ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до бакалаврської роботи

на тему: **“ АНАЛІЗ НАПРЯМКІВ ПІДВИЩЕННЯ НАДІЙНОСТІ СИСТЕМ ПЕРЕДАЧІ ДАНИХ”**

Виконала: студентка 4 курсу, групи ТСД-43
спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Аніщенко К.Я.
(прізвище та ініціали)

Керівник Плющ О.Г.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтроль _____
(прізвище та ініціали)

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Кафедра Мобільних та відеоінформаційних технологій
Ступінь вищої освіти бакалавр
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

Завідувач кафедри
Мобільних та відеоінформаційних технологій
_____ Л.І.Кирпач
“____” _____2021 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТЦІ

Аніщенко Кристині Ярославівні

1.Тема роботи: Аналіз напрямків підвищення надійності систем передачі даних,
керівник роботи: Плющ О.Г. к.т.н.,доцент,
затверджені наказом вищого навчального закладу від 12.03.2021 року № 65

2. Строк подання студентом роботи 24.05.2021 року
3. Вихідні дані до роботи:
   1. Телекомунікаційні мережі зв’язку;
   2. Програми ідентифікації типів додатків;
   3. Віртуальна приватна мережа;
   4. Алгоритм ідентифікації типів додатків;
   5. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити):
   1. Аналіз тенденції розвитку та основні відомості про телекомунікаційні мережі зв’язку;
   2. Аналіз теоретичного і практичного використання технології SSH при побудові корпоративної мережі;
   3. Дослідження особливостей застосування провадження VPN на основі різних технології в корпоративну мережу;
   4. Аналіз моделей і алгоритмів ідентифікації типів додатків тунельного трафіку.

5. Графічна частина роботи представлена на 14 слайдах презентації

6. Дата видачі завдання 15.03.2021

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури, формування завдання	17.03.2021	Викон.
2	Загальна характеристика телекомунікаційної мережі	31.03.2021	Викон.
3	Аналіз теоретичного і практичного використання технології SSH при побудові корпоративної мережі	07.04.2021	Викон.
4	Дослідження особливостей застосування провадження VPN в корпоративну мережу та їх порівняльна оцінка	22.04.2021	Викон.
5	Висновки по роботі, оформлення роботи	06.05.2021	Викон.
6	Розробка доповіді і презентації	23.05.2021	Викон.

Студентка _____ Аніщенко К.Я.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Плющ О.Г.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина бакалаврської роботи: 66 стор., 59 рис., 6 табл., 23 дж.

Об'єкт дослідження - процес ідентифікації типів додатків тунельного трафіку

Предмет дослідження – моделі та алгоритми ідентифікації типів додатків тунельного трафіку

Мета роботи – аналіз організації та особливості підвищення надійності систем передачі даних.

Методи дослідження. Для вирішення поставленої мети у роботі використовувалися методи теорії графів, теорії оптимізації, теорії телетрафіка, теорії ймовірностей і математичної статистики, чисельні методи розрахунку і аналізу, методи експертних оцінок.

У дипломній роботі виконано огляд сучасного стану, тенденції розвитку та особливості застосування технології зв'язку, на базі яких будуються корпоративні мережі. У другому розділі виконано огляд теоретичного і практичного використання технології SSH при побудові корпоративної мережі, алгоритм побудови каналу зв'язку за допомогою SSH-тунелів та принципи роботи. Третій розділ присвячено дослідженю застосування провадження VPN в корпоративну мережу, їх порівняльна оцінка. У практичній частині виконано дослідження моделей і алгорімов ідентифікації типів додатків тунельного трафіку. Виконано експериментальний і теоретичний аналізи досліджуваної моделі за допомогою якої можливий ефективний контроль і моніторинг типу діяльності користувачів, що використовують підозрілі програми.

КОНСТРУКТОР, IP/MPLS, IPSEC, ПРОВАЙДЕР, ТЕХНОЛОГІЯ, МЕРЕЖА, ТОПОЛОГІЯ, ПРОДУКТИВНІСТЬ, НАВАНТАЖЕННЯ, ПРОГРАМНИЙ ПАКЕТ, АЛГОРИТМ, ІТЕРФЕЙС, ПЛАНУВАННЯ, ПРОГРАМНИЙ ПАКЕТ, РЕЗЕРВ

ЗМІСТ

ВСТУП

Актуальність дослідження. Інтенсивне використання інтернет-додатків на базі різних технологій зв’зку в різних аспектах життя привело до збільшення обсягу переданого трафіку і одночасно до збільшення загроз безпеки інформації. Реакцією на це стало вдосконалення способів захисту даних і користувачів.

Найбільш відомим методом захисту даних є шифрування але при використанні шифрування управління трафіком і безпекою мережі стає складніше через неможливість здійснення перевірки вмісту зашифрованих пакетів

Безпека, надійність і дивовижна практичність - основні характеристики SSH. Саме це вигідно відрізняє SSH-доступ від інших варіантів управління серверами, інформаційними системами, веб-ресурсами чи обладнанням.

Надання доступу до веб-ресурсу через SSH - незмінно супроводжує здачу сайту в експлуатацію. Знати і вміти користуватися SSH - фундаментальні складові компетенції сучасного фахівця.

SSH є технологією, яка призначена для віддаленого виконання команд, а також для входу через мережу на інший комп'ютер. Використовуючи SSH можна завантажувати і копіювати файли між комп'ютерами, але частіше за все вона використовується для безпечної передачі файлів сайту між вашим комп'ютером і сервером хостинг-провайдера. Завдяки використанню цієї технології досягається надійна авторизація та безпечна передача інформації по відкритих каналах зв'язку.

Таким чином, бакалаврська робота, яка присвячена аналізу організації та особливості підвищення надійності систем передачі даних є своєчасною та актуальною.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ

1.1 Аналіз комунікативної моделі інфокомунікаційної мережі

Інфокомунікаційна мережа з’явилася в результаті еволюції засобів зв’язку й ЕОМ. Вона може одночасно поєднувати різні джерела та користувачів які споживають інформації. До них відноситься як просте термінальне обладнання, персональні комп’ютери, окремі люди, так і великі обчислювальні центри чи об’єкти, підприємства, розосереджені на великій території планети і навіть у космосі. Сукупність ресурсів мережі, задіяних у виробництві та наданні користувачам конкретної послуги або певного набору послуг, прийнято називати платформою надання послуг. Інфокомунікаційну мережу як фізичний об'єкт зображено на рис. 1.1.

Рис.1.1. Інфокомунікаційна мережа

Термінальними пристроями користувачів називають пристрої, призначені для роботи в мережі, якими є як кінцеві пристрої телекомунікаційних служб: телефонні апарати (стаціонарні, системні, мобільні, IP-телефонії), пристрої

телематичних служб (факсимільні апарати, відеотермінали тощо), так і багатофункціональні термінали на основі комп'ютерів. Під інфокомунікаційними службами розуміються всі наявні системи передавання та обробки інформації: телефонія, телеграфія, передавання даних, телебачення, а також служби: телеметрія, телекерування, теленаведення, телеконтроль, телеосвіта, телеторгівля, телебіржа, телеаукціон, телереклама, дистанційна аварійна сигналізація тощо. Інфокомунікаційну мережу можна уявити як систему, до якої входять користувачі, засоби різних видів зв’язку, обладнання для надання послуг і системи керування рис.1.2.

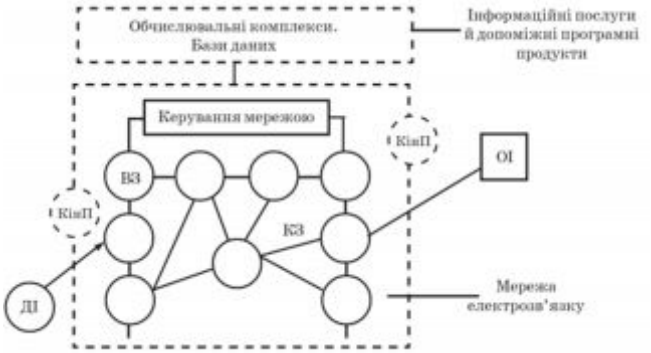


Рис.1.2. Схема інфокомунікаційної мережі

Користувачі (абоненти) є джерелами й споживачами інформації, користуються послугами інфокомунікаційної мережі та створюють потоки повідомлень різних видів і призначення. Мережа електрозв’язку складається з пунктів і ліній (каналів) зв’язку. Пункти мережі поділяються на кінцеві (КінП), у тому числі абонентські (АП), з апаратурою введення і виведення інформації, вузли зв’язку (ВЗ), що забезпечують розподіл інформації, і різні обчислювальні комплекси (центри), які забезпечують обробку й зберігання інформації. Вузли зв’язку, у свою чергу, поділяються на комутаційні (комутація каналів, повідомлень, пакетів) для розподілу інформації і мережеві (із кросуванням) для розподілу пучків каналів. Канали зв’язку (КЗ), об’єднані в лінії (ребра мережі) між окремими пунктами мережі, слугують для передавання (перенесення)

інформації у просторі. Як пункти, так і лінії (канали) здебільшого є стаціонарними, але існують і нестаціонарні (пересувні).

Структура інфокомунікаційної мережі. При вивченні процесів функціонування інфокомунікаційних мереж увага концентрується на тих властивостях, особливостях поводження і характеристиках складної системи, що змінюються з часом. Аналізуючи структуру інфокомунікаційних мереж, насамперед цікавляться властивостями і характеристиками цих складних систем, що не залежать від часу і зберігаються постійними, незмінними на всьому проміжку функціонування чи на значній його частині. Проте структурні та функціональні властивості тісно пов'язані між собою. Навіть добре вивчивши закони функціонування окремих елементів, але не знаючи структури системи, не можна уявити її як єдине ціле, а отже, зрозуміти, як вона функціонує. Так само, не дізнавшись хоча б про загальні закони функціонування системи, неможливо визначити її структуру. Таким чином, аналіз функціонування і вивчення структури взаємозалежні й взаємодоповняльні. Наведемо визначення поняття структури будь-якої складної системи. Спинимося на основних структурах мереж. Повнозв'язна мережа (рисунок 1.3, а) – сполучення вузлів за принципом «кожний із кожним». У такій мережі з N вузлами кількість ребер дорівнює N(N–1)/2.

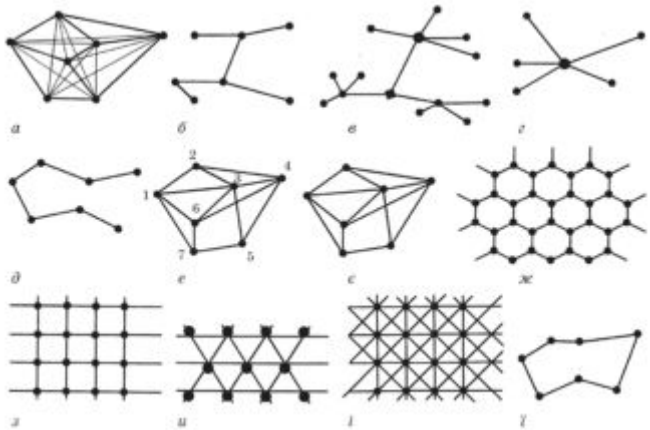


Рис.1.3. Види структур мереж

Деревоподібна рис. 1.3,*б* – між кожною парою вузлів може бути тільки один шлях. Кількість ребер у такій мережі дорівнює N–1. Частинними випадками

деревоподібної мережі є вузлова мережа рис. 1.3,*в* з ієрархічною побудовою і супідрядністю вузлів, зіркоподібна рис.1.3, *г* з одним вузлом і лінійна рис.1.3,*д*. Сітка – сіткоподібна мережа рис.1.3,*е–і*, в якій кожний вузол є суміжним тільки з невеликою кількістю інших вузлів, звичайно найближчих або таких, що мають велике тяжіння. Планарну (плоску) сітку можна зобразити на площині без перетину ребер рис. 1.3, *е*. Непланарну сітку не можна зобразити без перетину ребер (рис. 1.3, є). Частинним випадком сітки є петльова (шлейфна, кільцева) мережа рис. 1.3,*ї*, кількість ребер якої дорівнює N. Серед сіткоподібних структур можна виділити ряд «регулярних» структур із рівномірним розподілом пунктів (вузлів) за територією та однотипним з'єднанням між сусідніми вузлами. До них насамперед належать структури, у кожному пункті яких (крім розташованих по краях мережі) сходяться три ребра, «стільникова» структура, рис. 1.3,*ж*, чотири ребра «ґрати», рис. 1.3,*з*, шість рис.1.3,*и* і вісім ребер «подвійні ґрати», рис.1.3,*і*, тобто такі, ранг яких r = 3; 4; 6; 8. За великої кількості вузлів N у таких мережах кількість ребер наближено дорівнює rN/2. Реальна мережа, як правило, містить ділянки з різними структурами. Вибір структури мережі визначається насамперед економічними міркуваннями і вимогами щодо її надійності та життєздатності.

Різновиди комп'ютерних мереж. У одноранговій мережі всі комп'ютери рівноправні. Будь-який користувач мережі може отримати доступ до даних, що зберігаються на будь-якому комп'ютері і також користувачі самі вирішують, які дані на своєму комп'ютері зробити доступними по мережі. Однорангові мережі відносно прості. Оскільки кожен комп'ютер є одночасно і клієнтом і сервером, немає необхідності встановлювати могутній центральний сервер або інші компоненти, обов'язкові для складних мереж. Приклад однорангової мережі зображено на рис.1.4.

Рис.1.4 Однорангова мережа

Цим звичайно і пояснюється менша вартість однорангових мереж в порівнянні з вартістю мереж на основі сервера. В таких мережах зазвичай використовуються робочі станції (ПК) та найпростіше мережеве обладнання (концентратори і/або комутатори). Переваги однорангових мереж: - найбільш прості в установці і експлуатації; - операційні системи DOS та Windows володіють усіма необхідними функціями, що дозволяють будувати однорангову мережу.

Ієрархічні мережі. У ієрархічній мережі при побудові заздалегідь виділяються один або кілька комп'ютерів, які керують доступом користувачів до мережі, обміном даних по мережі, розподілом ресурсів та виконують безліч інших задач. Такий комп'ютер називають сервером. Будь-який комп'ютер, який має доступ до послуг сервера називають клієнтом мережі або робочою станцією. Сервер в ієрархічних мережах – це постійне сховище поділюваних ресурсів. Сам сервер може бути клієнтом тільки сервера вищого рівня ієрархії. Тому ієрархічні мережі іноді називаються мережами з виділеним сервером. Сервери звичайно являють собою високопродуктивні комп'ютери, можливо, з декількома паралельно працюючими процесорами, з вінчестерами великої місткості, з високошвидкісною мережевою картою (100 Мбіт/с і більше) та спеціальним програмним забезпеченням.

Ієрархічна модель мережі є більш кращою, тому що дозволяє створити найбільш стійку структуру мережі і більш раціонально розподілити ресурси. Також гідністю ієрархічної мережі є більш високий рівень захисту даних. Приклад такої мережі зображено на рис. 1.5.

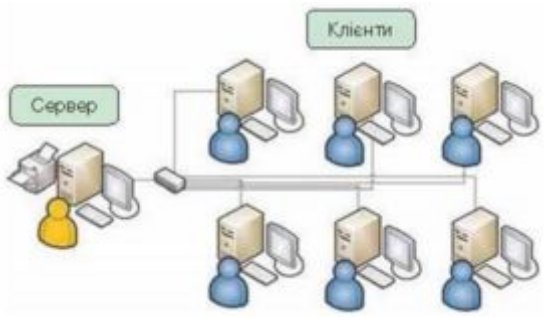


Рис. 1.5. Ієрархічна мережа

1.2 Огляд технології телекомунікаційної мережі

Технологія Ethernet. В інфокомунікаційних мережах, як правило, використовується середовище передачі даних, що розділяється, і основна роль відводиться протоколам фізичного і канального рівнів, оскільки ці рівні найбільшою мірою відображають специфіку інфокомунікаційної мережі. Тому використовуються мережеві технології – погоджений набір стандартних протоколів та програмно-апаратних засобів що їх реалізовують, достатній для побудови обчислювальної мережі. Мережеві технології також називають базовими технологіями або мережевою архітектурою інфокомунікаційної мережі. Мережева технологія або архітектура визначає топологію і метод доступу до середовища передачі даних, кабельну систему або середовище передачі даних, формат мережевих кадрів, тип кодування сигналів та швидкість передачі в інфокомунікаційній мережі.

У мережах Ethernet застосовуються топології типу «шина» і типу «пасивна зірка», а метод доступу до середовища передавання даних – «метод множинного доступу з розпізнаванням частоти-носія та виявленням колізій» (Carrier Sense Multiple Access with Collision Detection, CSMA/CD).

Завдяки тому, що кожні 5-7 років швидкість протоколів Ethernet збільшувалася в 10 разів, утворився ієрархічний ряд швидкостей Ethernet: 10 Мбіт/с (Ethernet), 100 Мбіт/с (Fast Ethernet, FE), 1 Гбіт/с (Gigabit Ethernet, GE), 10 Гбіт/с (10 Gigabit Ethernet, 10GE), і це ще не межа. Стандарти IEEE 802.x розроблялися Комітетом 802 Інституту інженерів з електротехніки та електроніки

(Institute of Electrical and Electronics Engineers, IEEE). У даних стандартах зосереджено рекомендації з проектування нижніх рівнів локальних сегментів.

Мережі Fast Ethernet і Gigabit Ethernet сумісні з мережами, виконаними за технологією (стандарту) Ethernet, тому легко і просто сполучати сегменти Ethernet, Fast Ethernet і Gigabit Ethernet в єдину обчислювальну мережу.

Особливості сімейства технологій FTTx. Архітектура побудови мереж оптичного доступу характеризується ступенем наближення оптичного мережевого терміналу до користувача. Сектор стандартизації Міжнародного Союзу Електрозв'язку (ITU-T) виділяє кілька характерних варіантів рис. 1.6.

Рис. 1.5. Архітектура побудови мереж оптичного доступу

Як видно з рис. 1.6, все архітектури FTTx (Fibertothe ...) припускають наявність ділянки з розподільними мідними кабелями, але чим він коротший, тим більше пропускна здатність мережі. Максимальне використання оптичних технологій передбачає структура FTTH, при якій оптичний мережевий термінал знаходиться в квартирі користувача і з'єднується короткими кабелями з кінцевими пристроями - телефоном, комп'ютером, телевізором і т.д. Вибір архітектури залежить від безлічі умов, і в першу чергу - від щільності розміщення абонентів. Але орієнтовно можна висловитися за застосування системи FTTB для багатоповерхових житлових будинків. Для приватної забудови або офісів, в залежності від платоспроможності замовника і його потреби в високошвидкісних додатках, більше підійде FTTC або FTTH.

Fiber To The X - поняття, описуюче загальний підхід до організації кабельної інфраструктури мережі доступу, в якій від вузла зв'язку до певного місця доходить оптичне волокно, а далі, до абонентського обладнання, - мідний кабель. Також можливий варіант прямого підключення оптичного волокна до клієнтського обладнання. Таким чином, FTTx - це фізичний рівень, але фактично це поняття охоплює велику кількість технологій канального та мережевого рівнів.

FTTx мають такі основні види архітектур:

- FTTN (Fiber to the Node) - волокно до мережевого вузла;

- FTTC (Fiber to the Curb) - волокно до мікрорайону, кварталу або групи будинків;

- FTTB (Fiber to the Building) - волокно до будинку;

- FTTH (Fiber to the Home) - волокно до житла (квартири, котеджу).

Головна відмінність в тому, наскільки близько до абонентського терміналу підходить оптичне волокно.

На сьогоднішній день проблему надання більш швидкісних та якісних послуг створює так звана “остання миля”. Але доведення оптичного волокна безпосередньо до абонента розширює можливості провайдера.

Запланований набір послуг, а саме (VoIP, швидкісний Інтернет, цифрове телебачення) та необхідна для їх надання смуга пропускання мають безпосередній вплив на вибір технології FTTx. Чим вище швидкість доступу і чим більший набір надання послуг, тим ближче до терміналу користувача повинна підходити оптика, в даній ситуації при використанні доволі ресурсоємного пакету потрібно використовувати технологію FTTH.

На рис.1.7 зображена узагальнена архітектура FTTx мережі. Через оптичний лінійний термінал (OLT) розташованому на центрально вузлі (CO), також званому головним закінченням, за допомогою оптичної розподільчої мережі (ODN) підключаються звичайна телефонна мережа та Інтернет.

