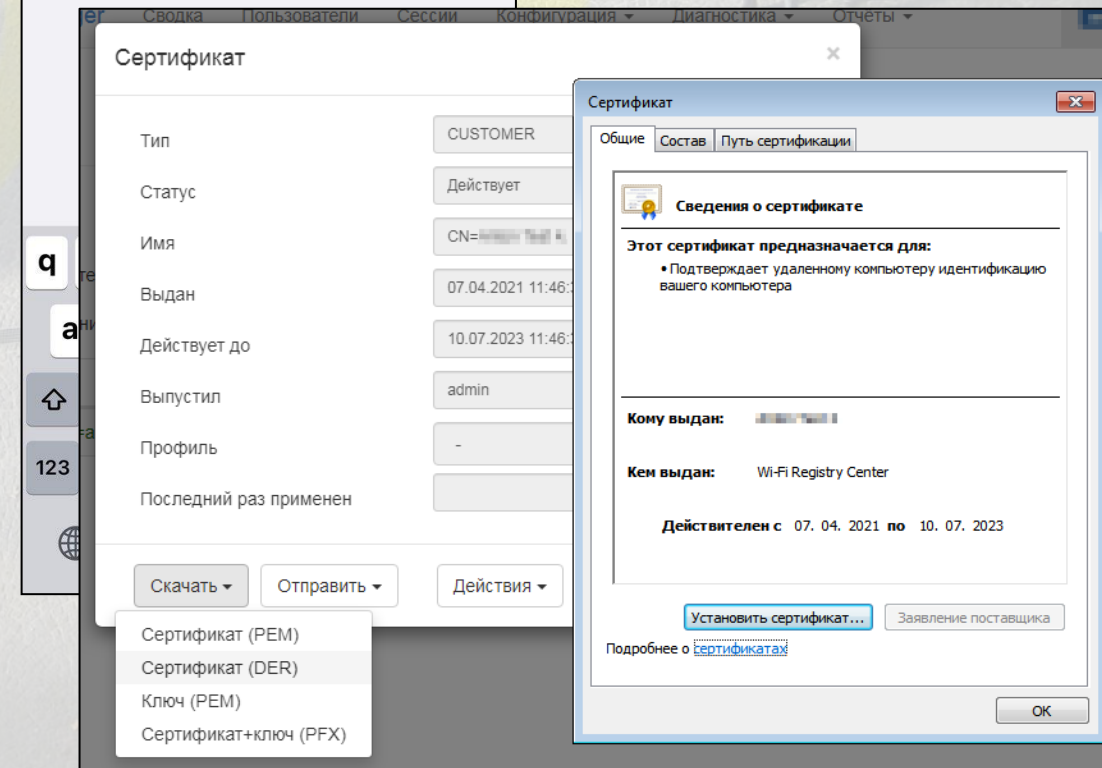
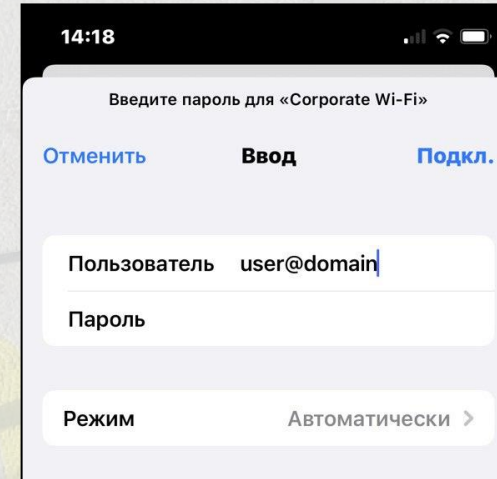


# Архитектура решения корпоративной авторизации



# 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
- Дашбоарды (Q3'22)
- Отчёты



## Модель профилей

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

Назначаемый VLAN ID или ACL  
 Вендор-специфичные RADIUS-атрибуты  
 URL редиректа на портал:  
 СМС-авторизация  
 самообслуживание (сертификат)  
 Параметры сессии:  
 длительность, скорость, объем  
 Правила создания и привязки:  
 учетных записей и сертификатов  
 MAC адреса к порту коммутатора  
 категорий и тэгов пользователя

**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:  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 openсорсу FreeRADIUS

## Работа с сертификатами

- Встроенный корневой УЦ
- Сертификаты от стороннего УЦ
- Для EAP-TLS
- Для работы RADIUS-сервера WNAM

**Сертификат**

Сертификат | Расширения сертификата | Статус сертификата

На данной странице отображен общий статус проверки полного пути сертификации.

