УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ РЕШЕНИЙ MFA С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Ж.М. Алимжанова[1], Н.Ж. Тойбек[2], А.К. Али[3], Н.М. Ниязбек[4]
[1,2,3,4]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
e-mail: nurtas.toibek@gmail.com
[2]ORCID ID: https://orcid.org/0009-0002-2180-0317
[3]ORCID ID: https://orcid.org/0009-0006-2165-0960
[4]ORCID ID: https://orcid.org/0009-0006-6105-6229

Аннотация. Эта статья посвящен 5 лучшим решениям MFA с открытым исходным кодом. Технологии быстро меняются, поэтому нам потребуется адаптировать решения MFA с открытым исходным кодом. Многофакторная аутентификация (MFA) — это метод и технология, которые будут использоваться для проверки личности пользователя. Чтобы пользователи могли войти в систему или совершить транзакцию, требуется как минимум два или более типов категорий учетных данных. Успешная комбинация как минимум двух независимых учетных данных является обязательным требованием метода MFA. Обычно он сочетает в себе одну из трех следующих категорий учетных данных:

1. Что знает пользователь: пароль или кодовую фразу
2. Что у человека есть: жетон безопасности, брелок или SIM-карта
3. Что представляет собой пользователь: биометрические данные, такие как отпечатки пальцев, сетчатка или радужная оболочка глаза, голос или распознавание лиц.

MFA требует, чтобы пользователь предоставил два или более фактора проверки, чтобы получить доступ к ресурсу, например к приложению или учетной записи в Интернете. MFA требуется один или несколько дополнительных критериев проверки в дополнение к логину и паролю, что снижает вероятность успешной кибератаки. Общедоступный код считается «открытым исходным кодом». Кроме того, инструменты и решения с открытым исходным кодом более безопасны, поскольку код может быть проверен и проверен кем угодно.

Ключевые слова: MFA, 2FA, LDAP, AAA, RADIUS, система аутентификации авторизации и учета событий, многофакторная аутентификация, решение с открытым исходным кодом.

Введение

Эта статья посвящен 5 лучшим решениям MFA с открытым исходным кодом:

1. Gluu Casa

Рисунок 1 - Значок Gluu Casa

Gluu Casa — это многофакторная аутентификация с открытым исходным кодом и самообслуживанием для повышения вашей цифровой личности. Это революционно. Casa предоставляет единую точку управления для конечных пользователей, которая позволяет им просматривать, регистрировать и удалять учетные данные MFA. Он также поставляется с аппаратными токенами, программными токенами, коммерческими услугами (такими как Duo), входом в социальные сети, биометрическими данными и мобильными устройствами. Он также является расширяемым. Когда появятся какие-либо новые технологии аутентификации, вы можете загрузить плагины, чтобы использовать их в своей организации с помощью Casa.[1]

Gluu Casa обеспечивает современную многофакторную аутентификацию, такую как адаптивная аутентификация, аутентификация на основе местоположения, а также доверенный браузер.

Преимущества Gluu Casa:

1. Развертывание облачных технологий
2. Casa — правильный выбор для вас, если вы любите Kubernetes или такие сервисы, как Amazon EKS, Google GKS или SUSE Rancher. Casa поддерживает облачные развертывания с использованием стандартных инструментов, таких как Helm. Он также поддерживает несколько серверных баз данных, включая LDAP, Couchbase, RDBMS, Amazon Aurora и Google Spanner.
3. Применять строгую аутентификацию
4. Только нужный человек на правильном устройстве может иметь доступ к приложениям. Заперев входную дверь, вы можете повысить уровень безопасности своего бизнеса. Casa предлагает OpenID Connect API в качестве интерфейса, а также стандартный JWT «id_token». Его также можно использовать для обеспечения соблюдения политики.
5. Больше никаких сбросов пароля
6. Даже не обращаясь в службу поддержки и не нарушая безопасность учетных данных, пользователи могут беспрепятственно регистрировать, управлять и удалять учетные данные без пароля на всех своих устройствах. MFA организации так же надежна, как и самый слабый рабочий процесс восстановления учетной записи!

2. Ory

Рисунок 2 - Значок Ory

Ory — крупнейшее сообщество решений MFA с открытым исходным кодом в мире безопасности облачных программных приложений. Он будет управлять пользователями и аутентифицировать их, устанавливать и проверять разрешения, защищать ваши API, приложения, данные и многое другое. Он имеет экосистему сервисов с четкими границами, которые решают вопросы аутентификации и авторизации.

