Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Методи захисту інформаційно-телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN

Виконав(ла): студент(ка) 6 курсу, групи СБм-61
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

		Стьопа Д.О.
	(підпис)	(прізвище та ініціали)
Керівник		Карпінський М.П.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Кареліна О.В.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Загородна Н.В.
	(підпис)	(прізвище та ініціали)
Рецензент		Лещишин Ю.З.
	(підпис)	(прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра кібербезпеки

(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ _____

(підпис) (прізвище та ініціали)

« » 20___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня **Магістр**

(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека

(шифр і назва спеціальності)

студенту Стьопа Дмитро Олександрович

(прізвище, ім'я, по батькові)

1. Тема роботи Методи захисту інформаційно-телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN

Керівник роботи д.т.н., професор Карпінський Микола Петрович

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*08*» *листопада* 2021 року № *4/7-941*.

2. Термін подання студентом завершеної роботи 14.12.2021

3. Вихідні дані до роботи Графік локальної домашньої мережі

4. Зміст роботи (перелік питань, які потрібно розробити)

Аналіз актуальності використання VPN технологій.

Аналіз наявних VPN технологій, впровадження самих підходящих.

Розробка VPN на базі вибраної технології ти її тестування.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н, доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., старший викладач		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	*Примітка*
	Опрацюваня завдання		
	Аналіз літературних джерел		
	Написання 1-го розділу		
	Розробка та аналіз мережі		
	Написання 2-го розділу		
	Написання 3-го розділу		
	Опрацювання питань розділу 4		
	Оформлення роботи		
	Перевірка на плагіат		
	Попередній захист		
	Захист		

Студент _____ Стьопа Д.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Карпінський М.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи захисту інформаційно-телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN // Дипломна робота ОР «Магістр» // Стьопа Дмитро Олександрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2021 // С. 63, рис. – 17, табл. – 0, слайдів – 10, додат. – 2.

Ключові слова: МЕРЕЖА, VPN, ПРОТОКОЛ, МАРШРУТИЗАТОР, ТУНЕЛЮВАННЯ, ЗАХИСТ СИСТЕМИ

В даній роботі було проаналізовано підходи до захисту мережі на базі рішення VPN. Визначено основні функціональні аспекти, виявлено ключові переваги та недоліки підходів, проаналізовано та опрацьовано отриману інформацію. Запропоновано варіант створення шифрованого VPN каналу на основі найбільш популярних рішень на сьогодні та на основі домашнього класу маршрутизаторів. Виконано тестування та отримано висновки на основі результатів.

ANNOTATION

Methods of securing information, telecommunication systems and networks from unauthorized access using VPN technology // Thesis of the Master degree // Stiopa Dmytro // Ternopil Ivan Puluj National Technical University, Department of Computer Informatiьion Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2021 // P. 63, Tables – 0, Fig. – 17, Diagrams – 0, Annexes. – 10, References – 2.

Keywords: NETWORK, VPN, NETWORK PROTOCOL, VPN, ROUTER, TUNNELING, SYSTEM SECURITY

This paper analyzes ways of securing a network using VPN technologies. It signifies main functional aspects, describes pros and cons of different approaches, analyzes and processes a data collected. A way of creating an encoded VPN tunnel, using trending solutions and a home-setup router was suggested. Tested and conclusions made.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN – Virtual Private Network

ІТС – Інформаційно-телекомунікаційна система

МЕ – Мережевий (Міжмережевий) екран

ПЗ – Програмне забезпечення

НСД – Несанкціонований доступ

КС – Комп’ютерна система

ОС – Операційна система

L2TP – Layer 2 Transport Protocol

PPP – Point-to-Point Protocol

IPsec – Internet Protocol Security

ВСТУП

Зі збільшенням глобальної мережі – збільшується кількість її користувачів. А чим більше користувачів – тим більше людей, які хочуть корисно скористатись публічністю Інтернету. Користуватись загальнодоступним каналом інформації стає як ніколи небезпечно.

Зловмисники намагаються поцупити персональну інформацію будь-якими способами та йдуть на всі міри. Одним з найпоширеніших способів – прослуховування (спуфінг) каналу, при якому зловмисник підключається до незахищеного середовища передачі інформації і зчитує та зберігає всі данні які транслюються крізь нього.

Через це з’являються все більше і більше нових методів та способів цей канал захистити. Одним з найпоширеніших та, мабуть, безпечніших – є створення віртуальної мережі або ж VPN.

Метод здобув свою популярність з декількох причинах:

- Гнучкість
- Відносна простота
- Шифрування каналу
- Анонімність
- Спосіб створення віддалених мереж

Мета роботи: Проаналізувавши тенденції знайти та запропонувати метод для створення локального шифрованого тунелю.

Об’єкт дослідження: Мережі, глобальні та локальні

Предмет дослідження: методи захисту мереж

Наукова новизна: метод створення мережі на основі комбінації протоколів передачі та шифрування інформації, що є підлаштоване під домашнє користування.

Практичне значення даної роботи: удосконалення методів захисту локальних мереж та об’єднання їх в єдину підмережу.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Інформаційно-телекомунікаційна система

Інформаційно-телекомунікаційною системою називають організаційно-технічну систему, яка виконує функції інформаційної системи, тобто такої системи, що реалізує певну технологію (або сукупність технологій) оброблення інформації та телекомунікаційної системи – технічної системи, що реалізує певну технологію (або сукупність технологій) передавання даних шляхом їх кодування у формі фізичних сигналів.

В вузькому розумінні, інформаційно-телекомунікаційна система – система, що являє собою сукупність телекомунікаційних та інформаційних систем, що у процесі роботи з інформацією діють як одна єдина функціональна система.

Інформаційно-телекомунікаційні системи включають будь-яку систему, що відповідає одному з трьох типів автоматичних систем:

- інформаційна система – організаційно-технічна система, що обробляє інформацію за допомогою програмного забезпечення та обчислювальної техніки;
- телекомунікаційна система – організаційно-технічна система, що надає можливість інформаційного обміну, використовуючи технічні та програмні засоби, шляхом передавання й приймання інформації у вигляді сигналів, знаків, звуків, зображень іншими способами;
- інтегрована система - сукупність кількох взаємопов'язаних інформаційно-телекомунікаційних систем, у яких функціонування однієї або кількох із них залежить від функціонування інших, завдяки чому цю сукупність у процесі взаємодії можна розглядати як одну систему.

Інформаційна система (ІС) - організований набір компонентів, що отримує, збирає, обробляє, передає, зберігає та віддає дані. Інформаційна система складається із обладнання, процесів, процедур, даних, операцій та людей. Кожна інформаційна система включає в себе наступні компоненти:

- вхід і вихід кожного компонента та системи в цілому;
- структура системи;
- мета і обмеження системи та її окремих компонентів.
- функції кожного компонента системи.

ІС не лише відображає функціонування суб’єкта управління, а й впливає на нього через органи управління. Це сукупність інформаційних процесів, які задовольняють інформаційні потреби на різних рівнях прийняття рішень. Його метою є вироблення інформації для використання (споживання) керівництвом. Тому він передбачає збір, передачу, зберігання, обробку та узагальнення інформації знизу вгору, а також специфікацію інформації зверху-вниз.

Метою ІС є опис економічного об'єкта, його станів і взаємодій, виражених в економічних показниках. Вона спрямована на своєчасне забезпечення керівництва необхідною та достатньою інформацією для прийняття рішень, якість яких забезпечує високоефективну роботу об’єкта управління та його підрозділів. Основними завданнями є:

- визначення джерел інформації;
- збір, реєстрація, обробка та видача інформації, що характеризує стан виробництва та управління;
- поширювати інформацію між керівниками, відділами та керівниками на основі їхньої участі в управлінні.

Ключовими елементами будь-якої організації є співробітники, структура, робочі процедури, політика та культура. Інформаційна система також є важливим інструментом для виконання функцій управління.

1.2 Інформаційно-телекомунікаційна мережа

З точки зору інформатики, комп’ютерна мережа, як прототип інформаційно-комунікаційної мережі являє собою єдиний комплекс, що включає територіально розподілену обчислювальну систему та її термінали, за допомогою використання комунікаційного обладнання, програмного

забезпечення та протоколів передачі або отримання інформації. І угоди для вирішення інформаційних, управлінських, обчислювальних або інших завдань.

До наведеного визначення комп’ютерної мережі можна віднести такі ознаки, кожна з яких представляє одну з важливих частин комп’ютерної мережі:

- функціональне призначення будь-якої комп’ютерної мережі пов’язане з передачею та прийомом інформації;
- мережа – це система обчислювальних пристроїв (терміналів), які обробляють інформацію та готують її до відправлення користувачеві;
- передача повідомлень та інформації здійснюється комутаційними пристроями, програмними та технологічними протоколами (набір правил, що регламентують формат і процедури обміну інформацією між користувачами та вузлами).

Поступово інформаційні, технічні, технологічні та комутаційні властивості мереж еволюціонували в більш компактну назву і перетворили її в поняття «інформаційно-телекомунікаційна мережа».

Відмітні ознаки використав законодавець при формулюванні визначення поняття, що міститься у ст. 2 Закону «Про інформацію», згідно з якою інформаційно-телекомунікаційна мережа визначається як технологічна система, призначена для передачі інформації по лініях зв’язку, доступ до якої здійснюється з використанням комп’ютерних технологій.

До складу інформаційно-телекомунікаційної мережі обов'язково має входити три елементи:

- обчислювальна техніка, або комп'ютери;
- канали зв'язку;
- спосіб доступу до каналу зв'язку (комутаційне обладнання).

Система доступу визначається відповідними умовами отримання інформації або ознайомлення з нею. Такі умови визначаються пропускним режимом або сукупністю організаційно-правових і технічних засобів. Вони

можуть включати, у зв’язку зі специфічними умовами функціонування мережі, різноманітні правила та заходи, спрямовані на отримання, передачу та дослідження інформації, у тому числі діяльність, пов’язану з використанням технічних засобів. Швидше, такі політики та дії можуть бути спрямовані на захист інформації в мережі, тобто на блокування доступу до інформації або її відновлення. Іншими словами, доступ — це завжди сукупність програмно-технічних засобів, комутаційних пристроїв, а також правил і заходів, що визначають можливості користувача мережі, тобто законодавчо встановлений склад, що має істотне юридичне значення.