Цепочка действительна.

Статус

- WNAM Lab Root CA
- Registry Server
- Егор Летов

[Просмотреть...](#)

Владелец: Егор Летов  
 Статус сертификата: Сертификат действителен  
 Подробности статуса: Сертификат действителен

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 групп
- Получение групп и атрибутов пользователя в момент авторизации
- NTLM-проверка пароля для EAP-PEAP/MSCHAPv2
- Multi-domain (Q3'22)

Имя домена	<input type="text" value="main"/>
Имя контроллера домена	<input type="text" value="dcb1"/>
Учётная запись	<input type="text" value="admin"/>
Пароль	<input type="password" value="*****"/>
URL для NTLM проверки	<input type="text" value="http://10.10.10.10/cgi/ntlmauth.cgi"/>
<input type="button" value="Обновить список групп"/> <input type="button" value="Удалить"/> <input type="button" value="Сохранить"/>	

#	Имя группы	Путь группы
<input type="checkbox"/>	Exchange Servers	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=main,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10
<input type="checkbox"/>	Users	CN=Users,CN=Builtin,DC=main,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10
<input checked="" type="checkbox"/>	Domain Users	CN=Domain Users,CN=Users,DC=main,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10,DC=10.10.10.10

# Траблшутинг

- Детальный лог подключения
- Совпавшие правила
- Примененные атрибуты
- Аккаунтинг трафика

### Параметры записи о сессии

<b>MAC</b>	5A:42:9F:04:97:39	<b>Время начала</b>	19.04.2022, 20:05:39
<b>Идентификатор</b>	79101234567@wnam.с	<b>Имя</b>	Василий Пупкин
<b>IP адрес</b>	IP адрес	<b>Метод</b>	EAP_TLS
<b>SSID</b>	Corporate Wi-Fi	<b>Фреймов</b>	10
<b>Площадка</b>	FNM В CWA	<b>Сервер доступа</b>	FNM LAB IOS XE
<b>Профиль аутентификации</b>	По сертификату (TLS)	<b>Тэг</b>	tls <span style="color: green;">✓</span>
<b>Профиль авторизации</b>	Все пользователи в VLAN 100	<b>Тэг</b>	<span style="color: green;">✓</span>

**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 по локальной базе или Active Directory
- Примененные атрибуты и ограничения
- Лог набранных команд
- Поиск «кто это сделал?»

Время	Логин	Откуда	Сервер доступа	Уровень	Фреймов	Статус
20.05.2022 17:33:21	testuser	172.16.130.5	R20 LAB SW 172.16.130.38	15	6	✓
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:

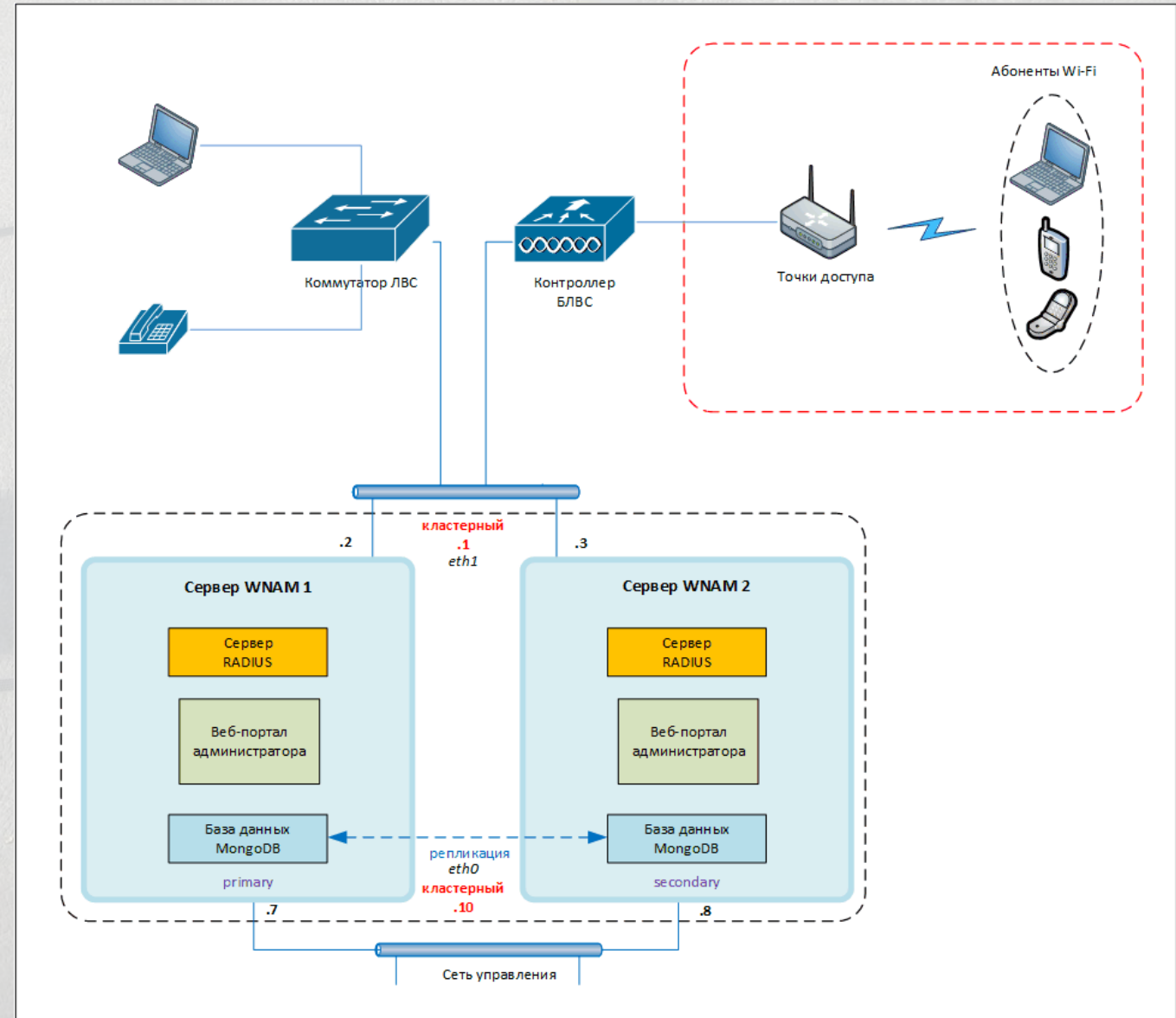
```

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

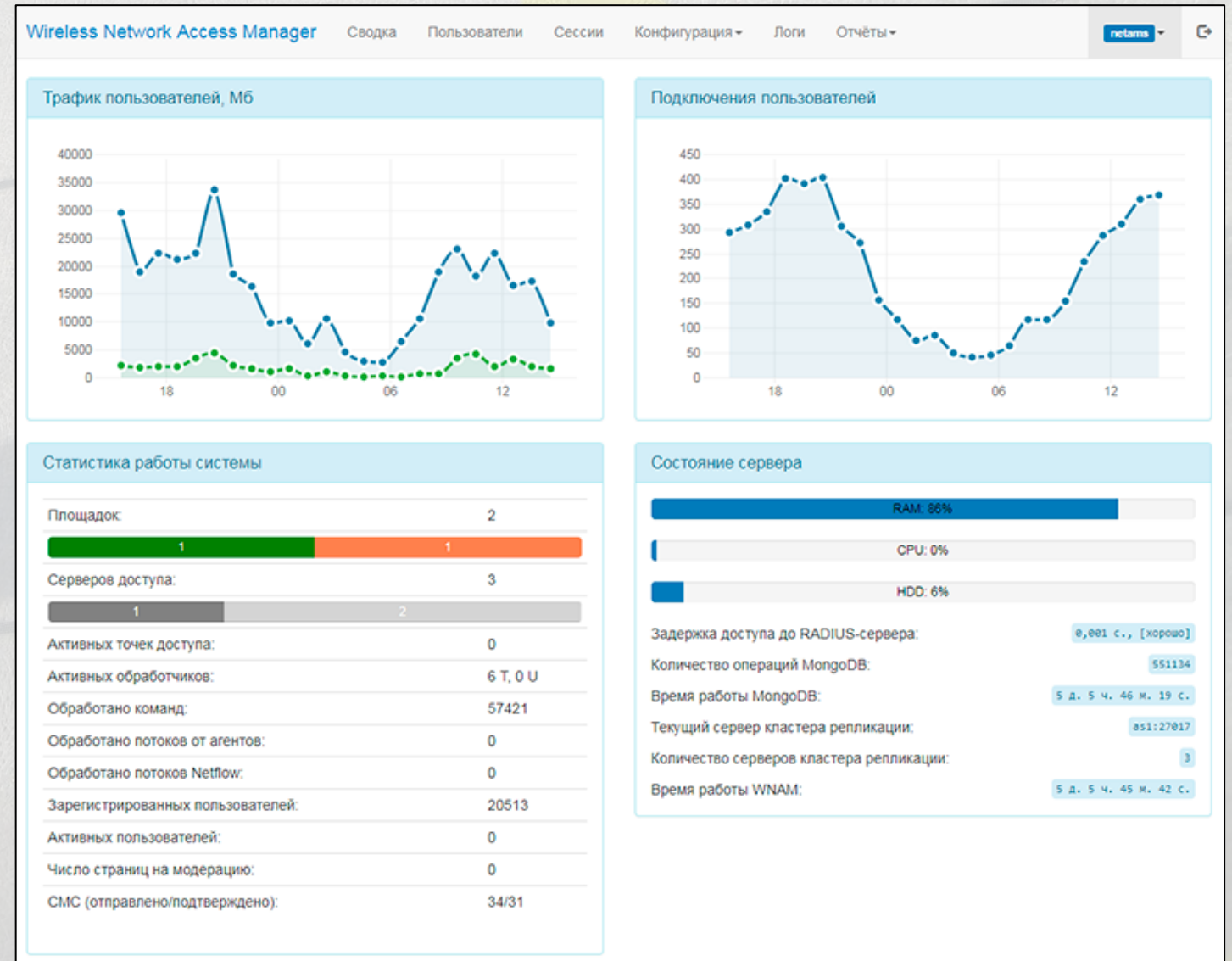
- Поддержка кластерной конфигурации
- Репликация базы данных
- Поддержка гео-распределенной конфигурации

Работает под управлением ОС Linux  
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



## Планы развития

Планы Q3'22:

- дополнительные дашборды по политикам, методам авторизации
- отчеты по источникам, типам авторизации, правилам, топ-10 и иные отчеты в системе отчетности
- авторизация VPN-подключений, и соответствующие доработки в правилах
- формирование загружаемого профиля мобильного устройства, содержащего TLS-сертификаты