Преимущества Ory:

1. Надежная защита
2. Ory предлагает надежную защиту от попыток взлома, таких как кейлоггеры и атаки грубой силы. Если злоумышленнику удастся скомпрометировать учетные данные, этой информации будет недостаточно, чтобы получить доступ к учетной записи.
3. Удобное управление пользователями
4. Он обеспечивает беспрепятственное управление пользователями, предоставляя идентификаторы, сохраняя информацию о пользователе, настраивая методы аутентификации и используя безголовый API.
5. Полностью гибкий
6. Он достаточно гибок с точки зрения аутентификации, авторизации, контроля доступа и делегирования, чтобы соответствовать изменяющимся потребностям вашего бизнеса.[2]

3. ForgeRock

Рисунок 3 - Значок ForgeRock

ForgeRock — это поставщик решений для идентификации с открытым исходным кодом, который предлагает возможности MFA. Это платформа цифровой идентификации, разработанная для любой облачной среды, которая предоставляет пользователям свободу самостоятельно выполнять действия, связанные с идентификацией и доступом. Это

решение улучшает взаимодействие с пользователем и повышает производительность, обеспечивая при этом результаты без ущерба для угроз кибербезопасности. Это решение может снизить затраты организации, предоставляя соответствующий уровень доступа ко всем системам и пользователям в нужное время, позволяя пользователям контролировать свой профиль, пароль и настройки конфиденциальности.

Преимущества ForgeRock:

1. Реализация широкого спектра мер аутентификации
2. Различные меры аутентификации, такие как безопасная многофакторная аутентификация (MFA) или методы двухфакторной аутентификации (2FA), реализуются ForgeRock Access Management.
3. Решения варьируются от простых и беспарольных вариантов до входа через социальные сети, до самых безопасных биометрических данных и требований уровня гарантии NIST 800-63.
4. Одна платформа, любое облако
5. ForgeRock предлагает различные гибкие варианты, такие как локальное, облачное или гибридное развертывание. Он также предоставляет различные инструменты DevOps, чтобы разработчики не тратили усилия на создание собственных инструментов для перемещения конфигураций между средами.[3]
6. API Security для защиты от вредоносной активности
7. Киберпреступники также нацелены на незащищенные API. Его Identity Gateway используется для мониторинга трафика API, ограничения объема трафика и обнаружения аномалий, чтобы поддерживать работоспособность сервисов и защищать от взломов и распределенных атак типа «отказ в обслуживании» (DDoS).

4. PrivacyIDEA

Рисунок 4 - Значок PrivacyIDEA

PrivacyIDEA — это решение с открытым исходным кодом, предоставляющее широкий спектр различных технологий аутентификации, включая MFA. Он поставляется с мощной и гибкой структурой политик, которая позволяет вам адаптировать PrivacyIDEA к вашим потребностям. Уникальные модули обработчиков событий позволяют встроить PrivacyIDEA в существующие рабочие процессы или создать новые рабочие процессы, которые лучше всего подходят для вашего сценария. Он также хорошо сочетается с другими и интегрируется с решениями для идентификации и аутентификации, такими как FreeRADIUS, simpleSAML, Keycloak или Shibboleth. Эта гибкость может быть причиной того, что такие организации, как World Wide Web Consortium и такие компании, как Axiad, используют PrivacyIDEA.[4]

Преимущества PrivacyIDEA:

1. Облачная защита
2. PrivacyIDEA предлагает различные гибкие варианты, такие как локальное, облачное или гибридное развертывание. Он защищает данные организации, предотвращая доступ неправильных пользователей. Только нужный человек к правильному устройству может предоставить доступ.
3. Ускорьте окупаемость времени
4. PrivacyIDEA поддерживает несколько географических регионов по всему миру. Увеличьте скорость и упростите реакцию вашей организации на глобальные потребности в услугах с помощью автоматизированного развертывания. Это уменьшит сложности, связанные с соблюдением географических требований. Чтобы достичь производительности и операционных целей для разработки, тестирования или производства, вы можете

настраивать и масштабировать развертывания по мере необходимости. Он даже имеет региональные параметры конфигурации, которые помогут вам соблюдать географические или нормативные ограничения.

