УДК 004.056.52:621.311
DOI: 10.31673/2409-7292.2024.040011

Шулімова Д. Д., Бойко А. О., Постніков Є. І., Войтишин А. Д., Коновал Р. М.

АЛЬТЕРНАТИВНІ СПОСОБИ БЕЗПЕЧНОГО ОТРИМАННЯ РЕЗУЛЬТАТІВ ВИМІРЮВАНЬ З ЕЛЕКТРОПІДСТАНЦІЙ

У цій статті описано проблему забезпечення безпечного доступу до вимірювального обладнання підстанцій через відкриті мережі, зокрема у випадках, коли основний канал зв’язку пошкоджено. З огляду на зростаючу цифровізацію енергетичних мереж та збільшення залежності від віддаленого моніторингу, ключовим аспектом є забезпечення захищеності переданих даних та безперебійності функціонування енергетичної інфраструктури. У статті детально розглянуто кілька підходів для забезпечення безпечного доступу. Основний акцент зроблено на використанні протоколу IEC 60870-5-101, який є стандартом для передачі даних між енергетичними об’єктами та системами управління. Протокол забезпечує сумісність різноманітного обладнання, що критично важливо для підтримки стабільної роботи підстанцій. Для підвищення безпеки пропонуються рішення, які включають використання VPN-з'єднань для створення захищених каналів передачі даних, сегментацію мережі та розділення VLAN для ізоляції трафіку критично важливих компонентів, а також багаторівневі заходи безпеки, що передбачають поєднання технічних і організаційних засобів захисту. Зокрема, у статті описуються методи впровадження міжмережевих екранів, систем виявлення вторгнень, шифрування даних і управління доступом. Стаття наголошує на важливості багатофакторного підходу до захисту від різних типів загроз, включаючи фізичний доступ, мережевий трафік і атаки на мікропрограми. Застосування такого підходу дозволяє комплексно вирішувати завдання забезпечення безпеки енергетичної інфраструктури та підтримувати надійну роботу обладнання в умовах підвищеного ризику.

Ключові слова: кібербезпека**,** енергетична безпека, VPN-сервер, CA, VLAN, Apache Kafka, RS232, SCADA, Firewall, критична інфраструктура, MFA, DMZ, IEC-60870-5-101.

Вступ

Система передачі є важливою частиною інфраструктури, і від її стабільної роботи залежить Національна енергетична безпека. Технічна комунікаційна мережа вимірювального обладнання підстанції фізично ізольована від Інтернету і використовує оптоволоконну мережу для передачі даних в центральну систему диспетчеризації та обліку. Однак при пошкодженні цієї наземної мережі зв'язок може бути втрачений, особливо під час атаки на підстанцію, що обмежить доступ диспетчера до поточних вимірювань, що може призвести до серйозних наслідків.

У середовищах з високим рівнем ризику слід використовувати відкриту мережу, щоб забезпечити доступ до обладнання станції без шкоди для безпеки. Це завдання вимагає міждоменного підходу, що забезпечує безпечну передачу даних і захист від несанкціонованого доступу. У цьому Технічному документі описані можливі технічні рішення для забезпечення безпечного доступу до вимірювального обладнання по відкритій мережі і способи застосування протоколу IEC 60870-5-101 для забезпечення двонаправленого обміну даними, що були скомпоновані та знайдені шляхом використання методу HACCP, який може включати розробку схеми, яка допоможе в ідентифікації критичних точок у IT-інфраструктурі, де потенційні ризики або вразливості можуть негативно вплинути на оперативну діяльність організації, а також методу SWIFT, який є ефективним інструментом аналізу, призначеним для ідентифікації потенційних ризиків у системах або процесах шляхом структурованого обговорення сценаріїв “що, якщо” та дозволяє оцінити можливі наслідки різних відхилень у роботі системи, виявляючи таким чином потенційні уразливості і вектори атак, що ще не були розглянуті[1].

Постановка проблеми

Розробка технічних рішень для автоматизації доступу диспетчерів до станційного обладнання та проведення вимірювань з його допомогою повинна відповідати певним вимогам безпеки. Зокрема, необхідно забезпечити захист від несанкціонованого доступу до даних, що зчитуються і унеможливити доступ до обладнання зовні. Технічна мережа зв’язку на підстанції оператора системи передачі фізично розділена і побудована на основі волоконно-

оптичного зв’язку, відокремленої від інтернету. У даній статті ми розглянемо можливі підходи до забезпечення безпечного доступу диспетчера до даних без ризику порушення цілісності системи та її елементів.

