Аутентификация с помощью Eduroam

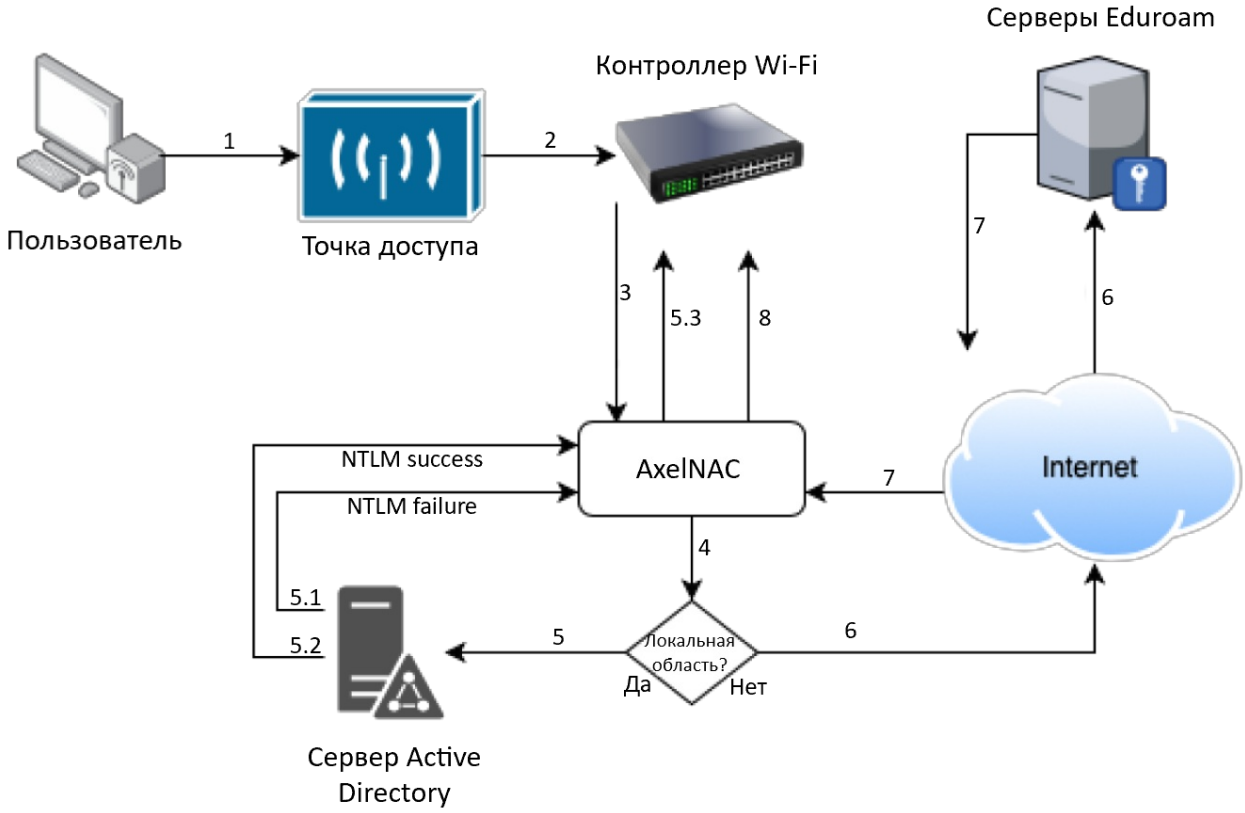
Введение

Eduroam (образовательный роуминг) — это защищенный сервис механизмов аутентификации доступа по всему миру, который разработан для международного научно-образовательного сообщества.

AxelNAC поддерживает аутентификацию с помощью Eduroam и позволяет учебным заведениям-участникам аутентифицировать пользователей, приезжающих из других учебных заведений, как локальных.

Процесс локальной аутентификации

На рисунке ниже показан процесс локальной аутентификации с помощью Eduroam:



1. Устройство подключается к SSID Eduroam.
2. Точка доступа направляет запрос на аутентификацию на контроллер беспроводной сети.
3. Контроллер отправляет RADIUS-запрос аутентификации в AxelNAC на UDP-порт 11812.
4. AxelNAC проверяет, является ли область локальной.
5. Если область является локальной, AxelNAC выполняет NTLM-запрос к контроллеру домена Active Directory для проверки личности.
    1. Active Directory подтвердил учетные данные.
    2. Active Directory не подтвердил учетные данные. AxelNAC отправляет сообщение RADIUS Reject.
    3. После успешной NTLM-аутентификации AxelNAC возвращает сообщение Radius Access Accept беспроводному контроллеру для применения производственной VLAN для этого MAC-адреса.
6. Если область не является локальной, AxelNAC проксирует RADIUS-запрос на серверы Eduroam.
7. Серверы Eduroam подтверждают личность.
8. AxelNAC возвращает сообщение Radius Access Accept беспроводному контроллеру для применения производственной VLAN для этого MAC-адреса.

Настройка источника аутентификации Eduroam

Для того чтобы создать новый источник аутентификации с помощью Eduroam, выполните следующие действия:

Шаг 1. В веб-интерфейсе AxelNAC перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации**.

