УДК 004.7

Гаврилюк В.А., магістрант
Бродський Ю. Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

Для надання найкращого рівня послуг корпорації дедалі частіше відкривають регіональні представництва. Це дозволяє не лише прискорити обслуговування, але й краще розуміти потреби локальних клієнтів. Разом з цим, компанії беруть на себе додаткову відповідальність за збереження конфіденційної інформації, розуміючи, що довіра – це найцінніший актив, тому безпеці даних надається вищий пріоритет. Саме тому в умовах зростання кількості філій та поширення гібридних моделей роботи, основним завданням стає забезпечення безпечної взаємодії між географічно розподіленими офісами та впровадження суворого контролю доступу до внутрішніх ресурсів.

Проблемним питанням залишається невідповідність нинішнього стану захисту багатьох корпоративних мереж сучасним кіберзагрозам. В процесі організації зв'язку між філіями, в яких відсутній належний рівень шифрування, а також централізовані механізми аутентифікації та авторизації, виникають суттєві ризики несанкціонованого доступу, перехоплення та модифікації конфіденційних даних. Крім зовнішніх загроз, актуальною залишається проблема неконтрольованого доступу в межах локальної мережі, що вимагає впровадження гранулярного контролю на рівні портів комутаторів. Необхідність аналізу методів захисту від загроз визначає основний напрям даного дослідження.

Метою дослідження є аналіз та розробка рекомендацій щодо проектування підсистем захисту корпоративних мереж із використанням технологій GRE over IPSec, RADIUS.

У процесі дослідження проведено порівняльний аналіз протоколів автентифікації RADIUS та TACACS+. Визначено, що, хоча TACACS+ забезпечує шифрування всього тіла пакета та розділення процесів авторизації й аутентифікації, RADIUS є відкритим стандартом (RFC 2865), що гарантує кращу сумісність у гетерогенних мережах та є єдиним вибором для реалізації мережевого доступу за стандартом 802.1x.

Також розглянуто типи VPN-технологій (Site-to-Site, Remote Access) та здійснено детальне порівняння GRE over IPsec із звичайним IPsec тунелюванням. Встановлено, що класичний IPsec не підтримує multicast-трафік, що унеможливлює коректну роботу протоколів

динамічної маршрутизації (OSPF, EIGRP) без значного ускладнення конфігурації. Використання комбінації GRE over IPsec нівелює цей недолік: GRE інкапсулює службовий та multicast-трафік у unicast-пакети, які потім надійно шифруються IPsec, забезпечуючи гнучкість та безпеку каналу.

Як приклад, в доповіді буде продемонстровано прототип рекомендованої інтегрованої моделі підсистеми захисту, яка поєднує тунелювання GRE over IPsec, щоб забезпечити захищений зв'язок між офісами та механізми 802.1x для контролю доступу.

Моделювання мережевої інфраструктури та відпрацювання сценаріїв захисту виконувалося у середовищі емуляції GNS3. Як програмно-апаратну основу задіяно віртуальні образи маршрутизаторів та комутаторів Cisco, а також обладнання Mikrotik. З метою реалізації централізованої політики AAA розгорнуто сервери RADIUS, а тестування клієнтського доступу виконується за допомогою віртуальних машин з ОС Windows.

Аналіз розробленого прототипу підтвердив, що система забезпечує конфіденційність передачі даних, коректну роботу протоколів динамічної маршрутизації через захищений канал та ефективне блокування неавторизованих пристроїв на рівні комутації, що доводить практичну життєздатність моделі для використання в корпоративних мережах.

На основі проведеного аналізу було розроблено рекомендації з метою забезпечення комплексного захисту корпоративної мережі, підвищення ефективності та безпеки бізнес-процесів. Однією з головних функцій запропонованої моделі є синергетичне поєднання надійного шифрування каналів зв'язку та централізованого, гранулярного контролю доступу до ресурсів, що дозволяє ефективно протидіяти сучасним загрозам.

Список використаних джерел:

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2016. 464 с..

2. Stewart M., Kensey D. Network Security, Firewalls, and VPNs. 3rd ed. Jones & Bartlett Learning, 2020.