Опис роботи рішення

1. Початковий запит на доступ для з’єднання

Користувач на валідному пристрої робить запит на підключення до веб-сервера підстанції через корпоративну мережу. Його запит спершу скеровується на VPN-сервер для ініціалізації з’єднання. Топологія мережі також передбчає використання політики BYOD [2] для створення з’єднання у разі, якщо пристрій має ключ та файл для VPN-з’єднання.

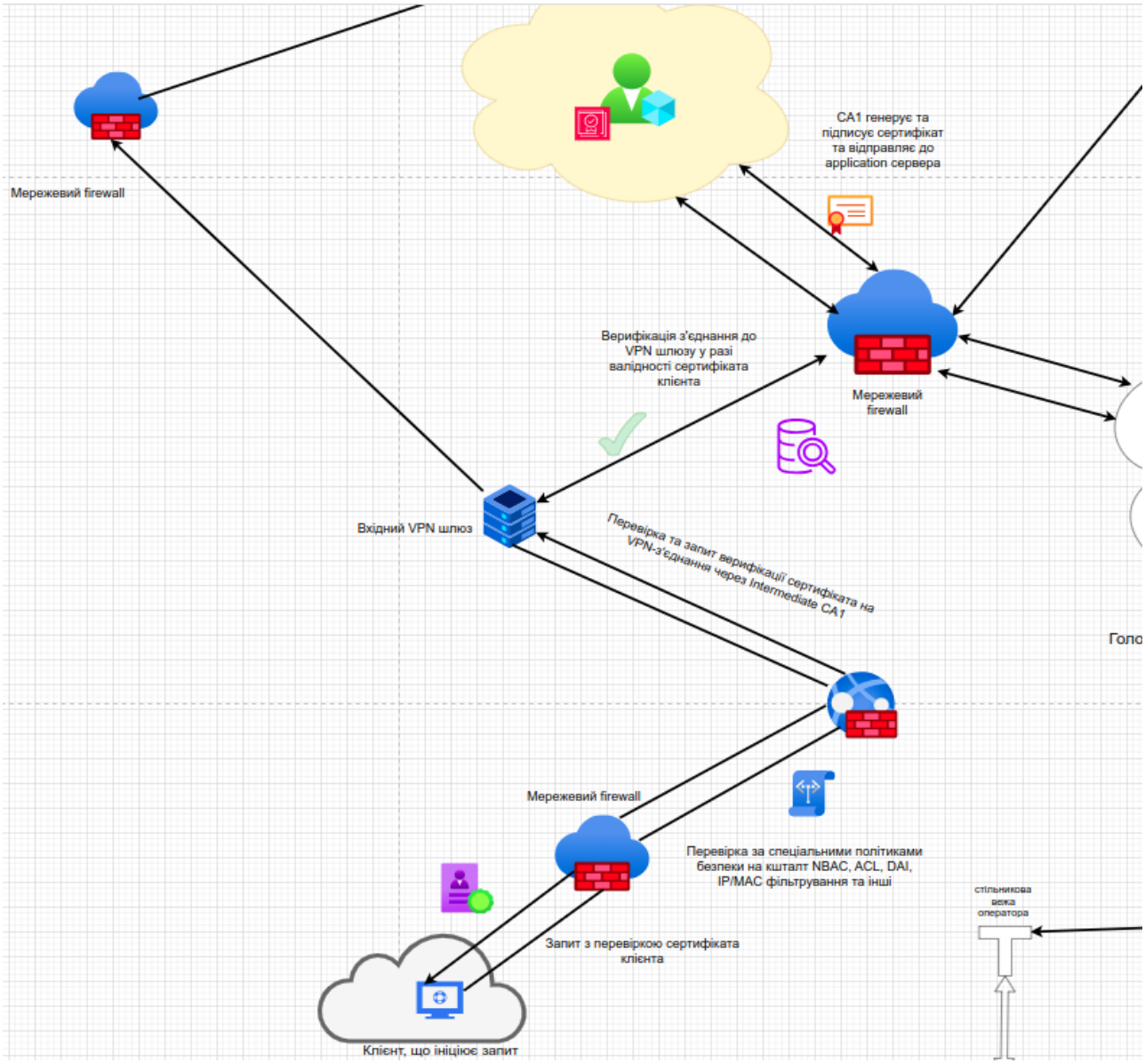

Рис. 1. Ініціалізація VPN-з’єднання

2. Перевірка доступу в корпоративній мережі

Запит проходить через корпоративний firewall та механізм Network-Based Access Control [3], де перевіряється, чи цей пристрій має дозвіл на доступ до ресурсів підстанції на основі політик безпеки на наявність відповідної пари зареєстрованих IP та MAC адрес, політик перевірки мережевого доступу, динамічного сканування ARP-пакетів тощо, з метою перевірки

© Шулімова, Д. Д., Бойко, А. О., Постніков, Є. І., Войтишин, А. Д., & Коновал, Р. М. (2024). Альтернативні способи безпечного отримання результатів вимірювань з електропідстанцій. Сучасний захист інформації, 4(60), 109–116. https://doi.org/10.31673/2409-7292.2024.040011.

