Глава 3. Аутентификация пользователей на Captive-портале

Captive-портал — это механизм аутентификации, применяемый в AxelNAC для управления доступом к сети через веб-интерфейс. Он используется в ситуациях, когда клиент не поддерживает 802.1X-аутентификацию или требует интерактивного подтверждения личности. Captive-портал перенаправляет пользователя на специальную веб-страницу, где он вводит свои учетные данные, подтверждает политику безопасности или проходит регистрацию. После успешной проверки AxelNAC назначает соответствующую роль или политику доступа (например, VLAN, уровень сетевых прав или временной доступ).

Captive-портал часто используется для гостей, BYOD-устройств или временных пользователей, которым неудобно или невозможно установить супликант для 802.1X. Этот метод обеспечивает базовый контроль доступа, но при этом опирается на механизмы веб-аутентификации, а не на протоколы уровня канала, как EAP-TLS или PEAP-MSCHAPv2.

Протокол работы Captive-портала

Работа Captive-портала основана на стандартных веб-протоколах **HTTP** или **HTTPS**. Когда клиент впервые пытается получить доступ в интернет, его запрос перенаправляется на специальный URL NAC-системы. Это называется **HTTP/HTTPS redirection**.

- При **HTTP-перенаправлении** клиент видит веб-страницу аутентификации без шифрования. Такой подход используется редко, поскольку данные могут быть перехвачены.
- При **HTTPS-перенаправлении** соединение между клиентом и NAC-сервером защищается TLS, а пользователь видит стандартный браузерный интерфейс с адресом портала.

После успешной авторизации сервер аутентификации сообщает сетевому оборудованию (через RADIUS CoA или API), что клиент подтвержден, и разрешает ему доступ в сеть.

Для обеспечения работы портала по протоколу HTTPS требуется указать необходимые сертификаты в настройках **Конфигурация - Настройки системы - SSL-сертификаты – HTTP**. Клиентское устройство должно доверять сертификату сервера.

Типовое использование портала в сценарии гостевого доступа

При подключении к открытой гостевой SSID сетевое оборудование **(NAS)** направляет **MAC-адрес клиента** в качестве логина и пароля на сервер AxelNAC. AxelNAC, используя механизм **MAC-Auth**, в ответ отправляет **RADIUS-Accept** и назначает клиенту роль **registration**, то есть статус «незарегистрированного пользователя».

Обычно для роли **registration** в профиле сетевого оборудования задаются:

- VLAN без доступа в интернет;
- ACL, разрешающий только обращение к Captive-порталу;
- ссылка для перенаправления на страницу регистрации.

Таким образом, клиент получает IP-адрес в изолированной сети регистрации и автоматически попадает на портал, где может завершить процесс аутентификации.

На портале пользователь вводит дополнительные данные для регистрации — например, электронную почту, номер телефона (с подтверждением по SMS), или использует спонсорский доступ. При необходимости возможна двухфакторная аутентификация. После успешной проверки NAC-система изменяет роль клиента на **продуктивную**, что означает применение другого VLAN и ACL, обеспечивающих выход в интернет и/или доступ к корпоративным ресурсам. В продуктивной роли ссылка на портал отсутствует, поэтому клиент больше не перенаправляется на страницу регистрации.

Сертификаты и структура X.509 v3

Если Captive-портал работает по **HTTPS**, сервер AxelNAC использует цифровой сертификат для установления защищенного канала с браузером клиента. Сертификат стандарта **X.509 v3** связывает открытый ключ с доменом портала и содержит идентификационные данные, сведения об издателе (CA), срок действия и цифровую подпись.

В версии X.509 v3 добавлены расширения, которые уточняют назначение сертификата, определяют альтернативные имена (SAN — например, fqdn портала), политику доверия и методы проверки статуса. При обращении к порталу браузер клиента проверяет сертификат по цепочке доверия — от сертификата сервера AxelNAC до корневого центра сертификации (CA). Если сертификат действителен и выдан доверенным CA, браузер устанавливает защищенное TLS-соединение без предупреждений.

Участие сертификата центра сертификации (CA)

Центр сертификации **(CA)** обеспечивает доверие между клиентом и Captive-порталом. Сертификат портала должен быть подписан доверенным CA, чтобы браузер распознал сайт как безопасный. Если сертификат самоподписанный или выдан внутренним CA, не установленным в хранилище доверенных корней клиента, браузер отобразит предупреждение — “Соединение небезопасно” или “Ненадежный сертификат”, а замок в адресной строке будет перечеркнут.

Такое предупреждение не влияет на работу Captive-портала, но вызывает недоверие у пользователей и может привести к отказу от ввода учетных данных. Поэтому в корпоративных сетях рекомендуется использовать сертификаты, подписанные публичным CA, либо заранее установить внутренний CA на все управляемые устройства.

CA также играет ключевую роль в защите от атак, связанных с подменой портала. Если сертификат Captive-портала выдан доверенным CA, злоумышленник не сможет создать поддельный портал с таким же доменным именем без компрометации

приватного ключа. Это гарантирует, что пользователи вводят данные именно на оригинальной странице AxelNAC.

Безопасность и практическое применение

Captive-портал обеспечивает совместимость с любыми устройствами, включая IoT и гостевые терминалы, но при этом уступает 802.1X-аутентификации по уровню защиты. Основные риски связаны с использованием самоподписанных сертификатов, отсутствием шифрования при HTTP, а также с возможностью фишинга на поддельных страницах.