- расширение механизма профилирования конечных устройств

В дальнейшем предполагается развивать:

- поддержку более сложных и гибких правил аутентификации и авторизации
- поддержку 802.1x LAN портов с подключением ноутбука через IP-телефон
- учёт занятости LAN-порта, и поиск устройства по всем портам коммутаторов (+история перемещений)

Приоритетные направления развития определяются потребностями заказчиков

## Поддержка продаж

### 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

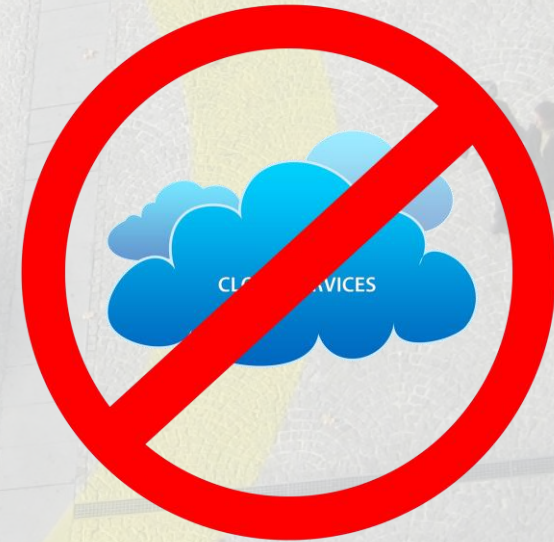
### Доработки

- 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/](https://www.netams.com/corp_auth/)**

**Запросить условия:**

**netams@comptek.ru**

**+7 (495) 789-65-65**