чи користувач, навіть якщо має дійсний сертифікат на з'єднання, виконує запит з дозволеного місця та мережі, тобто з диспетчерської чи іншого пункту з довіреними та безпечними мережами(якщо є перелік таких).

У разі успішного проходження першого, запит скеровується на перевірку на наступний firewall, де проходить перевірку сертифікату VPN-з'єднання та у разі успішної перевірки спрямовує до DMZ-зони [4].

3. Перевірка сертифікатів

Сервер VLAN перевіряє сертифікат користувача або пристрою для підтвердження його автентичності. Це може включати перевірку терміну дії сертифіката, підпису, а також політик доступу, встановлених для цього користувача або пристрою.

Якщо сертифікат валідний, сервер VLAN дозволяє підключення до VLAN підстанції.

4. Підключення до VLAN підстанції

Після проходження перевірки сертифікату, користувач отримує доступ до ресурсів, розташованих у VLAN підстанції, наприклад, до веб-сервера підстанції [5].

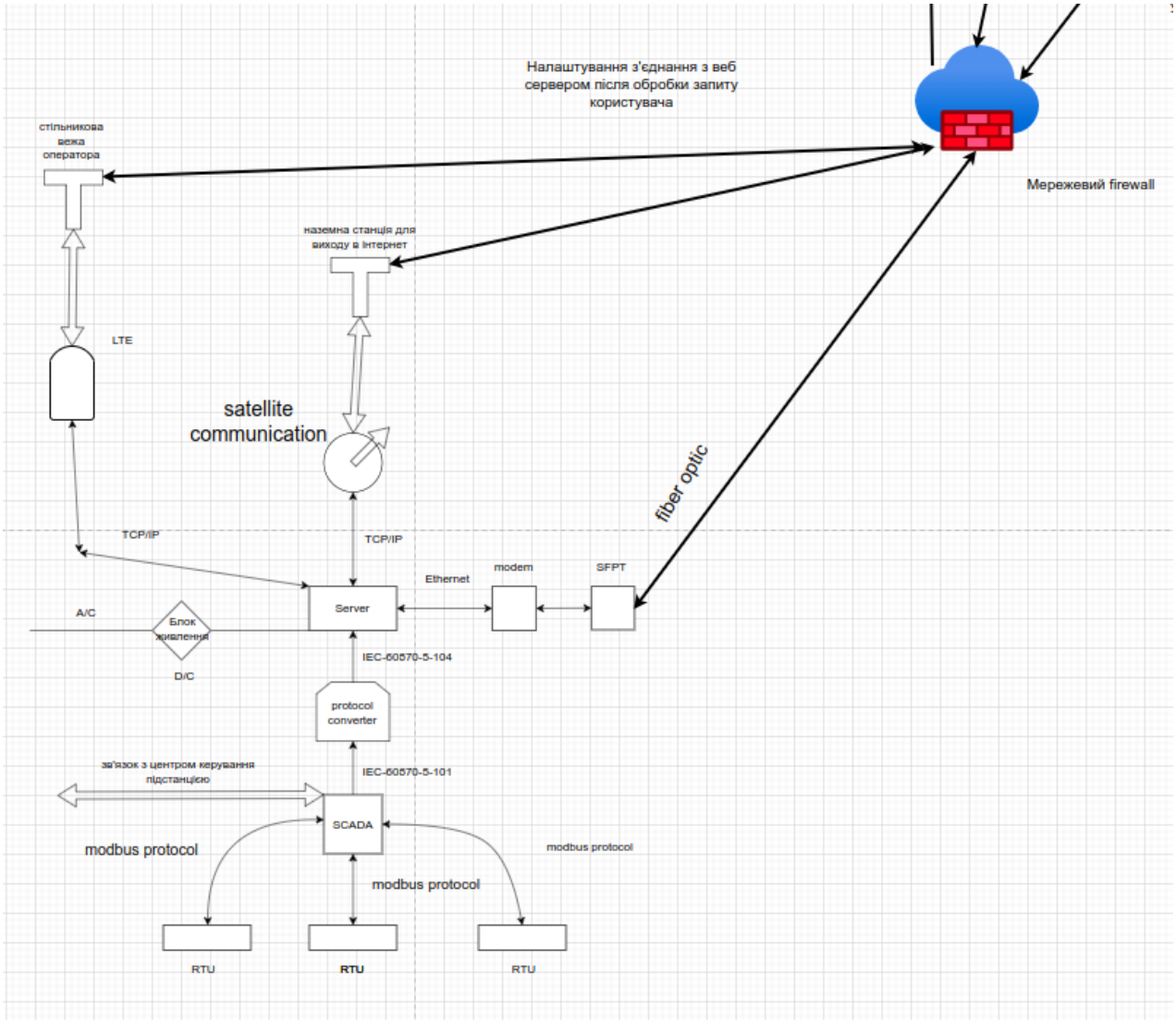

Рис 2. SCADA-система

5. Взаємодія з веб-сервером підстанції відбувається наступним чином.

Під'єднаний клієнь починає взаємодію з веб-сервером на підстанції, запитуючи необхідні дані або інформацію про необхідні метрики. Всі дані, що передаються між корпоративною мережею та VLAN підстанції, можуть бути шифровані для забезпечення додаткового рівня безпеки.

6. Моніторинг та аудит.

Всі дії виконувані клієнтом можуть бути журналізовані збережені для перевірки на відповідність політикам безпеки наприклад у базі даних VLAN мережі для забезпечення прозорості та виявлення можливих загроз.

