URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type= pdf&doi=0acc942471 ad2623f993be2e39374d675cfe9a8a

8. Jing N., Fan H., Zhai Y., Liu T. (2012). Data Warehouse Design and Optimization for Drilling Engineering. The Open Petroleum Engineering Journal. 5. 124-129. 10.2174/1874834101205010124.

9. Chaudhuri, S., & Dayal, U. (1997). An overview of data warehousing and OLAP technology. *SIGMOD Rec.*, *26*, 65-74. https://dl.acm.org/ doi/pdf/ 10.1145/248603.248616

УДК 004.77

РЕАЛІЗАЦІЯ ВИДАЧІ ДОДАТКОВИХ МЕРЕЖЕВИХ МАРШРУТІВ КЛІЄНТУ VPN НА ОСНОВІ ROUTEROS

Кудінов Є.О., аспірант
Харківський національний автомобільно-дорожній університет

Анотація. Проведено аналіз можливостей операційної системи RouterOS для реалізації видачі додаткових мережевих маршрутів для VPN-клієнтів типу точка-точка в умовах використання вбудованого серверу VPN та за допомогою зовнішнього серверу DHCP.

Ключові слова: RouterOS, Mkrotik, vpn, dhcp, point-to-point

На сьогоднішній день одним із важливіших завдань для багатьох організацій та підприємств є забезпечення своїх робітників надійним та простим доступом до своєї внутрішньої мережи з різних куточків світу. Вартість проекту також є дуже важливим параметром. Таким чином, більш перспективними виглядають недорогі та надійні пристрої з багатим списком підтримуваних протоколів маршрутизації та віртуальних приватних мереж (VPN). Кількість підтримуваних протоколів дозволяє забезпечити надійний да безпечний доступ користувачів у разі різних умов підключення до провайдерів інтернет-мереж, а також забезпечувати стабільне функціонування тунелів між підрозділами.

Одним із таких рішень є пристрої фірми MikroTik, яка виробляє власні маршрутизатори та обладнання з RouterOS за порівняно низькими цінами. Це робить їх рішення привабливими для бізнесу, який потребує надійного мережного обладнання за доступною вартістю. Можливість розгортання на архітектурі ARM (популярній у сучасних одноплатних комп’ютерах) і на стандартних x86-серверах робить RouterOS універсальним рішенням для багатьох сценаріїв використання, від домашніх користувачів до великих дата-центрів.

Більшість підприємств має розгалужену мережеву топологію. Через це єдина мережа такого підприємства складається з множини підмереж, кожна з яких має свою персональну адресу.

Налаштування маршрутизації та тунелювання трафіку при підключенні клієнта VPN до серверу може бути двох видів: повне тунелювання, коли увесь трафік користувача прямує через VPN-сервер, використовуючи нові маршрути; та спліт-тунелювання – лише певний трафік (наприклад, до корпоративної мережі) перенаправляється через VPN, решта ж трафіку йде безпосередньо до інтернет-провайдера.

Але при повному тунелюванні створюється надлишкове навантаження на канали зв'язку підприємства, а також уповільнення швидкості інтернету у користувача. Таким чином, дуже важливою задачею є відправити всі потрібні мережеві маршрути до внутрішніх мереж підприємства VPN-клієнту користувача. Здійснити це можливо за допомогою сервера DHCP.

Одними з простіших, з точки зору користувача, у налаштуванні клієнту VPN є протоколи точка-точка (sstp, l2tp, pptp, pppoe). RouterOS підтримує кожен з них, але, з точки зору цієї операційної системи, інтерфейси створені при підключенні клієнту VPN до її серверу VPN є динамічними і не можуть використовуватися у внутрішньому сервері DHCP [1,3].

Для вирішення цього питання треба розглянути алгоритм роботи VPN-клієнта при підключенні до VPN-сервера:

- Ініціація підключення до VPN-сервера.
- Встановлення PPP-з'єднання.
- Аутентифікація через PAP, CHAP, MS-CHAP.
- Налаштування каналу за допомогою LCP.
- Використання IPCP для отримання IP-адреси та інших базових мережевих параметрів.
- Відправлення запиту DHCPINFORM для отримання додаткових параметрів (DNS, WINS, маршрутів).
- Налаштування маршрутизації (повне або спліт-тунелювання).
- Передача зашифрованих даних через VPN.
- Моніторинг з'єднання.
- Завершення з'єднання та скасування налаштувань.

Згідно з цим алгоритмом, IPCP (Internet Protocol Control Protocol) використовується для конфігурації IP-параметрів між VPN-клієнтом і сервером. А після налаштування основних IP-параметрів через IPCP, VPN-клієнт може відправити запит DHCPINFORM до DHCP-сервера для отримання додаткових параметрів не передбачуваних IPCP, таких як: DNS-сервери, WINS-сервери, параметри проксі-серверів, маршрутизація. DHCPINFORM - це запит клієнта до DHCP-сервера для отримання додаткових мережевих параметрів (DNS-сервери, шлюз за замовчуванням тощо) без зміни IP-адреси. У відповідь DHCP -сервер надсилає відповідь (DHCPACK), в якій містяться додаткові параметри, такі як

DNS або маршрути. VPN-клієнт отримує ці дані та налаштовує відповідні параметри системи (наприклад, змінює налаштування DNS) (Рис.1) [2].