Ця політика визначає термін "засоби зв'язку" - апаратне та програмне забезпечення, включаючи будь-які з цих технічних засобів або їх комбінацію:

- обмін електронними повідомленнями, у тому числі: електронна пошта, передача голосової інформації через електронну пошту, короткі текстові повідомлення, мультимедійні повідомлення;
- інформація ТЗ у сфері доменних імен, доступу до інформаційних ресурсів, управління;
- віддаленого доступу;
- аутентифікації та ідентифікації.

Ці засоби зв’язку підлягають обов’язковому декларуванню (сертифікації) про відповідність вимогам стандарту. При цьому до кожного із зазначених вище технічних заходів встановлюються відповідні вимоги.

Інформаційно-телекомунікаційні мережі можуть бути:

- локальними;
- відомчими, що охоплюють одне відомство або корпорацію;
- регіональними, що об'єднують вузли міст, областей та інших територіальних одиниць;
- спеціального призначення (наприклад, захищена мережа державного підприємства);
- глобальними (Інтернет).

Захист інформації в ІТС - діяльність, спрямована на забезпечення безпеки інформації, що обробляється в ІТС та ІТС загалом, що запобігає або ускладнює можливість виникнення загроз, а також зменшує розмір потенційної шкоди в результаті загроз.

Захищена ІТС - ІТС, що здатна захистити оброблену в ній інформацію від ряду наперед визначених загроз.

Комп'ютерна мережа – це система зв'язку між двома або більше комп'ютерами. У ширшому розумінні комп'ютерна мережа — це система зв'язку по кабелю або повітряному зв'язку, самі комп'ютери різного функціонального призначення та мережеве обладнання. Для передачі інформації можуть використовуватися різні фізичні засоби, як правило, різні типи електричних сигналів або електромагнітне випромінювання. Носіями передачі в комп'ютерних мережах можуть бути телефонні кабелі та спеціальні мережеві кабелі: коаксіальні кабелі, кабелі на витій парі, волоконно-оптичні кабелі, радіохвилі, світлові сигнали.

Комунікаційні мережі можна класифікувати за топологією підключення пристрою. Основні топології:

- шина
- кільце
- зірка
- комбінована

1.3 Проблеми несанкціонованого доступу

Під несанкціонованим доступом слід розуміти доступ до інформації за допомогою засобів, включених до складу КС, що порушує встановлені правила розмежування доступу (ПРД). Несанкціонований доступ може бути реалізований як стандартними засобами, тобто набір програмно-апаратних засобів, включених до КС програмістом під час розробки або системним адміністратором під час роботи, включеним до затвердженої конфігурації КС,

так і за допомогою програмно-апаратного забезпечення, що входить до складу КС зловмисником. Основними методами НСД є:

- прямий доступ до об'єктів для отримання певного типу доступу;
- розробка програмно-технічних засобів посилань на об'єкти в обхід заходів безпеки;
- зміна заходів безпеки, що дозволяють здійснити НСД;
- впровадження програмних або апаратних механізмів у КС, які порушують її структуру та функції та дозволяють здійснити НСД.

Під захистом від НСД, звичайно, слід розуміти діяльність, спрямовану на забезпечення дотримання ПРД шляхом створення і підтримки системи заходів із захисту інформації. Проте зміст даного поняття дещо вужчий, ніж коло питань, що розглядаються. Тому політика безпеки КС може містити вимоги щодо забезпечення доступності інформації, які, наприклад, регламентують, що КС має бути стійка до відмов окремих компонентів. Цю вимогу не можна віднести до ПРД, проте її реалізація здійснюється засобами, що входять до складу комплексу захисту інформації. Тому система надання доступу щодо захисту інформації в КС від НСД охоплює коло питань, пов'язаних з створенням і підтримкою в дієздатному стані системи заходів, що спрямовані на забезпечення додержання вимог політики безпеки інформації під час її обробки в КС.

Під ризиком безпеки розуміють потенційно можливі впливи, події, процеси чи явища, які можуть прямо чи опосередковано зашкодити інтересам об’єктів інформаційних відносин.

Такий збиток розуміється як порушення безпеки інформації, що міститься та обробляється в комп’ютерній системі. З поняттям загрози безпеки тісно зв’язане поняття уразливості КС.

Уразливість КС є одним із найбільш вразливих місць системи, що дає можливість виникнення та реалізації загрози.

Атака на комп’ютерну систему – це дія зловмисника спрямована на пошук та використання вразливостей в системі.

Отже, атака є реалізацією загрози безпеці. За метою впливу розрізняють наступні основні типи загроз безпеки:

- порушення конфіденційності інформації;
- порушення цілісності інформації;
- порушення працездатності системи.

Основними видами загроз безпеці КС та інформації (загрози інтересам суб'єктів інформаційних відносин) є:

- стихійні лиха і аварії;
- зброї і відмови устаткування КС;
- наслідки помилок проектування і розробки компонентів КС;
- помилки експлуатації користувачів, операторів та іншого персоналу;
- навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

Природні небезпеки – це загрози, які пов’язані з впливом на КС та його елементи об’єктивних фізичних процесів або природних явищ, незалежних від людини. Штучні загрози – це загрози КС, викликані діяльністю людини. Серед штучних загроз, виходячи з мотивації дії, можна виділити:

- ненавмисні загрози, викликані помилками в діях персоналу, помилками в проектуванні, помилками в ПЗ, і т.п.;
- навмисні загрози, що являються безпосередніми намірами зловмисників.

Основними принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів.

Порушення безпеки ІТ – несанкціоноване використання ресурсів

За результатами розслідування, яке тривало шість місяців, ЦРУ (https://www.cia.gov) звільнило чотирьох співробітників за створення та використання секретного чату безпосередньо в мережі розвідувального підрозділу. Звільнених визнали неблагонадійними, тому їх не можна було працевлаштувати в подібні організації. Один з них займав високу посаду в американській розвідці. Ще 96 осіб отримали інші покарання.

Близько 160 співробітників, які фліртували, жартували або просто говорили про системи безпеки, брали участь у чаті, що був створений в середині 1980-х. В офіційній заяві ЦРУ цей інцидент назвав "грубим порушенням цілісності мережі". Цей скандал ще раз продемонстрував не лише наявність проблем інформаційної безпеки всередині ЦРУ, а й несерйозне ставлення до них. Можна нагадати, що наприкінці 1996 року Джона Дейча, директора Управління, звільнили за зберігання секретних матеріалів на домашньому комп’ютері, підключеному до Інтернету.

Загалом, люди становлять найбільшу загрозу інформаційній безпеці, тому необхідно передбачати саме їх навмисні чи ненавмисні дії, створюючи систему захисту.

Співробітники служб кібербезпеки поділяють усіх порушників на чотири категорії залежно від потерпілих: сторонні, які не знають компанію; сторонні, які знають компанію та колишніх співробітників; непрограмісти; і співробітники програмістів.

Межа між програмістами і звичайними користувачами в плані загрози останнім часом стала майже не помітна. Останні складають більшість співробітників, зазвичай мають базову комп’ютерну підготовку, і можуть використовувати спеціальне програмне забезпечення з дружнім інтерфейсом, яке можна знайти на піратських компакт-дисках, спеціальних розділах BBS, в Інтернеті та FidoNet. За оцінками експертів, лише чверть співробітників повністю лояльні, чверть співробітників вороже ставляться до компанії і не мають моральних обмежень, а лояльність решти працівників залежить від ситуації. Тому нелояльні співробітники, які контактують з комп’ютерами і

знайомі з системою, становлять серйозну загрозу для ІС. Перш за все, це організаційне питання, і технології тут можуть відігравати лише допоміжну роль.

Для позначення різних типів комп'ютерних злочинців використовуються різні терміни: «хакери», «зломники», «пірати», «шкідники».

Хакер - це загальний термін для людей, які вторгаються в комп'ютерні системи. Цей термін часто використовується для «божевільних програмістів» — згідно з легендою, слово «хак» спочатку використовувалося в Массачусетському технологічному інституті, щоб позначити проект без очевидного практичного значення, для того щоб просто отримати задоволення від процесу. Під терміном «хакер» у більш вузькому розумінні розуміють тих, хто отримує несанкціонований доступ до ресурсів для самоствердження. Останнє відрізняє хакерів від професійних зламувачів, які є серйозними порушниками безпеки, оскільки не мають моральних обмежень.

Група, що найбільше виділяється – пірати, фахівці, які спеціалізуються на крадіжці текстів, технічних знань тощо нових комерційних програмних продуктів. Звичайно, такі роботи виконуються на замовлення або залучають реальних покупців. У разі відсутності замовлень пірати можуть зосередитися на кредитних картках, банківських рахунках і телефонних дзвінках. У всіх випадках мотивацією є матеріальна вигода, а не цікавість чи пустощі.

Згідно з дослідженням IDG, 12% крадіжок спричинені зовнішніми зламами.

Так, наприклад, у січні 2021 року, популярна компанія, що займається розробкою ігор, CD Projekt Red, заявила про хакерську атаку, в результаті якої був викрадений вихідний код низки ігор, через що акції компанії впали на 5%. Код був виставлений на онлайн аукціон на форумах EXPLOIT з початковою ставкою у 1 мільйон доларів.

Шкідники намагаються втілити свої патологічні схильності в кіберпросторі – заражають його шкідливим ПЗ, частково або повністю руйнуючи мережі та системи. У більшості випадків вони завдають собі шкоди

без будь-якої користі (крім моральної сатисфакції). Помста часто є мотивацією. Іноді шкідників надихають руйнівні наслідки, які значно перевищують можливі позитивні успіхи, яких можна було б досягти з подібними зусиллями.

Тому однією з основних причин порушення інформаційної безпеки є наявність творчого потенціалу та неусвідомлення всіх наслідків своїх дій. Цей фактор існує незалежно від національності чи сфери професійної діяльності. Сучасне суспільство лише почало формувати правильне ставлення до комп'ютерних злочинців. Величезні збитки, завдані їх діяльністю, вже відомі. Зазвичай їх успіх пояснюється не навичками, а посередніми промахами в захисті системи (звідси й нове прізвисько-"ламер"). Вважається, що комп'ютерному злочину легше запобігти, ніж розслідувати після. Однак це повністю не вирішує проблему, адже крім бажання людей розважитися або піаритися, є такі характеристики як недбалість, холодні ділові розрахунки, садистський виступ і хвороблива уява. Тому комп'ютерна злочинність досі залишається об'єктом уваги експертів.