5. Простота использования и эксплуатации[5]

6. PrivacyIDEA осознает, что первоначальные затраты на закупку являются лишь частью общих затрат при внедрении решения. Таким образом, они разработали архитектуру развертывания для масштабируемости и простоты обслуживания. Обновления не должны останавливать вас на достигнутом и требовать операционных бюджетов, значительно превышающих ваши первоначальные инвестиции. Вопросов возникнуть не должно, технические специалисты всегда доступны и гарантируют своевременный ответ.

5. Authentik

Рисунок 5 - Значок Authentik

Authentik — это поставщик решений для идентификации с открытым исходным кодом, который предлагает возможности MFA. Особое внимание уделяется гибкости и универсальности. Даже в существующей среде вы можете использовать authentik для добавления поддержки новых протоколов, реализации регистрации/восстановления и т.д. в вашем приложении, чтобы избежать проблемы с ним и многое другое.

У него есть несколько полезных функций, таких как прокси-сервер, который вы можете использовать в кластере для добавления аутентификации к службам, или такие вещи, как панели мониторинга без пароля (Longhorn и т. д.).[6]

Преимущества Authentik:

1. Подходит для меняющихся потребностей бизнеса

2. Authentik обладает высокой гибкостью, что означает, что вы можете легко адаптироваться к изменяющимся потребностям вашего бизнеса. Его можно настроить для всех пользователей, включая сотрудников, клиентов и партнеров. Это устраняет необходимость в нескольких паролях, упрощает процесс входа в систему и улучшает взаимодействие с пользователем.

3. Повышает безопасность - Многофакторная аутентификация Authentic с открытым исходным кодом является наиболее эффективным средством обеспечения безопасности для защиты локальных и общедоступных облачных данных.

4. Легко использовать - Authentic упростила процесс аутентификации, предоставив простой контроль доступа.[7]

Результаты исследования

После краткого обзора, давайте углубимся в архитектуру одной из них, точнее детальнее про PrivacyIDEA

PrivacyIDEA — это система, которая используется для управления устройствами для двухфакторной аутентификации. Используя PrivacyIDEA, вы можете улучшить свои существующие приложения, такие как локальный вход, VPN, удаленный доступ, SSH-соединения, доступ к веб-сайтам или веб-порталам, с помощью второго фактора во время аутентификации. Таким образом, повышается безопасность ваших существующих приложений. Вначале были токены OTP, но добавлены другие средства аутентификации, такие как SSH-ключи. Появляются другие концепции, такие как обработка машин или регистрация сертификатов. PrivacyIDEA - это веб-приложение, написанное на Python на основе flask micro framework. Вы можете использовать любой веб-сервер с интерфейсом wsgi для запуска PrivacyIDEA. Например, это может быть Apache, Nginx или даже werkzeug. Устройство или элемент, используемые для аутентификации, по-прежнему называются

“токеном”. Вся информация о токенах хранится в базе данных SQL, при этом вы можете выбрать, какую базу данных вы хотите использовать. PrivacyIDEA использует SQLAlchemy для сопоставления базы данных с внутренними объектами. Таким образом, вы можете выбрать запуск PrivacyIDEA с SQLite, MySQL, PostgreSQL, Oracle, DB2 или другой базой данных. [8]

PrivacyIDEA предоставляет чистый REST API. Администраторы могут использовать веб-интерфейс или клиент командной строки для управления устройствами аутентификации. Пользователи могут войти в веб-интерфейс, чтобы управлять своими собственными токенами. Аутентификация выполняется через API или определенные плагины для FreeRADIUS, SimpleSAMLphp, Wordpress, Contao, Dokuwiki. . . либо предоставлять протоколы по умолчанию, такие как RADIUS или SAML, либо напрямую интегрироваться в приложения. Благодаря такой гибкости существует также множество различных способов установки и настройки PrivacyIDEA.

