SECTION 1. INFORMATION SYSTEMS AND TECHNOLOGIES

DOI https://doi.org/10.30525/978-9934-26-519-8-1

ORGANIZING REMOTE ACCESS TO THE OBJECT

ОРГАНІЗАЦІЯ ВІДДАЛЕНОГО ДОСТУПУ ДО ОБ'ЄКТУ

Kyrychek H. H.
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems and Networks National University «Zaporizhzhia Polytechnic» Zaporizhzhia, Ukraine

Киричек Г. Г.
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж Національний університет «Запорізька політехніка» м. Запоріжжя, Україна

Pestov O. D.
Student at the Faculty of Computer Sciences and Technologies National University «Zaporizhzhia Polytechnic» Zaporizhzhia, Ukraine

Пестов О. Д.
студент факультету комп'ютерних наук і технологій Національний університет «Запорізька політехніка» м. Запоріжжя, Україна

Tiahunova M. Yu.
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Computer Systems and Networks National University «Zaporizhzhia Polytechnic» Zaporizhzhia, Ukraine

Тягунова М. Ю.
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж Національний університет «Запорізька політехніка» м. Запоріжжя, Україна

На даний час, задача віддаленого доступу до стратегічно важливих об'єктів є дуже актуальною [1]. Її можна вирішити різними способами, при цьому більшість з них досить затратні [2, 3] Одним із таких способів є застосування виділених ліній зв'язку між об'єктом і віддаленим робочим місцем. Це досить надійне рішення, але воно вимагає значних фінансових і часових витрат, обмежує мобільність віддаленого оператора, який керує об'єктом та часто не є доступним, тому що не всі провайдери надають цю послугу. Метою роботи є

організація віддаленого доступу до об'єкту та реалізація моделі системи, що призначена для віддаленого керування об'єктами критичної інфраструктури, враховуючи різні умови виникнення надзвичайних ситуацій. Об'єктом дослідження є процес організації віддаленого доступу, застосовуючи накладену peer-to-peer мережу Yggdrasil. Предметом є моделі, методи і інструментальні засоби забезпечення керування віддаленими об'єктами.

Маємо, що для забезпечення мобільності віддалених операторів, ідеальним варіантом є доступ до об'єкту через Інтернет, але реалізація такого доступу потребує деяких зусиль [2] Навіть, якщо віддалений об'єкт вже має вихід у глобальну мережу, скоріше за все він знаходиться за пристроєм, який підтримує технологію NAT (Network Address Translation) відповідного провайдера [4]. Таким чином, пристрій з приватною локальною адресою, створює вихідні з'єднання з кінцевими пристроями у глобальній мережі, але пряме зворотне з'єднання для нього неможливе, бо він не має унікальної глобальної адреси. Зазвичай, це питання вирішується у провайдерів за додаткову плату, шляхом отриманням статичної глобальної IP-адреси [5]. Обійти NAT можна за допомогою використання власного виділеного VPN-серверу, але він теж вимагає наявності статичної відкритої IP-адреси або VPS-хостингу і має проблеми пов'язані із централізованістю [4]. Альтернативою такого VPN-серверу є накладена peer-to-peer мережа Yggdrasil, що побудована поверх протоколу IP [6]. В ній використовується простий протокол пошуку YggIP/key->coord, який схожий з пошуком ARP/NDP у широкомовній мережі Ethernet (виключає широкомовний трафік через мережу) [7]. Вузли відстежують, які вузли доступні за посиланням в дереві (батьківський і дочірні вузли), а також фільтр Блума ключів всіх вузлів, доступних по цьому з'єднанню (з усіченими ключами /64, щоб забезпечити пошук IP/префіксів). Пакет, отриманий за посиланням дерева, пересилається на інший лінк дерева, у якого пункт призначення знаходиться у фільтрі Блума.

Маємо, що в мережі Yggdrasil кожен вузол звертається до іншого за його внутрішньо-мережевою IPv6-адресою, а трафік між ними проходить через інші вузли поки не досягне отримувача. Таким мережам властиві самоконфігурація та децентралізованість [6]. Весь трафік у мережі шифрується відправником і розшифровується лише отримувачем, гарантуючи конфіденційність зв'язку. Вузли у одній локальній мережі знаходять один одного автоматично за допомогою multicast-розсилки [8]. Вузли, які знаходяться за пристроями, що підтримують технологію NAT, підключаються через публічні вузли, тому таке з'єднання завжди є вихідним [4]. Цю властивість Yggdrasil використовуємо для обходу NAT та зв'язку із віддаленим об'єктом, який

доступний поки активний хоча б один публічний вузол [9]. Такий підхід підвищує надійність системи, порівняно з централізованими рішеннями. Фільтрація трафіку за адресою відправника використовується, як міра безпеки разом із парольним захистом, оскільки адреси отримуються криптографічними методами [10].

