УДК 004.7

Малініч П. П.
Малініч І. П.
Томчук М. А.

РЕАЛІЗАЦІЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ VPN-ТЕХНОЛОГІЇ CISCO ANYCONNECT З ВИКОРИСТАННЯМ ПРОТОКОЛУ RADIUS

Вінницький національний технічний університет

Анотація
Розглянуто основні можливості мережевого протоколу RADIUS та існуючого програмного забезпечення для налаштування двофакторної автентифікації на VPN-технології Cisco AnyConnect. Проведено аналіз можливостей бібліотек мови програмування Python для створення власної підтримки двофакторної аутентифікації для протоколу RADIUS за допомогою таких популярних додатків як Google Authenticator та Microsoft Authenticator.

Ключові слова: комп'ютерні мережі, двофакторна аутентифікація, 2FA, MFA, VPN, RADIUS

Abstract
The main capabilities of the RADIUS network protocol and existing software for setting up two-factor authentication on Cisco AnyConnect VPN technology are reviewed. An analysis of the capabilities of the Python programming language libraries for creating own support for two-factor authentication for the RADIUS protocol using such popular applications as Google Authenticator and Microsoft Authenticator was figured out.

Keywords: computer networks, two-factor authentication, 2FA, MFA, VPN, RADIUS

Вступ

Двофакторна аутентифікація (2FA) є підвидом мультифакторної автентифікації (MFA) - це процес перевірки ідентифікації користувача за допомогою двох незалежних методів аутентифікації. У онлайн-сервісах традиційно виконувалась перевірка за логіном та паролем. Двофакторна аутентифікація надає додатковий шар захисту, оскільки для успішної аутентифікації зловмиснику потрібно мати не лише пароль користувача, але й фізичний доступ до мобільного телефону користувача. Технічно це досить важко реалізувати, тому цей підхід можна вважати дієвим. MFA на даний момент є необхідним рішенням для елементарної IT-безпеки користувача [1]. Існує багато різних методів для реалізації двофакторної автентифікації, таких як SMS-повідомлення, спеціальні мобільні додатки (наприклад, Google Authenticator, Microsoft Authenticator чи інші) або апаратні ключі [1]. Користувачі зазвичай можуть самостійно вибрати метод, який їм найбільше підходить з точки зору зручності та доступності. Деякі сервіси пропонують проходити двофакторну авторизацію лише за певних обставин. Наприклад, двофакторна аутентифікація може відбуватись лише при спробі входу з нового пристрою або з нової локації, забезпечуючи додаткову безпеку у випадку підозрілих дій.

Більш сучасний підхід до мобільних телефонів полягає у використанні програми для створення коду. Google Authenticator є поширеним разом із комерційними інструментами постачальників MFA, такими як Okta. Обидві ці служби використовують протокол TOTP (одноразові паролі на основі часу) і HOTP (одноразові паролі на основі HMAC) [2]. Вони детально описані в RFC 6238 [3] і RFC 4226 [4] відповідно.

Протокол RADIUS (Remote Authentication Dial-In User Service) був розроблений Livingston Enterprises, Inc. як протокол автентифікації сервера доступу та обліку. RADIUS дозволяє централізовано аутентифікувати користувачів із різних мережевих пристроїв (наприклад, маршрутизаторів, комутаторів, VPN-серверів тощо) [5]. Це спрощує управління автентифікацією і поліпшує безпеку, оскільки не потрібно налаштовувати окремі облікові записи на кожному пристрої. RADIUS також дозволяє використовувати політики авторизації для керування рівнем доступу користувачів до ресурсів мережі. Розширені можливості аутентифікації RADIUS передбачають автентифікацію за паролем, токеном OTP (одноразові паролі), а також за допомогою сертифікатів.

Можливості протоколу RADIUS для мультифакторної авторизації

Протокол RADIUS передбачає винесення процесу авторизації на окремий AAA-сервер, що значно ускладнює доступ до облікових даних користувача (такі як логін та пароль) при компрометації VPN-серверу [6]. Різні реалізації AAA-серверів RADIUS мають підтримку зовнішніх баз даних. Протокол RADIUS має чудову підтримку MFA, яка передбачена у його специфікації [5] (рис. 1).

