ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Атестаційна робота магістра

Метод побудови віртуальних тунелів Extranet-систем

Науковий керівник: доц. Ткачов В.М.
Виконав: студент групи СПм-21-2
Верховський І.В.

Мета та актуальність роботи

Кількість повідомлень про порушення систем безпеки та втрату даних

Мета дослідження полягає у виявленні найбільш ефективних методів побудови віртуальних тунелів, їх переваги та недоліки, аналізі можливостей використання цих технологій для забезпечення максимального рівня безпеки.

Актуальність: Попит на послуги VPN зростає у геометричній прогресії, сучасні організації все більше використовують мережі зовнішнього доступу для обміну даними зі своїми партнерами та клієнтами. І ще швидше зростає кількість атак.

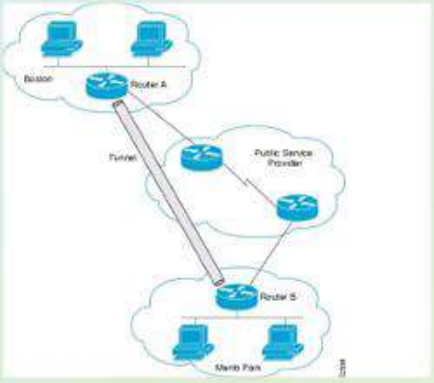
Постановка задачі

Завдання:

- Провести аналіз існуючих досліджень
- Дослідити протоколи та функції тунелів і VPN
- Дослідити види атак на корпоративні мережі
- Проаналізувати способи захисту каналів корпоративних мереж на базі VPN та тунелів
- Розглянути методи побудови віртуальних тунелів
- Дослідити та проаналізувати обладнання для побудови тунелів
- Провести експериментальні дослідження для оцінки ефективності та безпеки різних методів

Віртуальні тунелі

Віртуальний тунель - це метод забезпечення безпеки передачі даних в мережах, що базується на створенні безпечного каналу комунікації між двома вузлами мережі через незахищену мережу.

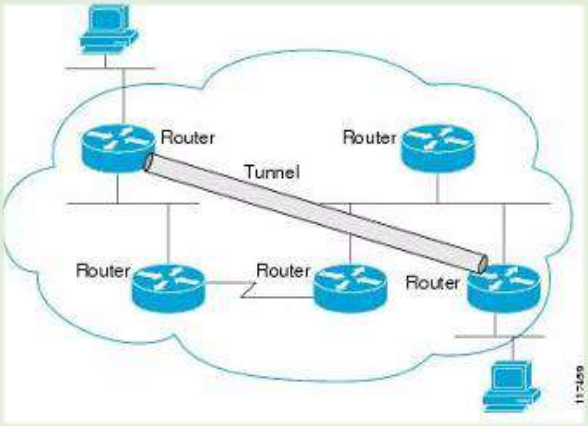


Основна ідея полягає в тому, що дані, які передаються між двома вузлами мережі, пересилаються через незахищену мережу упакованими в зашифрований пакет – таким чином вони захищені від прослуховування та модифікації. У той же час, зберігається прозорість мережі, тобто кінцеві вузли не знають про наявність тунелю та використовують його, як звичайний канал зв'язку

Класифікація методів та засобів тунелювання

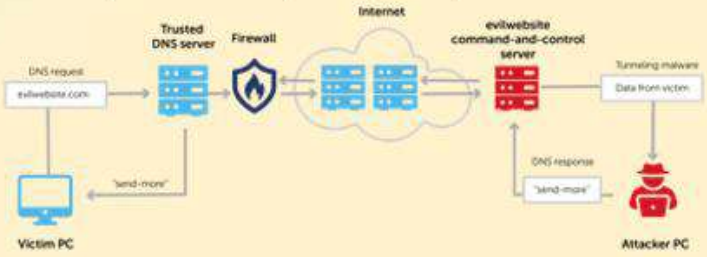
Класифікуються за:

- рівнем захисту;
- протоколом транспорту;
- рівнем мережевого стеку;
- типом мереж.