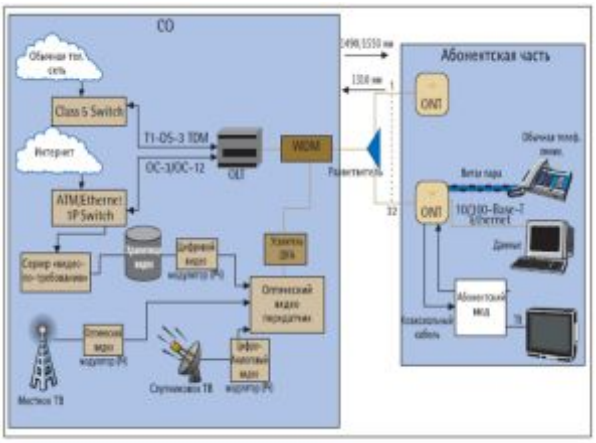


Рис. 1.7. Загальна архітектура FTTx

Для передачі даних і голосу використовуються наступні довжини хвиль: 1490 нм для прямого потоку і 1310 нм для зворотного. Послуги відео перетворюються в оптичний формат за допомогою оптичного відеопередавачі, що працює на довжині хвилі 1550 нм. Довжини хвиль 1550 нм і 1490 нм об'єднуються разом за допомогою WDM мультиплексора і передаються в прямому потоці. В даний час не планується передача відео в зворотному потоці.

В сумі три довжини хвилі (1310,1490 і 1550 нм) одночасно несуть різну інформацію в різних напрямках по одному і тому ж волокна.

Кабель живлення передає оптичний сигнал між CO та перехідником, який використовується для підключення декількох ONTк одному живить волокна. Кожному абоненту необхідний свій ONT, який забезпечує підключення різних послуг (звичайну телефонну лінію, Etherneti відео). Оскільки одна FTTx мережу зазвичай обслуговує до 32 абонентів, для обслуговування мікрорайону буде потрібно багато таких мереж, що беруть початок з одного CO.

1.3 Сучасний стан та перспективи розвитку безпроводових мереж зв’язку

Швидкі темпи розвитку технологій мобільного голосового зв'язку і високошвидкісної бездротової передачі даних змушують багатьох фахівців задуматися про перспективи використання та модернізацію нових стандартів і систем радіозв'язку. При цьому експертам і технічним фахівцям

телекомунікаційних компаній, операторам зв'язку і провайдерам послуг доводиться вирішувати складні завдання безболісного переходу до нових технологій при виконанні умов наступності і співіснування з більш старими технологіями, їх оптимального використання в інтересах операторів і користувачів.

Можливі напрямки вдосконалення і подальшого розвитку мереж зв'язку стандарту GSM в Україні, а також систем зв'язку інших стандартів, про які мова піде нижче, наведені на рис. 1.7. Тут же показані перспективи подальшого розвитку бездротового зв'язку в Україні на основі систем бездротової передачі даних і мобільного зв'язку 4G WiMAX та LTE, а також їх роль і місце в загальній структурі бездротового зв'язку в Україні та світі [9].

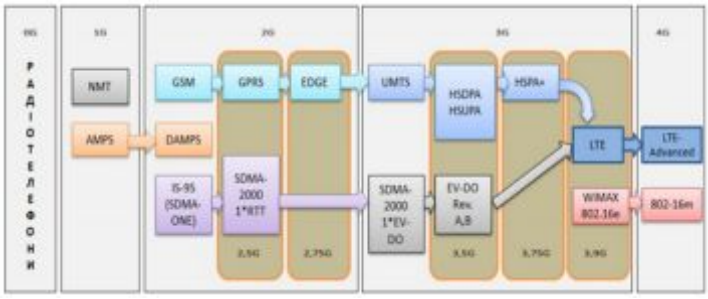


Рис. 1.7. Процес еволюції стандартів безпроводового зв'язку

Як видно з рис. 1.7 загальною тенденцією для всіх без винятку чинних українських операторів є їх поступовий перехід зі стандарту GSM на більш сучасні стандарти зв'язку 3-го і 4-го поколінь, такі як UMTS, CDMA 2000, WiMax і LTE.

На сьогоднішній день вже йде мова про появу 5G покоління мереж мобільного зв'язку. Компанія Samsung Electronics вже провела перші успішні експерименти з запуску даної технології. На даний момент зафіксована передача даних зі швидкістю 1,056 Гбіт/с на відстань до 2 км в частотному діапазоні 28 ГГц. Комерційну версія обладнання слід чекати не раніше 2022 року.

Проаналізуємо світові тенденції застосування вище описаних технологій. На сьогоднішній день 3G технологія є лідером у світовій тенденції. Але протягом

наступних 10-ти років ситуація зміниться і найбільшого розповсюдження набуде 4G технологія. А з 2021 року поступово набуватиме розповсюдження 5G.

Таблиця 1.1

Основні характеристики поколінь мобільного зв`язку

Покоління	1G	2G	2.5G	3 G	3.5G	4G
Швидкість передачі даних	1,9 Кбіт/с	14,4 Кбіт/с	284 Кбіт/с	2 Мбіт/с	3-14 Мбіт/с	1 Гбіт/с
Стандарт	NMT, TACS	CDMA, GSM	GPRS, EDGE	CDMA2000, UMTS	HSDPA	WiMax, LTE

Значно зросте кількість смартфонів і у 2020 році перевищить 5 млрд пристроїв. За прогнозами, у кінці 2020 році майже 1 млрд людей почне використовувати свої мобільні телефони для доступу до Інтернету. З загальної кількості більше ніж половину зростання складатиме Азіатсько-Тихоокеанський регіон, зокрема Китай та Індія. Проте, з огляду частки населення, в Африці спостерігатиметься стрімкіше зростання [13]. Технологія 4G за технічними характеристиками є потужнішою ніж 3G. Проте, технологія 3G продовжує розвиватися і, на сьогоднішній день, майже не поступається швидкостям 4G технології. Слід враховувати, що створення 4G мереж вимагає значного фінансування, а 3G технологія вже набула широкого розповсюдження і компаніям необхідно лише модифікувати вже створенні мережі, а не проектувати нові. Ще доволі довгий час 3G технологія зможе конкурувати з LTE мережами. Значного розповсюдження 4G технологія набуде протягом наступним 10 років та поступове перейде у 5G технологія. Більш детальна схема еволюції 4G у 5G зображена на рис. 1.8.

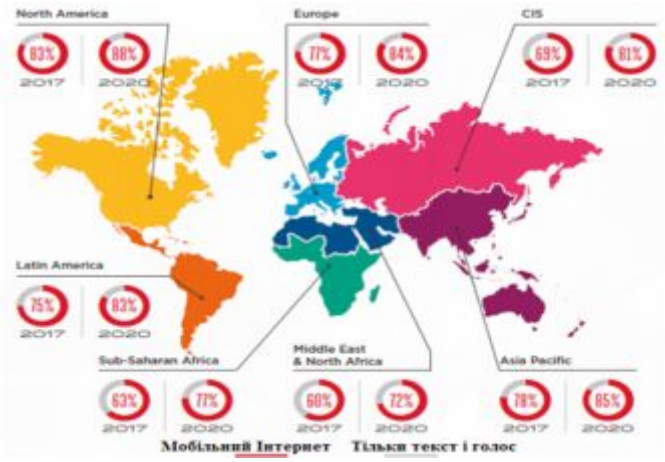


Рис. 1.8. Частка власників мобільних телефонів, які мають доступ до Інтернету

На сьогоднішній день, в Україні вже активно розвиваються мережі 4G, але також широкого розповсюдження протягом останніх років набула 3.5G технологія стандарту HSDPA. Кількість людей, що мають доступ до Інтернету в Україні постійно зростає. Якщо в 2014 році лише 47% людей мали доступ до Інтернету, то у 2019 році показник виріс до 66% [14] рис. 1.10.

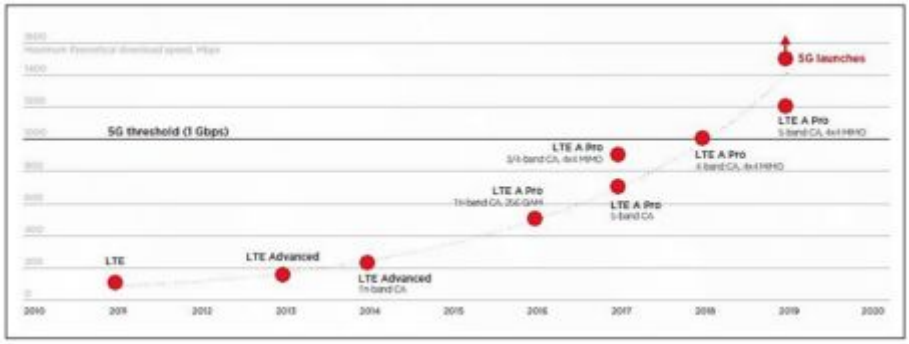


Рис. 1.9. Перехід від 4G технології до 5G

Рис.1.10. Відсоток людей, які мають доступ до Інтернету в Україні

1.4 Аналіз мереж та послуг на базі VPN

Сучасна корпоративна мережа повинна надавати набір послуг (сервісів), таких як електронна пошта, WWW, IP- телефонія, відео конференція. Якість виконання транспортних функцій мережею, забеспечуючих роботу цих телекомунікаційних служб, залежить від багатьох факторів і в першу чергу від правильної структирізації мережі, побудованої системи маршрутизації повідомлень в ній. Надійність доставки і затримка повідомлень напряму залежать від структури мережі та системи маршрутизації. На думку багатьох фахівців, VPN входить в трійку найважливіших технологій, які корпоративні користувачі збираються використовувати в найближчому майбутньому. Значимість цієї технології для будь-яких компаній, а тим більше для малобюджетних організацій, обумовлена, перш за все, тими економічним вигодами, які пов'язані з її впровадженням. Існують різноманітні способи побудови віртуальних приватних мереж [15-17]. Серед усього іншого, ці способи відрізняються розподілом функцій по підтримці VPN між корпоративною мережею і мережею загального користувача провайдера послуг VPN.

В одному випадку всі функції з підтримки VPN виконує мережу провайдера, а корпоративні клієнти тільки користуються послугами VPN.

Провайдер гарантує конфіденційність і якість обслуговування клієнтського трафіку від точки входу в мережу загального користування до точки виходу. При

цьому зусилля користувача по створенню віртуальної приватної мережі зводяться до укладення контракту з провайдером на надання VPN - послуг. Цей варіант найбільш підходить для невеликих організацій і підприємств, у яких найчастіше відсутні кваліфіковані фахівці з реалізації та підтримки VPN власними силами.

В іншому випадку підприємство організовує віртуальну приватну мережу власними силами, за рахунок застосування спеціальних VPN-продуктів в своєї мережі. В якості таких продуктів можуть використовуватися самі різні засоби: маршрутизатори та захисні екрани з додатковим програмним забезпеченням, що виконує шифрування переданих даних, а також спеціальні програмні і апаратні засоби для створення захищених каналів.

Структирізація мереж може бути фізичною і логічною. При фізичній структирізації використовують мережеві пристрої наприклад концентратори. Концентратори корисні не тільки для збільшення відстанні між взаємодіючими вузлами а і для збільшення надійності мережі. Можливості по фізичній структуризації обмежені.

Побудувати повноцінну віртуальну приватну мережу тільки силами підприємства, без участі провайдера, неможливо. Всі наявні на ринку VPN-продукти забезпечують вирішення тільки однієї з двох необхідних для імітації приватної мережі завдань, а саме, виконують захист переданих даних. Ніяких же способів підтримки заданого якості транспортного обслуговування ці продукти не надають[5].

Для сервіс-провайдерів технологія MPLS - це можливість економічною підтримки масштабованих послуг VPN в мережі IP. При цьому для захисту даних різних клієнтів використовується технологія поділу трафіку. Інжиніринг трафіку, якість послуг QoS (Quality of Service) і функції протоколу MPLS, що передбачають роботу без встановлення з'єднань (connectionless features), надають сервіс провайдерам небувалі можливості для нарощування VPN в своїй інфраструктурі без шкоди для продуктивності. якщо користувачеві потрібно забезпечити високий рівень безпеки, він може використовувати набір відповідних

протоколів (наприклад, IPSec), які дозволяють захистити дані в будь-яких каналах, де може виникати загроза несанкціонованого доступу.

Перспективність застосування технологій MPLS і VPN в мультисервісних мережах наступного покоління доводять темпи зростання даних технологій. Аналіз доходів зарубіжних сервіс-провайдерів і витрат корпоративних замовників, пов'язаних з технологією віртуальних приватних мереж, показує їх значне зростання в останні роки рис. 1.16.

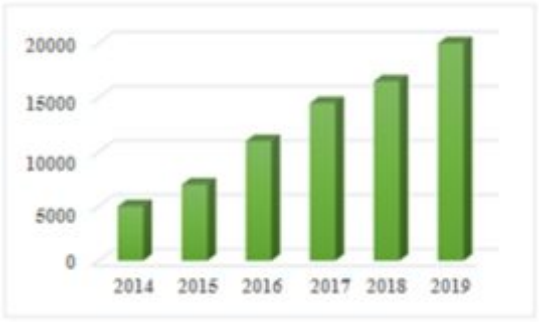


Рис.1.11. Витрати на VPN в світі (в млн. доларів США)

Компанія Cahners In-stat Group відзначає, що VPN, підтримувані провайдерами, стають самими поширеним на ринку видом послуг рис. 1.12 [18]. Кінцеві користувачі все частіше вимагають угод про гарантованій якості обслуговування SLA (Service Level Agreement), масштабованості і гнучкості мереж і широкого вибору постійно доступних послуг VPN. Все це змушує більшість компаній переходити від своїх власних віртуальних приватних мереж до мереж, які будуть експлуатуватися і обслуговуватися зовнішніми постачальниками послуг VPN.

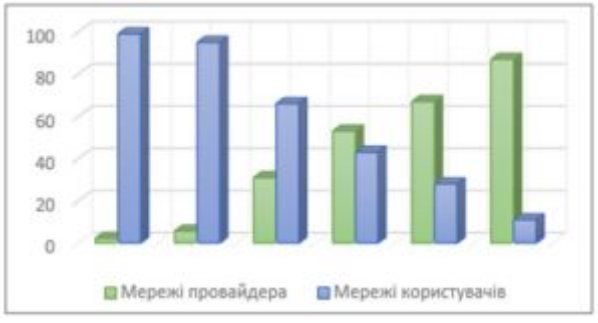


Рис. 1.12. Співвідношення VPN провайдерів і VPN які

належать користувачам (у відсотках від загальної кількості)

У недавньому минулому велика частина VPN в США була реалізована з використанням технологій ATM і Frame Relay. Однак за даними компанії Yankee Group частка технології IP для реалізації віртуальних приватних мереж зайяла майже весь ринок рис. 1.13.

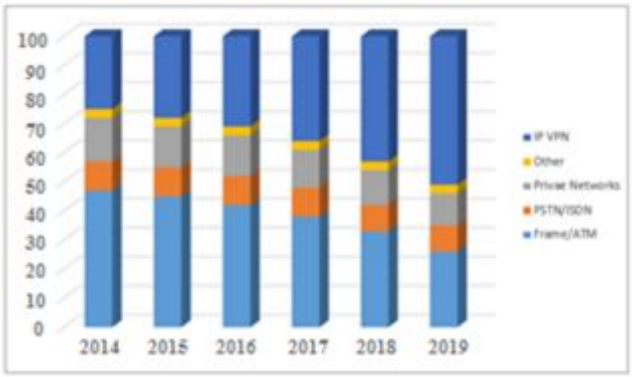


Рис. 1.13. Частка технології IP для реалізації віртуальних приватних мереж

Аналогічна ситуація спостерігається і в Україні. Якщо в 2009-2010 рр. регіональні компанії створювали мультисервісні мережі в основному на базі технології ATM (Asynchronous Transfer Mode), то сьогодні вони широко використовують технологію MPLS для надання послуг на базі протоколу IP і перш за все послуг VPN [19]. Ця технологія поступово розширює зону охоплення, і цілий ряд побудованих в Україні мереж MPLS різного масштабу показали можливість реалізації перспективних послуг в добре масштабованих і менш дорогих мережах.

Як приклад, компанія Київстар має одну з найбільш розгалужених в країні IP/MPLS-мереж з точками присутності в більш ніж 100 містах України і зарубіжжя. Основні вузли доступу розташовані в великих українських містах – Київ, Харків, Дніпро, Херсон, Одеса, Запоріжжя, Івано-Франківськ, Львів, Чернівці, Тернопіль, Луцьк і Хмельницький. IP/MPLS мережа розрахована на передачу трафіку на швидкостях до 10 Гбіт/с. У вузлах встановлені потужні

маршрутизатори, що дозволяє перевести магістральну мережу на канали 40 і 100 Гбіт/с.

Пріоритетний національний проект «Підприємство» підключає до мережі Інтернет віддалених офісів. Технічне рішення передбачає об'єднання всіх офісів в єдину віртуальну приватну мережу (VPN) «Підприємство» з організацією контрольованих точок виходу в мережу Інтернет в кожному суб'єкті, захищених міжмережевими екранами (firev/are) рис. 1.14. VPN побудована таким чином, що кожен хост повністю відкритий для всіх шкіл всіх користувачів української VPN «Підприємство». Це дозволяє легко зв'язати всі шкільні мережі в єдиний простір і організувати різні міжпідприємницькі мережеві сервіси.

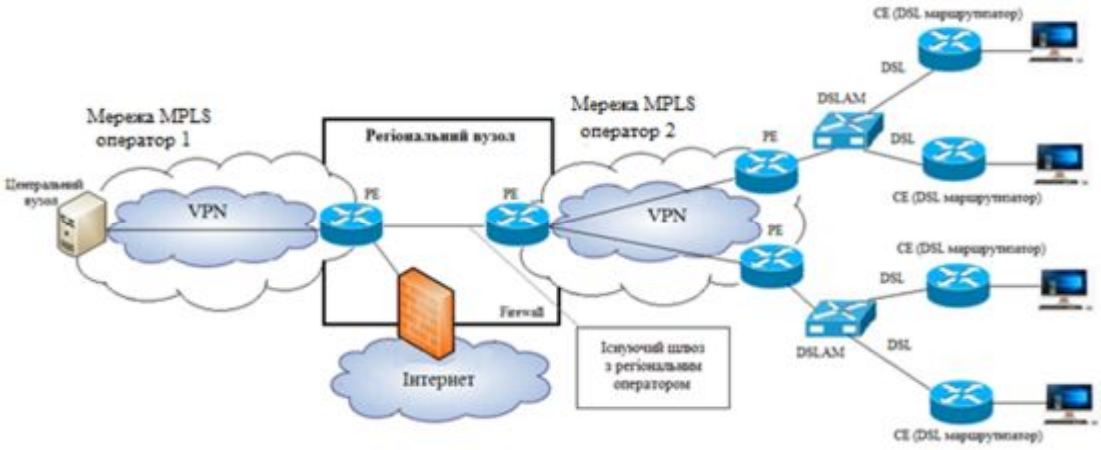


Рис. 1.14. Приклад схеми організації VPN мережі

Класифікація технологій реалізації VPN. Класифікувати VPN можна за кількома основними параметрами:

- за типом використовуваного середовища, за способом реалізації,
- за призначенням, по рівню мережевого протоколу і ін. [15].

Перш за все, всі віртуальні приватні мережі діляться на рис. 1.15:

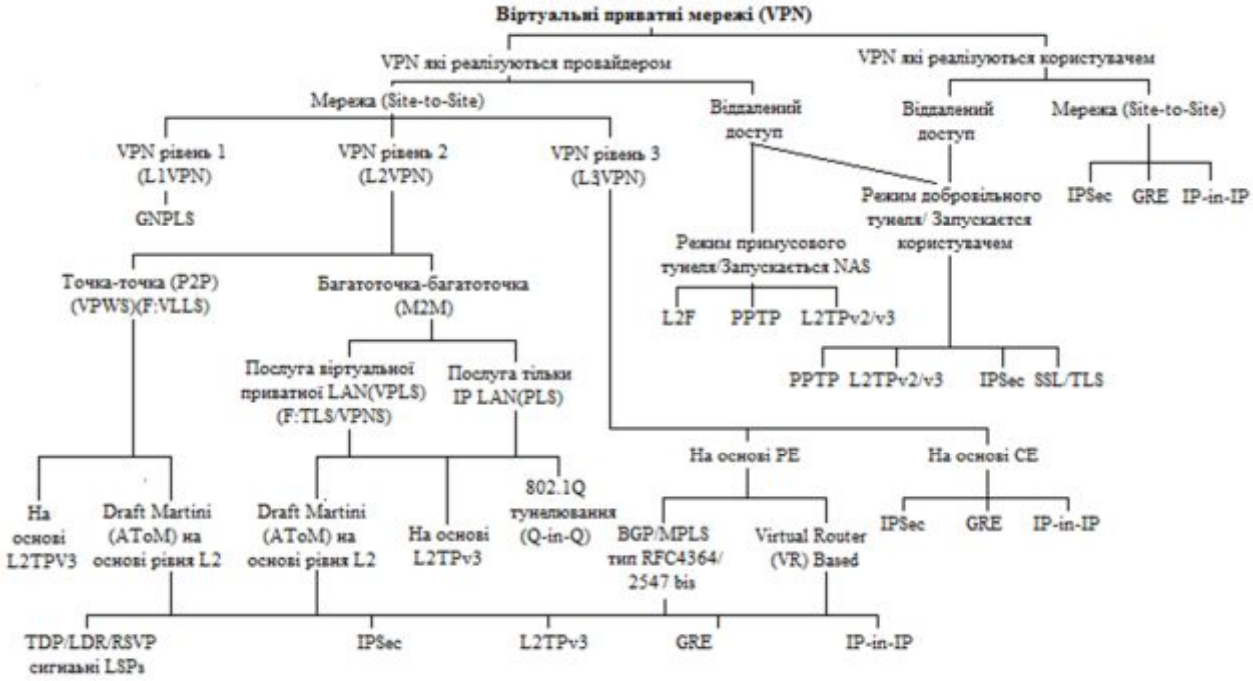


Рис. 1.15. Класифікація технологій реалізації VPN

- VPN, підтримувані обладнанням, яке встановлюється в приміщенні клієнта і служить для його підключення до магістралі сервіс-провайдера - так звані Customer - Provisioned VPN (CPVPN);

- VPN, підтримувані прикордонним обладнанням провайдера PE (Provider Edge) - так звані Provider-Provisioned VPN (PPVPN).