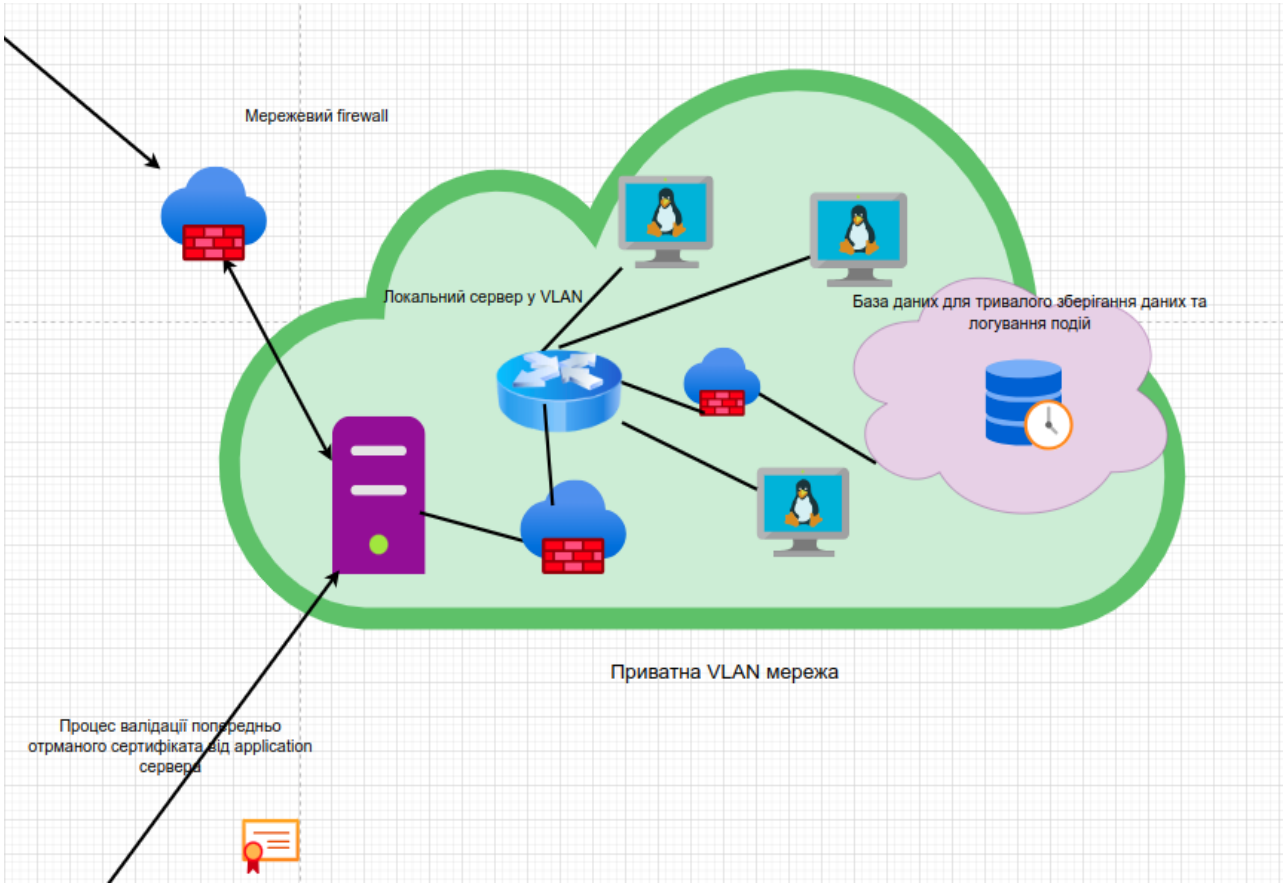

Рис. 3 Схематика моделі VLAN мережі

Серед додаткових аспектів варто виокремити, що VLAN мережа використовується для ізоляції трафіку підстанції від решти корпоративної мережі, що мінімізує ризик компрометації.

Додаткові заходи безпеки, такі як обмеження на виконання команд на серверній стороні, що можуть бути передані на підстанцію, та фільтрація трафіку, забезпечують, що навіть у разі несанкціонованого доступу, критичні частини системи будуть захищені.

Сфера застосування

Приклад застосування рішення

1) Віддалений моніторинг підстанцій в надзвичайних ситуаціях.

Якщо основна мережа пошкоджена внаслідок стихійних лих або військових дій, міждоменне рішення дозволяє диспетчеру отримувати важливі дані з підстанції через альтернативні канали. Це допомагає своєчасно виявляти збої, підтримувати безперервність мережі та швидко реагувати на надзвичайні ситуації.

2) Інтеграція мобільних станцій з тимчасовими об'єктами.

Коли необхідно використовувати мобільні підстанції та тимчасове обладнання, таке як мобільні генератори та аварійні Трансформатори, потужні міждоменні рішення, які можуть забезпечувати зв'язок по відкритій мережі, дозволяють підключати ці об'єкти до центральних систем моніторингу та управління без ризику для безпеки.

3) Забезпечення резервної зв'язку для промислових об'єктів.

Для великих компаній, що використовують енергетичну інфраструктуру, резервний доступ до вимірювального обладнання з використанням відкритої мережі може мати вирішальне значення для моніторингу енергоспоживання і швидкого відновлення аварійних операцій.

4) Розширений моніторинг та аналіз в міських електромережах.

У міських електромережах, де можливі перебої в роботі через високі навантажень і аварій, це рішення дозволяє здійснювати віддалений моніторинг обладнання навіть в умовах виходу з ладу основних мереж зв'язку. Дане рішення дозволяє своєчасно приймати рішення про перерозподіл навантажень і уникати відключень.

