УДК 004.75

Шелуха О.О., к.т.н., ст. викл.
Овсянніков Д.В., магістрант
Державний університет «Житомирська політехніка»

МЕТОДИ ТА ТЕХНОЛОГІЇ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ДОСТУПУ КОРПОРАТИВНОЇ МЕРЕЖ

В умовах зростаючої гібридної інфраструктури комп'ютерних мереж назріла необхідність переходу від застарілих VPN-рішень, що створюють єдині точки відмов і є складними для масштабування, до сучасних захищених архітектур. Авторами проведено дослідження, аналіз та практичне впровадження методів організації захищеного доступу до корпоративної мережі.

В ході дослідження було здійснено порівняльний аналіз методів поєднання віддалених підмереж та основних VPN протоколів (PPTP, OpenVPN, IPsec, IKEv2, L2TP), на основі якого було обгрунтувано вибір WireGuard, як оптимальної основи для створення віртуальних тунелів для віддалених хостів. Основні переваги обраної технології полягають у високій швидкості та високому рівню криптографічної безпеки, що стає можливим з використанням алгоритму ChaCha20 [1]. Розглянуто можливості технологію Mesh VPN-рішення Tailscale [2], що побудовано на основі зазначеного алгоритму, та досліджено можливості його застосування у поєднанні із технологією WireGuard. Зазначений підхід, на відмінну від більшості традиційних VPN-рішень, використовує децентралізовану однорангову топологію. Ще одним напрямом забезпечення безпеки мережі стала інтеграція Tailscale з дотримання концепції Zero Trust Networking.

На основі теоретичних даних, було проведено моделювання захищеної корпоративної мережі, яка базується на ієрархічній трирівневій моделі та складається з головного офісу, філіалу та віддаленого працівника. Зазначений проєкт було налаштовано в емуляційному середовищі GNS3, включаючи налаштування контролера домену, базових мережевих служб та інтеграцію Tailscale. Було розроблено і впроваджено підсистему захисту з використанням маршрутизаторів на базі дистрибутиву VyOS з можливістю налаштування міжмережевого екрану. Крім того, виконано розробку списків контролю доступу у Tailnet та налаштовано аутентифікацію клієнтів Tailscale через Single Sign-On із використанням системи автентифікації Google. Всі впроваджені засоби дозволять реалізувати гнучку мікросегментацію прав доступу з дотримання суворого принципу мінімальних привілеїв.

Практичне тестування розробленої моделі мережевої інфраструктури та впроваджених рішень показали коректність її функціонування. В ході роботи було отримано наступні результати:

1. Застосування списків доступу на рівні Tailnet дозволили провести блокування передачі трафіку між віддаленим користувачем та філією, тим самим підтвердивши реалізацію принципу мінімальних привілеїв в Tailscale.

2. Аналіз перехопленого трафіку за допомогою Wireshark дозволив зафіксувати наявність наскрізного шифрування всього корпоративного трафіку з використанням протоколу WireGuard, що зрештою гарантує повну конфіденційність переданої інформації через публічні мережі.

3. Практичне тестування інформаційного обміну між сегментами мережі продемонстрували наявність прямих підключень між віддаленими вузлами мережі, тим самим підтверджуючи факт забезпечення високої швидкості та надійності з'єднань в децентралізованій Mesh-топології Tailscale.

4. Перевірка можливості віддаленого користувача отримувати доступ до внутрішніх ресурсів корпоративної мережі довела те, що Tailscale здатний забезпечувати зв'язок між пристроями навіть з приватних мереж.

5. Впровадження Single Sign-On із використанням автентифікації Google дало можливість використовувати один створений обліковий запис для декількох сервісів, зокрема в Tailscale. Це, в поєднанні з автоматичним присвоєнням IP-адрес в мережі Tailscale, мінімізує кількість ручних налаштувань мережі, що є важливим для ефективного масштабування топології.

На основі розробленої моделі корпоративної інфраструктури та впроваджених рішень було перевірено ефективність застосування рішення Tailscale для організації захищеного доступу в корпоративній мережі, зокрема використання списків доступу, наявність наскрізного шифрування корпоративного трафіку і та коректність роботи методу Single Sign-On для зручної і безпечної автентифікації користувачів. Також було протестовано можливість підключення кінцевих вузлів з приватних мереж та наявність прямих підключень між сегментами Tailscale.

Список використаних джерел:

1. The ChaCha family of stream ciphers. URL: https://cr.yp.to/chacha.html

2. What is Tailscale? URL: https://tailscale.com/kb/1151/what-is-tailscale