І ті й інші VPN в свою чергу можна розділити на два класи в залежно від характеру організації зв'язку корпоративних користувачів:

- для підключення декількох філій однієї організації в одну віртуальну приватну мережу (так звані site-to-site VPN);

- для підключення віддалених користувачів до центрального офісу або філії компанії (так звані remote access VPN).

Віртуальні мережі можуть бути реалізовані на базі протоколів моделі OSI різних рівнів:

- другого (канального) - L2VPN;

- третього (мережного) - L3VPN;

- п'ятого (сеансового) - L5VPN.

Для реалізації VPN 2-го рівня (L2VPN) можуть бути використані такі протоколи і технології:

1. Тунельний протокол 2-го рівня L2TP (Layer 2 Tunnelling Protocol) (стандарт IETF RFC 2661) - мережевий протокол тунелювання канального рівня, що поєднує в собі протокол L2F (layer 2 Forwarding), розроблений компанією Cisco, і протокол PPTP корпорації Microsoft, дозволяє організовувати VPN із заданими пріоритетами доступу, проте не містить в собі засобів шифрування і механізмів аутентифікації (для створення захищеної VPN його використовують спільно з IPSec).

2. Тунельний протокол «точка-точка» PPTP (point-to-point tunneling protocol) (стандарт IETF RFC 2637) - тунельний протокол типу «точка-точка», що дозволяє встановлювати захищене з'єднання за рахунок створення спеціального тунелю в стандартній, незахищеній мережі; фактично PPTP поміщає (інкапсулює) кадри PPP в IP-пакети для передачі по глобальної IP-мережі, наприклад Інтернет.

3. Послуга віртуальної приватної локальної мережі VPLS (Virtual Private LAN Service) - пакети локальної мережі инкапсулируются з використанням технологією MPLS, яка забезпечує створення тунелів в мережі оператора зв'язку, які є незалежними від призначеного для користувача трафіку. VPLS використовує стандарти IEEE 802.Iq і MPLS Martini-drafts для інкапсуляції пакетів і їх транспорту.

4. Послуга віртуального приватного дрота VPWS (Virtual Private Wire Service) - дозволяє організовувати прозорі з'єднання (на другому рівні OSI: 802. Iq, Frame Relay, A T M і ін.) типу «точка-точка» через мережу MPLS.

5. Традиційні VPN.

Для реалізації VPN 3-го рівня (L3VPN) можуть бути використані такі протоколи і технології:

1. Набір протоколів IPsec (IP Security) - для забезпечення захистуданих, що передаються по міжмережевому протоколу IP, дозволяє здійснювати підтвердження автентичності та/або шифрування IP-пакетів.

Більшість сучасних реалізацій IPsec засноване на стандартах IETF RFC 2401. ..2412.

2. Загальна інкапсуляція маршрутів GRE (Generic Routing Encapsulation) - протокол тунелювання мережевих пакетів, розроблений фірмою Cisco, забезпечує інкапсуляцію пакетів мережевого рівня моделі OSI в IP пакети, використовується в поєднанні з протоколом PPTP для створення віртуальних приватних мереж.

3. Комбінована технологія BGP/MPLS – протокол прикордонного шлюзу BGP (Border Gateway Protocol) служить для прокладки маршрутів через опорну мережу MPLS. Заснована на стандарті IETF RFC 4364 (раніше RFC 2547bis).

4. Віртуальна приватна маршрутизації мережу VPRN (Virtual Private Routed Network) - використовуються для створення тунелів між вузлами транзитної мережі, а не між мережами що приєднуються через транзитну мережа. При цьому маршрутизація трафіку мереж, що приєднуються здійснюється в транзитній мережі. Заснована на стандарті IETF RFC 2764.

2. АНАЛІЗ ТЕОРЕТИЧНОГО І ПРАКТИЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SSH ПРИ ПОБУДОВІ КОРПОРАТИВНОЇ МЕРЕЖІ

SSH є технологією, яка призначена для віддаленого виконання команд, а також для входу через мережу на інший комп'ютер. Використовуючи SSH можна завантажувати і копіювати файли між комп'ютерами, але частіше за все вона використовується для безпечної передачі файлів сайту між вашим комп'ютером і сервером хостинг-провайдера. Secure Shell - так розшифровується абревіатура SSH. Завдяки використанню цієї технології досягається надійна авторизація та безпечна передача інформації по відкритих каналах зв'язку. SSH успішно замінює такі протоколи, як telnet, rlogin, rcp і rsh. Оскільки застосування перерахованих технологій пов'язано з деякими проблемами безпеки. Також авторизація з використанням IP-адрес (rlogin) і паролів (telnet і FTP) дуже вразлива з точки зору безпеки. SSH відмінно справляється з перерахованими вище завданнями. Навіть з огляду на те, що вхід в інший комп'ютер здійснюється за допомогою введення пароля. Цей пароль не може бути перехоплений, так як його передача здійснюється в зашифрованому вигляді.

Рис.2.1. Схема організації передачі даних з використанням технології SSH

2.1 Дослідження принципів роботи SSH-тунелю

SSH-тунелі створюються для вирішення 2-х незалежних завдань:

1. Забезпечення конфіденційності даних, що передаються по захищеному каналу

2. Створення сполучного мосту (або декількох мостів) між клієнтом і сервером через проміжні комп'ютери, так як клієнт може не мати прямого доступу до сервера. В цьому випадку конфіденційність є другорядною або зовсім не потрібно.

SSH-тунелі можуть бути організовані як в режимі перенаправлення окремих TCP-портів (Port forwarding), так і в режимі справжніх VPN-тунелів через віртуальні інтерфейси, коли передаватися може трафік будь-яких протоколів і з будь-яких портів. У даному розділі мною було розглянуто перший режим.

При роботі в режимі Port Forwarding пакет, що надходить на вхідний порт тунелю, повинен бути переданий в незмінному вигляді на його вихідний порт. Така схема застосовується в роботі інтернет-шлюзів: пакети з одного інтерфейсу передаються на інший без зміни і аналізу.

Таким чином, SSH-канал в цьому режимі з усією його інфраструктурою нагадує віртуальний шлюз з вхідним і вихідним інтерфейсами, але тільки за конкретною парі TCP-портів:

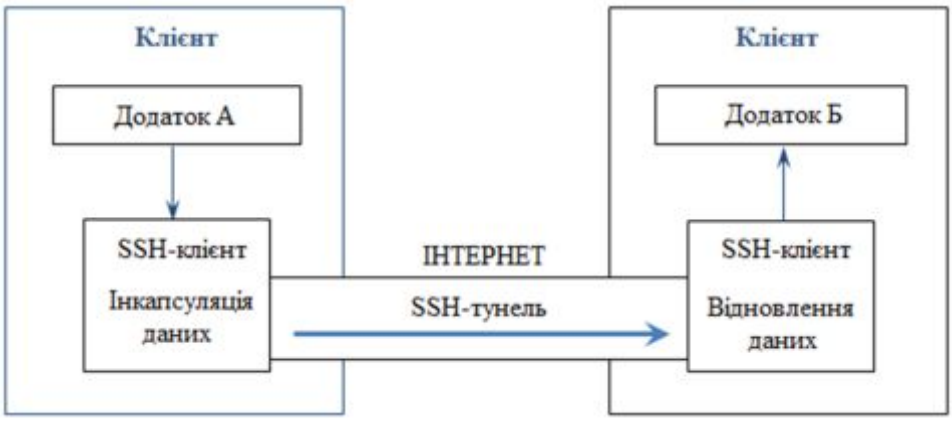


Рис.2.2. Схема організації з`єднання клієнт/сервер

Стрілкою зазначений напрямок ініціювання SSH-сесії. В даному випадку ініціатором з'єднання виступає Клієнт з встановленим на ньому PuTTY. Наведена вище схема є базовою, в якій взаємодіють лише 2 учасника клієнт і сервер. На

практиці ж між клієнтом і сервером може бути кілька проміжних хостів. І до потрапляння на вхід конкретного тунелю і після виходу з нього пакети можуть передаватися по незахищеним каналам.Для встановлення зв'язку з SSH-протоколу буде потрібен обліковий запис на SSH-сервері, яка може бути будь-який, в тому числі без яких би то не було прав і навіть без шелла, якщо ви відкриваєте на прослуховування непрівелігірованние порти від 1024 і вище. В іншому випадку необхідний рутовий доступ і значення директиви PermitRootLogin рівне yes або without-password.

Аналіз зв'язності і доступності учасників взаємодії. Приступаючи до вирішення завдання про те, як забезпечити доступ клієнта на сервер, корисно побудувати схему зв'язності учасників взаємодії по SSH-протоколу, оскільки саме з цього протоколу створюються тунелі, через які потім можна пропустити дані будь-якого іншого протоколу. Розглянемо ці кроки на базі розширеної схеми, що складається з Клієнта, проміжного Проксі-сервера і Сервера. На практиці такі схеми зустрічаються найчастіше. Якщо з'єднувати стрілками машини, доступні за SSH-протоколу, то можливі наступні варіанти, рис.2.3.

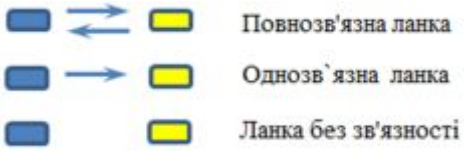


Рис.2.3. Схему зв'язності учасників взаємодії по SSH-протоколу

Зокрема, ми з'єднуємо стрілкою клієнта з проксі, якщо проксі доступний з клієнта на 22-му порту. Перебравши попарно всіх учасників взаємодії, отримаємо схему зв'язності. Наприклад, рис.2.4.

Рис. 2.4. Схему зв'язності

Стрілки схеми зв'язності показують, звідки може бути ініційований тунель на машину з SSH-сервером.

Після побудови схеми зв'язності необхідно переконатися в доступності учасників взаємодії один для одного з довільним протоколам і портам, оскільки до створеного тунелю потрібно якось підключатися, або, навпаки переправляти дані далі. Іншими словами, необхідно перевірити пінгуються вони чи ні. За аналогією зі схемою зв'язності можна побудувати схему доступності, яка як мінімум збігається зі схемою зв'язності, але частіше за все ширше її, рис.2.5.

Рис. 2.5. Схема доступності

Схема доступності показує, в якому напрямку можна передати дані по незахищених тунелем каналу.

Комбінація обох схем допомагає відповісти на питання про те, чи є принципова можливість встановлення з'єднання клієнта з сервером, а якщо її немає, то що треба додати, щоб її отримати.

Рис.2.6. Комбінація обох схем

Надалі ми будемо використовувати цими схемами для побудови каналу зв'язку.

Наведена вище схема дуже поширена: клієнт і сервер (найчастіше на базі Windows) знаходяться в різних локальних мережах за NAT, мають вихід в інтернет і «бачать» віддалений проксі-сервер, тоді як з проксі вони недоступні ні

по SSH ні по інших протоколах . На проксі, як правило, встановлена Nix-подібна операційна система, в якій SSH-сервер є за замовчуванням.

У схемах на базі Nix систем практично всі ланки повнозв'язні, оскільки на всіх машинах є SSH-сервери, а SSH-порти зазвичай відкриті для підключень.

Далі стрілка SSH-зв'язності вказуватися не буде, так як збігаються з напрямом ініціювання тунелю.

2.2 Алгоритм побудови каналу зв'язку за допомогою SSH-тунелів

Розберемо алгоритм побудови каналу зв'язку за допомогою SSH-тунелю на прикладі схеми, наведеної вище, де Клієнт і Сервер знаходяться в різних локальних мережах за NAT-ами, і можуть бути пов'язані тільки через Інтернет за допомогою деякого Проксі-сервера.

1. Складання схеми SSH-зв'язності.

SSH-сервер у нас є тільки на Проксі, тому ми можемо ініціювати 2 тунелі: з клієнта і з сервера, рис.2.7.

Рис. 2.7. Складання схеми SSH-зв'язності

Це схема з двома однозв'язного ланками.

2. Складання схеми доступності.

Клієнт і Сервер знаходяться за NAT, тому недоступні ззовні з Проксі, але проксі пінгується як з клієнта, так і з сервера, рис.2.8.

Рис. 2.8. Складання схеми доступності

3. Вибір ланки для створення тунелю.

Для забезпечення зв'язку між клієнтом і сервером досить одного тунелю - або клієнт-проксі, або проксі-клієнт, так як на що залишився ділянці пакети можна передати по незахищених каналу.

Тунель клієнт-проксі виглядає краще, оскільки в такому випадку всі операції по організації зв'язку ми змогли б зробити з клієнта, і з нього ж за умовами завдання потрібно працювати з сервером.

Пакети, що надходять на вхід тунелю на комп'ютері Клієнта, передаються на Проксі і потім повинні перенаправлятися на адресу призначення (Destination), яким є сервер. Однак згідно зі схемою доступності, сервер недоступний з проксі через інтернет, рис.2.9.

Рис. 2.9. Вибір ланки для створення тунелю

Тому для передачі пакетів не обійтися без створення другого тунелю між проксі і сервером, рис.2.10.

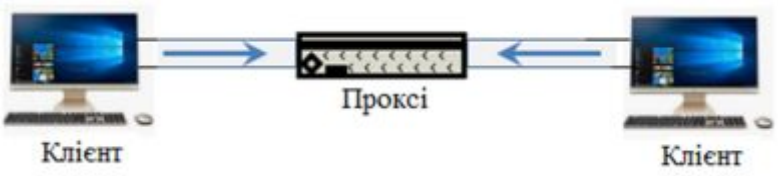


Рис. 2.10. Створення другого тунелю між проксі і сервером

А ось перший тунель, на який ми сподівалися, буде в такій схемі надлишковий - ми можемо направляти пакети з клієнта на проксі через незахищену середу безпосередньо без використання тунелю:

Рис. 2.11. Направляти пакету через незахищену середу

Тунель Клієнт-Проксі можна залишити лише в тому випадку, якщо це важливо з точки зору конфіденційності (по ньому щось передається відкритим текстом і т.п.).

4. Вибір типу тунелю Проксі-Сервер: прямий або зворотний.

Насправді тип тунелю вже визначений. Запити клієнта надходять на порт джерела (Source Port), який знаходиться на Проксі, а тунель ініціюється з Сервера. Це означає, що напрямок ініціювання тунелю і запитів клієнта будуть протилежні. Отже тунель буде зворотним (опція -R).

5. Прописування параметрів підключення і створення тунелю.

Таким чином, вимальовується наступний алгоритм побудови каналу зв'язку:

- скласти схему SSH-зв'язності, виходячи з розташування SSH-серверів;

- скласти схему доступності;

- вибрати ланка: Клієнт-Проксі або Проксі-Сервер (для розширеної схеми) ;

- вибрати напрямок ініціювання тунелю, якщо ланка повнозв'язну;

- вибрати тип тунелю, відштовхуючись від направлення запитів клієнта: прямий або зворотний;

- написати формули пробросу портів в PuTTY (Source port, Destination і додаткові опції) для кожного тунелю.

Розуміючи описані вище принципи, легко виставити правильні настройки як на вкладці SSH-Tunnels в PuTTY, так і в командному рядку OpenSSH-клієнта. Зокрема, справедливі наступні аксіоми:

- Source port - це порт тунелю, на який надходять запити Клієнта.

Якщо напрямок ініціювання тунелю і запитів Клієнта збігаються (прямий тунель), то порт знаходиться на тому ж кінці, що і PuTTY і є для PuTTY локальним (опція -L, Local). На відміну від петлевого IP-адреси на вході тунелю,

дані на виході з тунелю можуть передаватися куди завгодно, в тому числі на хости з іншими IP-адресами.

Цього достатньо, щоб виставити правильні настройки для всіх варіантів SSH-тунелів. Найбільш типові з них представлені далі на конкретних прикладах.

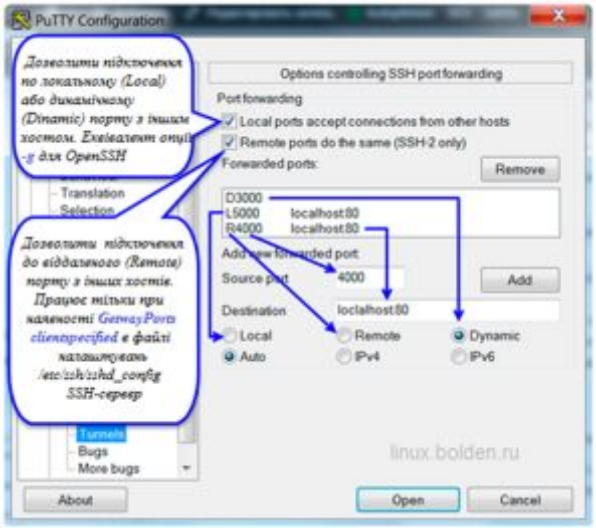


Рис. 2.12. Приклад налаштування організації підключення

Приведемо, також, синтаксис командного рядка OpenSSH клієнта в термінах PuTTY, якщо ви захочете ініціювати тунель з якою-небудь Nix-системи за базовою схемою:

```
ssh [-g] [-p port] [Source port]:[Destination] user@Сервер
```

і за розширеною схемою:

```
ssh [-g] [-p port] [Source port]:[Destination] user@Прокси
```

Тут під [Source port] розуміється порт з ключами, наприклад: -L 5000 (прямий тунель), -R 5000 (зворотний тунель) або -D 5000 (динамічний кидок порту; в цьому випадку [Destination] опускається)

[-p port] - з'єднатися з сервером або Проксі на порт, відмінний від 22.

[-g] - опція, що дозволяє підключення до локального (Local) або динамічному (Dynamic) порту не тільки з localhost, а й з зовнішніх адрес.

Для вирішення аналогічної можливості підключення до віддаленого (Remote) порту з зовнішніх адрес необхідно прописати в файлі конфігурації SSH-сервера / etc / ssh / sshd_config опцію:

```
GatewayPorts clientspecified
```

завдяки якій включення цієї можливості проводиться за запитом клієнта, або

```
GatewayPorts yes
```

коли ця опція включена завжди.

Базова схема взаємодії. У базовій схемі взаємодії беруть участь лише 2 комп'ютери, з'єднані тунелем.

За цією схемою можливі 2 види тунелів - прямий і зворотний, в залежності від того, з якого боку виконується ініціювання SSH-сесії. Згідно з цим, PuTTY завжди знаходиться на тому кінці тунелю, де стрілка починається.

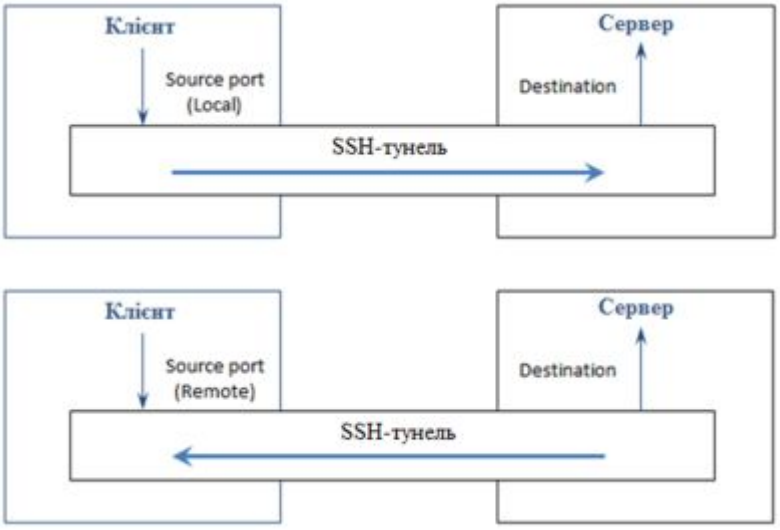


Рис. 2.13. Можливі види тунелів

Розширена схема взаємодії. Розширенням базової схеми є схема з проміжним проксі-сервером, до якого або підключається Клієнт, або з якого встановлюється з'єднання з сервером. Тут можливі 4 варіанти.