Как уже говорилось PrivacyIDEA можно интегрировать с Доменом Каталогов, с помощью протокола LDAP, чтобы он мог добавлять пользователей прямо с AD(Active Directory). В рисунке 6 показан пример добавление LDAP Resolver. Здесь использован протокол LDAP, но можно и использовать защищенную версию LDAPS. Тогда нужно испортировать сертификаты. Здесь нужен учетная запись пользователя с привилегией чтение домменных пользователей. Внизу можно быврать целый домен или же филтровать их по группе.[9]

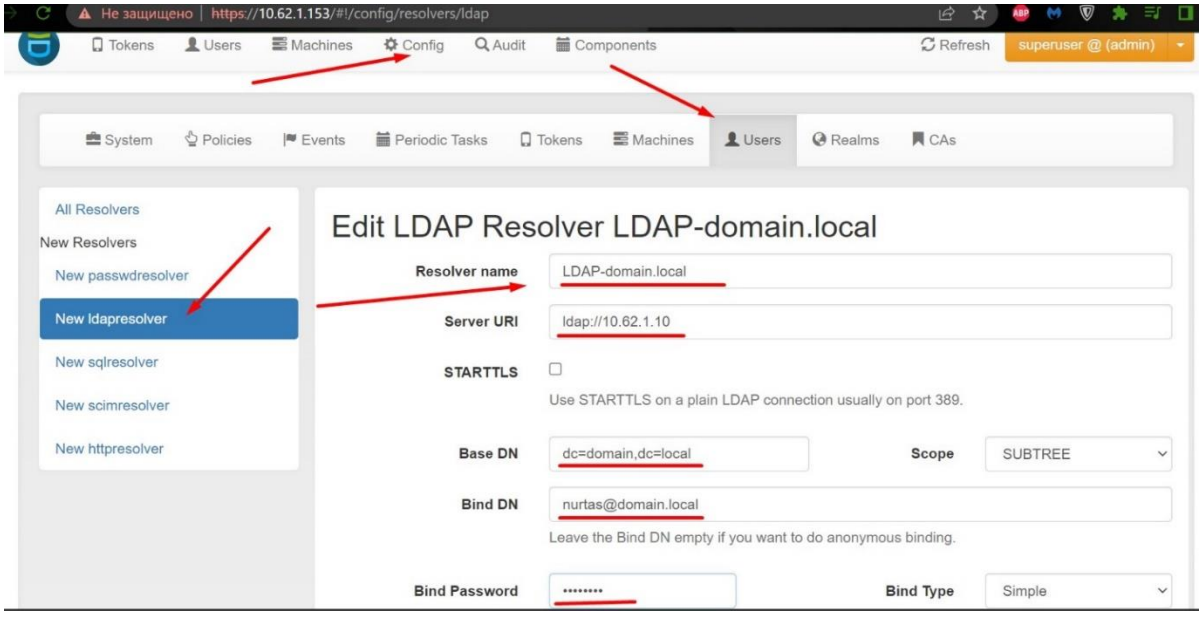

Рисунок 6 - Добавление удаленных пользователей

На рисунке 7, показаны все доступные методы аутентификации, и здес обычно в продакшне используют методы TOTP и HOTP. Больше всего используется метод TOTP, который на основе времени вычиляет OTP(One Time Password). И меняется по умолчанию каждые 60 секунд. Сейчас этот метод считается относительно безопасным.