З моменту повсюдного впровадження комп'ютерних технологій розробка проблем кіберзлочинності та протидії їм привертала увагу провідних криміналістів. Статистика таких злочинів почалася з 1958 року. Тоді під ними розуміли випадки пошкодження та крадіжки комп'ютерної інформації, техніки, НСД до комп'ютерів, комп'ютерного шахрайства. У 1996 році вперше було використано комп'ютер для пограбування банку (Міннесота).

Сьогодні високотехнологічна злочинна діяльність набирає обертів. В загальному, об'єктами НСД можуть бути апаратні засоби (комп'ютери або периферійні пристрої), ну або ж програмне забезпечення та бази даних, середовищем яких є комп'ютери. У першому випадку злочини можна кваліфікувати за звичайними правовими нормами (крадіжка, злом, розбій, тощо). В інших випадках, коли комп'ютер є одночасно і інструментом, і предметом, злочин відносять до окремої категорії (див. розділ XVI КК України).

1.4 Реалізація VPN

При вході локальної мережі у відкритий Інтернет-простір виникають переважно два види загроз: несанкціонований доступ до даних під час передачі даних у відкритій мережі та доступ до внутрішніх ресурсів КТС. Захист інформації при передаванні даних по відкритих каналах досягається за допомогою таких заходів: взаємна автентифікація всіх сторін, пряме та зворотне шифрування перетворення даних, а також перевірка автентичності та цілісності отриманих даних.

Організація захисту за допомогою технології віртуальної приватної мережі (VPN) передбачає формування безпечного «віртуального тунелю» між вузлами відкритої мережі, який недоступний для потенційних зловмисників. Переваги такої технології очевидні: апаратна реалізація досить проста, немає необхідності створювати або орендувати дорогу виділену мережу, можна використовувати дешевий і відкритий Інтернет, а швидкість передачі даних через тунель така ж, як і в орендованої мережі.

Віртуальна приватна мережа заснована на трьох методах реалізації: тунельному, шифруванні та аутентифікації.

Тунель забезпечує передачу даних між двома точками - кінцями тунелю, щоб джерело даних і приймач приховували всю мережеву інфраструктуру, розташовану між ними.

Середовище передачі тунелю збирає пакети даних використовуваного мережевого протоколу на вході тунелю і передає їх до виходу неушкодженими. Встановлення тунелю достатньо для з’єднання двох мережевих вузлів, тому з точки зору запущеного на них програмного забезпечення вони здаються підключеними до локальної мережі. Однак не можна забувати, що насправді ця пара даних повинна проходити через безліч проміжних вузлів у відкритій загальнодоступній мережі.

Тільки реалізуючи ці три властивості, можна захистити інформаційні ресурси компанії та фізично незахищені канали зв’язку від НСД та витоку інформації.

1.5 Архітектура VPN

Усі продукти, що використовуються для створення VPN, можна розділити на дві категорії: програмне забезпечення та апаратне забезпечення. Програмні рішення VPN, як правило, є готовими програмами, встановленими на окремих комп’ютерах, що підключених до мережі.

Оскільки для створення VPN на основі спеціального програмного забезпечення потрібна окрема комп’ютерна система, такі рішення зазвичай важче розгорнути, ніж апаратні. Створення такої системи передбачає налаштування сервера на розпізнавання комп’ютера та його операційної системи, VPN-пакетів, кожної підключеної мережевої карти та спеціальних засобів для прискорення процесу шифрування.

Безумовно, простіше розгорнути обладнання VPN. Для цього необхідно підключити мережеві пристрої (комутатори, концентратори, маршрутизатори), які підтримують протокол VPN.

Виділяють чотири варіанти побудови VPN мережі.

"Intranet VPN". Дозволяє об’єднати кілька розподілених філій однієї організації в захищену мережу та взаємодіяти через відкриті канали зв’язку. Ця опція широко використовується в усьому світі і в основному реалізується розробниками.

"Remote Access VPN". Безпечна взаємодія між частиною мережі компанії (головний офіс або філія) та окремими користувачами, які підключаються до ресурсів компанії з дому. Віддалений користувач зазвичай не має статичної адреси, замість того, щоб підключатися до захищеного ресурсу через виділений сервіс VPN, він підключається до захищеного ресурсу з власного комп’ютера, на якому встановлено програмне забезпечення, що реалізує функцію VPN.

"Client / Server VPN". Ця технологія захищає дані, що передаються між двома вузлами корпоративної мережі. Особливістю цієї опції є те, що VPN встановлюється між вузлами, як правило, в одному сегменті мережі, наприклад

між робочими станціями та серверами. Ця вимога, зазвичай, виникає, коли у фізичній мережі потрібно створити декілька логічних мереж.

"Extranet VPN" Призначений для мереж, «зовнішніми» користувачами (партнерами, замовниками, клієнтами тощо), рівень довіри яких значно нижчий за рівень довіри співробітників.

Висновки до першого розділу

Коли об’єднання кількох локальних мереж в різних організаціях або структурах для створення приватної мережі є дорогим або займає занадто багато часу, але вам потрібно захистити дані, що передаються між сегментами мережі - ідея побудови власної віртуальної мережі є надзвичайно актуальною. Адже не завжди дозволяється передавати дані у відкритих загальнодоступних мережах. Однак ви можете захистити лише з’єднання між окремими комп’ютерами з різних сегментів мережі, але якщо політика компанії вимагає безпеки більшості інформації, захистити кожен окремий канал і комп’ютер стає набагато складніше. Крім того, захищаючи окремі канали, інфраструктура мережі компанії залишається прозорою для зовнішніх спостерігачів. Для вирішення багатьох проблем архітектура VPN використовується для шифрування всього інформаційного потоку, що передається через публічну мережу.

2 АНАЛІЗ ТА ПОШУК РІШЕНЬ VPN. ОПРАЦЮВАННЯ НАЙКРАЩОГО.

Насправді, найкращий спосіб створити систему, повністю стійку атак - це розірвати всі зв’язки із зовнішнім світом. Мінімальна міра - заборона доступу до Інтернету в комерційних цілях.

До уваги беруться мережі як домашнього, невеликі локальні так і великі корпоративні. Для узагальнення та більш вузького розуміння про мережу, як домашню, мережу університету або корпорації, буде говоритись як про корпоративну мережу.

Захищена VPN — це поєднання локальної мережі та персонального комп’ютера через відкриті зовнішні канали що передає інформацію у єдину віртуальну мережу підприємства, забезпечуючи тим самим безпеку циркуляції даних.

Під час підключення локальної корпоративної мережі до відкритої, існує два основних типи загроз безпеки:

- НСД до даних компанії, що передаються через відкриті мережі;
- НСД до внутрішніх ресурсів локальної мережі компанії, отриманий зловмисником під час несанкціонованого доступу до внутрішньої мережі.

2.1 Засоби VPN

Відповідно до концепції безпеки віртуальної мережі, логічна структура мережі складається лише з мережевого обладнання підприємства і не має нічого спільного з фізичною структурою основної мережі (наприклад, Інтернет).

Такі пристрої, як маршрутизатори та комутатори, приховані від користувачів і пристроїв у мережі компанії. Завдяки тунелюванню можна приховати сервіси VPN від Інтернет-інфраструктури.

Захищена VPN повинна включати засоби захисту від НСД, внутрішні ресурси для локальної мережі компанії та дані компанії, що передаються через

відкриту мережу. Тому інструменти VPN можуть включати дуже широкий спектр пристроїв безпеки: маршрутизатори з вбудованою фільтрацією пакетів, проксі-сервери, багатофункціональні міжмережевих екранів, апаратні та програмні шифри, які передають трафік.

Засоби VPN дуже різноманітні. Вони можуть різнитися один від одного по безлічі характеристик:

- точки розміщення пристроїв;
- тип платформ, на яких ці засоби виконують операції;
- функціональні можливості;
- протоколи автентифікації і алгоритми шифрування.

Характеристики та конфігурація VPN значною мірою залежать від типу використовуваного обладнання. За технічною реалізацією розрізняють переважно наступні види:

- окреме ПЗ, яке доповнює стандартне рішення функціями VPN;
- Незалежний апаратний пристрій на основі виділеної операційної системи реального часу з двома або більше мережевими інтерфейсами та підтримкою апаратного шифрування
- засоби VPN, вбудовані в комутатор або маршрутизатор;
- розширення МЕ за рахунок додаткових функцій захищеного каналу.

Також відоме комбіноване обладнання VPN, яке включає функції VPN, а також функції керування маршрутизатором, МЕ та пропускною здатністю.

Пристрій може діяти як шлюз безпеки або клієнт у VPN.

Шлюз безпеки (security gateway) VPN – це мережевий пристрій, який підключається до двох мереж і виконує функції шифрування та аутентифікації для багатьох хостів, що стоять за ним.

Розташування шлюзу безпеки VPN дозволяє всьому трафіку, призначеному для внутрішньої мережі компанії, проходити через нього. Мережеве підключення шлюзу VPN є прозорим для користувачів за шлюзом; воно представлено виділеною лінією, навіть якщо воно фактично прокладено

через відкриту мережу комутації. Адреса шлюзу VPN вказується як зовнішня адреса вхідного тунельного пакету даних, а внутрішня адреса пакету даних є адресою конкретного хоста за шлюзом.

Шлюз безпеки VPN може бути розроблений як окреме програмне рішення, окремий апаратний пристрій, або у вигляді маршрутизатора або ME, доповненого функціями VPN.

Клієнт VPN — це програмне забезпечення або комплекс програмно-апаратних засобів, які зазвичай виконуються на ПК. Таке мережеве ПЗ було модифіковано для шифрування та перевірки трафіку, яким обмінюється даний пристрій і VPN або інші клієнти VPN. Через обмеження вартості реалізація клієнта VPN зазвичай є програмним рішенням, яке доповнює стандартну операційну систему (Windows або UNIX).