Аналіз існуючих досліджень

Дослідження показали, що використання протоколів тунелювання є важливим елементом забезпечення безпеки даних у Extranet-системах. При виборі протоколу варто ретельно аналізувати його характеристики та порівнювати їх з потребами організації.

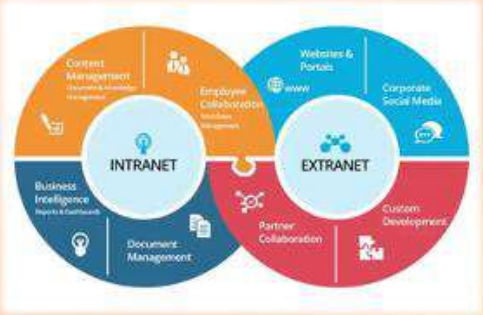


В результаті автори прийшли до висновку, що OpenVPN є найбільш безпечним протоколом серед розглянутих, атакож відзначили, що інші протоколи, зокрема PPTP, мають серйозні проблеми з безпекою, які можуть бути використані для атак на мережу.

Extranet-системи

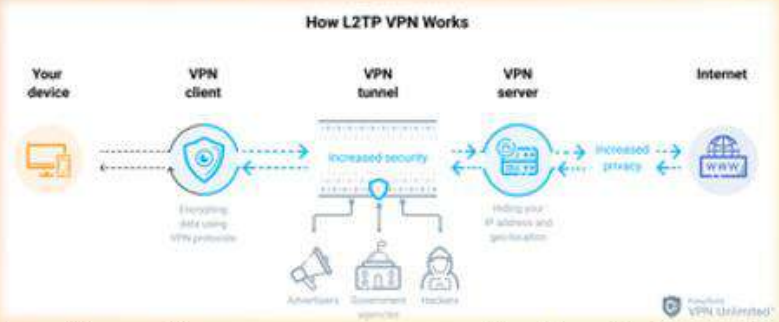
Extranet є захищеною від несанкціонованого доступу корпоративною мережею, яка забезпечує обмін даними всередині компанії, між різними компаніями, підприємствами та іншими сторонами, що мають обмежений доступ до внутрішніх мереж організації.

За допомогою Extranet-систем компанії можуть співпрацювати та обмінюватися даними з постачальниками, клієнтами та іншими зацікавленими сторонами, що покращує ефективність бізнес-процесів та підвищує конкурентоспроможність



L2TP

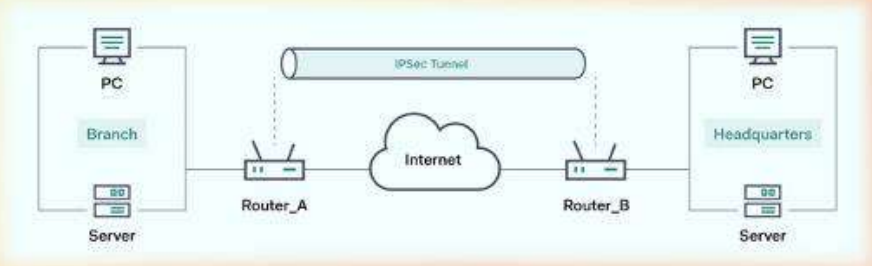
L2TP наслідує та розширює кращі якості PPTP та L2F. Серед наслідуваного також відсутність можливості шифрування засобами самого лише L2TP. З-поміж транспортних протоколів використовує виключно UDP.