В принципі, всі чотири варіанти розширеної схеми рівноправні, якщо абстрагуватися від конкретної реалізації SSH-клієнта. Але якщо ми розглядаємо

роботу через PuTTY, то ініціювати тунелі ми можемо тільки з машин на базі Windows, тобто найчастіше або від клієнта, або від сервера.

Ситуації, в яких SSH-сесія за допомогою PuTTY ініціюється з проміжного сервера, досить рідкісні, так як проксі-сервери зазвичай являють собою машини без графічної оболонки під управлінням Nix-подібних ОС, і замість PuTTY там буде OpenSSH.

Для повноти картини нижче розглянуто і синтаксис OpenSSH клієнта в термінах PuTTY, якщо раптом вам знадобиться ініціювати тунель за допомогою OpenSSH.

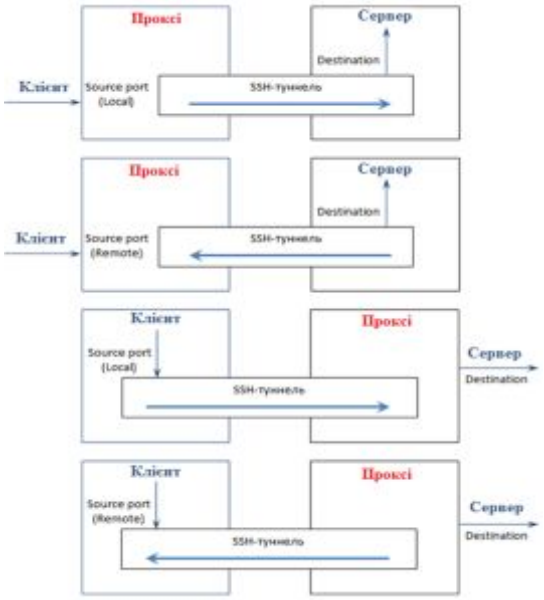


Рис. 2.14. Розширена схема взаємодії

2.3 Практичні приклади застосування SSH-тунелів

Прямий тунель за базовою схемою. Схема зв'язності і доступності системи клієнт/NAT.

Рис.2.15. Схема зв'язності і доступності системи клієнт/NAT

Розглянемо захист відкритого протоколу від перехоплення на прикладі POP3.

Замість того, щоб отримувати пошту на локальному комп'ютері безпосередньо через інтернет і піддавати себе ризику втрати пароля, переданого у відкритому вигляді, ми отримуємо її через тунель з поштовим сервером на порт 110. Поштовий клієнт в даному випадку повинен бути налаштований на отримання листів з адреси localhost:5000

Схема наведена в ілюстративних цілях, оскільки всі поштові клієнти зараз вміють працювати за захищеними протоколам, а вибір портів строго обмежений.

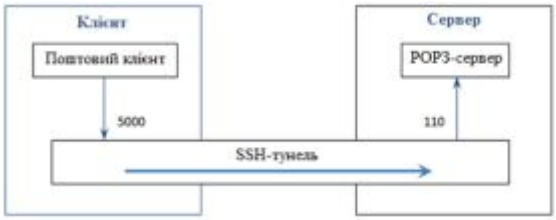


Рис.2.16. Схема взаємодії

Рис. 2.17. Налаштування організації підключення

Еквівалентна команда для OpenSSH клієнта:

```
Клиент# ssh -L 5000:Сервер:110 user@Сервер
```

Зворотний тунель за базовою схемою. Схема зв'язності і доступності для системи сервер/NAT, рис.2.18.

Рис.2.18 Схема зв'язності і доступності для системи сервер/NAT

Це той випадок, коли вам по локальній мережі потрібно зайти з одного комп'ютера (клієнт) на інший (сервер), але прямого з'єднання з ним не передбачено. Однак, з сервера доступ до клієнта є. Для цього SSH-сесія ініціюється з сервера, тобто з комп'ютера, до якого ми хочемо підключитися. В результаті створюється зворотний тунель.

Для підняття зворотного тунелю на клієнта необхідно встановити SSH-сервер і вказати, з якого віддаленого порту (Remote Source port) на який локальний для PuTTY буде виконуватися кидок.

Рис.2.19 - Схема взаємодії

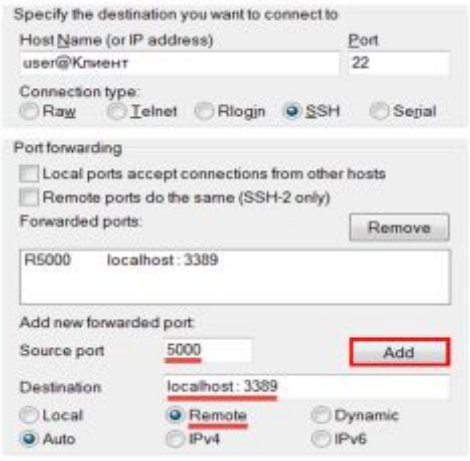


Рис.2.20. Налаштування організації підключення

Еквівалентна команда для OpenSSH клієнта:

```
Сервер# ssh -R 5000:localhost:3389 user@Клиент
```

Прямий тунель на SOCKS proxy. Схема зв'язності і доступності для системи клієнт – NAT, рис.2.21.

Рис. 2.21. Схема зв'язності і доступності для системи Клієнт - NAT

Така схема дозволяє безпечно підключатися до інтернету через неперевірені джерела, наприклад Wi-Fi точки доступу в кафе і ресторанах. Весь трафік йде через точку доступу в зашифрованому вигляді з віддаленого Сервера.

Як відомо, браузер надсилає запити до сайтів в інтернет з довільних портів WAN-інтерфейсу комп'ютера. У PuTTY такий режим передбачений в у вигляді опції Dynamic. Всі запити браузера через тунель спрямовуються з деякого вихідного порту 5000 на комп'ютері з SSH-клієнтом, а на іншому кінці призначаються динамічно. Тому кінцевий порт не прописується.

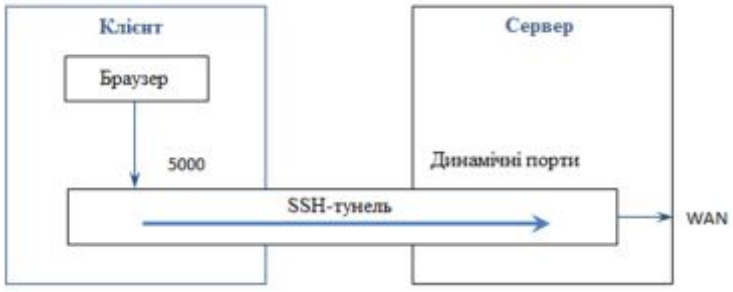


Рис. 2.22. Схема взаємодії

Оскільки браузери не вміють працювати через SSH-тунелі безпосередньо, в установках з'єднання через проксі-сервер потрібно вибрати підключення через

SOCKS (v5) на адресу localhost: 5000 і видалити localhost або 127.0.0.1 з поля «Не використовувати проксі для:", якщо він там прописаний автоматично.

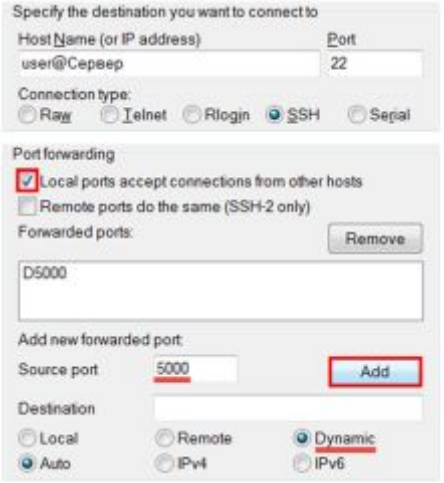


Рис. 2.23. Налаштування підключення

Еквівалентна команда для OpenSSH клієнта:

```
Клиент# ssh -D 5000 user@Сервер
```

Додаючи опцію -g, яка еквівалентна опції PuTTY «Local ports accept connections from other hosts», можна дозволити іншим комп'ютерам підключатися до Клієнта на зазначений порт і перетворити його, таким чином, в точку доступу.

Зворотний тунель на SOCKS Proxy. Схема аналогічна попередній, тільки зі зворотним схемою зв'язності (клієнту заборонений вихід в інтернет).

Рис. 2.24. Схема зв'язності і доступності для системи Клієнт – NAT зі зворотним схемою зв'язності

Це означає, що ініціювати тунель ми можемо тільки з сервера. Очевидно, що на Клієнта повинен бути розгорнутий SSH-сервер. Для клієнтів на базі

Windows хорошим вибором буде Bitvise SSH-сервер на 443 порту. FreeSSHd сервер із зворотними тунелями при практичному дослідженні не заробив..

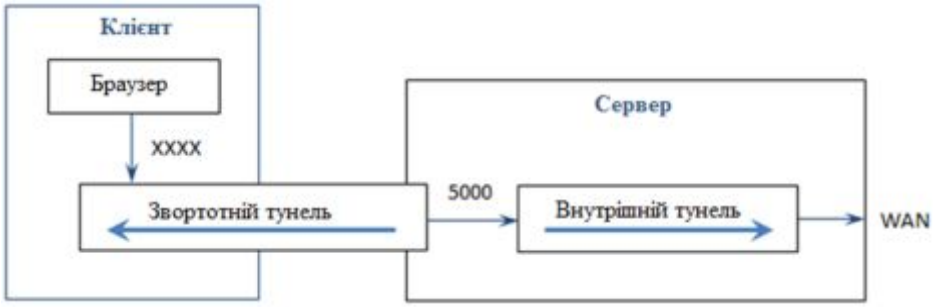


Рис.2.25. Схема взаємодії

Отже, щоб схема працювала, потрібно зробити з сервера Socks proxy на 5000-му порту, створивши тунель з самим собою:

```
Сервер# ssh -D 5000 user@Сервер
```

А після цього встановити зворотний тунель з клієнтом, в якому запити на порт XXXX перенаправляються на 5000 порт нашого Socks proxy:

```
Сервер# ssh -R XXXX:localhost:5000 user@Клиент
```

Особливість такої схеми в тому, що зворотні тунелі по ланцюжку можна прокидати і далі на інші комп'ютери, що не мають доступу в інтернет.

Ця ідея лежить в основі аналогічної схеми з даної статті, але в ній тунель ініціюється в зворотному напрямку виразом такого вигляду:

```
Прокси# ssh -D 5000 -R XXXX:localhost:5000 user@Сервер
```

А вже потім до Сервера за допомогою зворотного тунелю підключається комп'ютер, який не має доступу в інтернет:

```
Прокси# ssh -D 5000 -R XXXX:localhost:5000 user@Сервер
```

Однак в даному випадку інтернет-запит на порт Сервера XXXX по зворотному тунелю перенаправляється на комп'ютер, який грає роль Проксі-сервера, а потім повертається на сервер, щоб бути обслужених на ньому ж:

```
Сервер# ssh -R YYYY:localhost:XXXX user@Компьютер
```

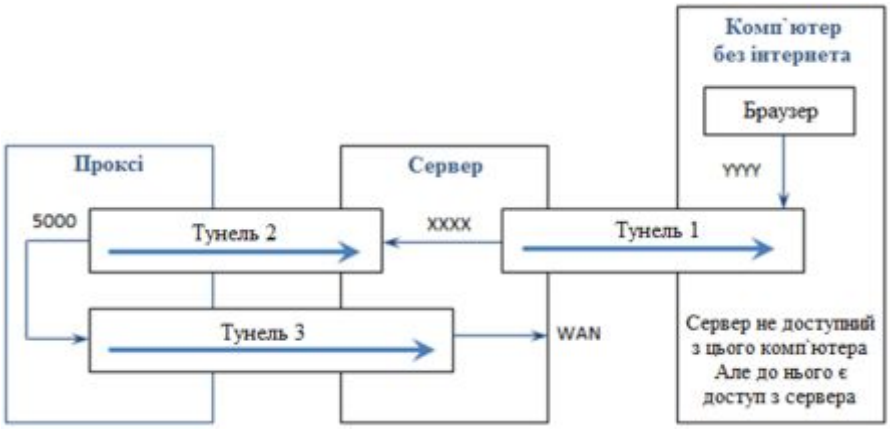


Рис. 2.26. Схема взаємодії

Очевидно, що в такому способі використовується зайва петля, що складається з Тунелів 2 і 3, яку ми виключили вище, організувавши роздачу інтернету безпосередньо з самого Сервера.

Прямий тунель на проміжний SSH-сервер. В даному випадку тунель створюється з проміжним проксі-сервером, а вже з нього виконується підключення до кінцевого віддаленого серверу. Така схема виручає тоді, коли з локального комп'ютера немає прямого доступу в інтернет, але є доступ до деякого сервера всередині локальної мережі, який підключений до інтернет. Приклад схеми зв'язності і доступності для випадку, коли клієнт і проксі знаходяться за NAT, а сервер доступний з Інтернету, рис.2.27.

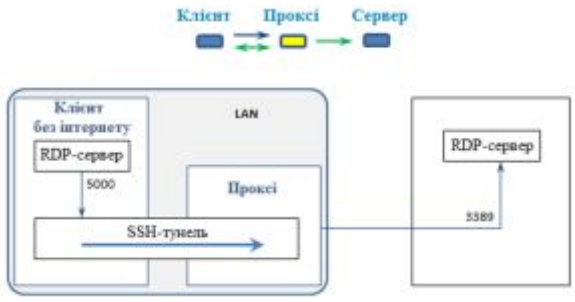


Рис.2.27. Приклад схеми зв'язності і доступності для випадку, коли клієнт і проксі знаходяться за NAT, а сервер доступний з Інтернету

В іншому випадку Сервер знаходиться у віддаленій локальної мережі і недоступний з інтернету безпосередньо, але до нього можна підключитися через

проміжний Проксі в тій же локальній мережі. Можлива схема зв'язності і доступності для випадку, коли проксі є шлюзом, а клієнт розташований за NAT у власній LAN, рис.2.28.

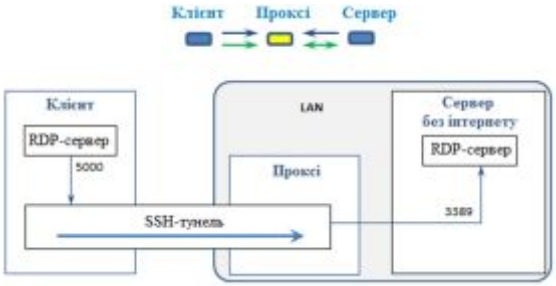


Рис. 2.28. Схема зв'язності і доступності для випадку, коли проксі є шлюзом, а клієнт розташований за NAT у власній LAN

В обох випадках Клієнтові потрібно підключитися на адресу localhost: 5000.

Рис. 2.29. Налаштування підключення

Еквівалентна команда для OpenSSH клієнта:

```
Клиент# ssh -L 5000:Сервер:3389 user@Прокси
```

Зворотний тунель на проміжний SSH-сервер. Ця схема вже детально розглядалася в самому початку, рис.2.30.

Рис. 2.30. Схема зв`язаності

В даному випадку нам потрібно зайти з домашнього комп'ютера на віддалений, до якого немає доступу з Інтернет, але є проміжний Проксі, доступний як для клієнта, так і для сервера. Ми з'ясували, що зв'язок можна налагодити лише з допомогою зворотного тунелю Сервера з Проксі.

Для вирішення віддаленого підключення клієнта необхідно також відзначити опцію [Remote ports do the same]. Ця опція працює тільки в тому випадку, коли дозвіл на підключення на віддалений порт за запитом клієнта дозволено в файлі конфігурації ssh-демона Проксі-сервера /etc/ssh/sshd_conf:

|*GetewayPorts clientspecified*

Після цього сервер повинен стати доступним з клієнта по RDP на адресу Проксі:5000

Рис. 2.31. Схема взаємодії

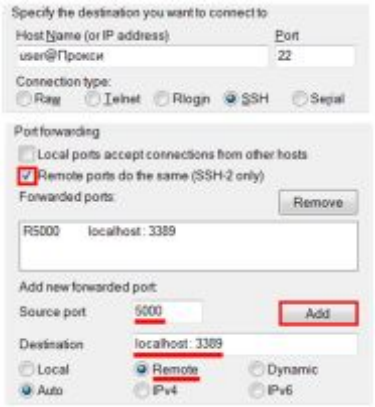


Рис. 2.32. Налаштування підключення

Еквівалентна команда для OpenSSH клієнта:

```
Сервер# ssh -R 5000:localhost:3389 user@Прокси
```

3 ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ VPN В КОРПОРАТИВНУ МЕРЕЖА ТА ЇХ ПОРІВНЯЛЬНА ОЦІНКА

3.1 Реалізація корпоративної мережі на основі технології OpenVPN

Для наглядного прикладу об'єднаємо в одну корпоративну мережу офіс, склад і наші сервера у провайдера. Для цього нам потрібно побудувати захищені канали - тунелі тільки між маршрутизаторами, так як немає необхідності підключати кожен комп'ютер окремо.

Отже: є 3 маршрутизатора під управлінням ОС CentOs. Перекидання пакетів з Інтернету в мережу і назад здійснюється за допомогою технології NAT і правил iptables.

Дамо для зручності маршрутизаторів імена: В офісі: Office; На складі: Sklad; Колокація (сервера у провайдера): Colo; Магазин №1: mag1; Магазин №2: mag2; Мережеві налаштування маршрутизаторів:

Таблиця 3.1

Налаштування маршрутизатору Office

Мережа	Інтерфейс	IP адреса	Маска	Шлюз
Інтернет	eth2	213.182.175.230	255.255.255.252	213.182.175.229
Локальна	eth1	192.168.53.250	255.255.255.0	-

Таблиця 3.2

Налаштування маршрутизатору Sklad

Мережа	Інтерфейс	IP адреса	Маска	Шлюз
Інтернет	eth2	79.142.87.206	255.255.255.252	79.142.87.211
Локальна	eth1	192.168.0.1	255.255.255.0	-

Таблиця 3.3

Налаштування маршрутизатору Colo

Мережа	Інтерфейс	IP адреса	Маска	Шлюз
Інтернет	eth2	195.2.240.68	255.255.255.252	195.2.240.60
Локальна	eth1	172.16.100.8	255.255.255.0	-

Налаштування hardware маршрутизаторів в магазинах не грають ролі, тому їх пропустимо.

Приступимо до встановлення та налаштування.

CentOS (Community ENTerprise Operating System) - дистрибутив Linux, заснований на комерційному Red Hat Enterprise Linux компанії Red Hat і сумісний з ним. CentOS використовує програму yum для скачування і установки оновлень з репозиторіїв. Вся робота по налаштуванню і установці виробляється віддалено, використовуючи OpenSSH сервер на маршрутизаторах і клієнт putty.

Налаштуємо першим маршрутизатор Colo. Цей маршрутизатор буде виступати в ролі OpenVPN сервера.

Пакет OpenVPN не доступний в стандартному репозиторії, тому підключаємо додатковий репозиторій rpmforge:

colo> rpm -Uhv

http://apt.sw.be/redhat/el5/en/x86_64/rpmforge/RPMS//rpmforge-release-0.3.6-1.el5.rf.x86_64.rpm

Ця команда завантажує rpm пакет сховища та встановлює його.

Тепер нам став доступний пакет OpenVPN, встановлюємо його:

colo> yum install openvpn

OpenVPN встановлений. Далі потрібно згенерувати кореневий сертифікат сервера, сертифікати та ключі клієнтів, сертифікат і ключ сервера, tls ключ.