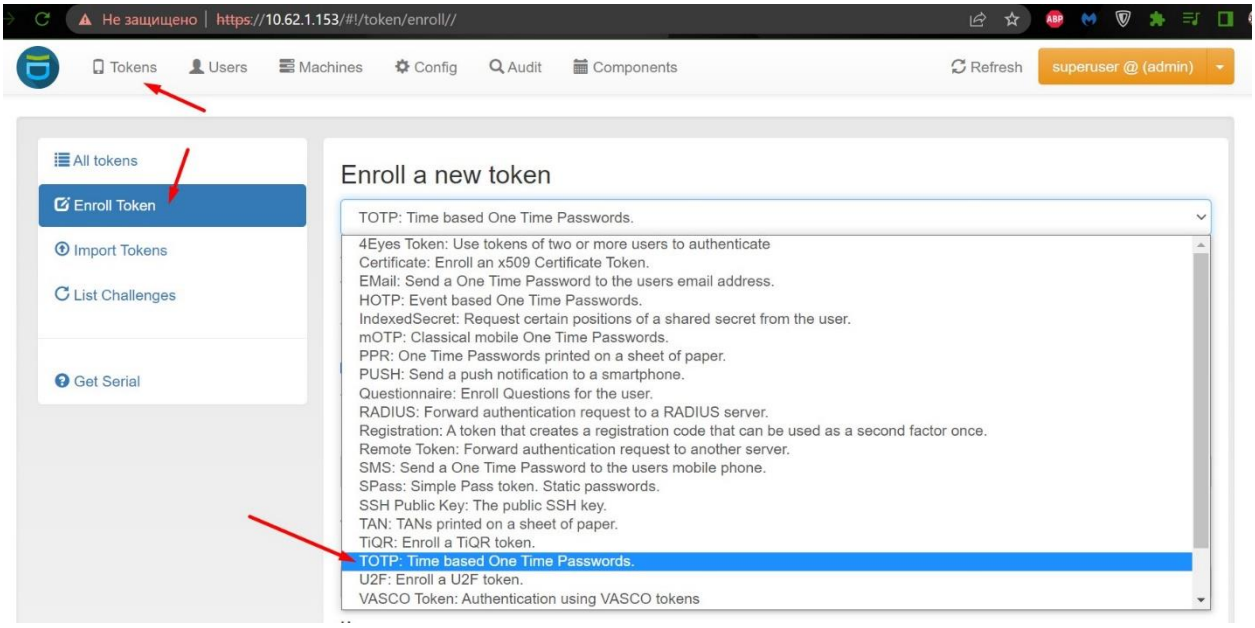

Рисунок 7 - Доступные методы в PrivacyIDEA

В PrivacyIDEA есть модуль FreeRADIUS, и с помощью него он может интегрироваться разными сетевыми устройствами и NAD(Network Access Device). На рисунке 8 показано добавление RADIUS клиента в FreeRADIUS. Только после добавление PrivacyIDEA будет работать с ним, это как добавление в доверенные устройства.

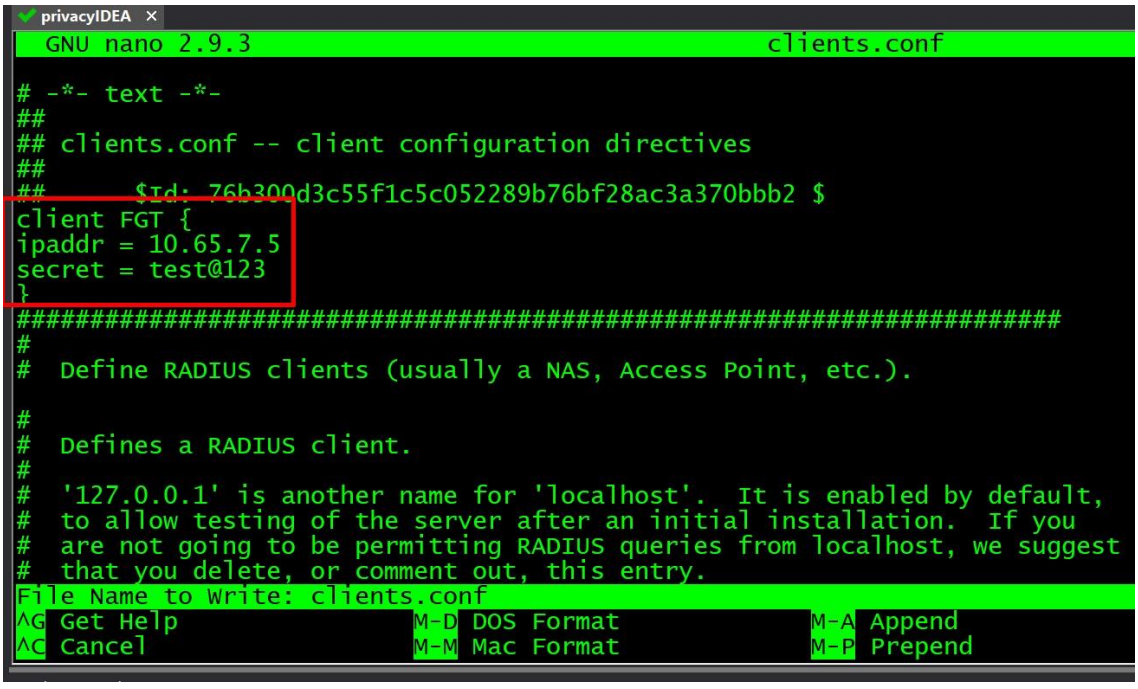

Рисунок 8 - Добавление RADIUS клиента

Как пример RADIUS клиента, мы взяли межсетевой экран нового поколение(NGFW) FortiGate, и рисунке 9, показан добавление RADIUS сервера FreeRADIUS в FortiGate. FortiGate может дальнейшем использовать этот RADIUS сервер в настройках Remote Access VPN или же в политиках и т.д.