Для захисту інформації зазвичай використовуються протоколи IPsec. При роботі з таким з'єднанням можна використовувати протоколи AH, ESP та IKE. Прото це негативно впливає на швидкість, через додавання окремого другого етапу обробки даних

IPsec

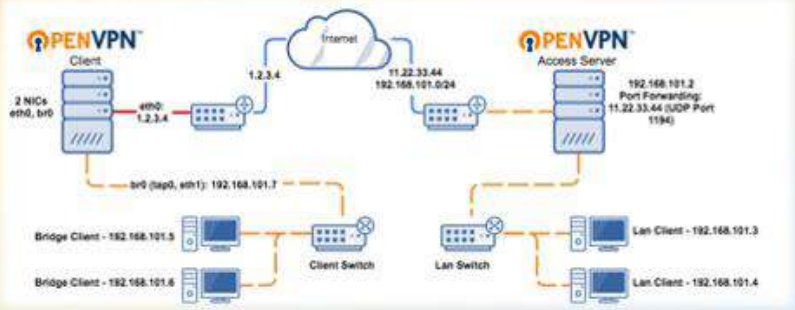
IPsec (IP Security) – це набір протоколів зв'язку для створення безпечних з'єднань в мережі. IP – загальноприйнятий стандарт, що визначає, як інформація передається в Інтернеті. IPsec додає шифрування та автентифікацію, щоб зробити цей протокол безпечнішим.



Слід зазначити, що IP не є частиною набору IPsec, IPsec працює безпосередньо поверх IP. Здатний використовувати транспортні протоколи TCP та UDP

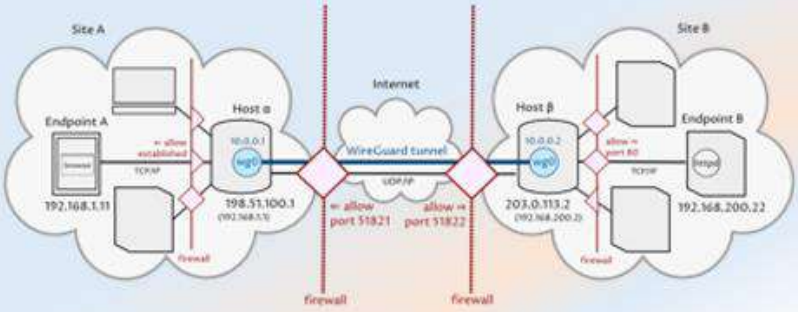
OpenVPN

OpenVPN здатний використовувати транспортні протоколи TCP та UDP, щоробить OpenVPN більш привабливою альтернативою IPsec в ситуаціях, коли інтернет-провайдер може блокувати специфічні протоколи VPN. Проте проблема відома як «TCP Meltdown Problem», робить використання TCP небажаним.



WireGuard

WireGuard – вільне та відкрите програмне забезпечення і протокол зв'язку, розроблений з оглядом на простоту використання, високу швидкість і малу поверхню атаки. Використовує найсучасніші методи шифрування. Як і OpenVPN, надає можливість розширення функціоналу за допомогою сторонніх додатків та скриптів.



MikroTik

Продукція MikroTik відноситься до напівпрофейсійного сегменту. Конкуренції з нею не витримують домашні маршутизатори, як TP-Link, Xiaomi та інші, адже їх надійність та безпека можуть задовольнити хіба що не надто вимогливого домашнього користувача, адже значно поступаються можливостями, надійністю, безпекою та потужністю апаратного забезпечення.

RouterOS

RouterOS – спеціалізована операційна система, призначена виключно для побудови мереж з маршрутизаторів, фаєрволів, бриджів, базових станцій, VPN-серверів та інших пристроїв керування ними.

Вона є є дуже потужним інструментом для створення мереж і керування ними, включаючи в свій арсенал величезну кількість функцій для роботи мало не з усіма можливими мережевими протоколами.