Для цього переходимо в конфігураційний каталог OpenVPN і створюємо каталог під наші майбутні ключі і каталог під конфігураційні файли клієнтів:

colo> cd /etc/openvpn

colo> mkdir keys

colo> mkdir ccd

Завантажуємо змінні для генерації ключів в пам'ять і починаємо генерувати сертифікат авторизації:

colo>./vars

colo>./build-ca

Generating a 1024 bit RSA private key

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

 # Країна
Country Name (2 letter code) [US]:RU
 # Провінція
State or Province Name (full name) [CA]:SPB
 # Місто
Locality Name (eg, city) [SanFrancisco]:SPB
 # Назва фірми
Oganization Name (eg, company) [Fort-Funston]:server
 # Відділення фірми
Organizational Unit Name (eg, section) []:server
 # Ім`я сервера OpenVPN
Common Name (eg, your name or your server's hostname) [Fort-Funston
CA]:server
Name []:server
Email Address [me@myhost.mydomain]:
Створюємо сертифікат X.509 для сервера:
colo> ./build-key-server server
 # Країна
Country Name (2 letter code) [US]: RU
 # Провінція
State or Province Name (full name) [CA]:SPB
 # Місто
Locality Name (eg, city) [SanFrancisco]: SPB

 # Назва компанії

Organization Name (eg, company) [x]:server

 # Відділ компанії

Organizational Unit Name (eg, section) []:server

 # Ім`я сервера OpenVPN

Common Name (eg, your name or your server's hostname) []:server

 # Поштова адреса

Email Address [root@localhost]:

Please enter the following 'extra' attributes

to be sent with your certificate request

 # Пароль

A challenge password []:123456789

 # Назва організації

An optional company name []:server

Далі постане питання про підписуванні сертифіката, погоджуємося.

Створюємо ключ для office:

colo> ./build-key-server office

Generating a 1024 bit RSA private key

.....++++++

.....++++++

writing new private key to 'client.key'

Таким же способом, створюємо ключі для складу і двох магазинів.

Створюємо ключ Діффі Хельман для обміну ключами по незахищеному каналу:

colo> ./build-dh

Створюємо ключ для tls-аутентифікації:

colo> openvpn --genkey --secret keys/ta.key

Після всіх цих маніпуляцій в каталозі keys/з'являються такі файли:

- ca.crt - Головний CA сертифікат, цей файл потрібен і клієнту і серверу;

- dh1024.pem - ключ Діффі Хельман, цей файл потрібен тільки серверу;

- server.crt - Сертифікат сервера, потрібен тільки серверу;

- server.key - Ключ сервера, потрібен тільки сервера (секретний файл);

- office.crt, sklad.crt, mag1.crt, mag2.crt - Сертифікати клієнтів, потрібні тільки відповідним клієнтам;

- office.key, sklad.key, mag1.key, mag2.key - Ключі клієнтів, потрібні тільки відповідним клієнтам (секретні файли);

- ta.key - TLS-ключ, потрібен і клієнтам і сервера.

Отже, на сервері залишаються файли ca.crt, dh1024.pem, server.crt, server.key, ta.key, а клієнтам віддаються ca.crt, dh1024.pem і їх ключі з сертифікатами.

На цьому операції з генерацією ключів і сертифікатів закінчені, переходимо до налаштування сервера і клієнтів. Створюємо конфігураційний файл server.conf наступного вмісту.

Створюємо файли з настройками для клієнтів. У каталозі / etc / openvpn / ccd на сервері створюємо файл office, sklad, mag1, mag2 (ім'я файлу - ім'я якій видано сертифікат) такого змісту:

office

ifconfig-push 10.10.200.2 10.10.200.1

iroute 192.168.53.0 255.255.255.0

sklad

ifconfig-push 10.10.200.3 10.10.200.1

iroute 192.168.53.0 255.255.255.0

mag1

ifconfig-push 10.10.200.4 10.10.200.1

mag2

ifconfig-push 10.10.200.5 10.10.200.1

Цими настройками видали клієнтам з відповідними сертифікатами віртуальні ip адреси, шлюз 10.10.200.1 і задали маршрут через тунель до мережі за клієнтами. Для магазинів маршрут не задано, так як в нашу задачу не входить підключення цих мереж.

На цьому настройка сервера закінчується, запускаємо OpenVPN:

colo> service openvpn start

Якщо все правильно, то повинно з'явитися віртуальне tun пристрій:

colo> ifconfig tun0

tun0 Link encap: UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 00-00

inet addr: 10.10.200.1 P-t-P: 10.10.200.2 Mask: 255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU 1500

Metric: 1

RX packets: 9 errors: 0 dropped: 0 overruns: 0 frame: 0

TX packets: 24 errors: 0 dropped: 0 overruns: 0 carrier: 0

collisions: 0 txqueuelen: 100

Якщо пристрій не з'явилося, значить є помилки в конфігураційних файлах. Дивимося лог і усуваємо помилку, далі знову стартуємо.

Переходимо до налаштування клієнтів. Всі конфігураційні файли однакові, тому розглянемо один з них. На маршрутизаторах office і sklad встановлюємо OpenVPN, так само як і для сервера.

На цьому настройка OpenVPN закінчена. Копіюємо ці файли на office і sklad. Далі запускаємо OpenVPN. Якщо не запустився, дивимося логи.

Але на цьому ще не все. Тепер нам треба включити трансляцію адрес (NAT) щоб пакети від клієнтської машини, потрапляючи на сервер могли піти в Інтернет і відповідно повертались назад:

colo> iptables -t nat -A POSTROUTING -s 10.10.200.0/24 -o eth1 -

j MASQUERADE

Тепер 3 мережі «бачать» одне одного. Налаштуємо підключення з магазинів до серверів. На комп'ютерах в магазинах, варто операційна система Windows. Беремо з офіційного сайту дистрибутив OpenVPN і встановлюємо. Потім в установленому каталозі в папку config кладемо наші ключі і конфігураційний файл mag1. Після цього можна запускати.

На цьому етапи настройки завершені. Маючи захищену корпоративну мережу, можна підключатися безпосередньо до серверів. Перевірити шифрацию можна, прослухавши трафік на одному з роутерів командою TCPDUMP.

Приклад виведення нешифрованих трафіку:

18: 27: 15.752295 IP cl230-175-182-213.cl.metrocom.ru.40887>
195.2.240.68.ssh:. 2826496: 2827944 (1448) ack 1009 win 10080
<Nop, nop, timestamp 2791385847 256970382>
18: 27: 15.752347 IP 195.2.240.68.ssh> cl230-175-182-
213.cl.metrocom.ru.40887:. ack 2783056 win 65535 <nop, nop, timestamp
256970382 2791385774, nop, nop, sack 1 {2785952: 2827944}>
18: 27: 15.755042 IP cl230-175-182-213.cl.metrocom.ru.40887>
195.2.240.68.ssh: 2827944: 2829392 (1448) ack 1009 win 10080
<Nop, nop, timestamp 2791385850 256970382>
18: 27: 15.755096 IP 195.2.240.68.ssh> cl230-175-182-
213.cl.metrocom.ru.40887:. ack 2783056 win 65535 <nop, nop, timestamp
256970382 2791385774, nop, nop, sack 1 {2785952: 2829392}>

Приклад зашифрованого:

18: 24: 18.247960 IP 195.2.240.68.sieve> cl230-175-182-
213.cl.metrocom.ru.sieve: UDP, length 113
18: 24: 18.248040 IP 195.2.240.68.sieve> cl230-175-182-
213.cl.metrocom.ru.sieve: UDP, length 113
18: 24: 18.250915 IP cl230-175-182-213.cl.metrocom.ru.sieve>
195.2.240.68.sieve: UDP, length 1441
18:24:18.251291 IP 195.2.240.68.sieve > cl230-175-182-
213.cl.metrocom.ru.sieve: UDP, length 113

3.2 Реалізація корпоративної мережі на основі технології SSH

SSH-тунель. Припустимо, що офіс, склад і магазини працюють тільки на серверах в термінальному режимі. Тоді існує дуже простий, а найголовніше

швидкий спосіб організації VPN тунелю. За допомогою пакета OpenSSH на software маршрутизаторах можна робити шифрований канал тільки по одному потрібного порту. Для роботи з термінальним сервером, клієнти використовують протокол RDP, який використовує 3389 порт.

Синім, відзначений ssh-тунель, по якому буде працювати RDP протокол.

Реалізація, як говорилося раніше, дуже проста, тільки у OpenSSH є недолік: при великому просте каналу він рветься. Але і для цієї проблеми є просте рішення. Пакет autoSSH, по додатковому порту при просте шле heartbeat пакет і канал не падає.

Схема такої роботи представлена на рис.3.1.

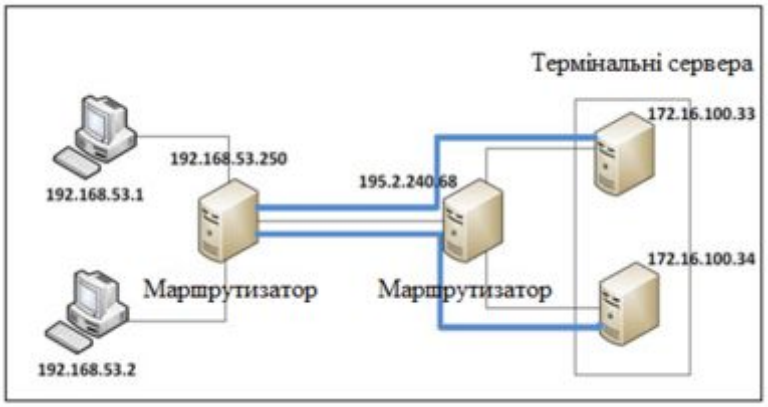


Рис. 3.1.Використання SSH-тунелів

Створимо 2 канала до двох термінальних серверів:

colo> export AUTOSSH_DEBUG=1

colo> export AUTOSSH_GATETIME=0

colo> export AUTOSSH_PORT=20037

Розглянемо команди докладніше:

colo> autossh -f -N –g –c aes256 -l root -L 1002:172.6.100.33:3389

На цьому налаштування шифрованого тунелю закінчена і можна працювати. Якщо нам потрібно додати ще один тунель, то за допомогою команди export AUTOSSH_PORT = 20050 додаємо ще один порт для посилки heartbeat пакетів і прописуємо ту ж команду підняття ssh тунелю, але вже з іншим портом.

SSH VPN. Реалізуємо ту ж схему корпоративної мережі, яку створювали за допомогою пакета OpenVPN, але вже за допомогою вбудованого в linux системи пакета OpenSSH. Нам вистачить розглянути з'єднання 2-х мереж, так як для підключення ще одного постачальника послуг потрібно буде провести ті ж самі дії.

З версії 4.3, OpenSSH підтримує пристрої tun / tap, що дозволяють створювати зашифровані тунель. Це дуже схоже на OpenVPN, заснований на TLS.

Шифрований тунель створюється на основі одного TCP з'єднання, що вельми зручно, для швидкого підняття простого VPN, на IP.

Спочатку потрібно дописати в конфігураційний файл OpenSSH рядки, що він має право створювати пристрої tun / tap і заходити з правами root. У файлі конфігурації / etc / ssh / sshd_config, повинні стояти такі опції:

PermitRootLogin yes

PermitTunnel yes

У нас є дві мережі, мережа office з адресою 192.168.53.0/24 і мережу colo з адресою 172.16.100.0/24. Для створення захищеної VPN мережі потрібно виконати наступні дії:

1. Підключитися з одного маршрутизатора через SSH на інший з опцією -w;
2. Налаштування IP адреси SSH тунелю робиться раз на сервері і на клієнті.
3. Додати маршрут для обох мереж.
4. Якщо потрібно, включити NAT на внутрішньому інтерфейсі шлюзу.

Будемо підключатися з мережі office до мережі colo. З'єднання починається з маршрутизатора office, а команди виконуються на маршрутизаторі мережі colo, тобто, налаштовуємо маршрутизатор colo:

За допомогою опції w с параметрами 0: 0 говоримо, що при підключенні створити на клієнті і сервері віртуальні пристрої tun0. Параметр -c включає шифрацию, параметр -C стиснення трафіку.

office> ssh –c aes256 -C –w0:0 root@195.2.240.68

Наступні команди вже виконуються на маршрутизаторі мережі colo. Задаємо ip адресу і маску підмережі

colo> ifconfig tun0 10.0.1.1 netmask 255.255.255.252

Додаємо маршрут до мережі office

colo> route add -net 192.168.53.0 netmask 255.255.255.0 dev tun0

Вмикаємо NAT, якщо не включений

colo> echo 1 > /proc/sys/net/ipv4/ip_forward

На цьому настройка закінчена, VPN мережа побудована. Для підключення окремих комп'ютерів з операційною системою Windows (магазини), використовується клієнт SSH Putty.

3.3 Оцінка продуктивності каналів корпоративної мережі

У розділах 3.1 і 3.2 розглянуті дві технології (OpenVPN, SSH) створення захищених корпоративних мереж, використовуючи VPN. На сьогоднішній день технологія OpenVPN лідирує на ринку побудови захищених мереж, в той час як туннелирование за допомогою SSH тільки починає входити в повсякденність. Для того щоб зрозуміти яку технологію необхідно застосувати в реальних умовах при конкретних вимогах, пропонованих корпоративної мережі, потрібно оцінити їх продуктивність і обгрунтувати їх переваги і недоліки.

Почати слід з продуктивності захищених каналів. На рис. 3.2 представлена побудована корпоративна мережа, продуктивність захищених каналів якої, використовуючи програму iPerf, необхідно оцінити. За допомогою клієнтської частини генерується трафік і відправляється на серверну частину. При отриманні даних генерується звіт про швидкість передачі даних.

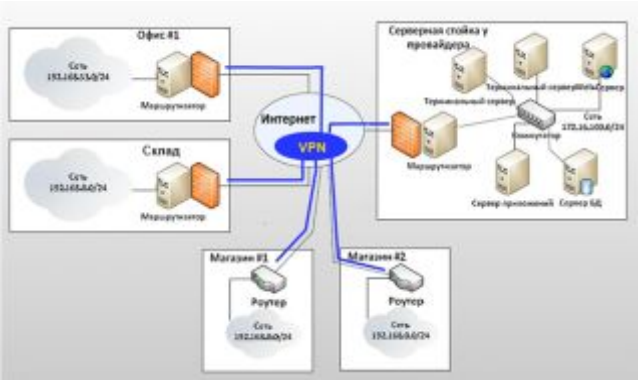


Рис.3.2. Корпоративна мережа

Оцінка продуктивності при використанні технології OpenVPN. Для побудови графіків продуктивності каналу створеного за допомогою OpenVPN будемо використовувати дані, отримані при тестуванні з додатка А.

На рис. 3.3 представлені графіки значень RTT. З них видно, що різниця між каналом без VPN і каналом з використанням VPN, не є суттєвою.

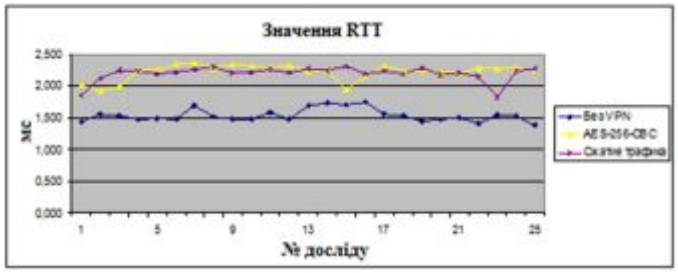


Рис.3.3. Графіки значень RTT

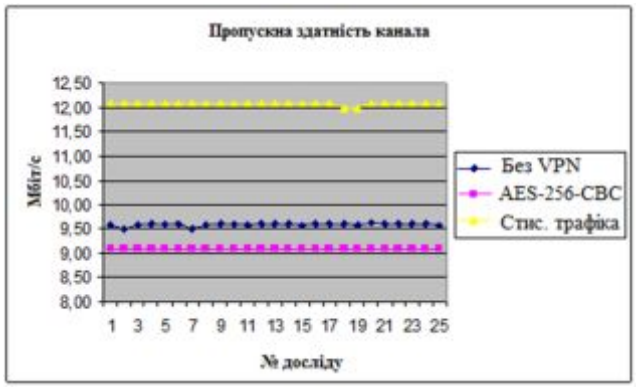


Рис. 3.4. Графіки пропускної здатності каналу

На рис. 3.4 представлені графіки пропускної здатності каналу, з яких можна зробити наступні висновки:

- При використанні створеного каналу VPN з шифрацией за допомогою ключа AES-256-CBC втрата в продуктивності 0,5 Мбіт/сек, що склало 5,1% від каналу без використання VPN;

- При включенні стиснення шифрованого трафіку спостерігаємо приріст швидкості в 3 Мбіт/сек, що склало 32.9%.

На рис. 3.5 представлені графіки завантаження ЦП на маршрутизаторах при використанні OpenVPN с шифрацией трафіку, при включеному і вимкненому стисненні.

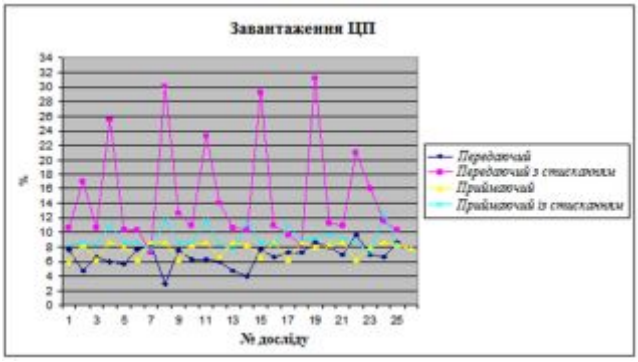


Рис.3.5 Графіки завантаження ЦП

За середнім значенням завантаження, як і належало, найвищу навантаження дає шифрация трафіку з використанням стиснення - 14.992%.

Грунтуючись на отриманих графіках, зробимо оцінку продуктивності каналів VPN, побудованих за допомогою OpenVPN:

1. Критерій «Завантаження ЦП» при отриманих значеннях є несуттєвим, оскільки це маршрутизатор і інших процесів вимагають велике споживання ЦП немає.

2. Критерій «RTT» також є несуттєвим, оскільки різниця від часу відгуку при дослідах без VPN виявилася найменше на 0,5 мс.

3. На графіках пропускної здатності каналів можна спостерігати падіння швидкості при використанні коштів VPN на 0,5 Мбіт/сек в середньому. В даний час це не є суттєвим, так як Інтернет-провайдери надають свої послуги на великих швидкостях, де таке падіння не буде грати великої ролі.

4. При використанні стиснення трафіку видно помітний приріст до пропускної здатності каналу, на 3 Мбіт/сек. Звичайно при цьому сильно зростає завантаження на ЦП, але як говорилося раніше, це не грає великої ролі.

Підведемо підсумки. Створюючи захищену корпоративну мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифруванням переданих даних і приростом швидкості за рахунок стиснення трафіку з зручністю обміну інформацією. Технологія OpenVPN повністю виправдовує себе. Її використання веде до зростання продуктивності праці з інформацією по мережі. З мінусів виділяється деяка складність настройки і створення VPN мережі. З плюсів - кросплатформеність.

Оцінка продуктивності при використанні технології SSH. Для побудови графіків продуктивності каналу створеного за допомогою SSH будемо використовувати дані, отримані при тестуванні з додатка Б.

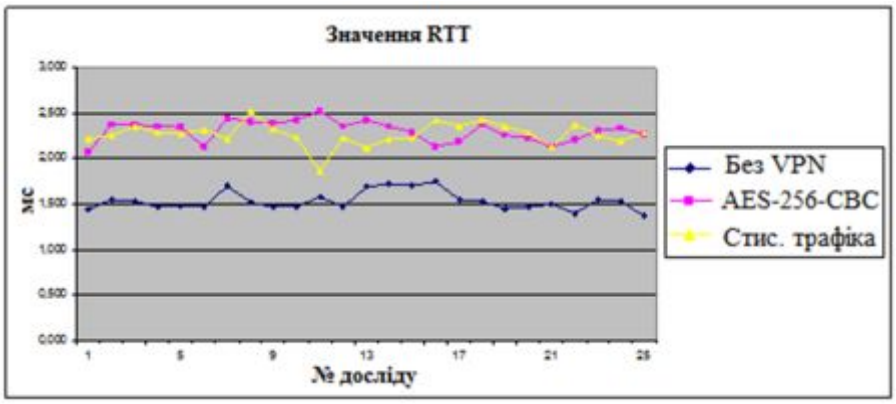


Рис. 3.6. Графіки значень RTT

На рис. 3.6 представлені графіки, за якими можна судити про час відгуку при роботі ssh. В середньому час збільшилася на 0.8 мс. Це значення не є критичним навіть для самих вибагливих програм.

На рис. 3.7 представлені графіки пропускної здатності каналу. Результати вийшли приблизно такими ж, що і при використанні OpenVPN.

На рис. 3.8 представлені графіки завантаження ЦП при використанні SSH з шифруванням з стисненням трафіку і без. При включенні шифрування видно великий стрибок навантаження на ЦП. Середнє значення - 37.9%. Це досить багато, але не є критичним.