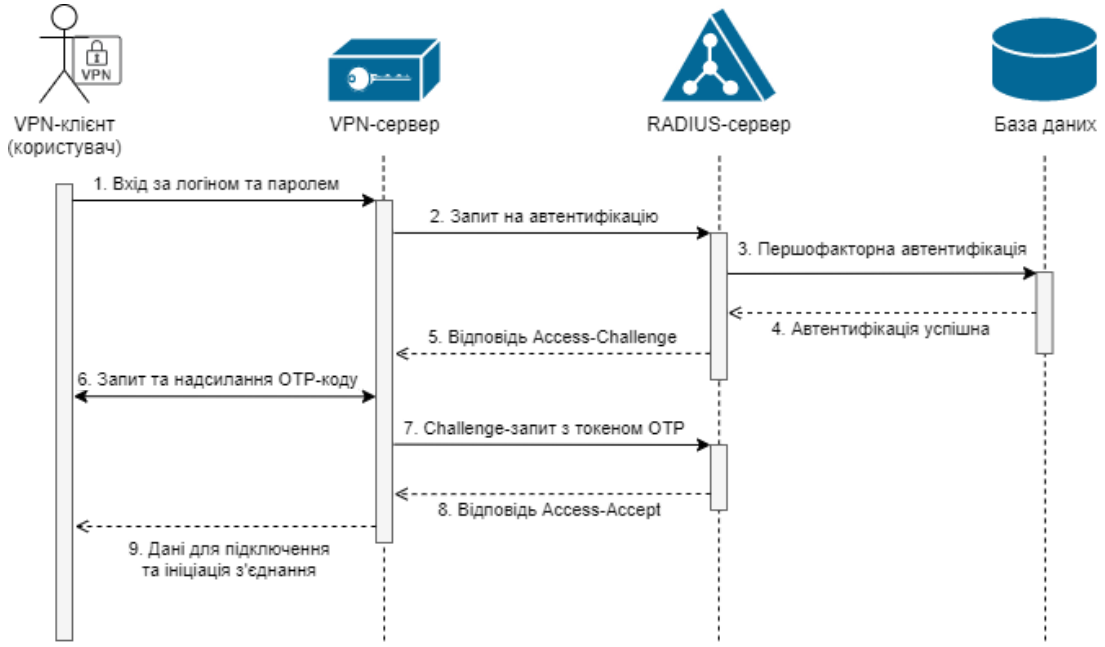

Рисунок 1 - Діаграма встановлення з’єднання з використанням MFA на базі RADIUS

Розглянуто можливості найбільш популярного OpenSource-серверу для даного протоколу - FreeRADIUS [7]. Схоже що у даного продукту немає підтримки найбільш популярних для користувачів мобільних додатків для генерації TOTP, таких як Google Authenticator чи Microsoft Authenticator. Тому розглянуто можливість створити власну реалізацію підтримки даних додатків за допомогою бібліотеки Python pyrad [8], яка має підтримку Access-Challenge у режимі серверу, а також використовуючи бібліотеку pyotp [9], що має підтирмку мобільних автентифікаторів. Таким чином усувається необхідність у використанні середовища аутентифікації PAM [10] операційної системи як додаткового прошарку для підключення цієї бібліотеки.

Налаштування серверу Cisco AnyConnect на базі мережевого екрану Cisco ASA для використання двофакторної автентифікації

Існує дві основні реалізації серверу Cisco Anyconnect: VPN-сервер шлюзу Cisco ASA та Open Source-сервер OpenConnect, який є повністю сумісним з технологією Cisco Anyconnect. Підтримка протоколу RADIUS у сервері OpenConnect реалізована за допомогою сторонніх бібліотек.