VPN-тунелі можна створювати для різних типів вузлів – це може бути локальна мережа (LAN) зі шлюзом безпеки, або це може бути окремий комп’ютер для віддалених користувачів і мобільних користувачів. Щоб створити віртуальну приватну мережу для великого підприємства, потрібні VPN-шлюз і VPN-клієнт. Шлюз VPN слід використовувати для захисту корпоративної локальної мережі, а VPN-клієнт — для захисту віддалених і мобільних користувачів, яким потрібно підключатися до корпоративної мережі через Інтернет.

2.2 Варіанти побудови захищених каналів VPN

У разі інтеграції локальної мережі та у разі доступу до локальної мережі віддалених або мобільних користувачів необхідно забезпечити безпеку обміну інформацією. При розробці VPN зазвичай розглядаються два основних варіанти (рис. 2.1):

- захищений віртуальний канал між локальними мережами (“мережа-мережа”);
- захищений віртуальний канал між користувачем і локальною

мережею (“користувач-мережа”).

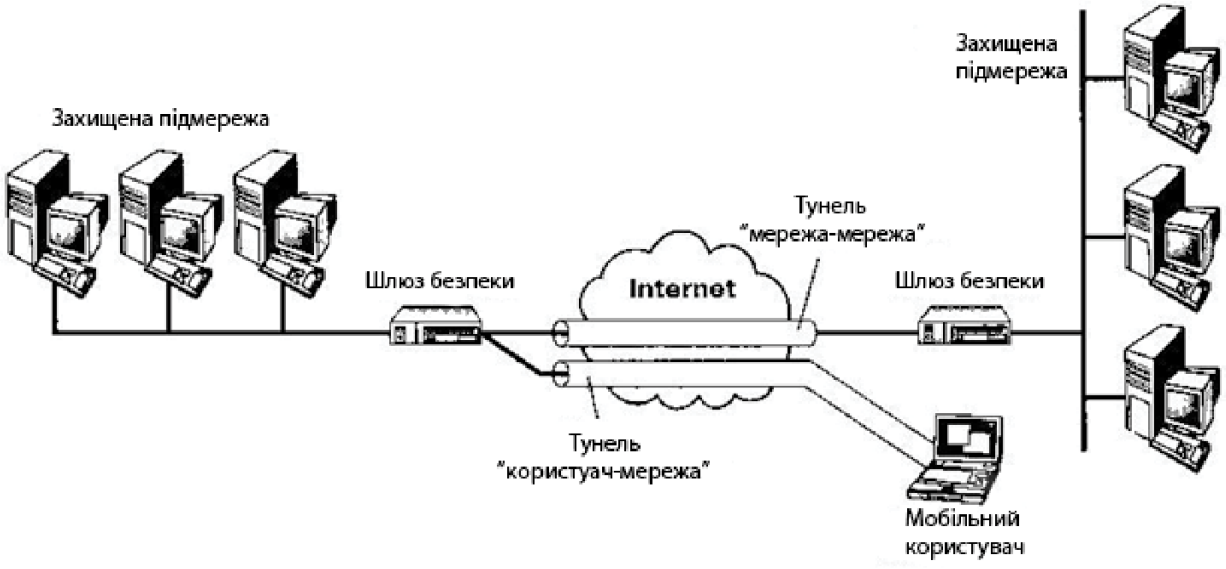

Рисунок 2.1. Тунелі типу «мережа-мережа» та «користувач-мережа»

Перша схема підключення дозволяє замінити дорогі орендовані лінії між офісами та створити захищені і постійно доступні канали між ними. У цьому випадку шлюз безпеки діє як інтерфейс між тунелем і локальною мережею; користувачі локальної мережі використовують тунель для зв’язку одне з одним. Багато компаній використовують цей тип VPN як заміну або доповнення до існуючих WAN-з'єднань (наприклад, Frame Relay).

Другим варіантом безпечних VPN-тунелів є встановлення з’єднань з віддаленими або мобільними користувачами. Створення тунелю ініціює клієнт. Він запускає спеціальне клієнтське програмне забезпечення на своєму комп’ютері для зв’язку зі шлюзом, який захищає віддалену мережу. Цей тип VPN замінює комутовані з’єднання і може використовуватися разом із традиційними методами віддаленого доступу.

При об’єднанні локальних мереж тунелі формуються лише між прикордонними Інтернет-провайдерами або маршрутизаторами локальної мережі. Через віддалений доступ до локальної мережі створюється тунель між сервером віддаленого доступу інтернет-провайдера і прикордонним Інтернет-провайдером або маршрутизатором локальної мережі.

Віртуальна корпоративна мережа, побудована на основі цієї опції, має хорошу масштабованість і керованість. Сформований тунель безпеки повністю прозорий для клієнтських комп'ютерів і серверів у локальній мережі, а сама мережа є частиною цього типу віртуальної мережі. Програмне забезпечення цих вузлів залишається незмінним.

Існуюча інфраструктура корпоративної мережі може бути підготовлена до використання рішень VPN за допомогою обох, як програмного так і апаратного забезпечення.

2.3 Сервіси безпеки мережі

При створенні захищеного VPN завдання інформаційної безпеки є дуже важливим. За загальноприйнятими визначеннями під безпекою даних розуміють забезпечення їх конфіденційності, цілісності та доступності. Щодо завдань VPN стандарти безпеки можна визначити таким чином:

- конфіденційність – гарантія того, що дані можуть бути відомі лише законним відправникам і одержувачам під час передачі через захищений канал VPN;
- цілісність – гарантія, що передані дані зберігаються під час проходження через захищений VPN-тунель. Будь-які спроби змінити, модифікувати, знищити або створити нові дані будуть виявлені та відомі законним користувачам;
- доступність – гарантія того, що законні користувачі завжди можуть використовувати інструменти VPN. Доступність засобів VPN – це комплексний показник, який залежить від багатьох факторів: надійності впровадження, якості обслуговування, ступеня захисту самого інструменту від зовнішніх атак.

Конфіденційність забезпечується різними методами та алгоритмами симетричного та асиметричного шифрування. Цілісність зазвичай досягається за допомогою різних варіантів технології електронного підпису на основі симетричних і асиметричних методів шифрування та односторонніх функцій.

Автентифікація базується на множинних і одноразових паролях, цифрових сертифікатах, смарт-картках, суворих протоколах перевірки ідентичності та гарантує, що VPN-з’єднання встановлюються лише між законними користувачами, щоб запобігти доступу небажаних людей до тунелю.

Авторизація – це надання певних видів прав абонентам, які довели свою легітимність (автентичність), включаючи різні способи шифрування свого трафіку. Авторизація та контроль доступу зазвичай реалізуються однаково.

Для убезпечення даних, що передаються у віртуальній приватній мережі, необхідно вирішувати такі основні завдання мережевої безпеки:

- взаємна автентифікація користувачів при встановленні з'єднання;
- конфіденційність, цілісність і автентичність інформації, що передається;
- авторизація та управління доступом.

2.4 Протоколи VPN

Протокол VPN визначає, як система VPN взаємодіє з усіма системами в Інтернеті та рівень безпеки трафіку. Враховуючи використання внутрішнього обміну інформацією, взаємодія не є пріоритетом, але якщо все навпаки, вашу власну протоколи використовувати не слід. Іншими словами, протокол VPN впливає на рівень безпеки всієї системи. Причина в тому, що між двома кінцевими вузлами використовується шифрування. Якщо інформація не захищена, зловмисник може перехопити ключ і розшифрувати трафік.

Щоб створити VPN за допомогою апаратного та програмного забезпечення, важливо дотримуватися стандартного механізму, заснованого на безпеці протоколу Інтернету (IPSec). У ньому детально представлені метод ідентифікації та метод шифрування, ініціалізації тунелю. Недоліком є те, що він орієнтований на використання IP-адрес.

Наступними протоколами, які використовуються для створення VPN, є протокол тунелювання «точка-точка» (PPTP), протокол переадресації другого рівня (L2F) і протокол тунелювання другого рівня (L2TP), які поєднують два вищезазначені протоколи. Але вони не є комплексними і не повністю функціональні.

Інший протокол, Internet Key Exchange (IKE) забезпечує передачу інформації через тунелі, усуваючи зовнішні перешкоди. Його завдання — безпечно керувати та обмінюватися ключами шифрування між віддаленими вузлами. IKE використовує механізм шифрування з відкритим ключем для автоматичного виконання процесу передачі ключів. IKE змінює ключ підключення, що підвищує конфіденційність переданої інформації. Одночасна інкапсуляція — забезпечує мультиплексування кількох протоколів передачі через один канал.

Протокол Link Control Protocol (LCP) – протокол "точка-точка" (PPP), що визначає гнучкий LCP, який використовується для встановлення, налаштування та перевірки каналів зв'язку. LCP погоджується з форматом інкапсуляції, розміром пакета, параметрами налаштувань, роз'єднанням та параметрами аутентифікації.

Протокол управління мережею визначає конкретні параметри конфігурації для конкретного протоколу передачі.

Для створення VPN-тунелів використовуються протоколи PPTP, L2TP, IPsec і OpenVPN.

2.5 Аутентифікація

Аутентифікація здійснюється з допомогою відкритого тестування (plain text) або схем запиту/відповіді. З звичайним текстом все зрозуміло: клієнт надсилає пароль на сервер, а сервер порівнює його зі існуючим і надає/забороняє доступ. Відкрита аутентифікація майже відсутня.

Схема запит/відгук набагато більше поширена. Загалом це виглядає так:

- клієнт надсилає запит серверу (request) на аутентифікацію;
- сервер генерує випадковий код (challenge) та повертає;
- клієнт знімає хеш зі свого пароля (хешування є результатом хеш-функції, яка перетворює масив вхідних даних довільної довжини в рядок вихідних бітів фіксованої довжини), шифрує їм код і повертає його серверу;
- аналогічну операцію виконує сервер та порівнює свій результат з результатом клієнта;
- якщо є збіг – клієнт вважається автентифікованим.

На першому етапі аутентифікації клієнтів і серверів VPN, використовуються протоколи L2TP поверх IPSec.