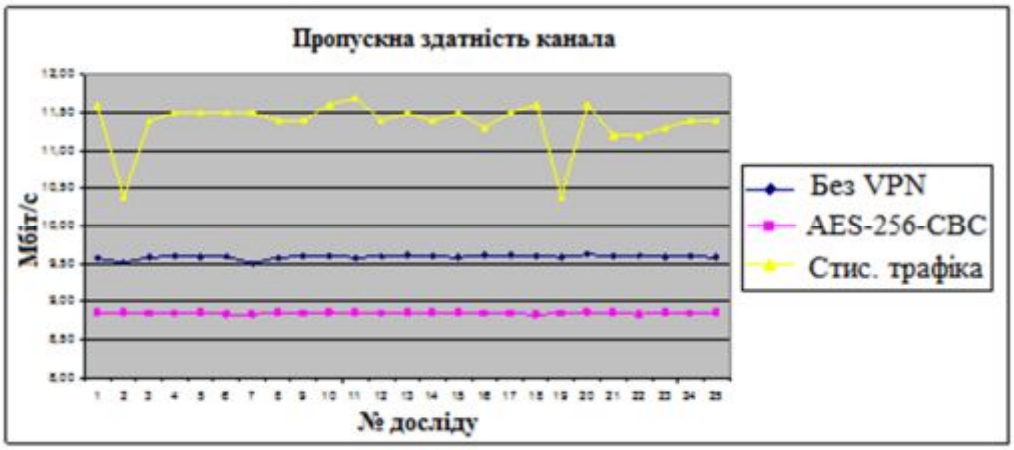


Рис.3.7. Графіки пропускної здатності каналу

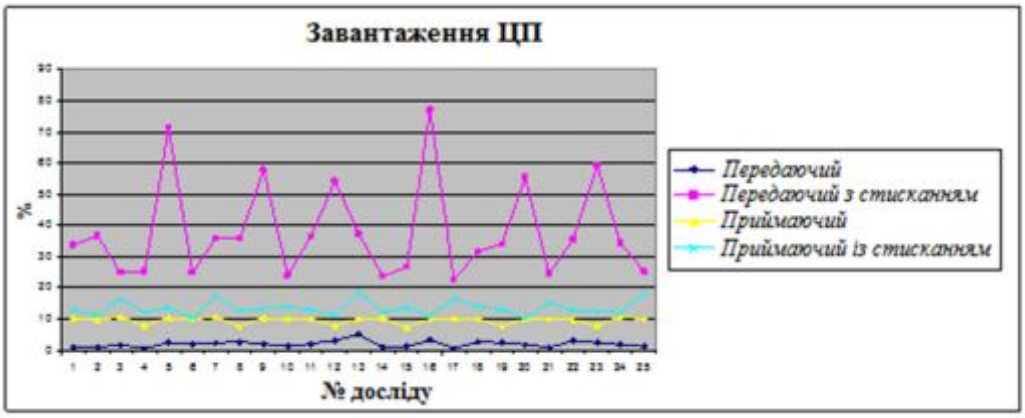


Рис.3.8. Графики загрузки ЦП

З отриманих даних можна зробити наступний висновок: продуктивність при використанні стиснення трафіку зросла приблизно на 25%, але при цьому значно зросло навантаження на ЦП. З переваг цієї технології хочеться виділити можливість створення ssh-тунелів по окремих портів, що за певних умов дає безліч плюсів, наприклад, можливість мати автоматичне включення резервного каналу, при відсутності зв'язку на одному з маршрутизаторів.

Вибір між технологіями SSH і OpenVPN. Складемо порівняльну таблицю, грунтуючись на отриманих дослідним шляхом даних.

Таблиця 3.4

Порівняння технологій

	OpenVPN	SSH
Складність створення	Досить складна настройка. Складність настройки маршрутизації для декількох мереж, можливі труднощі з firewall.	Легка настройка, яка не потребує особливих знань. На все створення йде не більше 10 хвилин.
Масшта-бованість	Підключення ще однієї мережі або клієнта, тягне за собою зміну конфігураційних файлів на сервері і додавання їх на клієнта. За рахунок OpenVPN клієнта під Windows має перевагу перед SSH. Не вимагає навчання персонал	Для підключення ще однієї мережі потрібно повторити ті ж дії, що і при об'єднанні попередніх. Для підключення Windows комп'ютерів, потрібно одноразове навчання персоналу.
Продук-тивність	За рахунок стиснення можна добитися відмінних результатів, що перевищують вихідну сполуку. Стиснення йде вибірково, тобто що стиснути можна - пропускається. Це зменшує навантаження на ЦП.	Продуктивність трохи нижче, ніж у OpenVPN. Стискається весь трафік - великі навантаження на ЦП.
Заванта-ження ЦП	В середньому не більше 15%	В середньому не більше 38%
Кросплатфо-рменість	Так	Так
RTT	На 0,5 мс більше, ніж у вихідного з'єднання	На 0,8 мс більше, ніж у вихідного з'єднання
Докумен-тація	Маса документації на офіційному сайті. Численні форуми та обговорення.	Документація є в вбудованому довіднику. Інформації по налаштуванню поки що мало.
Додаткові можливості	-	Створення ssh-тунелів.
Впровад-ження в існуючу мережу	Можуть бути проблеми з налаштуванням firewall'a.	Легке впровадження.

Продовження таблиці 3.4

Порівняння технологій

	OpenVPN	SSH
Захищеність	Шифрація 256 бітовим AES ключем	Шифрація 256 бітовим AES ключем
Поширеність	Лідируюча технологія створення VPN мереж.	Сам протокол ssh існує дуже давно, але створення ssh VPN мереж на сьогоднішній день зустрічається рідко.

Розглянувши всі плюси і мінуси, кращим рішенням буде використання обох технологій разом. Від SSH взяти SSH-тунелі, а від OpenVPN створення VPN мереж.

3.4 Аналіз моделей і алгорімов ідентифікації типів додатків тунельного трафіку

Модель ідентифікації типу додатків в тунелі мережевого трафіку. Одним з найбільш відомих способів обходу фільтрації на брандмауер є передача трафіку через проміжний додатковий сервер (проксі-сервер, VPN-сервер, і т.п.), що знаходиться за межами мережі, в якій виконуються фільтрація і моніторинг. Протокол інкапсуляції, так само званий тунельним протоколом (тунельним додатком), дозволяє відправити трафік хоста за призначенням через проксі-сервер і часто застосовує шифрування трафіка. До тунельних протоколів можна віднести:

1. Тунельний протокол на IP рівні, також званий сервісом віртуальної приватної мережі - VPN (virtual private network), де весь трафік хоста проходить через цей тунель. Найвідомішим тунельним протоколом на IP рівні є протокол IPSec [20]. У цьому типі тунелю весь трафік хоста, до якого включається трафік будь-якої програми з любимо віддаленим хостом, відправляється до VPN сервера, звідки цей трафік передається (Пересилається кожен пакет) за адресою наполіг призначення, як показано на рисунку 3.9.

2. Тунельне додаток на TCP рівні (див. рис.3.10), де цей тип тунелю використовується для передачі трафіку однієї програми [21] по адресою тунельного сервера з використанням одного TCP з'єднання, а трафік інших додатків проходить за звичайним маршрутом. Найбільш відомими тунельними додатками на TCP рівні є TOR [22] і Secure Shell protocol (SSH) [22], де ці програми використовуються в основному для перегляду веб-сайтів без моніторингу в брандмауері.

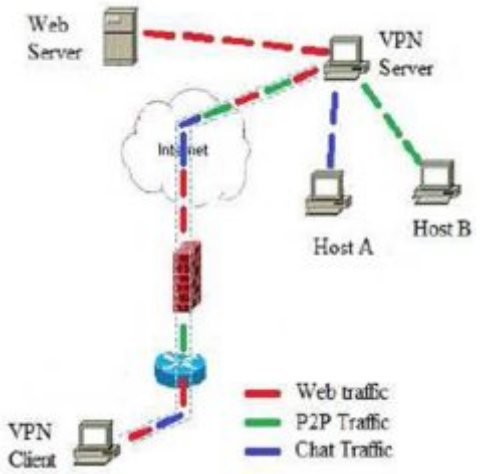


Рис. 3.9. VPN сервіс на рівні IP протоколу

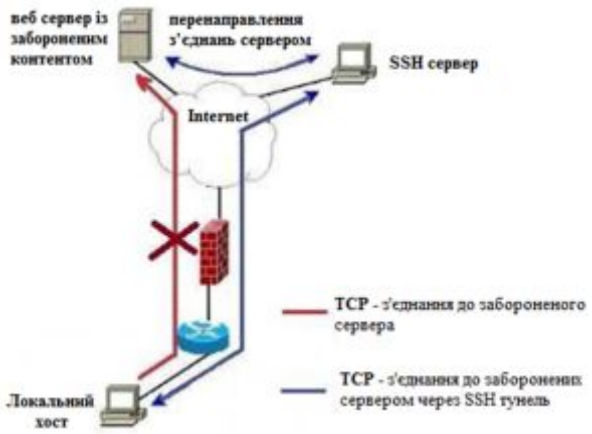


Рис. 3.10. Тунельне додатки (SSH tunnel) на рівні TCP протоколу

В роботі [23] представлений метод ідентифікації SSH-тунелю і типу програми в тунелі. У цій роботі використовуються два вектора параметрів: довжина пакета і інтервал часу між пакетами. Головними недоліками цього

підходу є, по-перше, те, що SSH тунель проводить тільки один TCP сеанс і на основі цього припущення розраховуються вхідні параметри моделі. Однак більшість з поширених додатків одночасно генерують кілька TCP сеансів для виконання їх сервісу, як в разі чат-додатків, де використовуються окремі TCP сеанси для передачі даних і управління каналом зв'язку, і також в разі веб-додатків, де кожні окремі частини веб-сторінки відправляються в окремих TCP сеансах. По-друге, нові версії SSH додатків (тунелів) додають випадкове число байтів на перенесених пакетах (надмірність), тому сигнатура додатки, обчислена на основі довжини перенесених пакетів, не є адекватною в цьому виді тунелю.

Метою цього розділу є ідентифікація типу додатки в TCP тунельного трафіку за умови використання тільки однієї програми під час спостереження тунелю.

Параметри моделі ідентифікації типу додатки в тунелі трафіку. Досліджена в цьому випадку модель ITPTT складається з двох частин, кожна з яких базується на основі такої ж CMM, як і в моделі ідентифікації трафіку СПД. У кожній частині моделі використовується окреме спостережуване значення.

У першій частині використовується послідовність кількості пакетів

Count (i), Які проходять через тунель в перебігу певного інтервалу часу *T*, причому *Count (i)* ВИЗНАЧАЄТЬСЯ які належать їм чином:

$$Count(i) = |X|; X = \{P_t : iT < t \leq (i+1)T\} \quad (3.1)$$

де *i* - номер спостережуваного значення в послідовності спостереження.

Щоб підвищити продуктивність моделі, пропонується використання модельних спостережуваних значень. Модельне значення *C (i)* визначаються наступним чином:

- якщо *Count (i)* <1000 пакетів, то

$$C_i = \left[\frac{Count(i)}{10} + 1\right] \quad (3.2)$$

- якщо *Count (i)*≥ 1000, то $C_i = 100$

При використанні модельного значення діапазон спостережень стане рівним {1, ..., 100}. Поріг 1000 пакетів вибирається з умови, що число пакетів в інтервалах спостережень для більшості типів додатків не перевищує 1000.

Параметри СММ в першій частині моделі рівні

$$\theta_c = \{\pi_c, A_c, B_c,\} \tag{3.3}$$

У другій частині моделі в якості значення спостережуваного параметра використовується послідовність максимального часу між пакетами *MaxT(i)* протягом певного інтервалу часу *T* (див. рис. 3.11), де *MaxT (i)* визначається наступним чином:

$$MaxT(i) = Max(t_{k+1} - t_k): iT < t_{k+1}, t_k \leq (i+1)T \tag{3.4}$$

Тут t_k - час прибуття *i*-го пакета і порядкової номер спостережуваного значення в послідовності набдюденія.

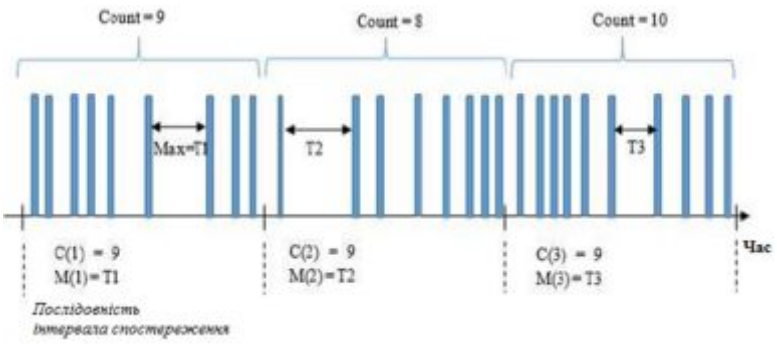


Рис.3.11. Спостережувані значення моделі ІТПТТ

Для підвищення продуктивності моделі в роботі пропонується використання модельних спостережуваних значень. Модельне значення максимального часу між пакетами *M(i)* визначається наступним чином:

$$M(i) = \left[10 \cdot lg\left(MaxT(i)\right) + 1\right] \tag{3.5}$$

а час t_k прибуття пакетів вимірюється за шкалою з кроком 10^{-7} в секунд.

Тому діапазон значень *MaxT(i)* дорівнює {1, ..., 10^{-7} }, а діапазон модельного значення *M(i)* стане рівним {1, ..., 71}.

Параметрами другій частині моделі є:

$$\theta_m = \{\pi_m, A_m, B_m\} \tag{3.6}$$

Оскільки спостерігаються значення не залежать один від одного, вдається побудувати дві самостійні моделі СММ і обчислити вірогідність поява спостереження (O_c, O_m) в трафіку додатки *App* наступним чином:

$$P(O_c, O_m | O_{app,c}, O_{app,m}) = P(O_c | \theta_{app,c}) P(O_m | O_{app,m}) \quad (3.7)$$

При дослідженні моделі використовується діапазон зміни станів від 2 до 10 для обох частин моделі. Отримані результати показали, що 3 стану в кожній частині моделі для всіх досліджуваних типів додатків забезпечують максимальну точність ідентифікації типів додатків.

Аналіз алгоритмів і програм ідентифікації типів додатків в тунелі трафіку. Для реалізації моделі ІТПТТ використані алгоритми, раніше розроблені для моделі ідентифікації трафіку СПД: алгоритм обчислення параметрів моделі СММ на основі процедури Баума-Велша і алгоритм ініціалізації значень параметрів моделі.

Алгоритм захоплення трафіку тунелю фіксує всі, хто проходить через тунель пакети, а також обчислює час прибуття кожного пакета і інтервал часу між послідовними пакетами, як показано на рис.3.12.

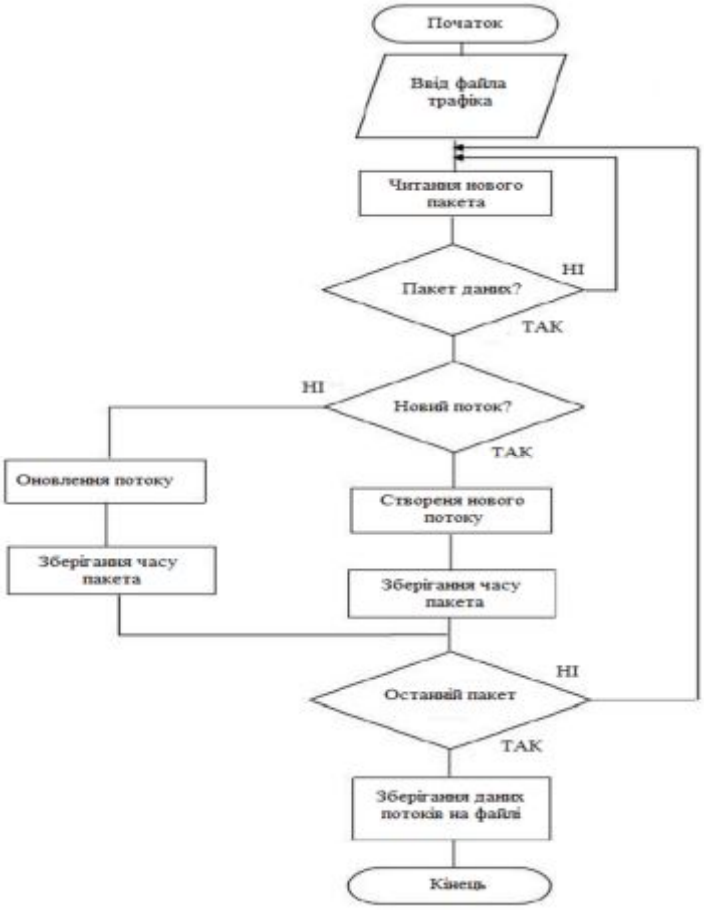


Рис.3.12. Схема алгоритму захоплення тунельного трафіку для мереж передачі даних

Ці алгоритми можна використовуватися в новій моделі без зміни. Крім них для вирішення завдання захоплення трафіку тунелю розглянуто ще два алгорити, розроблених спеціально для реалізації моделі ІТПТТ. Такими алгоритмами є алгоритм захоплення трафіку тунелю і алгоритм обчислення спостережуваних значень. Для тестування досліджуваної моделі був проведений етап її навчання з трафіком додатків до його проходження через тунель, при цьому в кожному наборі трафіку використаний тільки один тип додатки. Записані дані пакетів зберігаються в окремому файлі для кожного типу додатки. Алгоритм реалізований с використанням програмного продукту - Visual Studio (C #). Схема алгоритму обчислення спостережуваних значень C і M наведена на рис.3.13.

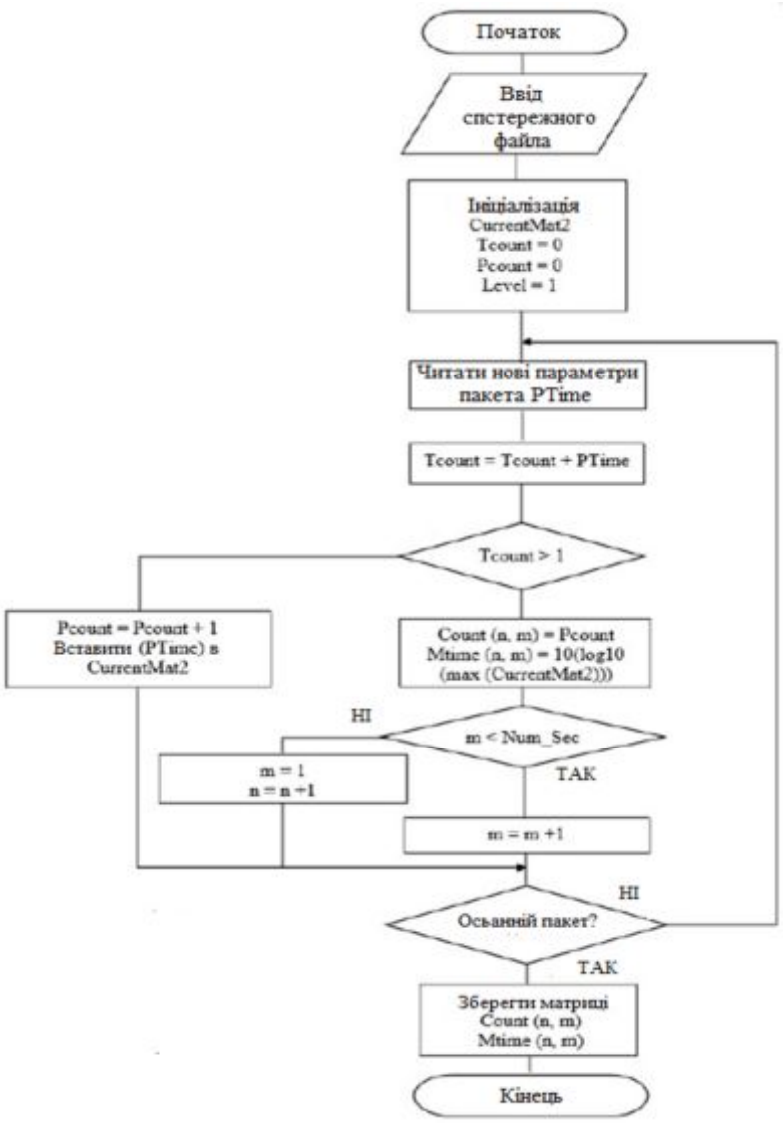


Рис. 3.13. Схема алгоритму обчислення спостережень моделі ІТПТТ

У цьому алгоритмі вхідними даними є послідовності спостережень (вихідні результати алгоритму захоплення тунельного трафіку), а виходами алгоритму - дві матриці розмірами $n \times m$, де n - довжина кожного спостереження (nT) і m - число спостережень. Одна матриця використовується для збереження спостережуваних значень С і друга для збереження М.

