

Бухарова Л.Д., студентка

Гвоздецька К.П., студентка

Харківський національний університет радіоелектроніки, м. Харків

Кафедра Електронних обчислювальних машин

ОСНОВИ ТУНЕЛЮВАННЯ, ЯК РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

В даний час існує безліч варіантів реалізацій технології VPN, з певними перевагами і недоліками. Одною найпоширеніших реалізацій є віртуальні приватні мережі на основі техніки тунелювання [1].

Тунелювання – це мережева технологія, яка дозволяє інкапсулювати один тип пакету протоколу в дейтаграму іншого протоколу. Наприклад, з'єднання Windows VPN можуть використовувати пакети протоколу тунелювання (PPTP) від точки до точки, щоб інкапсулювати і відправляти приватний мережевий трафік, такий як трафік TCP / IP в загальнодоступній мережі, такий як Інтернет.

Так клієнт тунелю або сервер використовує протокол передачі даних тунелю для підготовки даних для передачі [2, 3]. Наприклад, коли клієнт тунелю відправляє корисне навантаження на тунельний сервер, він спочатку додає заголовок протоколу передачі даних тунелю в корисне навантаження. Потім клієнт відправляє отримане інкапсульоване корисне навантаження по мережі, яка направляє його на сервер тунелів. Сервер тунелів приймає пакети, видаляє заголовок протоколу передачі даних тунелю і пересилає корисне навантаження в цільову мережу.

Існує два типи тунелювання: добровільне та обов'язкове. Добровільне тунелювання – користувач або клієнтський комп'ютер може видати запит VPN для настройки і створення добровільного тунелю. Добровільне тунелювання відбувається, коли клієнтський комп'ютер або сервер маршрутизації створює віртуальне з'єднання з цільовим сервером тунелів [4].

При примусовому тунелюванні клієнтський комп'ютер розміщує виклик віддаленого доступу в NAS з підтримкою тунелювання в ISP. Наприклад,

корпорація могла б укласти контракт з інтернет-провайдером для розгортання загальнонаціонального набору FER.

Таким чином, у зв'язку з популярністю Інтернету і стека TCP / IP ситуація, коли несучим протоколом транзитної мережі зазвичай виступає протокол IP, а протоколом-пасажиром – деякий каналний протокол, є дуже поширеною. Разом з тим застосовуються і інші схеми інкапсуляції, такі як інкапсуляція IP в IP, Ethernet в MPLS, Ethernet в Ethernet. Подібні схеми інкапсуляції потрібні не тільки для того, щоб узгодити транспортні протоколи, а й для інших цілей, наприклад для шифрування вихідного трафіку або для ізоляції адресного простору транзитної мережі провайдера від адресного простору для користувача мереж [5].

Література

1. Ruban I.V., Churyumov G.I., Tokariev V.V., Tkachov V.M. Structural-functional reconfiguration of computer systems with reconstruct structure. Проблеми інформатики та моделювання: тези доповідей 19-ї міжн. наук.-техн. конф., м. Одеса, 11-16 вер. 2019р. Одеса, С.71 — 72.
2. 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. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 1 (63). – С. 90-95. – doi:<https://doi.org/10.26906/SUNZ.2021.1.090>.
3. Tkachov, V., Kovalenko, A., Kuchuk, H., & Ni, I. (2021). Метод забезпечення живучості високомобільної комп'ютерної мережі. *Advanced Information Systems-Sučasni informacijni sistemi*, 5(2), 159-165.
4. Kuchuk, N., Kovalenko, A., Tkachov, V., Rosinskiy, D., & Kuchuk, H. (2021). Predicting traffic anomalies in container virtualization. *Computer And Information Systems And Technologies*.
5. Tkachov V. Principles of Constructing an Overlay Network Based on Cellular Communication Systems for Secure Control of Intelligent Mobile Objects / Vitalii Tkachov, Andriy Kovalenko, Mykhailo Hunko and Kateryna Hvozdet'ska // Информационные технологии и безопасность. Материалы XIX Международной научно-практической конференции ИТБ-2020. – К.: ООО «Инжиниринг», 2020.