5) Підтримка "розумних" мереж (Smart Grid) [6].

Міждоменні рішення можуть застосовуватися для підключення вимірювальних приладів в інтелектуальних мережах, де для швидкої оцінки стану мережі може знадобитися віддалений доступ до підстанцій та інших об'єктів. Відкрита мережа забезпечує інтеграцію даних у режимі реального часу та оптимізує управління розподілом енергії [7].

Ці приклади ілюструють широкі можливості міждоменних рішень, які забезпечують надійний і безпечний доступ до критично важливих даних навіть в ситуаціях, коли основні комунікації порушені.

Вектори атак на концепт

У нашій концепції передачі даних можна виділити кілька основних ризиків та вразливостей [8], які потребують уваги спеціалістів [9].

Фізичний доступ до обладнання є однією з важливих загроз. Неавторизований доступ до серверів чи іншого обладнання може призвести до маніпуляцій або перехоплення даних. Наприклад, відсутність замків у серверних кімнатах, неналежний контроль доступу чи залишені без нагляду портативні пристрої створюють значні ризики. До того ж соціальна інженерія може стати способом, за допомогою якого зловмисники отримують доступ, видаючи себе за авторизованих осіб. Захист включає фізичне обмеження доступу, охорону серверів і регулярний аудит безпеки.

Ще однією загрозою є атаки на рівні прошивки [10]. Зловмисники можуть модифікувати прошивку серверів або мережевого обладнання для перехоплення даних чи впровадження шкідливого коду. Наприклад, програмні закладки (backdoor) [11] у BIOS чи UEFI дозволяють створити прихований доступ до системи. Також небезпеку становлять атаки через підроблені оновлення прошивки. Захистом може стати використання цифрових підписів та верифікація прошивки.