Шаг 2. Создайте источники RADIUS для каждого из серверов Eduroam, которые необходимо определить. Для этого нажмите **Новый внутренний источник** и выберите **RADIUS** в выпадающем списке.

Шаг 3. Заполните поля **Имя**, **Описание**, **Хост**, **Порт**, **Секретная фраза** и отключите параметр **Отслеживать** (информацию по настройке этого источника можно найти на платформе Eduroam) и нажмите **Создать**.

Шаг 4. Вернитесь в раздел **Источники аутентификации** нажмите **Новый дополнительный источник** и выберите **Eduroam** в выпадающем списке.

Шаг 5. Заполните все обязательные поля, а также укажите источники RADIUS, созданные в шаге 3 в поле **Eduroam RADIUS AUTH**, укажите порт прослушивания аутентификации и установите в поле **Тип** значение **Keyed Balance**.

Шаг 6. Для корректной работы внешних и внутренних студентов с источником Eduroam необходимо:

- в поле **Локальные области** определить области, которые используют локальные пользователи;
- создать общее правило, которое будет назначать роль (например, **Eduroam**) внешним пользователям;
- создать два различных профиля подключения для внешних и локальных пользователей (см. ниже).

Создание профиля подключения для аутентификации внешних пользователей

Для того чтобы создать профиль подключения для внешних студентов, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения → Новый профиль подключения**.

Шаг 2. Создайте профиль подключения с именем **External_eduroam**, активируйте параметр **Регистрировать устройства автоматически** и добавьте фильтр **Область** со значением **Eduroam**.

Шаг 3. Добавьте ранее созданный источник Eduroam для сопоставления с внешними пользователями.

Создание профиля подключения для аутентификации локальных пользователей

Для того чтобы создать профиль подключения для локальных студентов, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Профили подключения → Новый профиль подключения**.

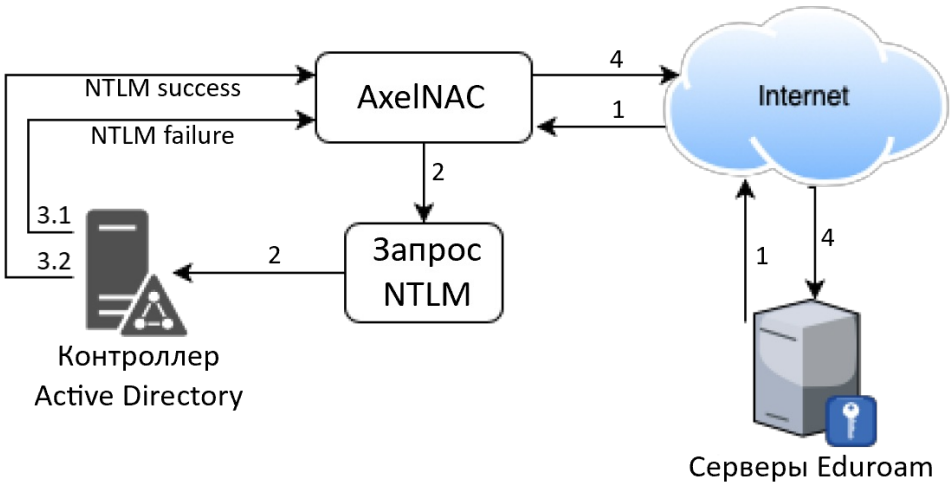
Шаг 2. Создайте профиль подключения с именем **Local_eduroam**, активируйте параметр **Регистрировать устройства автоматически** и добавьте фильтр **SSID** со значением **Eduroam**.

Шаг 3. Добавьте источник Active Directory для аутентификации локальных пользователей.

Данный профиль необходимо создавать только после создания профиля подключения для внешней аутентификации Eduroam. В противном случае запрос для локальных студентов будет совпадать с запросом для внешних студентов.

Процесс входящей аутентификации (TLRS — AxelNAC)

На рисунке ниже показан процесс входящей аутентификации с помощью Eduroam:



1. Eduroam отправляет RADIUS-запрос аутентификации на публичный IP-адрес (NAT/PAT), привязанный к AxelNAC на управляющем IP-адресе (Management VIP для кластера) на UDP-порт 1812.
2. AxelNAC пересылает NTLM-запрос контроллеру Active Directory.
3. Ответ NTLM:
    1. Active Directory подтвердил учетные данные.
    2. Active Directory не подтвердил учетные данные.
4. AxelNAC отвечает серверам Eduroam либо сообщением RADIUS Access Accept при успешной аутентификации, либо сообщением RADIUS Access Reject при неуспешной аутентификации. AxelNAC устанавливает область Eduroam для всех успешных аутентификаций.

Источник аутентификации настраивается так же, как и для локальной аутентификации.

Для данного варианта аутентификации нет необходимости создавать профиль подключения в AxelNAC. FreeRADIUS будет выполнять только NTLM-аутентификацию и не будет отправлять RADIUS-запрос в AxelNAC API.

ID статьи: 937
Последнее обновление: 31 мар., 2025
Обновлено от: Михалева А.
Ревизия: 4
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Источники аутентификации -> Аутентификация с помощью Eduroam
https://docs.axel.pro/entry/937/