L2TP поверх IPSec використовує локальні сертифікати, які він отримує від служб аутентифікації. Сервер і клієнт обмінюються сертифікатами і створюють безпечне з'єднання ESP SA (Security Association). Після того, як L2TP завершує процес аутентифікації комп’ютера, виконується аутентифікація на рівні користувача. Для аутентифікації може використовуватись будь-який протокол, навіть PAP, щоб публічно передати ім’я користувача та пароль. Це повністю безпечно, оскільки L2TP шифрує весь сеанс через IPSec. Однак використання MSCHAP для аутентифікації користувачів (використання різних ключів шифрування для перевірки вашого комп’ютера та ідентичності користувача) може покращити безпеку.

Шифрування PPTP гарантує, що ніхто не зможе отримати доступ до даних, коли вони надсилаються через Інтернет.

Тому зв’язка «тунель - аутентифікація - шифрування» дозволяє передавати дані між двома точками через загальнодоступну мережу, імітуючи роботу локальної мережі. Іншими словами, ці інструменти дозволяють побудувати VPN.

Ще одна перевага VPN-з'єднання полягає в тому, що система адресації, що використовується в локальній мережі, може бути використана для адресації.

Фактична реалізація віртуальної приватної мережі виглядає наступним чином. Сервер VPN встановлюється в локальній мережі офісу компанії. Віддалений користувач (або маршрутизатор) використовує програмне забезпечення клієнта VPN, щоб ініціювати процес з'єднання із сервером.

Автентифікація користувача – перший етап встановлення VPN-з'єднання. У разі підтвердження авторизації настає другий етап - клієнт і сервер узгоджують деталі безпеки підключення. Після цього буде створено VPN-з'єднання для забезпечення обміну інформацією між клієнтом і сервером у вигляді кожного пакету даних, який проходить шифрування/дешифрування та перевірку цілісності – процес аутентифікації даних. Основною проблемою VPN є відсутність встановлених стандартів аутентифікації та обміну зашифрованою інформацією. Ці стандарти все ще розробляються, тому продукти різних виробників не можуть автоматично встановлювати VPN-з'єднання та обмінюватися ключами. Ця проблема сповільнює популярність VPN, оскільки важко змусити різні компанії використовувати продукти одного виробника, тому важко об'єднати мережі компаній-партнерів у так званий екстранет.

2.6 Авторизація і управління доступом

Система авторизації обробляє легальних користувачів, що успішно пройшли автентифікацію. Метою системи авторизації є надання конкретним законним користувачам прав доступу до мережевого ресурсу, визначеному системним адміністратором.

Система авторизації не тільки надає законним користувачам певні права доступу до файлів, принтерів та каталогів, але й регулює шифрування пакетів даних, створення цифрового підпису та доступ до певних пристроїв VPN.

Програма авторизації реалізується програмним забезпеченням, вбудованим в операційну систему або прикладну програму. При створенні авторизаційного ПЗ використовуються два методи:

- централізована авторизація;
- децентралізована авторизація.

Основною метою централізованої системи авторизації є реалізація принципу єдиного входу. Процесом надання ресурсів користувачам керує сервер. Централізований метод авторизації реалізований в таких системах як Kerberos, RADIUS, TAGACS.

Завдяки методу децентралізованого процесу авторизації кожна робоча станція оснащена функціями безпеки. У цьому випадку доступ до кожної програми має контролюватись шляхом захисту операційного середовища, в якому працює програма. Адміністратори мережі повинні контролювати інструменти безпеки, які використовуються всіма типами програм. Коли ви видаляєте або додаєте нових користувачів, ви повинні налаштувати права доступу до кожної програми або системи.

У великомасштабних мережах зазвичай використовується комбінація цих методів для надання законним користувачам доступу. Сервер віддаленого доступу обмежує користувачів у доступі до великих мережевих елементів — підмереж, сегментів мережі або корпоративних серверів. Кожен окремий веб-сервер обмежує доступ користувачів до своїх внутрішніх ресурсів (каталогів, програм або принтерів).

Зараз активно розвивається так званий рольовий контроль доступу. Це не стільки вирішення проблеми безпеки, як покращення керованості системи. Кожному користувачеві можна призначити кілька ролей одночасно, і кожна роль надає йому певні права.

Складність інформаційної системи в основному характеризується кількістю зв'язків, які вона містить. Оскільки ролей менше, ніж користувачів і дозволів, розподіл ролей допомагає зменшити складність, тим самим покращуючи керованість системи.

Крім того, рольова модель, заснована на контролі доступу, може реалізувати такі важливі принципи, як поділ обов’язків (тому, наприклад,

неможливо скомпрометувати ключові процеси самостійно). Ролі можуть визначати статичні або динамічні несумісні відносини (наприклад, сутність не може грати дві ролі одночасно).

2.7 Класифікація віртуальних приватних мереж

Різні автори по-різному класифікували VPN. Найбільш часто використовуються наступні три класифікаційні ознаки:

- рівень моделі OSI на якому розгорнутий сервіс;
- структурне технічне рішення;
- технічна реалізація.

2.8 Класифікація VPN за рівнем моделі OSI

Для безпечної технології передачі даних у публічних (незахищених) мережах використовується термін «захищений канал». Термін «канал» підкреслює той факт, що деякі віртуальні шляхи, прокладені в мережі з комутацією пакетів, забезпечують захист даних між двома вузлами мережі (хостами або шлюзами).

Для побудови захищених каналів можна використовувати системні інструменти, реалізовані на різних рівнях моделі взаємодії відкритої системи OSI (рис. 2.2).

Рисунок 2.2. Рівні протоколів захищеного каналу

Класифікація VPN за робочим рівнем моделі OSI становить велику зацікавленість, оскільки функції VPN залежать від обраного рівня модулі OSI та її сумісності з додатками ІС, а також сумісності з іншими методами захисту.

За робочим рівнем моделі OSI виділяють такі групи VPN:

- VPN канального (2) рівня;
- VPN мережевого (3) рівня;
- VPN сеансового (5) рівня.

2.9 VPN канального рівня

VPN, що використовуються на рівні тунельного рівня OSI, дозволяють інкапсулювати різні типи трафіку рівня 3 (і вище) і будувати віртуальні тунелі «точка-точка» (маршрутизатор – маршрутизатор або персональний комп’ютер – шлюз локальної мережі). До цієї групи входять продукти VPN, що використовують протоколи L2F і PPTP, а також нещодавно затверджений стандарт L2TP, спільно розроблений Cisco Systems і Microsoft.

Протокол PPTP заснований на протоколі PPP і широко використовується в з'єднаннях "точка-точка", наприклад, під час роботи на виділеній лінії. Протокол PPTP надає прозорість функцій безпеки для програм і служб на прикладному рівні і не залежить від використовуваного протоколу мережевого

рівня. Зокрема, протокол PPTP може переносити пакети даних в мережах IP і IPX, DECnet або NetBEUI. Однак, оскільки протокол PPP використовується не у всіх мережах PPTP не можна розглядати як універсальний.

Коли організації віддалено отримують доступ до локальної мережі, L2TP може бути найчастішим рішенням (оскільки він в основному базується на Windows). У той же час рішення другого рівня навряд чи буде важливим для взаємодії з локальною мережею, тому що якщо потрібно кілька тунелів із загальнодоступними кінцевими точками, масштабованість недостатня.

2.10 VPN мережевого рівня

Продукти VPN мережевого рівня інкапсулюють IP в IP. Одним із відомих протоколів цього рівня є SKIP, який поступово замінюється новим протоколом IPSec для аутентифікації, тунелювання та шифрування пакетів даних IP. Протокол IPSec, стандартизований комітетом Internet Engineering Task Forc, увібрав в себе всі найкращі рішення для шифрування пакетів даних, і його мають включити як обов’язковий компонент протоколу IPv6.

Протокол IPSec забезпечує стандартний метод ідентифікації користувача або комп’ютера під час ініціювання тунелю, стандартний метод використання шифрування кінцевої точки тунелю та стандартний метод обміну ключами шифрування та керування ними між кінцевими точками.

IPSec швидко стає популярним і може стати основним способом VPN для взаємодії з локальною мережею. У той же час пам’ятайте, що специфікація IPSec орієнтована на IP, тому вона не підходить для трафіку, що передається на будь-який інший протокол мережевого рівня. IPSec може працювати з L2TP, тому ці два протоколи забезпечують більш надійне шифрування, ідентифікацію та цілісність даних. Тунель IPSec між локальними мережами може підтримувати кілька окремих каналів даних, надаючи цьому типу додатків перевагу в масштабованості над технологією другого рівня.

Говорячи про IPSec, слід згадати про протокол Internet Key Exchange (IKE), який захищає передану інформацію від зовнішніх перешкод. Він

вирішує проблему безпечного керування та обміну ключами шифрування між віддаленими пристроями. Протокол IKE заснований на шифруванні з відкритим ключем, який автоматично здійснює обмін ключами та встановлює безпечне з’єднання, тоді як IPSec шифрує та «підписує» пакети даних. Крім того, IKE дозволяє змінювати ключ встановленого з'єднання, що підвищує конфіденційність переданої інформації.

2.11 VPN сеансового рівня

Деякі VPN реалізують інший метод, який називається проксі-сервером. Цей метод працює над транспортним рівнем і ретранслює трафік з захищеної мережі до загальнодоступного Інтернету для кожного сокета. (IP-сокети визначаються комбінацією TCP-з'єднання та певного порту або даного порту UDP. IP-адреса не має п'ятого рівня сеансу, але операції, орієнтовані на сокет, зазвичай називають операціями на рівні сеансу.)

Шифрування інформації, що передається її термінатором та ініціатором, зазвичай виконує транспортний рівень TLS. Щоб стандартизувати канал аутентифікації через МЕ, альянс IETF визначив протокол під назвою SOCKS. Зараз для стандартизації реалізації каналів-посередників використовується SOCKS v.5.

2.12 Класифікація за способом технічної реалізації

За технічною реалізацією розрізняють такі групи VPN:

- на основі мережевої ОС;
- на основі МЕ;
- на основі маршрутизаторів;
- на основі ПЗ;
- VPN на основі спеціального обладнання з вбудованим криптографічним процесором.

2.13 VPN на основі мережевої ОС

Візьмемо, як приклад, операційну систему Window, розглянемо впровадження VPN на основі мережевої ОС. Щоб створити VPN, Microsoft надає протокол PPTP, інтегрований у мережеву операційну систему Windows. Для організацій, які використовують корпоративну операційну систему Windows, це рішення виглядає привабливим. VPN на базі Windows використовує клієнтську базу даних, що зберігається в первинному контролері домену (PDC). Під час підключення до сервера PPTP користувач авторизується через протоколи CHAP, PAP або MS CHAP. Шифрування використовує нестандартний власний протокол шифрування «точка-точка», а 40-бітний ключ отримується після встановлення з'єднання.