Мережевий трафік є ще однією точкою атаки. Тут можливі перехоплення чи модифікації даних через такі методи, як атаки "людина посередині" (MITM), ARP spoofing чи sniffing. Крім того, DDoS-атаки можуть виводити сервери з ладу. Для захисту рекомендується використовувати VPN, TLS або інші протоколи шифрування.

Ризик несанкціонованого доступу також залишається актуальним. Відсутність багатофакторної автентифікації, відкриті мережеві порти, надмірні привілеї користувачів або застаріле програмне забезпечення створюють можливості для проникнення. Захист передбачає впровадження строгих механізмів автентифікації та авторизації, зокрема багатофакторну автентифікацію.

На рівні додатків можливі вразливості, які дозволяють зловмисникам експлуатувати недоліки програмного забезпечення. Наприклад, Remote File Inclusion, неправильна

© Шулімова, Д. Д., Бойко, А. О., Постніков, Є. І., Войтишин, А. Д., & Коновал, Р. М. (2024). Альтернативні способи безпечного отримання результатів вимірювань з електропідстанцій. Сучасний захист інформації, 4(60), 109–116. https://doi.org/10.31673/2409-7292.2024.040011.

десеріалізація чи компрометація API можуть дати доступ до системи. Для запобігання необхідно регулярно оновлювати програми та проводити тестування на проникнення.

Ізоляція даних також потребує уваги. Змішування даних із різних джерел без належного розмежування доступу може призвести до витоків. Наприклад, неправильно налаштована сегментація мережі дозволяє отримати доступ до критичних даних через менш захищені ділянки. Використання VLAN чи інших технологій для ізоляції допоможе уникнути таких проблем.

Проблеми з передачею даних можуть виникати через втрати зв'язку або відсутність шифрування. Це відкриває можливості для перехоплення трафіку, підміни даних або впровадження шкідливих пакетів. Для забезпечення надійності потрібно використовувати механізми повторної передачі, цифрові підписи та хешування.

Нарешті, недостатній моніторинг і журналювання подій ускладнює виявлення та реагування на загрози. Впровадження систем моніторингу та автоматичних сповіщень дозволить оперативно виявляти потенційні загрози

Використані технології

1) VPN-з'єднання через VPN-сервер та VPN-клієнт з сертифікатом на з'єднання для підключення до сегменту буферної(DMZ) зони.

2) Буферна(DMZ) зона для верифікації з Application сервером для створення запитів на валідацію сертифікату клієнта при запиті на підключення(перехід) до іншого VLAN сегменту.

3) Три Акредитованих центри сертифіка́ції ключів (АЦСК)/ Certificate Authority(CA), один центральний та два проміжних, для верифікації з'єднань та перевірки сертифікатів/ключів, що надаються клієнтом при переходах між різними сегментами мереж [12].

4) Сегментована корпоративна VLAN мережа диспетчерської з БД для логування та створення тимчасових бекапів переданих даних з підстанції.

5) Сервер на основі Raspberry PI та конвертер протоколів MGate, що підключені до станційного обладнання для збору та передачі інформації та конвертують дані з порту RS232/485 з IEC 60870-5-101[13] у IEC 60870-5-104/Ethernet.

6) LTE, фізичне оптоволоконне з'єднання та супутникове з'єднання (Starlink) як альтернативні способи/канали збору інформації.

7) Фаєрволи/брандмауери розташовані вздовж усього периметру підключення для контролю прохідних вузлів між сегментами та всередині сегментів.

8) Серверне ПЗ у вигляді Ubuntu Server [14] (для підтримки концентрації інформації та її передачі) та диспетчерське ПЗ Apache Kafka (для приймання та конвертації отриманих даних).

Apache Kafka – це розподілена потокова платформа подій із відкритим кодом, яка використовується тисячами компаній для високопродуктивних конвеєрів даних, потокової аналітики, інтеграції даних і критично важливих програм [15]. Перед розповіддю про можливості та компоненти Kafka, треба дізнатися, що таке кластер. Кластер - група однакових або подібних елементів, зібраних разом.

Основні компоненти Kafka:

Producers – це процеси, які надсилають дані до Kafka. Кожне повідомлення у темі має унікальний ідентифікатор або offset, що дозволяє відстежувати порядок і забезпечувати доступність даних для споживачів.

Topics – це частини даних, де зберігаються повідомлення. Теми діляться на розділи, що дозволяє зберігати повідомлення у вигляді логів. Кожне повідомлення записується в один з розділів теми та отримує унікальний зсув у рамках цього розділу.