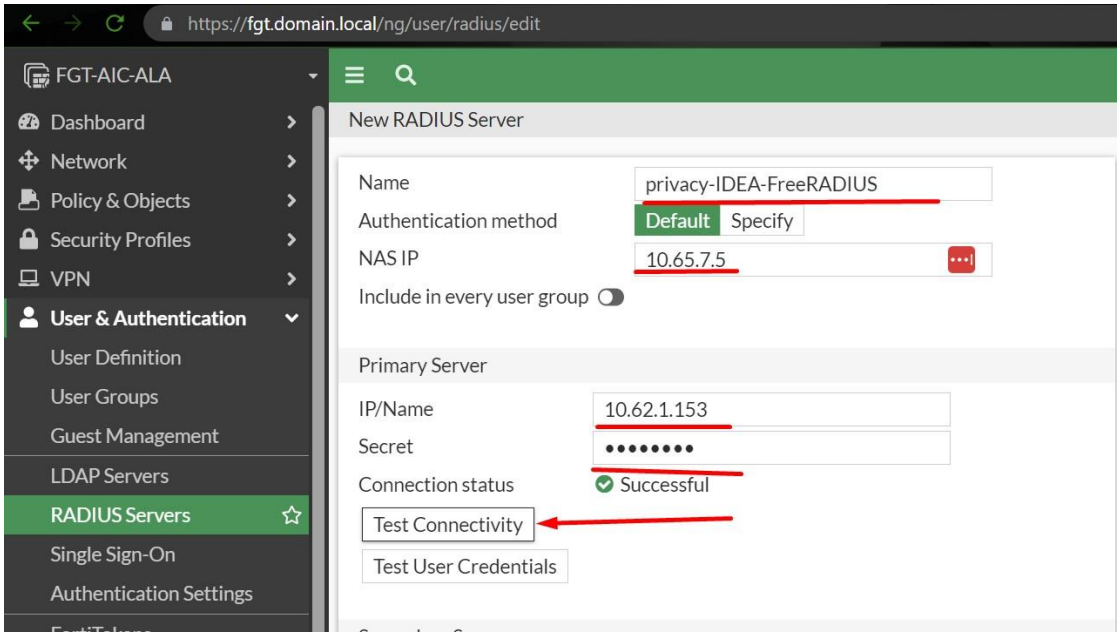

Рисунок 9 - Добавление RADIUS сервера

После добавление RADIUS сервера, можно используя разные встроенные утилиты, проверить связь между RADIUS сервером и клиентом. В рисунке 10, виден что статус связи установлен, а в нижнем поле показывает неправильные учетные данные. Он так показывает потому что, после первой аутентификации логин и пароль, наш RADIUS сервер спрашивает для этого пользователя второй фактор, потому что для этого пользователя уже настроен многофакторная аутентификация.