Налаштовується підтримка RADIUS на офіційній реалізації серверу Cisco Anyconnect (на базі мережевого екрану Cisco ASA) за допомогою групових політик, які встановлюють порядок автентифікації. Для підтримки двофакторної аутентифікації не потрібно окремих налаштувань на стороні серверу, достатньо типових налаштувань для настройки AAA-серверу (рис. 2).

```
aaa-server AAA_GROUP protocol RADIUS
 aaa-server AAA_GROUP host 10.10.10.10
!
tunnel-group VPN_GROUP type remote-access
!
group-policy POL_GROUP attributes
 authentication-server-group AAA_GROUP
 tunnel-group VPN_GROUP webvpn-attributes
!
```

Рисунок 2 - Приклад конфігурації з’єднання з RADIUS-сервером на платформі Cisco ASA

Сервер OpenConnect також підтримку протоколу RADIUS за допомогою бібліотек libradius-client чи radcli [11]. Конфігурація на альтернативному сервері OpenConnect є можливою, однак конфігурація підключення до RADIUS виненеса у окремий файл [12]. Перевагами даної реалізації є незалежність від середовища аутентифікації користувачів PAM, яка використовується у UNIX-подібних ОС для автентифікації системних користувачів. Це зменшує поверхню можливої хакерської атаки, оскільки PAM не прийматиме участі у автентифікації.

Висновки

Розглянуто як працює підхід двофакторної аутентифікації у VPN-технології Cisco AnyConnect, а також шляхи її налаштування. Визначено протокол RADIUS, як найбільш універсальний та зручний спосіб підключення двофакторної аутентифікації у VPN-з’єднаннях.

Попри те, що існують досить потужні реалізації серверів RADIUS, таких як FreeRADIUS, їх власних можливостей недостатньо реалізації двофакторної аутентифікації за допомогою популярних мобільних додатків. Саме тому проведено аналіз можливостей бібліотек мови програмування Python для підтримки протоколу RADIUS та таких популярних додатків двофакторної аутентифікації як Google Authenticator та Microsoft Authenticator.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке двофакторна автентифікація, і як вона працює? [Електронний ресурс]. Державна служба спеціального зв'язку та захисту інформації України. URL: https://amazic.com/how-ai-platforms-such-as-gpt-change-the-devsecops-game/ (дата звернення: 11.06.2023).
2. Multi-Factor Authentication with OpenVPN | Community Edition [Електронний ресурс]. URL: https://openvpn.net/blog/multi-factor-authentication-with-openvpn-community-edition/ (дата звернення: 11.06.2023).
3. M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). Totp: Time-based one-time password algorithm (No. rfc6238).
4. M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). Hotp: An hmac-based one-time password algorithm (No. rfc4226).
5. Understanding RADIUS - Cisco [Електронний ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/net_mgmt/access_registrar/1-7/concepts/guide/radius.html
6. Малініч П. П. Негативні безпекові чинники у локальних Ethernet-мережах та абонентських мереж останньої милі [Електронний ресурс] / П. П. Малініч, І. П. Малініч, О. О. Коваленко // Матеріали LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022). – Вінниця, 31 травня 2022 р. – Електрон. текст. дані. – 2022. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15614.
7. FreeRADIUS Technical Guide (PDF) [Електронний ресурс]. URL: https://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf (дата звернення: 11.06.2023).
8. Initial eap-md5 implementation [Електронний ресурс]. URL: https://github.com/pyradius/pyrad/pull/42 (дата звернення: 11.06.2023).
9. PyOTP - The Python One-Time Password Library [Електронний ресурс]. URL: https://pyauth.github.io/pyotp/ (дата звернення: 11.06.2023).
10. Enable 2FA on FreeRADIUS with OpenLDAP Users [Електронний ресурс]. URL: https://sysopstechnix.com/enable-2fa-on-freeradius-with-openldap-users/ (дата звернення: 11.06.2023).
11. OpenConnect VPN projects repository: /ocserv/src/auth/radius.c [Електронний ресурс]. URL: https://gitlab.com/openconnect/ocserv/-/blob/master/src/auth/radius.c
12. Mauro Gaspari. Ocserv Authentication - RADIUS (radcli) [Електронний ресурс]. URL: https://ocserv.gitlab.io/www/recipes-ocserv-authentication-radius-radcli.html

Малініч Павло Павлович — студент групи 1ПІ-22м, факультет Інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, e-mail: pavlo.malinich@vntu.edu.ua

Малініч Ілля Павлович — асистент кафедри Комп’ютерних наук, Вінницький національний технічний університет

Томчук Микола Антонович — канд. техн. наук, доцент кафедри Обчислювальної техніки, Вінницький національний технічний університет