Brokers – це вузли, які керують даними, що надходять до Kafka та зберігають їх. Кілька брокерів можуть бути об'єднані в кластер, що підвищує надійність і масштабованість системи.

Consumers – це процеси, які отримують дані з Kafka. Також споживачі можуть об'єднуватися в групи, що дозволяє рівномірно розподіляти обробку повідомлень між споживачами.

Zookeeper – це сервіс для керування кластером, що відповідає за координацію брокерів, керування конфігураціями і відстеження стану кластеру.

Apache Kafka надає можливості обробляти великі обсяги даних та події у реальному часі. Завдяки своїй архітектурі, Kafka може обробляти дані навіть якщо деякі кластери відмовлять, що підтверджує її надійність та стійкість. Kafka дозволяє додавати більше брокерів до кластеру, щоб розподілити навантаження на обробку даних, що забезпечує лінійне масштабування. Також Kafka може зберігати повідомлення протягом певного періоду часу, що дозволяє користувачам відтворювати їх у будь-який момент [16].

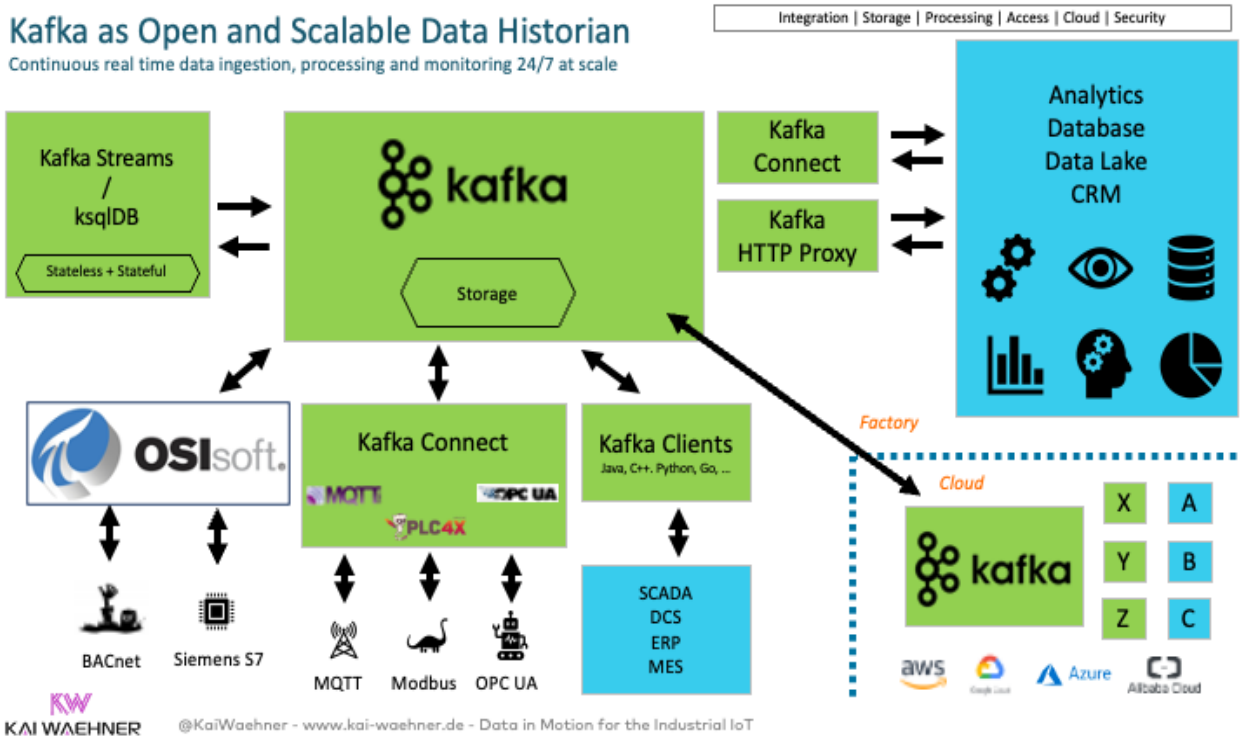

Рис. 4. Схематичний опис видів застосування програмного забезпечення Apache Kafka

Висновок

Аналіз можливостей безпечного доступу до даних підстанції в разі пошкодження основного каналу мережі показав, що багаторівневе міждоменне рішення є ефективним для підтримки стабільності енергетичної інфраструктури: шляхом інтеграції таких технологій, як VPN-з'єднання, VLAN, протоколи IEC 60870-5-101 та IEC 60870-5-104 можна інтегрувати для забезпечення безпечної та стабільної передачі даних. Високий рівень безпеки вимагає впровадження додаткових механізмів контролю, таких як багатофакторна автентифікація, міжмережеві екрани, моніторинг подій і обмеження фізичного доступу до обладнання; використання резервних каналів зв'язку, таких як LTE і супутниковий зв'язок, забезпечує доступ до критично важливих даних навіть в аварійних ситуаціях і гарантує, що проблеми будуть своєчасне виявлення проблем та підтримання стабільної роботи системи.