Як перевагу даного рішення слід зазначити, що вартість рішення на основі мережевої операційної системи значно нижча за вартість інших рішень.

Недолік такої системи – недостатня захищеність PPTP.

2.14 VPN на основі маршрутизаторів

Цей метод створення VPN передбачає використання маршрутизатора для створення безпечного каналу. Оскільки вся інформація, що відправляється з локальної мережі, переходить через маршрутизатор, цілком природно взяти на себе завдання шифрування.

Прикладом пристрою VPN на маршрутизаторі є пристрій Cisco Systems. Починаючи з iOS 11.3, маршрутизатори Cisco підтримують L2TP і IPSec. Окрім простого шифрування інформації, Cisco також впровадила інші функції VPN, такі як тунельна аутентифікація та обмін ключами. Додатковий модуль шифрування сервісного адаптера шифрування Encryption Service Adapter (ESA) можна використовувати для покращення продуктивності маршрутизатора.

2.15 VPN на основі МЕ

Більшість виробників міжмережевих екранів включають функції тунелювання та шифрування даних. Це рішення засноване на простому міркуванні: оскільки інформація проходить через МЕ, чому вона не шифрується одночасно? Модуль шифрування додається до самого програмного забезпечення.

До недоліків такого підходу можна віднести високу вартість рішення на робочому місці та залежність продуктивності на апаратному забезпеченні. Використовуючи МЕ на ПК, слід пам’ятати, що подібні варіанти підходять лише для невеликих мереж з обмеженим обсягом переданої інформації.

Прикладом рішення на основі МЕ є продукт Firewall-1 розробника Check Point Software Technologies.

2.16 VPN на основі ПЗ

Програмні рішення також використовуються для створення VPN. Реалізація такого типу рішення використовує спеціальне ПЗ що працює на спеціальному комп’ютері, і в більшості випадків виступає в ролі проксі-сервера. Комп’ютер з таким ПЗ може бути розташований на МЕ.

Прикладом програмного рішення є Digital AltaVista Tunnel 97. При використанні цього програмного забезпечення клієнт підключається до сервера Tunnel 97, реєструється та обмінюється ключами. Шифрування базується на ключі шифрування 56 або 128 біт RC 4. Зашифрований пакет даних інкапсулюється в інші пакети даних IP і надсилається на сервер. Під час роботи сервер Tunnel 97 перевірить цілісність за допомогою MD5. Крім того, кожні півгодини система сама перегенеровує ключ, що значно підвищує безпеку.

Переваги програмного пакета AltaVista Tunnel 97 - простота встановлення та проста в управлінні. До недоліків можна віднести нестандартну архітектуру і низьку продуктивність.

2.17 VPN на основі спеціального обладнання з вбудованим криптографічним процесором.

Варіант створення VPN на спеціальному обладнанні можна використовувати для мереж, які потребують високої продуктивності. Наприклад, продукт cIPro-VPN від Radguard. Пристрій виконує апаратне шифрування інформації, та має швидкість передачі 100 Мбіт/с.

cIPro-VPN обслуговує механізм керування ключами ISAKMP/Oakley та IPSec. Крім того, пристрій транслює мережеві адреси і може бути оснащений спеціальними платами, які виконують функції ME.

Недоліком такого рішення є його висока вартість.

2.18 Побудови захищених корпоративних мереж на основі VPN-рішення

2.18.1 Основні варіанти рішень

У потенційних клієнтів є широкий спектр апаратного та програмного забезпечення для розгортання VPN: від інтегрованих багатофункціональних і спеціалізованих пристроїв до чистих програмних продуктів.

Виділяють такі основні види рішень VPN:

- програмні.
- інтегровані;
- спеціалізовані;

Програмно реалізовані VPN-продукти поступаються за продуктивністю виділеним пристроям, але мають достатньо потужностей для реалізації мереж VPN. Слід зазначити, що у випадку віддаленого доступу необхідна дуже мала пропускна здатність. Таким чином, чисті програмні продукти можуть легко забезпечити достатню продуктивність для віддаленого доступу. Безсумнівними перевагами такого підходу є гнучкість і простота використання, а також відносно невисока вартість.

Інтегроване рішення VPN включає МЕ, функції маршрутизації та комутації. Основною перевагою цього методу є централізація управління елементами. Для компаній, які не потребують високопродуктивної корпоративної мережі, зниження вартості мережевого обладнання є одним з першочергових завдань, а найефективніше - інтегроване рішення, що дозволяє сконцентрувати всі функції на одному пристрої. Однак слід зазначити, що чим більше функцій виконує пристрій, тим очевиднішими будуть втрати продуктивності.

Висока продуктивність є основною перевагою спеціалізованого обладнання VPN. Більш висока швидкість цього типу системи пояснюється шифруванням, що виконується спеціальним чіпом.

Обсяг обчислень, що необхідно виконати при роботі з пакетами VPN, у 50-100 разів перевищує кількість обчислень, необхідних для обробки звичайних пакетів. Якщо мережа підприємства виконує різні види діяльності, які вимагають високого обміну трафіком, то для ефективної обробки пакетів даних VPN рекомендується використовувати спеціальне обладнання. Спеціальне обладнання VPN забезпечує високий рівень безпеки, але за високу вартість.

Як правило, в основному використовують комбіновані VPN на основі існуючих рішень.

Так як нас цікавить VPN на базі маршрутизаторів, розглянемо це рішення детальніше.

2.18.2 Створення VPN на базі маршрутизаторів

Сьогодні майже усі провідні виробники маршрутизаторів та іншого мережевого обладнання заявили, що їхні продукти підтримують різні протоколи VPN. В Україні беззаперечним лідером на цьому ринку є Cisco Systems, тому побудову корпоративної VPN рекомендується продемонструвати на рішенні компанії.

Починаючи з версії Cisco IOS 12.x, побудова VPN-тунелів на основі маршрутизаторів Cisco здійснюється через операційну систему. Якщо

операційна система встановлена на прикордонних маршрутизаторах Cisco в інших філіях компанії, можна створити корпоративну VPN, яка містить набір віртуальних безпечних тунелів типу «точка-точка» від одного маршрутизатора до іншого (рис. 2.3). Далі використовується діаграма VPN бренду, отриману на веб-сайті виробника, як ілюстрацію. Зазвичай для шифрування даних у каналі за замовчуванням використовується алгоритм шифрування DES з довжиною ключа 56 біт.

Нещодавно компанія запустила новий продукт– Cisco VPN client, що дозволяє створювати безпечні з'єднання «точка-точка» між вузлами (включно з видаленими) і маршрутизаторами Cisco, що дозволяє побудувати internet- та localnet-VPN.

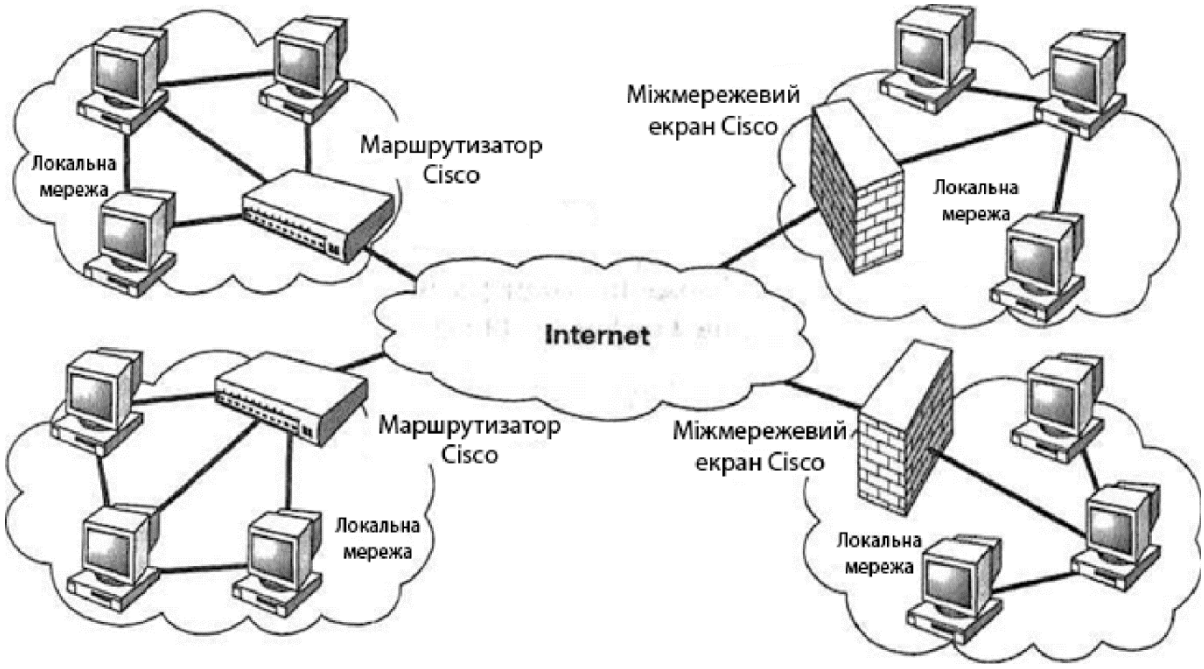

Рисунок 2.3. Типова схема побудови корпоративної VPN на базі маршрутизаторів Cisco

Для реалізації VPN тунелю маршрутизатори Cisco використовують протокол канального рівня L2TP (створений на базі L2F і PPTP) і протокол IPSec.

Протокол L2TP інкапсулює протоколи мережевого рівня в пакети канального рівня, що підтримують доставку в каналах «точка-точка». Незважаючи на те, що цей протокол і надає рішення проблем безпеки, він не має специфікації шифрування, автентифікації і перевірки цілісності, що передається по загальнодоступній мережі, а також управління криптографічними ключами. Основна перевага L2TP - його незалежність від транспортного рівня, що дозволяє йому використовуватись в гетерогенних мережах. Достатньо важливою перевагою L2TP є його сумісність з ОС Windows, через що, в принципі, можна створювати комбіновані VPN на базі продуктів Cisco та Microsoft. Проте його «канальна природа» послужила причиною його найбільшого недоліку: для гарантованої передачі пакету всі проміжні маршрутизатори мають підтримувати цей протокол, що, очевидно, дуже важко гарантувати. Через це компанія Cisco сьогодні почала звертати увагу до просування сучаснішого протоколу - IPSec.