З метою створення резервних каналів зв'язку через мережу Інтернет, використовуємо мережі мобільних операторів зв'язку, шляхом підключення до них локальних робочих місць керування віддаленим об'єктом. Вони мають підключені USB-модеми або мобільні телефони із підтримкою протоколу RNDIS (Remote Network Driver Interface Specification), який дозволяє пристрою емулювати мережевий інтерфейс Ethernet поверх інтерфейсу USB.

Віддалене керування об'єктом здійснюється із трьох віддалених робочих місць. Клієнти мережі Yggdrasil налаштовуються з використанням наявного файлу конфігурації [11]. При додаванні віддаленого робочого місця до системи, його Yggdrasil адресу вносимо до списку кінцевих вузлів на кожному із підключених робочих місць за допомогою утиліти YggVPN, встановлюємо клієнт TigerVNC [12] та перевіряємо з'єднання з об'єктом (рис. 1).

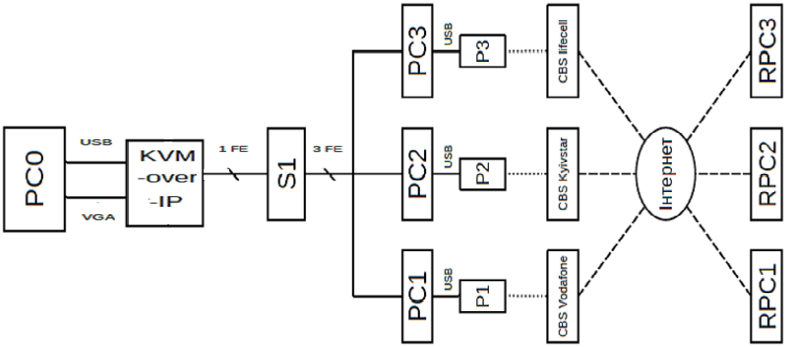

Рис. 1. Схема мережі

Тестований екземпляр системи реалізовано на конкретному прикладі з використанням клієнтського/серверного програмного забезпечення TigerVNC та додатку droidVNC-NG з віддаленого керування телефонами. Система є децентралізованою – для віддаленого керування об'єктом достатньо мати в доступі публічний вузол та одне віддалене і локальне робоче місце. Засобами мережі Yggdrasil та парольним захистом VNC-серверів забезпечується конфіденційність зв'язку та виключається несанкціонований доступ до об'єкту.

Література:

1. Конституція України: Закон України “Про критичну інфраструктуру” від 21.06.2024 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 03.10.2024).

2. Киричек Г. Г., Щетінін М. О. Конфігурація серверів з використанням Ansible. Publishing House “Baltija Publishing”. 2021. С. 15–17.

3. Cheruvu S., Kumar A., Smith N., Wheeler DM. IoT software security building blocks. Demystifying Internet of Things Security: Successful IoT Device / Edge and Platform Security Deployment. 2020. P. 213–346.

4. Рудьковський О. Р., Киричек Г. Г. Програмний комплекс з підтримки розподіленої взаємодії мережевих пристроїв та додатків. *Вчені записки ТНУ ім. В.І. Вернадського. Серія «Технічні науки».* 2021. Вип. 32(71), № 2. С.229–234.

5. Киричек, Г. Г. Керування інформаційними потоками на всіх рівнях ієрархії отримання знань. *Радіоелектроніка, інформатика, управління.* 2010. № 1. С. 70–78.

6. Yggdrasil Network. URL: https://yggdrasil-network.github.io/ (дата звернення: 03.10.2024).

7. Kothari K., Palwankar T., Dubey A., Parate P. Tor vs Yggdrasil: Comparative Study of Two Different Communication System. In 2022 International Conference on Inventive Computation Technologies (ICICT). IEEE. 2022. P. 452–456.

8. Kirichek G., Kyrychek D., Hrushko S., Timenko A. Implementation the protection method of data transmission in network. IEEE International Conference on Advanced Trends in Information Theory (ATIT’2019). 2019. P. 129–132.

9. Tang W., Han Y., Ai T., Li G., Yu B., Yang X. Yggdrasil: Reducing Network I / O Tax with (CXL-Based) Distributed Shared Memory. Proceedings of the 53rd International Conference on Parallel Processing. 2024. P. 597–606.

10. Новіков О. М., Стьопочкіна І. В. Методи штучного інтелекту у кібербезпеці. 2022. URL: https://ela.kpi.ua/handle/123456789/47605 (дата звернення: 03.10.2024).

11. Costa PA, Rosa A., Leitão J. Enabling Wireless Ad Hoc edge systems with yggdrasil. Proceedings of the 35th Annual ACM Symposium on Applied Computing. 2020. P. 2129–2136.

12. TigerVNC. URL: https://tigervnc.org/ (дата звернення: 03.10.2024).