Таким чином, для отримання клієнтом VPN додаткових маршрутів, потрібно забезпечити доставку DHCPINFORM від клієнту до серверу DHCP, а від DHCP-серверу до VPN-клієнту доставку пакета DHCPACK.

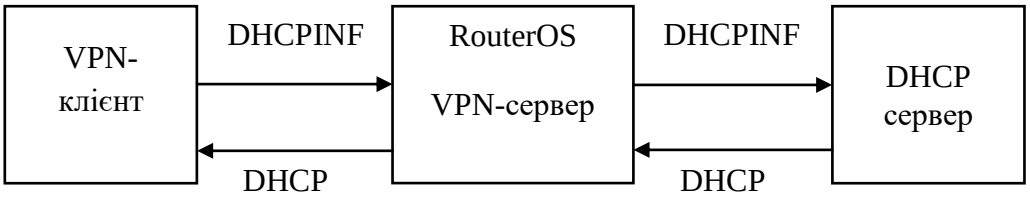

Рис.1 – Схема отримання опцій DHCP клієнтом VPN від серверу

Насамперед, треба забезпечити сервер DHCP, встановлений на сторонню операційну систему, яка не є RouterOS. Це може бути будь-яка ОС -Windows, Linux, *BSD та інші.

У даному випарку на схемі (Рис.1) вбудований VPN-клієнт розташовано на ОС Windows, а DHCP-сервер, у цьому випадку використовується isc-dhcp-server, на ОС FreeBSD. За налаштунками VPN-серверу, клієнт отримує ip-адресу 192.168.2.30, а ОС з сервером DHCP має адресу 192.168.112.10.

Після отримання ip-адреси від серверу VPN клієнт відправляє широкомовний (broadcast) пакет DHCPINFORM, який треба перенаправити до сервера DHCP.

Це реалізується за допомогою ланцюжка mangle та nat брандмауера RouterOS. Mangle застосовується для маркування з’єднань тільки широкомовних пакетів від клієнтів VPN, спрямованих по протоколу udp на 67 порт. Дія dst-nat ланцюжка перенаправляє широкомовний пакет від клієнта до DHCP-сервера вже від адреси самого маршрутизатора RouterOS. У відповідь на пакет DHCPINFORM сервер DHCP відправляє пакет DHCPACK. Завдяки маркуванню з’єднань на етапі відправки DHCPINFORM від клієнту та src-nat ланцюжка, пакет DHCPACK потрапляє до клієнту [4].

Таким чином, для реалізації схеми (Рис.1) у брандмауері RouterOS потрібно додати три правила (Рис.2):

```
/ip firewall mangle
add action=mark-connection chain=prerouting comment=\
    "dhcp request mark for pptp/sstp" dst-address=255.255.255.255 dst-port=67 \
    in-interface=all-ppp new-connection-mark=dhcp passthrough=no protocol=udp
/ip firewall nat
add action=dst-nat chain=dstnat comment=dhcp_relay_for_vpn dst-address=\
    255.255.255.255 dst-port=67 in-interface=all-ppp protocol=udp \
    to-addresses=192.168.112.10
add action=src-nat chain=srcnat connection-mark=dhcp to-addresses=\
    192.168.112.10
```

Рис.2 – Правила брандмауера

Тут було розглянуто реалізацію видачі додаткових мережевих маршрутів VPN-клієнтам у конфігурації point-to-point на основі RouterOS. Використання цієї технології дозволяє забезпечити гнучке управління мережевими маршрутами та підвищити ефективність і безпеку передачі даних через VPN-з'єднання. Описана методологія з використанням RouterOS дозволяє оптимізувати роботу віддалених користувачів з внутрішніми ресурсами організації, забезпечуючи при цьому мінімальну затримку та стабільність підключень.

Застосування додаткових маршрутів через VPN дозволяє значно зменшити навантаження на мережу, покращити її масштабованість та підвищити рівень доступності сервісів для віддалених користувачів. У процесі дослідження також було продемонстровано переваги використання RouterOS завдяки його підтримці широкого спектру мережевих протоколів та можливостей щодо налаштування централізованої видачі інформації о маршрутах клієнтам.

Отже, впровадження даної технології є доцільним рішенням для компаній, які використовують віддалений доступ до корпоративних мереж і прагнуть підвищити ефективність та безпеку передачі даних через VPN-з'єднання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *RouterOS - RouterOS - MikroTik Documentation*. (б. д.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/
2. Droms, R. (no date) *RFC 2131: Dynamic Host Configuration Protocol*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc2131 (Accessed: 29 September 2024).
3. Xu, Z., & Ni, J. (2020, December). Research on network security of VPN technology. In *2020 International Conference on Information Science and Education (ICISE-IE)* (pp. 539-542). IEEE.
4. Towidjojo, R. (2023). *Mikrotik Kung Fu: Kitab 4*. Jasakom