Зараз IPSec – один з протоколів Internet, що працюють, і є досконалими в плані безпеки. Він забезпечує автентифікацію, перевірку на цілісність і шифрування на рівні кожного пакету. Також використання протоколом мережевого рівня є стратегічною перевагою IPSec, так як VPN технології працюють повністю прозоро для всіх без виключення додатків і мережевих сервісів.

Але є недоліки IPSec - підтримка виключно стеку TCP/IP і великий об'єм службової інформації, що в перспективі викликає зниження швидкості обміну даними на каналах зв'язку.

При створенні VPN на основі маршрутизатора важливо пам’ятати, що використання лише цього методу не вирішує проблему загальної безпеки інформації компанії, оскільки всі інформаційні ресурси залишаються відкритими для атак ззовні. Для захисту цих ресурсів зазвичай

використовується МЕ, що знаходиться за прикордонним маршрутизатором, тому вся конфіденційна інформація знаходиться у «відкритому» вигляді на шляху від маршрутизатора до МЕ і далі. Це означає, що маршрутизатор повинен бути якомога ближче до МЕ, бажано в загальнодоступному захищеному приміщенні.

Одним із найбільших недоліків побудови VPN на основі маршрутизатора є те, що рішення однієї тільки проблеми захисту інформації компанії від зовнішніх атак розподіляється між кількома функціонально незалежними пристроями (наприклад, маршрутизаторами та МЕ). У разі визначення відповідальності за витік мережевої інформації цей метод може спричинити серйозні організаційні та технічні проблеми.

Висновки до другого розділу

Проаналізувавши значну частину сучасних рішень та технологій, найкращим варіантом для дослідження, демонстрації та тестування буде використати підхід створення мережі на основі маршрутизатора. Такий підхід явно покаже що відбувається на прикладі самої звичайної домашньої мережі, яку має буквально кожен будинок, в якому є Wi-Fi роутер.

3 РОЗРОБКА МЕРЕЖІ НА БАЗІ РІШЕНЬ VPN

3.1 Опис характеристик

Для подальших операцій буде використовуватись маршрутизатор MikroTik hAP ac².

Основні характеристики:

- Частоти: 5 ГГц + 2.4 ГГц (двухдіапазонний)
- Інтерфейси:
  - WAN 10/100/1000
  - чотири LAN 10/100/1000
  - USB 2.0 type A
- Пікова швидкість портів 1 Гбіт/с
- Пікова швидкість Wi-Fi 1167 Мбіт/с

- Стандарти зв’язку Wi-Fi:
  - Wi-Fi 802.11b/g/a,
  - Wi-Fi 4 (802.11n),
  - Wi-Fi 5 (802.11ac)
- Антени внутрішні
- Підтримка протоколів DHCP, IPsec, L2TP, NAT, PPPoE, PPTP
- Вбудований Firewall
- Процесор IPQ-4018 (4 ядра, номінальна частота 716 МГц)
- Об’єм оперативної пам’яті 128 МБ
- Операційна система RouterOS на базі ядра Linux

Можливостей та варіантів розгортання VPN на даному маршрутизаторі є велика кількість. Проте існують 2 принципіально різних підходи до вирішення такої проблеми:

1) Створення L2 тунелю типу site-to-site за допомогою EOIP Tunnel. Мабуть, найшвидший спосіб об’єднання таких мереж. Без шифрування такі рішення являються найшвидшими рішеннями по тунелюванню.

2) VPN з'єднання рівня L3 за технологією клієнт-сервер, типу PPTP, L2TP, SSTP, OpenVpn. Такі з'єднання використовуються як для об'єднання офісів так і для підключення віддалених співробітників. Працює через NAT.

3.2 Налаштування L2TP протоколу

Спочатку налаштуємо простий L2TP тунель без шифрування, зробимо заміри, додамо шифрування та перевіримо знову.

Для початку потрібно задати пул адрес (рис. 3.1), на яких дана мережа буде прокладатись. Для цього створює новий пул, задаючи його назву та проміжок адрес.

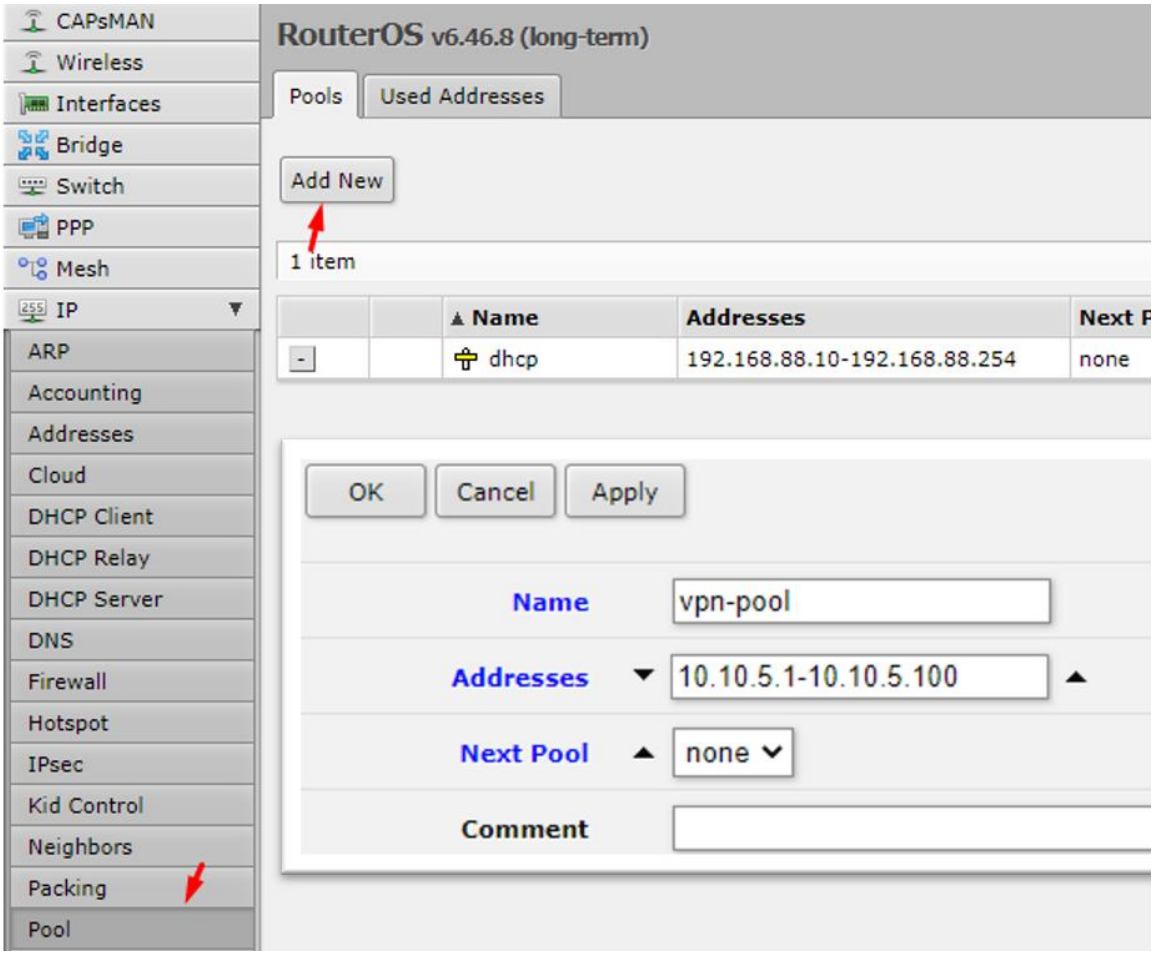

Рисунок 3.1. Створення пулу адресів для використання нашої мережі

Створюємо профіль для тунелю PPP (рис.3.2), вказуючи назву та пули адрес на який він буде розташований.

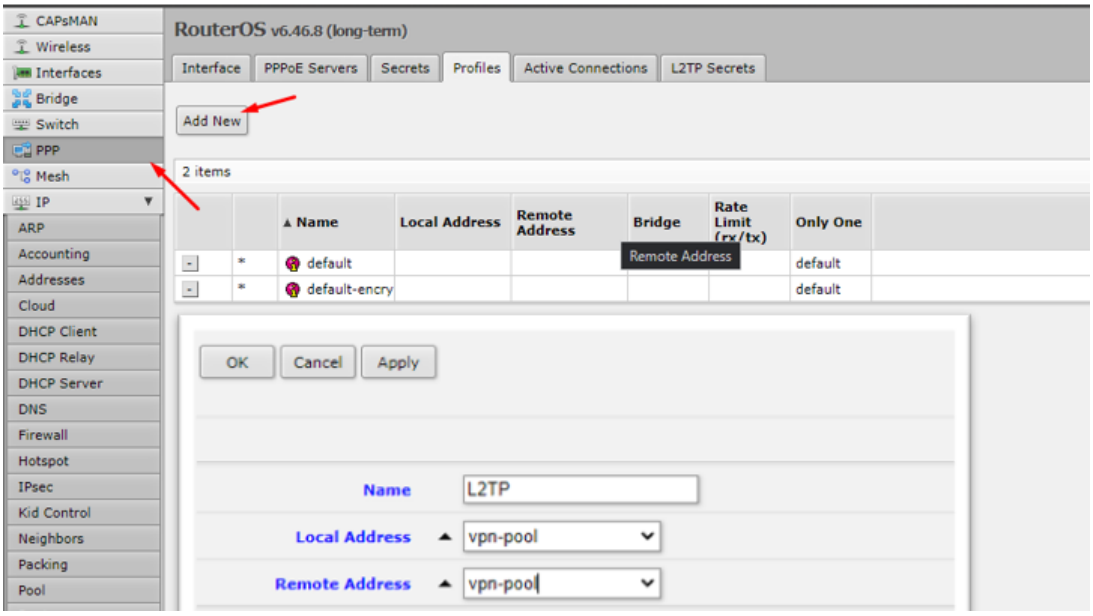

Рисунок 3.2. Створення профілю тунелю PPP

Створюємо користувача (рис.3.3), його пароль, вибираємо сервіс l2tp та профіль «L2TP», який ми створили раніше.