Настройка работы Captive-портала

В лабораторной среде EVE-NG находятся виртуальные коммутаторы, которые не поддерживают access-листы. Из-за этого, когда клиент подключается к сети, проходит аутентификацию по 802.1X и получает ACL и ссылку для перенаправления на страницу регистрации, он просто теряет соединение с сетью. Чтобы избежать этого, для виртуальных коммутаторов используется другой механизм — «DNS-Enforcement». В этом режиме клиенту назначается только VLAN, а перенаправление выполняется за счет подмены DNS-ответов.

Учтите, что DNS-Enforcement не может работать с NAT.

Настройка проводного подключения к порталу

Добавление нового сетевого устройства

Добавьте новое сетевое устройство, выполнив следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Сетевые устройства** и нажмите **Новое сетевое устройство**. Выберите группу сетевых устройств, в которую должно входить сетевое устройство.

Шаг 2. На вкладке **Определение** заполните следующие параметры:

- **IP-адрес/MAC-адрес** — IP-адрес коммутатора.
- **Тип** — выберите профиль для вашего коммутатора или серии коммутаторов.
- **Режим** — Продуктивный.
- **Метод реаутентификации** — RADIUS.

Шаг 3. На вкладке **Роли** активируйте параметр **Базовый режим**. Перейдите к блоку **Назначение Local ACL** и заполните следующие параметры:

- **Назначать Local ACL** — Включено.
- **registration** — укажите имя ACL reg_acl, который будет использоваться для Web-redirect.

Шаг 4. Перейдите к блоку **Назначение URL веб-аутентификации** и заполните следующие параметры:

- **Назначать URL веб-аутентификации** — Включено.
- **registration** — http(s)://адрес_AxelNAC/Cisco::Catalyst_2960.

Шаг 5. На вкладке **RADIUS** заполните следующие параметры:

- **Секретная фраза** — ключ, указанный на коммутаторе.
- **Использовать CoA** — Включено.
- **CoA-порт** — 3799.

После этого настройте ваш коммутатор, объявив на нем VLAN. Далее необходимо настроить Captive-портал для AxelNAC.

Настройка Captive-портала в AxelNAC

https://docs.axel.pro/kb_upload/image/image-2024-1-9_14-10-54.png

Для того чтобы настроить работу Captive-портал в AxelNAC, выполните следующие шаги:

Шаг 1. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс на котором необходимо включить функционал Captive-портал.

Шаг 2. В строке **Дополнительный демон (демоны) прослушивания** добавьте значение **портал** из выпадающего списка, затем нажмите **Сохранить**.

Шаг 3. Перейдите в раздел **Статус → Службы** и перезапустите следующие службы:

- haproxy-portal;
- httpd.portal;
- iptables.

Если используемое сетевое оборудование не поддерживает перенаправление на Captive-портал, включая случаи работы с виртуальным сетевым оборудованием (которое не поддерживает нативное перенаправление), выполните дополнительные настройки.

Дополнительные настройки:

Шаг 1. На сетевом устройстве создайте выделенный VLAN, в который будут направляться пользователи, подлежащие перенаправлению (redirect).

Шаг 2. На DHCP-сервере для этого VLAN укажите в параметре **DHCP Option 6** (DNS-сервер) IP-адрес сервера AxelNAC.

Шаг 3. Перейдите в блок **Конфигурация → Сетевое взаимодействие → Интерфейсы → Маршрутизируемые сети** и нажмите **Новая маршрутизированная сеть**.

Шаг 4. В открывшемся окне на вкладке **Основное** заполните следующие поля:

- **Маршрутизированная сеть**: заполните собственным значением;
- **Маска сети**: 255.255.255.0;
- **Тип**: Применение DNS Enforcement.

Шаг 5. На вкладке **Маршрутизация** укажите адрес шлюза, который будет использоваться для этой сети.

Шаг 6. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выберите интерфейс на котором необходимо включить функционал Captive-портал.

Шаг 7. В строке **Дополнительный демон (демоны) прослушивания** добавьте значение **dns** из выпадающего списка, затем нажмите **Сохранить**.

Шаг 8. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Интерфейсы** и выполните перезапуск сервисов **iptables**, **pfdns**.

Шаг 9. Перейдите в раздел **Конфигурация → Сетевое взаимодействие → Passthrough** и заполните следующие поля в открывшемся окне:

- **Перехват прокси**: Включено;
- **Порт перехвата прокси-сервера:** 80 и 443.

Настройка области

Для дальнейшей конфигурации сетевых соединений создайте область, выполнив следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Домены → Области** и нажмите **Новая область**.

Шаг 2. На вкладке **Основное** заполните поле **Область**, введя имя вашего домена.

Вы можете не создавать область, если создали ее ранее. В этом случае на вкладке **Области** нажмите на созданную вами ранее область, чтобы перейти в режим редактирования.

Шаг 3. Нажмите **Создать** в левом нижнем углу страницы.

После этого перезапустите сервис **radiusd-auth**.

ID статьи: 1443
Последнее обновление: 16 дек., 2025
Обновлено от: Ильина В.
Ревизия: 5
База знаний AxelNAC -> Обучающие материалы -> Обучающие курсы -> Конфигурация сетевых соединений -> Раздел 1. Аутентификация пользователей -> Глава 3. Аутентификация пользователей на Captive-портале
https://docs.axel.pro/entry/1443/