

АЛГОРИТМ ОРГАНІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ ДО ЗАХИЩЕНОГО СЕГМЕНТУ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Чепурна І.С.

Науковий керівник – к. т. н., доц. Ткачов В.М.

Харківський національний університет радіоелектроніки, каф. ЕОМ,

м. Харків, Україна

e-mail: iryna.chepurna@nure.ua

The article considers the application of remote client access in corporate networks using VPN tunneling based on the Proxmox virtual environment. The problem of secure connection of remote users with the internal network of the enterprise through the use of virtualization and VPN technologies is investigated. Emphasis is placed on analyzing the effectiveness of using Proxmox virtualization technology to create secure connections and ensure secure access of remote users to corporate resources. The advantages of using Proxmox-based VPN tunneling in the context of ensuring confidentiality, integrity and availability of data in corporate networks are discussed.

Сучасний стан розвитку інформаційних технологій є двигуном у розвитку інформаційного суспільства. Зокрема, моделі організації ІТ-екосистем бізнесу та державного сектору відкриває все частіше стикаються з необхідністю побудови підходу до створення дистанційних робочих місць. Так, багато організацій застосовують рішення віртуальних приватних мереж для забезпечення безпеки зв'язку до таких робочих місць та призначені забезпечити умови безпечної роботи.

Одним із шляхів досягнення зазначених вище рішень є те, що, наприклад, під час локдаунів та проблема, яка виникла у потребі дистанційного доступу до ресурсів, може бути вирішена за рахунок створення віртуальних тунелів, які можуть бути створені з використанням технологій віртуалізації [1].

Розглядаючи популярні рішення віртуалізації мережних функцій, варто звернути увагу на VPN, як технологію створення захищених віртуальних тунелів між віддаленими вузлами мережі та кінцевими користувачами в мережі Інтернет. Під час передачі даних через такі віртуальні тунелі, вони шифруються, а пристрої відправника та отримувача маскуються, забезпечуючи безпечне з'єднання. Однак, основним недоліком такого рішення є зменшення швидкості передачі даних через процедури кодування та декодування [2].

Як відомо, застосування засобів віртуалізації надає значні переваги у розгортанні повноцінних мережних інфраструктур організацій для віддаленого доступу та в умовах обмеженого ресурсного забезпечення.

На рис. 1 зображено типову схему підключення мережного клієнта до корпоративної комп'ютерної мережі через OpenVPN-сервер, який з метою підвищення рівня відмовостійкості, розгортається на віртуальній машині. Віддалені користувачі можуть підключатися зі стаціонарних чи мобільних пристроїв до даного сервера. Враховуючи особливості транспортного середовища (проміжні мережі вендорів) можливі різні сценарії організації як тунелів, так і засобів, які забезпечують криптостійкість їх роботи.

В рамках даної роботи розглядається сценарій, де у якості мережного вузла виступає контейнер Proxmox, на якому безпосередньо розгортається OpenVPN-сервер. Загальнодоступна IP-адреса корпоративної комп'ютерної мережі дозволяє здійснити безпечне з'єднання від користувацького комп'ютера до мережного вузла. Таким чином, VPN-сервер виконує функції захищеного мережного шлюзу для доступу до захищеного сегменту корпоративної комп'ютерної мережі (рис. 1).



Рисунок 1 – Схема підключення користувачів через VPN-сервер до захищеного сегменту корпоративної комп'ютерної мережі

Налаштування VPN-серверу, формування сертифікатів для користувачів, адміністрування трафіку в даній схемі здійснюється за допомогою веб-інтерфейсу OpenVPN GUI [3].

Можливість використання в OpenVPN стандартних протоколів TCP і UDP дозволяє, наприклад, на відміну від IPsec обійти обмеження, коли Інтернет-провайдер або мережне обладнання, яке використовується, не підтримує або блокує відомі VPN-протоколи. За результатами проведених досліджень щодо використання OpenVPN в різних гетерогенних середовищах, встановлено, що найбільш відповідним для впровадження системи безпечного підключення віддалених користувачів до захищеного сегменту корпоративної комп'ютерної мережі є програмне забезпечення,

яке може мати як уніфіковані, так і не стандартні інтерфейси взаємодії із зовнішньою мережею. Рішення на основі OpenVPN-сервера відрізняється простотою адміністрування, здатністю читати сертифікати та приватні ключі найуживаніших операційних систем, використанням двосторонньої автентифікації сертифікату.

Віртуалізація цього рішення дозволяє розгорнути віддалений доступ до ресурсів корпоративної комп'ютерної мережі, забезпечуючи захист доступу та зменшуючи ймовірність несанкціонованого доступу до ресурсів мережі. Використання контейнерів Proxmox дозволяє встановлювати додаткові сервіси для обслуговування корпоративної комп'ютерної мережі в окремих контейнерах, що призводить як до економії апаратних ресурсів, так і до оптимального їх використання, а механізми віддаленого доступу у такій комбінації спрощують механізми їх взаємодії з віддаленими користувачами.

За результатами проведених досліджень та тестування реальної системи встановлено, що подібні рішення надають високий рівень доступності ресурсів для віддалених користувачів з урахуванням вимог безпеки та надійності. Подальші дослідження необхідно спрямувати на розробку дієвих механізмів мульти-VPN-з'єднань у агрегованих системах доставки контенту.

Список використаних джерел

1. Simon, M., Huraj, L. (2023). VirtualBox and Proxmox VE in Network Management: A User-Centered Comparison for University Environments. In: Silhavy, R., Silhavy, P. (eds) Networks and Systems in Cybernetics. CSOC 2023. Lecture Notes in Networks and Systems, vol 723. Springer, Cham. https://doi.org/10.1007/978-3-031-35317-8_44

2. Ткачов В.М. Застосування технології OpenVPN в рамках сервісу «Health Tracker» / В.М. Ткачов, А.О. Карасьов // 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова, 12-14 грудня 2018 року. – Одеса. – 2018. – С. 157-158.

3. Ткачов В.М. Застосування технології OpenVPN в рамках сервісу «Health Tracker» / В.М. Ткачов, А.О. Карасьов // 73-я науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова, 12-14 грудня 2018 року. – Одеса. – 2018. – С. 157-158.

4. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.