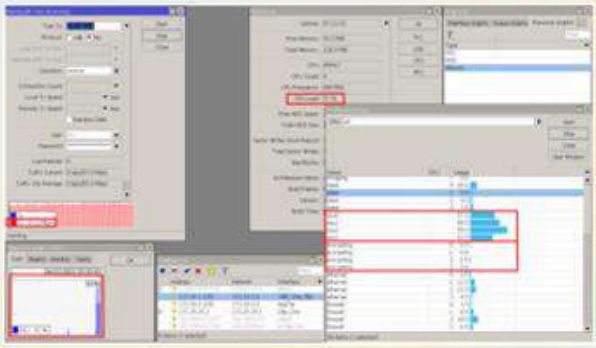
Побудова тунелів

Для моделювання корпоративної мережі використано реальне обладнання та канали зв'язку провайдера. У тестовій схемі використовувалися hAP ac lite, у яких наявний апаратний чіп шифрування. Використовувалися канали провайдера з обмеженням в 100 Мбіт/с.

В експериментах розглянуто ефективність за швидкістю відправлення чи прийому даних мережевих протоколів тунелювання із врахуванням шифрування, типу з'єднання транспортного рівня. Розглянуто завантаження процесора, корисна пропускна здатність на прийом та передачу.

Проведення експериментів

Для проведення експериментів послідовно налаштовувався один із зазначених типів тунелів. З метою максимізації репрезентативності результатів, для кожного з протоколів використано режим передачі даних за допомогою протоколу UDP та зі встановленням з'єднання – протокол TCP.



Результати експериментів

Для тунелів, для яких можливо використовувати як транспортний протокол TCP та UDP, було проведеного два експерименти, що підтвердили вже отримані результати. Одним з основних критеріїв використання тунелів є корисна пропускна здатність каналу. Загальні результати моделювання наведено в таблиці.

Протокол	Завантаження CPU, %	Rx, Mbps	Tx, Mbps
L2TP/IPsec	48	40.3	41.1
OpenVPN TCP	40	16.2	12.8
OpenVPN UDP	24	30.2	10.4
WireGuard	65	69.7	89.4

За результатами експериментів беззаперечним лідером виявився WireGuard. Отже у випадках, коли швидкість є ключовою характеристикою, однозначним вибором є саме цей протокол.

Безпека

WireGuard використовує найсучасніші методи шифрування: X25519, ChaCha20, Poly1305, SipHash, BLAKE2s. Може надавати додатковий рівень симетричного шифрування завдяки підтримці PSK.

WireGuard не встановлює з'єднання. Автентифікація забезпечується в першому запиті з хендшейком, який встановлює симетричні ключі, що використовуватимуться для передачі даних.

Висновки

В ході роботи було:

– досліджено протоколи, функції тунелів та VPN;

– досліджено види атак на корпоративні мережі;

– проаналізовано способи захисту каналів корпоративних мереж на базі VPN та тунелів;

– розглянуто методи побудови віртуальних тунелів;

– досліджено та проаналізовано обладнання для побудови тунелів

Використання протоколу WireGuard зарекомендувало себе як найбільш універсальне, адже, перевершуючи в швидкості конкурентів, також пропонує більш високий рівень захисту, що є ключовими факторами при виборі.

ДОДАТОК Б

Сертифікат про прийняття статті до публікації в журналі «Науковий огляд»

Центр Міжнародного наукового співробітництва „ТК Меганом"
Інститут наукового прогнозування
кафедра економічної теорії Львівської комерційної академії
кафедра суспільно-політичних наук Вінницького національного технічного університету
кафедра філософських та соціальних наук Чернівецького торговельно-економічного інституту
Київського Національного торговельно-економічного університету
Хмельницький торговельно-економічний інститут
Асоціація „Аналітикум"

СЕРТИФІКАТ

виданий бакалавру комп'ютерної інженерії, Ігорю Верховському та кандидату технічних наук, доценту, Віталію Ткачову, Харківський національний університет радіоелектроніки в тому, що їх стаття «МЕТОДИ ПОБУДОВИ ВІРТУАЛЬНИХ ТУНЕЛІВ EXTRANET-СИСТЕМ» прийнята до публікації в випуску журналу «Науковий огляд» № 4(89)2023, що запланований до виходу 10 червня 2023 року.

Директор Центру Міжнародного
наукового співробітництва «ТК Меганом» Савченко В. А.

16 травня 2023 р.