Бродський Ю. Б., к.т.н., доцент,
Рудюк Б. М., здобувач
Державний університет «Житомирська політехніка»

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА РІВНЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ CISCO DMVPN

Корпоративні мережі є ключовою інфраструктурою для бізнесу. Вони використовуються для зберігання, обробки та передачі важливої інформації, а також для забезпечення зв'язку між співробітниками, клієнтами та партнерами. Внаслідок цього корпоративні мережі є привабливою мішенню для хакерів та інших зловмисників.

Забезпечення безпеки корпоративних мереж є вельми важливим завданням для будь-якої компанії. Несанкціонований доступ до цих мереж може призвести до витоку конфіденційної інформації, фінансових втрат та завдати серйозної шкоди репутації компанії. Тому компанії повинні активно працювати над вдосконаленням заходів безпеки і регулярно проводити аудит своїх мереж, щоб виявити потенційні слабкі місця і вразливості. Підтримка безпеки корпоративних мереж стає невід'ємною частиною сучасного бізнесу, і важливо приділяти їй належну увагу.

Одним із найбільш актуальних завдань захисту корпоративної мережі є забезпечення безпеки тунельного зв'язку між віддаленими філіями. Технологія Cisco DMVPN дозволяє вирішити це завдання шляхом використання динамічного тунелю (Dynamic Multipoint VPN), який забезпечує шифрування трафіку між філіями, а також аутентифікацію і авторизацію учасників тунелю.

Основна перевага DMVPN полягає в можливості створення динамічних тунелів без необхідності ручного налаштування на кожному з вузлів. Вона використовує протоколи IPsec і GRE (Generic Routing Encapsulation), що дозволяє створити шифровані тунелі для безпечної передачі даних через незахищені мережі, такі як Інтернет. Крім того, DMVPN дозволяє ефективно використовувати ресурси мережі, зменшуючи трафік і обчислювальні витрати.

Також, DMVPN надає можливість створювати мережі з точки-до-точки або з точки-до-багатьох, що робить її ідеальним рішенням для організацій з розподіленою інфраструктурою. Це спрощує побудову складних мереж і дозволяє забезпечувати зв'язок між різними вузлами в мережі, навіть якщо вони розташовані в різних фізичних локаціях. Таким чином, DMVPN є потужним і гнучким інструментом для забезпечення зв'язку і безпеки в розподілених мережах.

Безпека в DMVPN забезпечується за рахунок наступних механізмів:

Зашифрований тунель: DMVPN використовує різні методи шифрування, такі як IPSec, для створення зашифрованого тунелю між різними вузлами мережі. Це дозволяє захистити передачу конфіденційних даних через незахищені мережі, такі як Інтернет;

Динамічне налаштування тунелів: DMVPN дозволяє автоматично налаштовувати тунелі між вузлами, що спрощує керування VPN і дозволяє додавати нові підключення без необхідності ручного налаштування;

Централізоване управління: Cisco DMVPN може бути інтегрованим з централізованими системами управління, такими як Cisco Identity Services Engine (ISE). Це дозволяє контролювати доступ до мережі, вимагаючи аутентифікації, авторизації та обліку (AAA) для кожного підключення;

Мультифакторна аутентифікація: підключає додатковий шар безпеки;

Перевірка безпеки мережі: за допомогою Cisco DMVPN можна встановити засоби моніторингу та реагування на інциденти для виявлення та відповіді на потенційні загрози безпеці мережі [2].

Отже, DMVPN дозволяє заощадити час та зусилля при налаштуванні мережі, спрощує розгортання та управління мережею, зменшує ймовірність помилок та підвищує загальну надійність і безпеку інфраструктури. Таким чином, DMVPN стає потужним інструментом для організацій, що прагнуть поєднати безпеку та ефективність у своїй корпоративній мережі.

Список використаних джерел

1. Cisco Dynamic Multipoint VPN. URL: https://www.cisco.com/c/en/us/products/collateral/security/dynamicmultipoint-vpndmvpn/data_sheet_c78-468520.html.
2. DMVPN – Concepts & Configuration. URL: https://learningnetwork.cisco.com/s/article/dmvpn-conceptsampconfiguration.