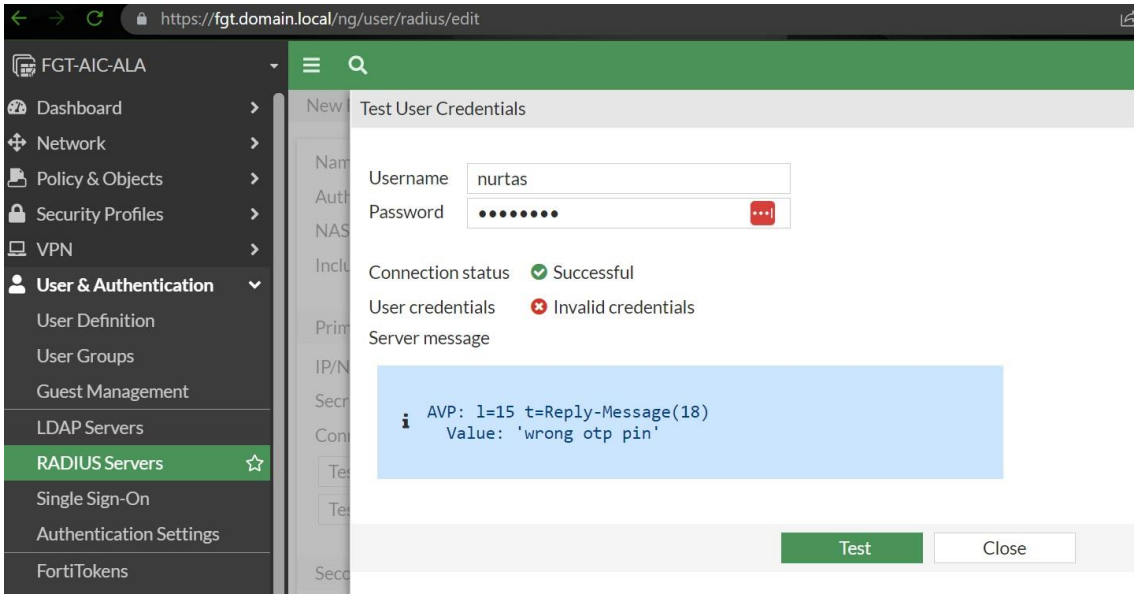

Рисунок 10 - Проверка связи с AAA сервер

Поэтому ответ неправильный OTP нормально, потому что, это графическая утилита полвольяет только отправить первый фактор логин и пароль.

Подведение итогов

Все упомянутые выше решения MFA с открытым исходным кодом являются наиболее популярными решениями MFA, доступными на рынке, и широко используются, а также популярны.

Список литературы

[1] Ussatova O., Nyssanbayeva S., Wojcik W. Development of an authentication model based on the second factor in an automated control system. Вестник КБТУ. Алматы, 2019. 16. 115-118.
[2] Nyssanbayeva S., Wojcik W., Ussatova O. Algorithm for generating temporary password based on the two factor authentication model. Przegląd Elektrotechniczny. Polan, 2019. 5. 101-106.
[3] VPN vulerabilty and Risk Report, 2021. Holger Schulze.
[4] Ussatova O., Nyssanbayeva S., Wojcik W. Software implementation of two-factor authentication to ensure security when accessing an information system. Вестник КазНУ им. аль-Фараби. Алматы, 2019. 87-95.
[5] Ussatova O., Nyssanbayeva S. Generators of one-time two-factor authentication passwords. Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. Poland, 2019. 2. 60-64.
[6] Усатова О.А., Нысанбаева С. Е. Обеспечение защиты информационной системы с помощью двухфакторной аутентификации. Сборник науч.конф. «Современные проблемы информатики и вычислительных технологий». Алматы, 2019. 337-343.
[7] Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication [Text] / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon. Computers & Security. 2017. 65. 14–28. DOI: 10.1016/j.cose.2016.09.009
[8] Harini, N. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code [Text] / N. Harini, T. R. Padmanabhan. International Journal of Engineering and Technology. 2013. 5(2). 1087–1094.
[9] D'Mello, D. P. An Alternative Approach in Generation and Possession of Backup Codes in MultiFactor Authentication Scheme [Text] / D. P. D'Mello // BIJIT - BVICAM's International Journal of Information Technology. 2015. 7(2). 883–885.

References

[1] Ussatova O., Nyssanbayeva S., Wojcik W. Development of an authentication model based on the second factor in an automated control system. Vestnik KBTU. Almaty, 2019. 16. 115-118.
[2] Nyssanbayeva S., Wojcik W., Ussatova O. Algorithm for generating temporary password based on the two factor authentication model. Przegląd Elektrotechniczny. Polan, 2019. 5. 101-106.
[3] VPN vulerabilty and Risk Report, 2021. Holger Schulze.
[4] Ussatova O., Nyssanbayeva S., Wojcik W. Software implementation of two-factor authentication to ensure security when accessing an information system. Vestnik KazNU im. al'-Farabi. Almaty, 2019. 87-95.
[5] Ussatova O., Nyssanbayeva S. Generators of one-time two-factor authentication passwords. Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. Poland, 2019. 2. 60-64.
[6] Usatova O.A., Nysanbayeva C. E. Obespecheniye zashchity informatsionnoy sistemy s pomoshch'yu dvukhfaktornoy autentifikatsii. Sbornik nauch.konf. «Sovremennyye problemy informatiki i vychislitel'nykh tekhnologiy». Almaty, 2019. 337-343.
[7] Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication [Text] / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon. Computers & Security. 2017. 65. 14–28. DOI: 10.1016/j.cose.2016.09.009
[8] Harini, N. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code [Text] / N. Harini, T. R. Padmanabhan. International Journal of Engineering and Technology. 2013. 5(2). 1087–1094.
[9] D'Mello, D. P. An Alternative Approach in Generation and Possession of Backup Codes in MultiFactor Authentication Scheme [Text] / D. P. D'Mello // BIJIT - BVICAM's International Journal of Information Technology. 2015. 7(2). 883–885.