Для обчислення модельних спостережуваних значень С і М в кожному інтервалі часу Т використовуються дві спеціальні тимчасові матриці.

Алгоритм обчислення спостережень моделі ІТПТТ реалізований з використанням програмного середовища MATLAB.

Тестування моделі ідентифікації типів додатків в тунелі трафіку. Для тестування моделі ITPTT використані набори трафіку мереж передачі даних, які створені для дослідження і є загальнодоступними при певних умовах.

Набори трафіку складаються з двох типів. Перший тип служить для навчання і дослідження трафіку додатків, коли набори трафіку зняті до їх проходження через тунель. Другий тип наборів трафіку служить для тестування моделі, коли ці набори зняті після проходження потоків трафіку в тунелі. Як тунельного додатки використовувалося TOR- додаток рис. 3.14. Час спостереження *T* в моделі приймалося рівним 1 с.

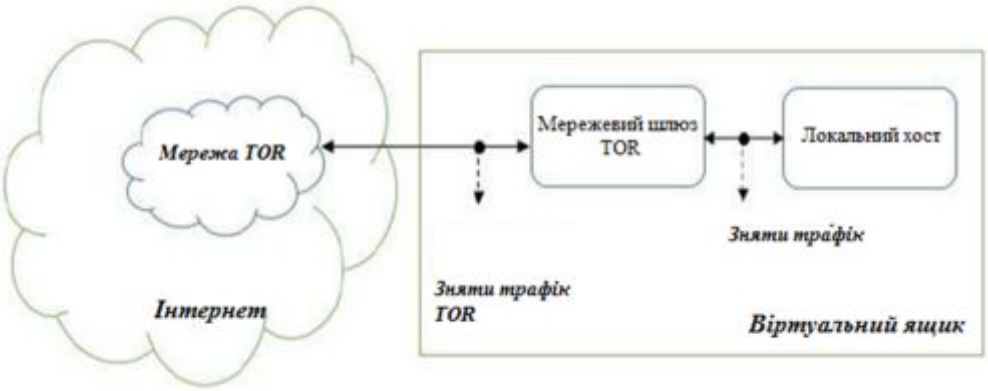


Рис.3.14. Структура і місце захоплення трафіку

Використані при тестуванні набори трафіку складалися з трафіків шести типів додатків:

1. Веб трафік, який включає трафік протоколів HTTP і HTTPS, що використовуються для навігації веб-сайтів в таких областях, як сайти університетів, новин, туристичних агентств, Вікіпедії, facebook і т.п.

Всі сайти відвідуються користувачами з використанням браузерів (Firefox і Chrome).

2. Чат-трафік, що включає трафік додатки для миттєвого обміну повідомленнями (месенджери) і трафік різних відомих чат-додатків, наприклад, Facebook, Hangout, Skype, AIM і ICQ.

3. Трафік передачі файлів. Цей тип трафіку використовується при обміні файлами і електронними документами через мережу. Для генерації цього типу трафіку використані три програми: передача файлів по Skype, FTP по SSH (SFTP) і FTP по SSL (FTPS).

4. Трафік P2P, використовується пірінговими додатками, які застосовуються для передачі файлів, особливо торрент-файлів. Для генерації цього трафіку скачували різні торрент-файли з дистрибутива Kali linux

(Https://www.kali.org) і відтворювалися сеанси трафіку за допомогою програми Vuze (https://www.vuze.com). При цьому використовувалися різні комбінації навантаження, щоб відтворювати більш загальна поведінка трафіку.

5. VoIP-Трафік, який складається з трафіку додатків голосового зв'язку в мережах передачі даних. Для генерації цього типу трафіку використані три програми: Facebook, Hangout і Skype.

6. Відео-трафік, який складається з трафіку додатків потокового відео, що вимагають безперервний і стабільний потік даних. Для генерації трафіку цього типу додатків використані трафики HTML5 і flash для перегляду відео Youtube і сервісів Vimeo за допомогою Chrome і Firefox.

Більш докладно число пакетів (до і після тунелю) і час спостережень для використаних типів додатків наведені в табл. 3.5.

На рис. 3.15 і 3.16 приведені гістограми числа пакетів в одиницю часу для кожного досліджуваного типу додатки. У кожній гістограмі по осі X відкладено число пакетів в одиницю часу, а по осі У - число отриманих спостережуваних значень. З рис. 3.15 *а* і 3.15 *б* слід, що спостережувані значення для веб- і чат-трафіку близькі один до одного (більшість спостережуваних значень містить менше 10 пакетів).

Так як ці типи трафіку залежать від дій користувача. Трафік P2P (див. рис. 3.16*б*) містить два основних діапазону кількості пакетів в залежності від доступної швидкості з'єднань. Крім того з рис.3.16*в* випливає, що VoIP додатки використовує кілька певних діапазонів пакетів в залежності від способу кодування і стану дзвінка (мовчання або мова).

Таблиця 3.5

Кількості пакетів і час спостереження для кожного типу трафіку

Тип додатки	використовувані додаток	кількість пакетів до тунелю	кількість пакетів після тунелю	час спостереження (Секунди)
Передача файлів	FTP, SFTP	386678	396656	10710
Веб	HTTP, HTTPS	419337	436224	7870
Чат	AIM_Chat, facebook_chat,	10402	11556	1060
P2P	p2p_multipleSpeed, p2p_vuze	1695735	1916045	10050
VoIP	Facebook_Voice, Hangouts_voice,	465066	489834	10090
Відео	Youtube-Flash,	473838	507121	1300

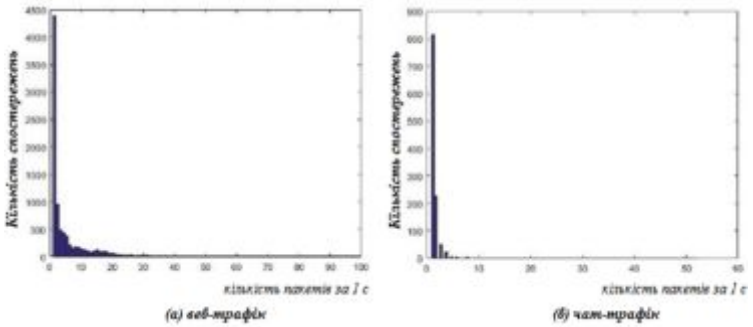


Рис.3.15. Розподіл кількості пакетів для кожного досліджуваного Додатку

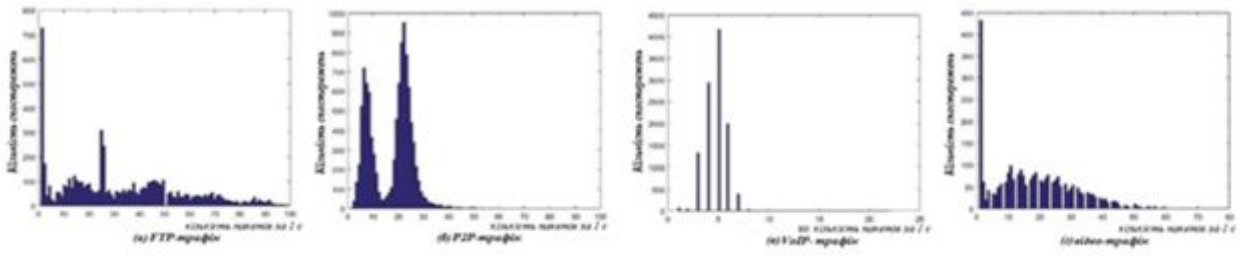


Рис.3.16. Розподіл кількості пакетів для кожного досліджуваного додатки

На рис.3.17 наведені гістограми значень максимального інтервалу часу між двома послідовними пакетами протягом кожного спостереження.

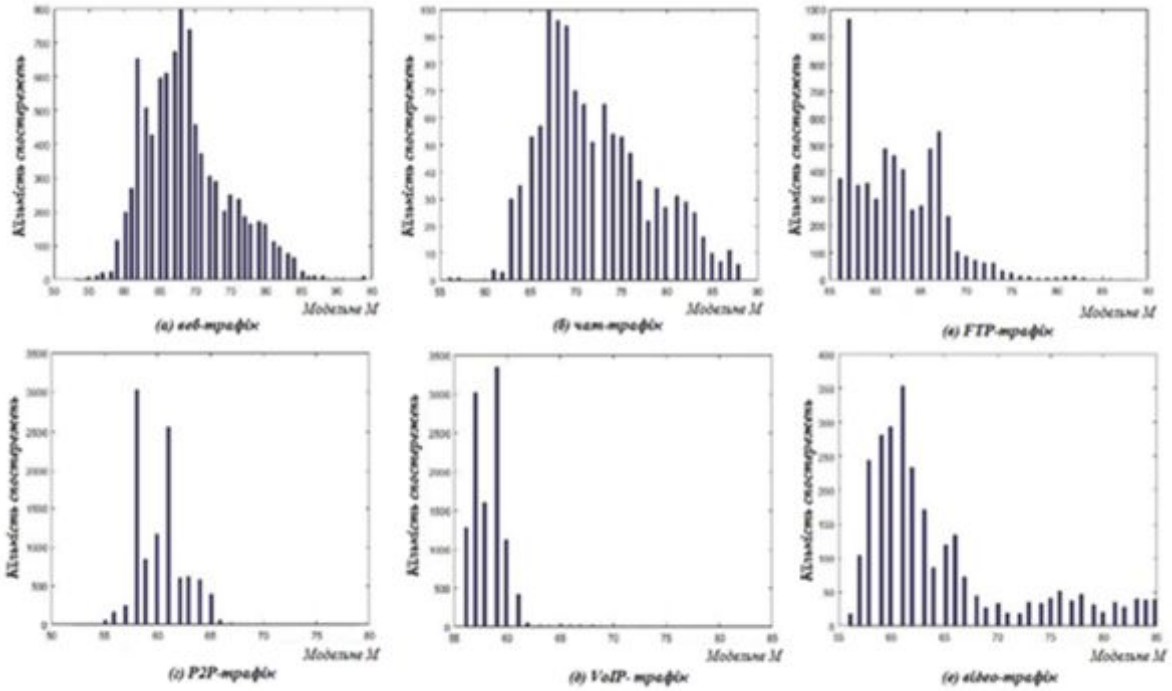


Рис. 3.17. Гістограми максимального інтервалу часу між двома послідовними пакетами для досліджуваних додатків

На рис. 3.18, показаний характер зміни показника точності (precision) моделі для різних типів трафіку. З рисунку слід, що FTP трафік ідентифікується з точністю понад 90% при спостереженні тунелю за 10 секунд або більше. Чат і веб мають хорошу точність ідентифікації (~ 85%) при спостереженні тунелю за 15 секунд, а трафики VoIP і P2P ідентифікуються з точністю (~ 75%) за той же час спостереження. У той же час, відео трафік має низьку точністю ідентифікації (60% за 20 секунд або вище).

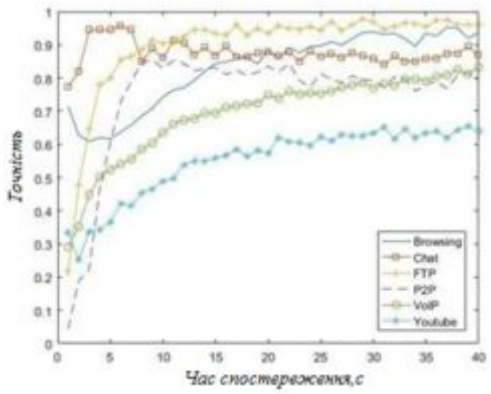


Рис. 3.18. Вплив часу спостереження на точність ідентифікації типів додатків в тунелі трафіку

На рис. 3.19 наведено зміна повноти (recall) моделі ідентифікації типу додатки в тунелі трафіку за час спостереження.

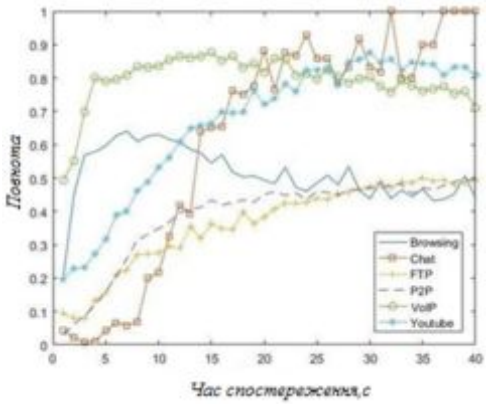


Рис. 3.19. Вплив часу спостереження на валідність ідентифікації типів додатків в тунелі трафіку

З рисунка слід, що три типи трафіку (VoIP, чат і відео) мають повноти більше 75%, а три типи трафіку (FTP, P2P і веб) мають повноти ідентифікації близько 50%. Отримані результати є виправданими через те, що FTP і P2P використовуються для передачі файлів і володіють подібними характеристиками, а всі типи трафіку включають в себе частину веб-трафіку, де використані додатки для генерації різних типів трафіку базуються на веб-сервісі. Тому існує взаємний вплив веб-трафіку на інші досліджувані типу трафіку, яке відбивається на результатах експерименту.

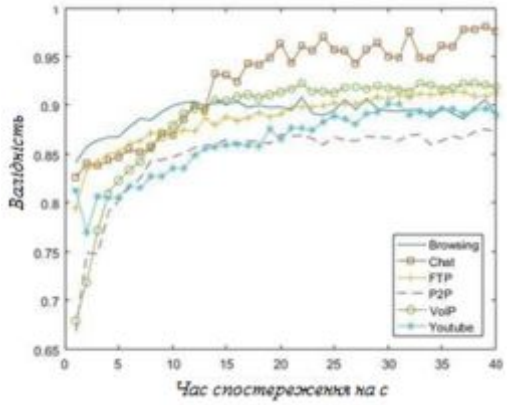


Рис. 3.20. Вплив часу спостереження на валідність ідентифікації типів додатків в тунелі трафіку

З цього рисунку слід, що значення валідності ідентифікації для всіх типів трафіку, крім чат-трафікп більше 85% при спостереженні тунелю не менше 15 секунд при цьому і причому чат-трафік ідентифікується з валідність більше 95% за той же час спостереження. На рис.3.21 представлено зміна частки помилок в розглянутій моделі для ідентифікації типів додатків в тунелі трафіку. З чого випливає, що частка помилок ідентифікації всіх типів додатків не перевищує 15% при спостереженні тунелю більш 15с.

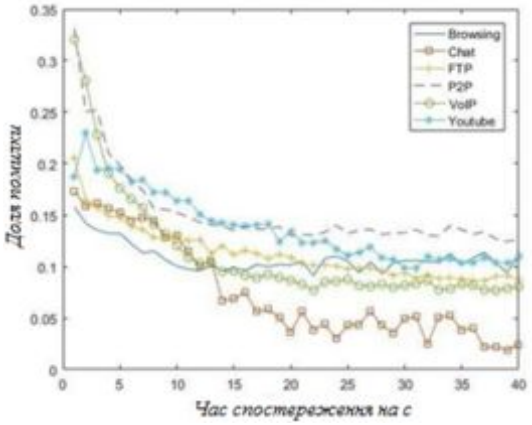


Рис.3.21. Вплив часу спостереження на частку помилок ідентифікації типів додатків в тунелі трафіку

ВИСНОВКИ

Отже виконавши поставлені завдання, у дипломній роботі проаналізовано тенденції розвитку мереж зв’язку на базі різних стандартів і технологій, що показує різноманітність їх вибору для побудови корпоративної мережі.

У другому розділі виконано огляд теоретичного і практичного використання технології SSH при побудові корпоративної мережі, алгоритм побудови каналу зв'язку за допомогою SSH-тунелів та принципи роботи, завдяки якій можливо досягти надійної авторизації та безпечної передачі інформації по відкритих каналах зв'язку.

Досліджено особливості застосування провадження VPN на основі різних технології в корпоративну мережу, та виконано їх порівняння. Розглянувши всі переваги і недоліки, я прийшов висновку що кращим рішенням буде використання обох технологій разом. Від SSH взяти SSH-тунелі, а від OpenVPN створення VPN мереж

У практичній частині виконано аналіз моделей і алгоритмів ідентифікації типів додатків тунельного трафіку. Експериментальний і теоретичний аналізи трафіка підтверджують можливість виконання з її допомогою моніторингу та ідентифікації типів додатків в тунелі трафіка, даючи можливість виявити шкідливі тип даних що можуть вплинути на якість переданої інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 2001 г. 668 с.

2. Олег Колесников, Брайан Хетч. LINUX. Создание виртуальных частных сетей (VPN). - Издательство "КУДИЦ-ОБРАЗ" 2002 г. 464 с.

3. Андреев А.М., Усовик С.В. Модель трафика корпоративной телекоммуникационной сети с пакетной коммутацией в задаче кластеризации при условии ограниченного наблюдения // Инженерный журнал: наука и инновации. 2012. № 6. 20 с.

4. Никитин А.В., Пяттаев В.О., Никульский И.Е., Филиппов А. А. Концепция построения мультисервисной сети оператора связи. //Вестник связи. 2015 №5. - с. 47-49, №7. - с. 41-45.

5. Никитин А.В., Микульский П.П., Филиппов А.А. Особенности внедрения технологий PON на сети оператора, занимающего существенные рыночные позиции. // Вестник связи. 2017, №8.- с.7-9.

6. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. - СПб.: Наука и техника, 2014.

7. Симонина О.А., Яновский Г.Г. Характеристики трафика в сетях IP.// Труды учебных заведений связи. СПб., 2004, с.8-14.

8. Воробієнко, С. П. Оцінка конкурентоспроможності телекомунікаційних послуг / Воробієнко С. П. // Зб. наук. пр. ОНАЗ ім. О. С. Попова. – Одеса: 2008. – С. 119–122.

9. Усик С. П. Аналіз послуг мобільного зв’язку на ринку України / С. П. Усик, С. А. Пономаренко // Сталий розвиток економіки. – 2013. –№.3 (20). – С. 341–346.

10. Голубицкая Е. А. Маркетинг в телекоммуникациях. / Е. А. Голубицкая, Е. Г. Кухаренко. – М.: 2005 – 145 с.

11. Гранатуров В. М. Аналіз конкурентоспроможності телекомунікаційних послуг: монографія / В. М. Гранатуров, С. П. Воробієнко. – К.: Освіта України, 2009. – 254 с.

12. Звіт «Global B2C E-commerce Report 2016» Ecommerce Foundation Raadhuisstraat 22 1016 DE Amsterdam,the Netherlands [Електронний ресурс]. – Режим доступу: https://www.ecommercewiki.org/ wikis/www. ecommercewiki.org/ images/5/56/Global_B2C_Ecommerce_Report_2016.pdf

13. Звіт «Глобальні тенденції мобільного зв'язку 2017 року» GSMA Intelligence за вересень 2017 року [Електронний ресурс]. – Режим доступу: https://www.gsmaintelligence.com/research/?file=3df1b7d57b1e63a0cbc3d58 5feb82dc2&download

14.Consumer Barometer Survey [Електронний ресурс]. – Режим доступу: https://www.consumerbarometer.com/en

15. Росляков, А. В. Виртуальные частные сети. Теория и практика применения/ А. В. Росляков. - М.: Эко-Трендз, 2016. - 304 с.

16. Lewis, M. Comparing, Designing, and Deploying VPNs/ M. Lewis. – Cisco Press- 1080 p.

17. Запечников, С. В. Основы построения виртуальных частных сетей: учеб. пособие для вузов/С. В. Запечников, Н. Г. Милославская, А. И. Толстой. - М.: Горячая линия-Телеком. - 249 с.

18. Росляков, А. В. Системы поддержки операционной деятельности провайдеров услуг VPN/А. В. Росляков, Т.О. Абубакиров, А. А. Росляков// Технологии и средства связи. - 2018. - №2. - С. 60-62.

19. Росляков, А. В. Программа проектирования виртуальных частных сетей VPN-DESIGNER/А. В. Росляков, А. В. Сергеев//VII Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникаций», Самара, 2016. - С. 161-162.

20. S. Kent. IP Encapsulating Security Payload (ESP) / S. Kent // RFC 4303 (PROPOSED STANDARD), December. – 2015.

21. Miller S., Curran K., Lunney T. Traffic Classification for the Detection of Anonymous Web Proxy Routing // International Journal for Information Security Research (IJISR) . 2019. № 5(1). С. 538-545.

22. Киянов и.р. Tor и луковая маршрутизация // Научные труды КубГТУ. 2016. № 13. С 129-135.

23. Dusi M., Crotti M., Gringoli F., Salgarelli L. Detection of Encrypted Tunnels across Network Boundaries // in Proceedings of the 43rd International Conference on Communications, Beijing, China. 2018. C. 1738-1744.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

БАКАЛАВРСЬКА РОБОТА

на тему:

«АНАЛІЗ НАПРЯМКІВ ПІДВИЩЕННЯ НАДІЙНОСТІ СИСТЕМ ПЕРЕДАЧІ ДАНИХ»

Виконала студентка 4 курсу
Аніщенко К.Я.