Перелік посилань

1. Шульга, В. П., Іванченко, Є. В., Вишневська, Н. С., & Бербер, А. С. (2024). Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави. Duikt.edu.ua. https://journals.duikt.edu.ua/index.php/dataprotect/article/view/3002/2902 (date of access 18.11.2024)

© Шулімова, Д. Д., Бойко, А. О., Постніков, Є. І., Войтишин, А. Д., & Коновал, Р. М. (2024). Альтернативні способи безпечного отримання результатів вимірювань з електропідстанцій. Сучасний захист інформації, 4(60), 109–116. https://doi.org/10.31673/2409-7292.2024.040011.

2. Скибун, О. Ж., Гайдур, Г. І., & Гахов, С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Dut.edu.ua. https://journals.dut.edu.ua/index.php/dataprotect/article/view/2910/2807 (date of acess 18.11.2024)

3. Fortinet. (2023). What Is Network Access Control (NAC) ? Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-network-access-control (date of access 12.11.2024)

4. What is a DMZ network and why would you use it? | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-dmz (date of access 12.11.2024)

5. Wali, A., & Alshehry, F. (2024). A Survey of Security Challenges in Cloud-Based SCADA Systems. Computers, 13(4), 97. https://doi.org/10.3390/computers13040097 (date of access 13.11.2024)

6. Ukrinform. (2024, May 14). Розбудова Smart Grid - шлях до підвищення стійкості енергосистеми України. Ukrinform.ua; Укрінформ. https://www.ukrinform.ua/rubric-economy/3863598-rozbudova-smart-grid-slah-do-pidvisenna-stijkosti-energosistemi-ukraini.html (date of access 12.11.2024)

7. Cybersecurity and the Smarter Grid URL: https://www.sciencedirect.com/science/article/pii/S1040619014001791

8. Хавер, А. В., & Савченко, В. А. (2024). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Dut.edu.ua. https://journals.dut.edu.ua/index.php/dataprotect/article/view/2786/2685 (date of access 18.11.2024)

9. Abdelkader, S., Amissah, J., Kinga, S., Geofrey Mugerwa, Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., & Prokop, L. (2024). Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks. Results in Engineering, 23(102647), 102647–102647. https://doi.org/10.1016/j.rineng.2024.102647 (date of access 14.11.2024)

10. Zerg. (2023, October 16). Частина 9. Злом апаратної частини системи. (Злом прошивки) - HackYourMom. HackYourMom. https://hackyourmom.com/osvita/chastyna-9-zlom-aparatnoyi-chastyny-systemyzlom-proshyvky/ (date of access 12.11.2024)

11. Бекдор - що це таке, принцип роботи бекдора і як його видалити. ESET. (2018). ESET. https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bekdor/?srsltid=AfmBOorijopA88kBnmvRzcnIHH9ZhZptvVcH3TdnAYwIW32F5MClYkrr (date of access 12.11.2024)

12. Panda Security. (2023, April 27). What Is a Root Certificate? - Panda Security. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/what-is-a-root-certificate/ (date of access 12.11.2024)

13. IEC 60870-5 Driver Guide - IEC 60870-5-101 (Configuring an IEC 60870-5 Channel). (2022). Schneider-Electric.com. https://tprojects.schneider-electric.com/GeoSCADAHelp/Geo%20SCADA%202022/Content/IEC608705DriverGuide/IEC608705101.htm (date of access 12.11.2024)

14. Introduction | Server documentation. (n.d.). Ubuntu. https://ubuntu.com/server/docs (date of access 12.11.2024)

15. Apache Kafka. (n.d.). Apache Kafka. https://kafka.apache.org/documentation/ (date of access 12.11.2024)

16. Waehner, K. (2022, October 4). A cloud-native SCADA System for Industrial IoT built with Apache Kafka - Kai Waehner. Kai Waehner. https://www.kai-waehner.de/blog/2022/10/04/cloud-native-scada-system-for-industrial-iot-with-apache-kafka/ (date of access 12.11.2024)

Надійшла 26.11.2024