Київ 2021

Мета бакалаврської роботи

2

Мета роботи – аналіз організації та особливості підвищення надійності систем передачі даних.

Об'єкт дослідження – процес ідентифікації типів додатків тунельного трафіку

Предмет дослідження - моделі та алгоритми ідентифікації типів додатків тунельного трафіку

Завдання бакалаврської роботи:

1. Аналіз тенденції розвитку та основні відомості про інформаційні мережі зв'язку.
2. Аналіз теоретичного і практичного використання технології SSH при побудові корпоративної мережі.
3. Дослідження особливостей застосування провадження VPN на основі різних технології в корпоративну мережу.
4. Аналіз моделей і алгорімов ідентифікації типів додатків тунельного трафіку.

Базова комунікативна модель інфокомунікаційної мережі 3

Рис.1. Інфокомунікаційна мережа

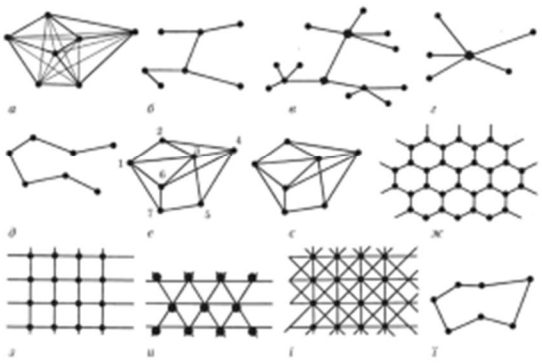


Рис.2. Види структур інфокомунікаційних мереж

Рис.3. Однорангова мережа

Рис.4. Ієрархічна мережа

Технології інфокомунікаційної мережі 4

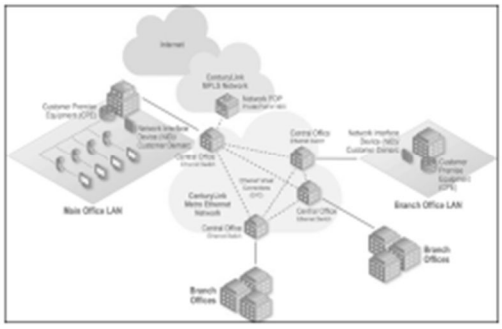


Рис.5. Архітектура мережі на базі сімейства технологій Ethernet

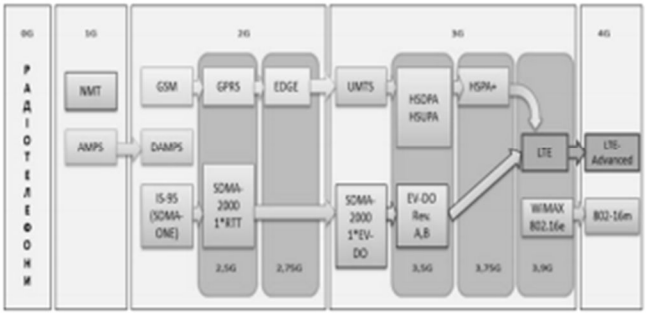


Рис.7. Процес еволюції стандартів безпроводового зв'язку

Рис.6. Архітектура побудови мереж оптичного доступу

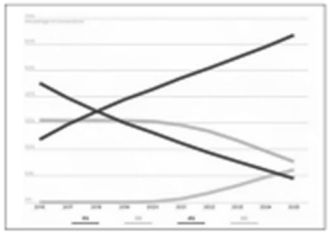


Рис.8. Розподілення технологій

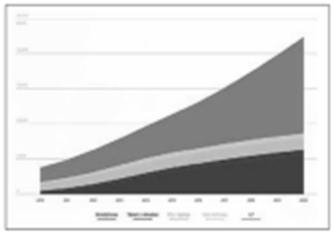


Рис.9. Розподілення пристроїв

Аналіз перспектив впровадження мереж та послуг VPN 5

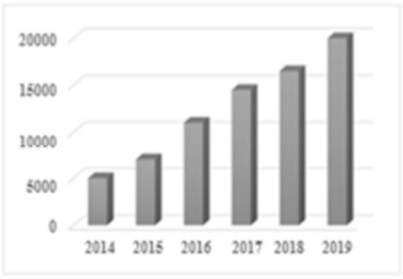


Рис.10. Витрати на VPN в світі

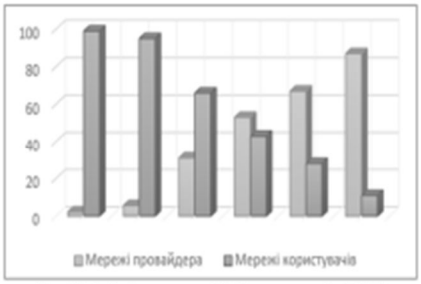


Рис.11 Співвідношення VPN провайдерів і VPN які належать користувачам

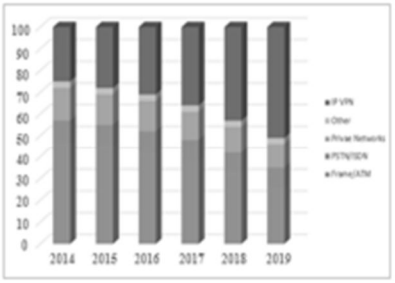


Рис.12. Частка технології IP для реалізації віртуальних приватних мереж

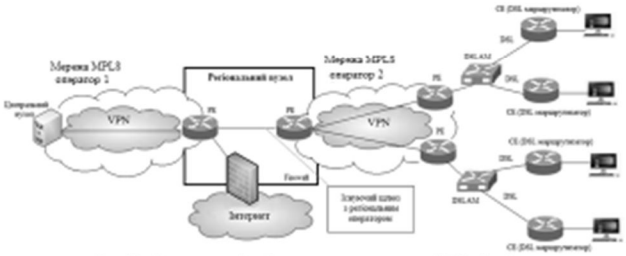


Рис.13. Схема організації загальноукраїнської VPN «Освіта»

На думку багатьох фахівців, VPN входить в трійку найважливіших технологій, які розвиваються і мають великі перспективи на найближче майбутнє. Існують різноманітні способи побудови віртуальних приватних мереж. Ці способи відрізняються розподілом функцій по підтримці VPN між корпоративною мережею і мережею загального користувача провайдера. Виконуючи завдання бакалаврської роботи мною було проаналізовано перспективи впровадження та використання мереж та послуг VPN

Принципи роботи SSH-тунелю 6

Рис.14. Схеми зв'язності і доступності учасників взаємодії

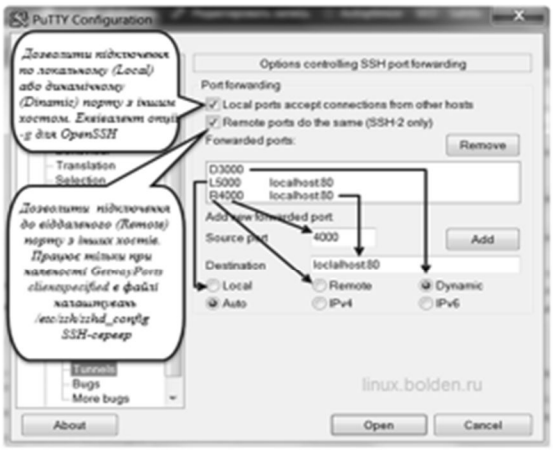
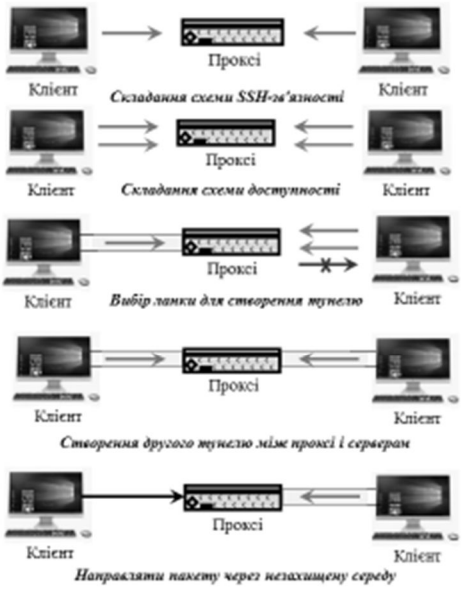


Рис. 16. Приклад налаштування організації підключення

Рис.15.Алгоритм побудови каналу зв'язку за допомогою SSH-тунелів



Практичні приклади застосування SSH-тунелів 7

Прямий та зворотній тунель за базовою схемою

Рис.17. Прямий тунель за базовою схемою

Схема зв'язності і доступності системи клієнт/NAT

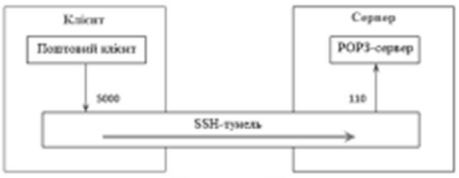


Схема взаємодії

```
Клієнт# ssh -L 5000:Сервер:110 user@Сервер
```
- Еквівалентна команда для OpenSSH клієнта

Налаштування організації підключення

Рис.18. Зворотний тунель за базовою схемою

Схема зв'язності і доступності для системи сервер/NAT

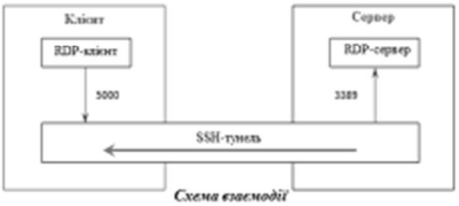


Схема взаємодії

```
Сервер# ssh -R 5000:localhost:3389 user@Клієнт
```
- Еквівалентна команда для OpenSSH клієнта

Налаштування організації підключення

Практичні приклади застосування SSH-тунелів 8

Прямий та зворотній тунель на проміжний SSH-сервер

Рис.20. Прямий тунель

Приклад схеми зв'язності і доступності для випадку, коли клієнт і проксі знаходяться за NAT, а сервер доступний з Інтернету

Схема зв'язності і доступності для випадку, коли проксі є шлюзом, а клієнт розташований за NAT у власній LAN

```
Клієнт# ssh -L 5000:Сервер:3389 user@Прокси
```
- Еквівалентна команда для OpenSSH клієнта

Налаштування організації підключення

Рис.21. Зворотний тунель

Схема зв'язності

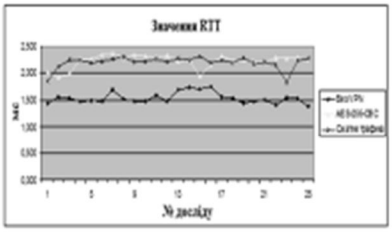
Схема взаємодії

```
Сервер# ssh -R 5000:localhost:3389 user@Прокси
```
- Еквівалентна команда для OpenSSH клієнта

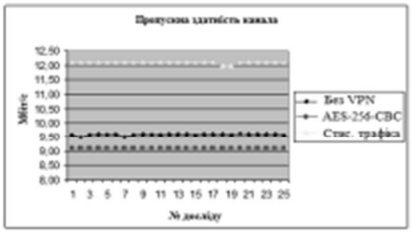
Налаштування організації підключення

Оцінка продуктивності каналів корпоративної мережі 9

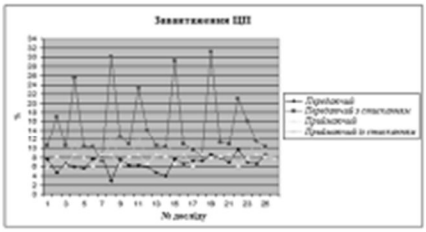
Рис.22. Оцінка продуктивності при використанні технології OpenVPN



Графіки значень RTT

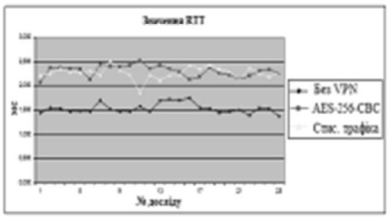


Графіки пропускної здатності каналу

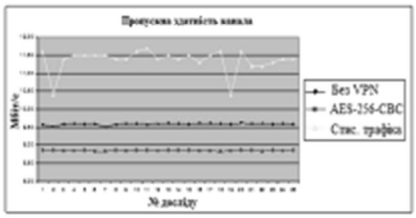


Графіки завантаження ЦП

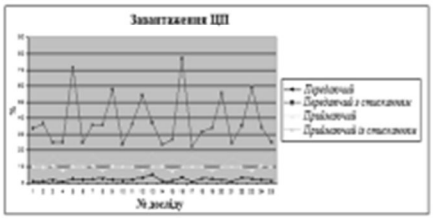
Рис.23. Оцінка продуктивності при використанні технології SSH



Графіки значень RTT



Графіки пропускної здатності каналу



Графіки завантаження ЦП

Модель ідентифікації типу додатків в тунелі мережевого трафіку 10

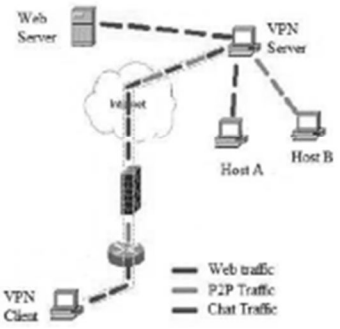


Рис.24.VPN сервіс на рівні IP протоколу

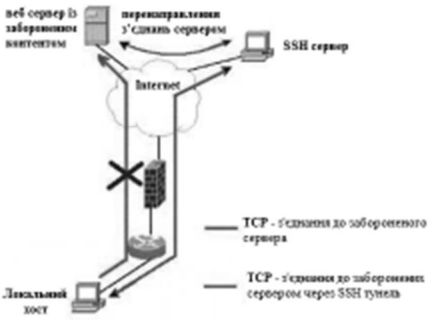


Рис. 25. Тунельне додатки (SSH tunnel) на рівні TCP протоколу

Математичні параметри моделі ідентифікації типу додатки в тунелі трафіку

$$Count(i) = |X|;\ X = \{P_t : iT < t \le (i+1)T\},$$

$$MaxT(i) = Max(t_{k+1} - t_k) :\ iT < t_{k+1}, t_k \le (i+1)T.$$

$$M(i) = \left[10 \cdot lg\left(MaxT(i)\right) + 1\right],$$

$$\theta_m = \{\pi_m,\ A_m, B_m\}.$$

$$P\left(O_c, O_m \middle| \theta_{app,c}, \theta_{app,m}\right) = P\left(O_c \middle| \theta_{app,c}\right) P\left(O_m \middle| \theta_{app,m}\right).$$

Аналіз алгоритмів і програм ідентифікації типів додатків в тунелі трафіку 11

Рис.26. Схема алгоритму захоплення тунельного трафіку для мережепередачі даних

Рис.27. Схема алгоритму обчислення спостережень моделі ІПТТ

Тестування моделі ідентифікації типів додатків в тунелі трафіку 12

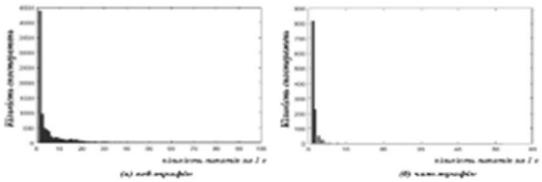


Рис. 29. Розподіл кількості пакетів для кожного досліджуваного додатку

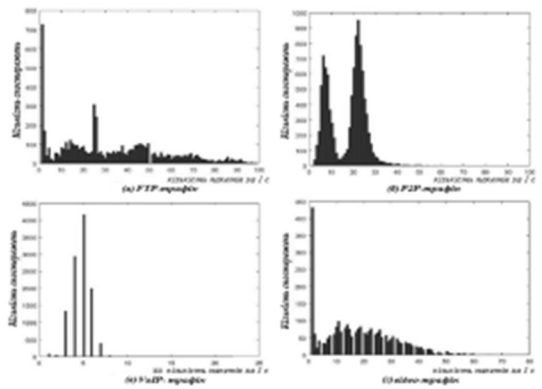


Рис.30. Розподіл кількості пакетів для кожного досліджуваного додатки

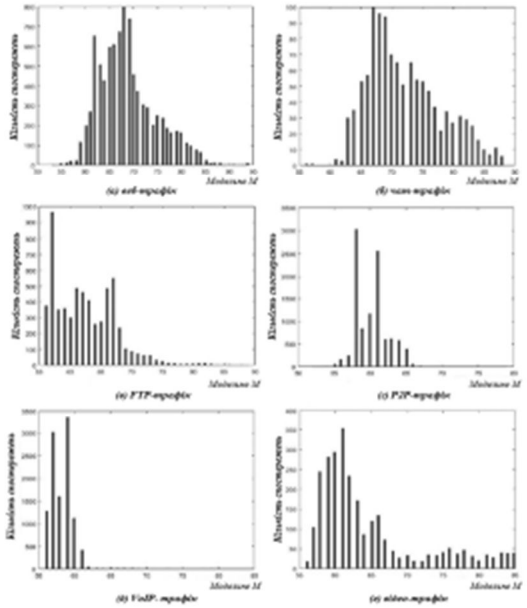


Рис.31. Гістограми максимального інтервалу часу між двома послідовними пакетами для досліджуваних додатків

Оцінки якості моделі ідентифікації типів додатків в тунелі трафіку 13

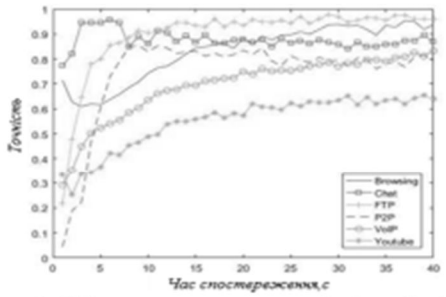


Рис.32. Вплив часу спостереження на точність ідентифікації типів додатків в тунелі трафіку

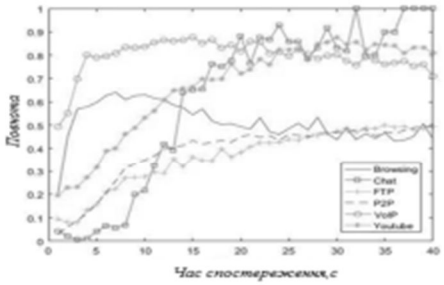


Рис. 33.Вплив часу спостереження на валідність ідентифікації типів додатків в тунелі трафіку

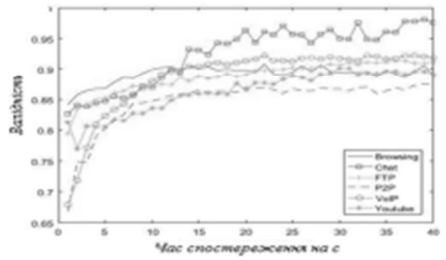


Рис.34. Вплив часу спостереження на валідність ідентифікації типів додатків в тунелі трафіку

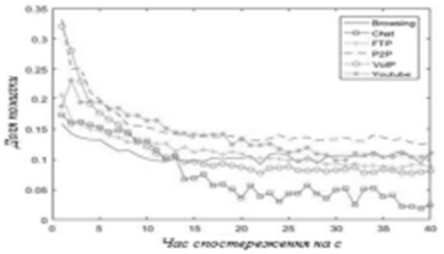


Рис.35. Вплив часу спостереження на частку помилок ідентифікації типів додатків в тунелі трафіку

Висновки 14

Отже виконавши поставлені завдання, у дипломній роботі проаналізовано тенденції розвитку мереж зв'язку на базі різних стандартів і технологій, що показує різноманітність їх вибору для побудови корпоративної мережі.

У другому розділі виконано огляд теоретичного і практичного використання технології SSH при побудові корпоративної мережі, алгоритм побудови каналу зв'язку за допомогою SSH-тунелів та принципи роботи, завдяки якій можливо досягти надійної авторизації та безпечної передачі інформації по відкритих каналах зв'язку.

Досліджено особливості застосування провадження VPN на основі різних технологій в корпоративну мережу, та виконано їх порівняння. Розглянувши всі переваги і недоліки, я прийшов висновку що кращим рішенням буде використання обох технологій разом. Від SSH взяти SSH-тунелі, а від OpenVPN створення VPN мереж

У практичній частині виконано аналіз моделей і алгоритмів ідентифікації типів додатків тунельного трафіку. Експериментальний і теоретичний аналізи трафіка підтверджують можливість виконання з її допомогою моніторингу та ідентифікації типів додатків в тунелі трафіка, даючи можливість виявити шкідливі тип даних що можуть вплинути на якість переданої інформації.

Апробація результатів. Основні положення і результати бакалаврської роботи доповідались і обговорювались на 2-х Науково-технічна конференціях, які проходили в Державному університеті телекомунікацій.