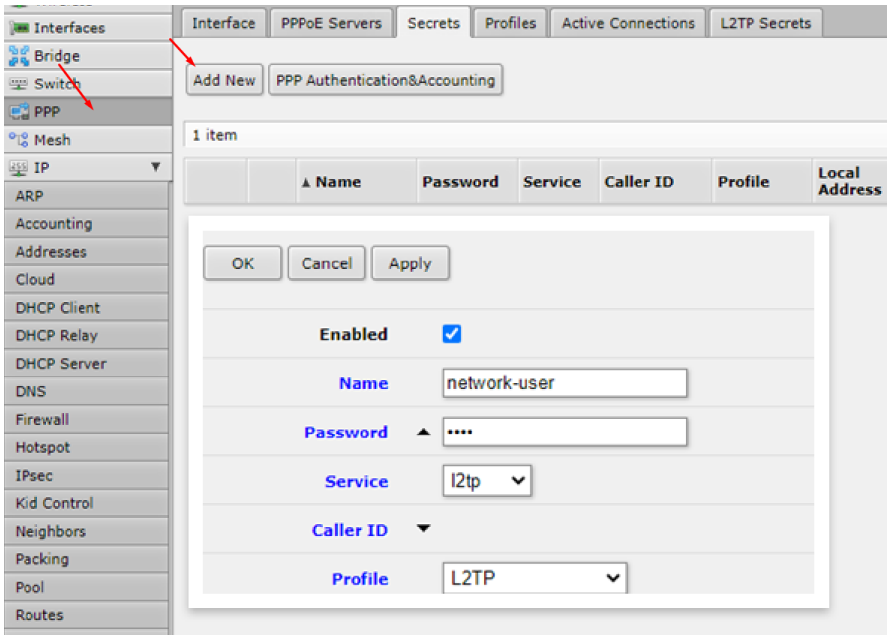

Рисунок 3.3. Створення користувача

Створюємо та піднімаємо L2TP сервер (рис.3.4), вказуючи створений раніше профіль

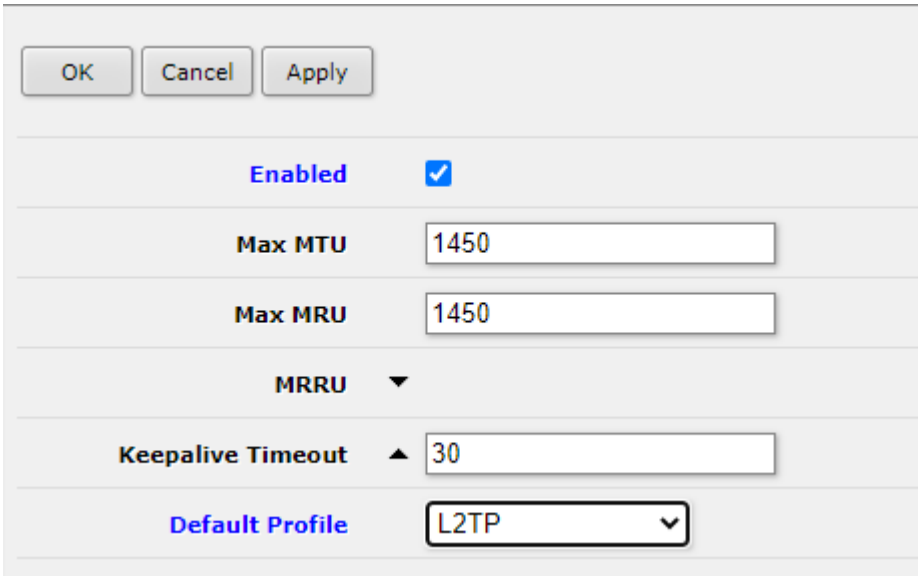

Рисунок 3.4. Конфігурація L2TP серверу

VPN сервер налаштований. Тепер створимо для нього постійний інтерфейс (рис.3.5), щоб на його основі створювати статичні маршрути.

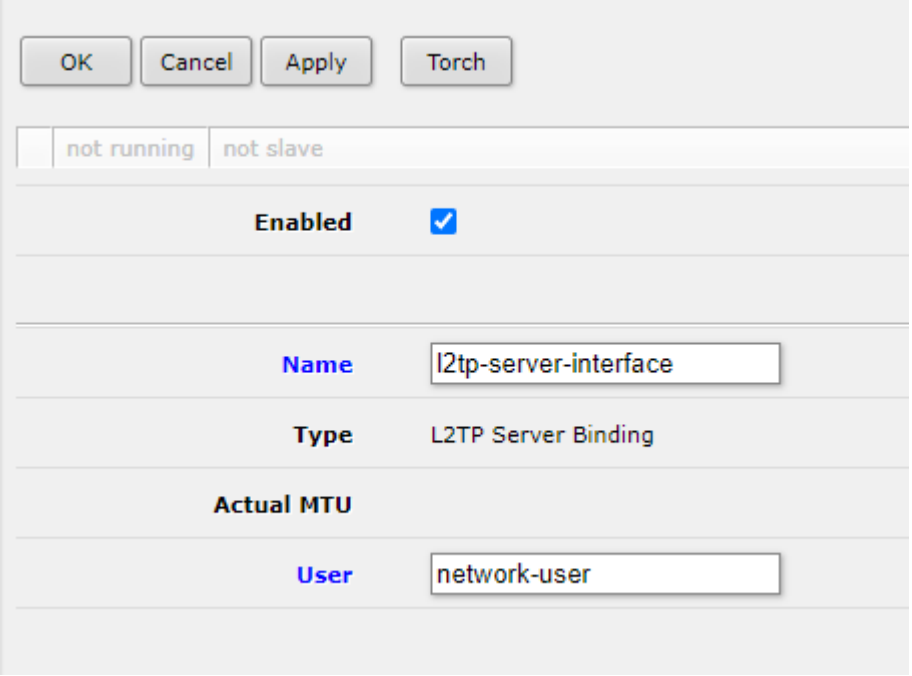

Рисунок 3.5. Створення L2TP інтерфейсу

Створюємо статичний маршрут (рис.3.6) за допомогою якого абоненти локальної мережі серверу зможуть підключатись до локальної мережі через віддалений маршрутизатор та VPN клієнт.

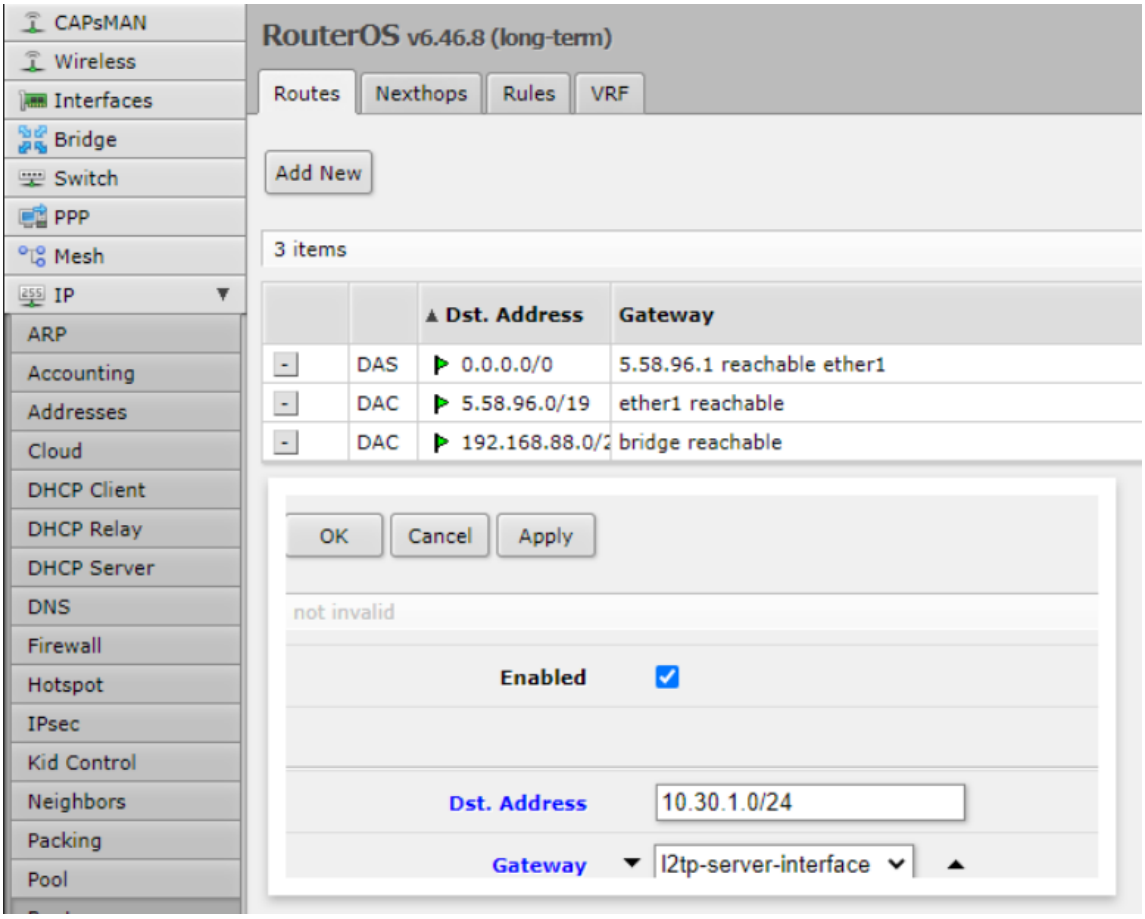

Рисунок 3.6. Створення маршруту для серверної частини

Необхідно налаштувати фаєрвол маршрутизатора (рис.3.7) для коректної роботи L2TP з’єднання.

На сервері необхідно створити наступні правила фаєрволу, щоб до L2TP можна було достукатись. Необхідно дозволити протокол UDP та його порти 1701,500,4500, інтерфейс вказуємо створений нами L2TP

Також окремо додаємо дозвіл протоколу ipsec-esc.

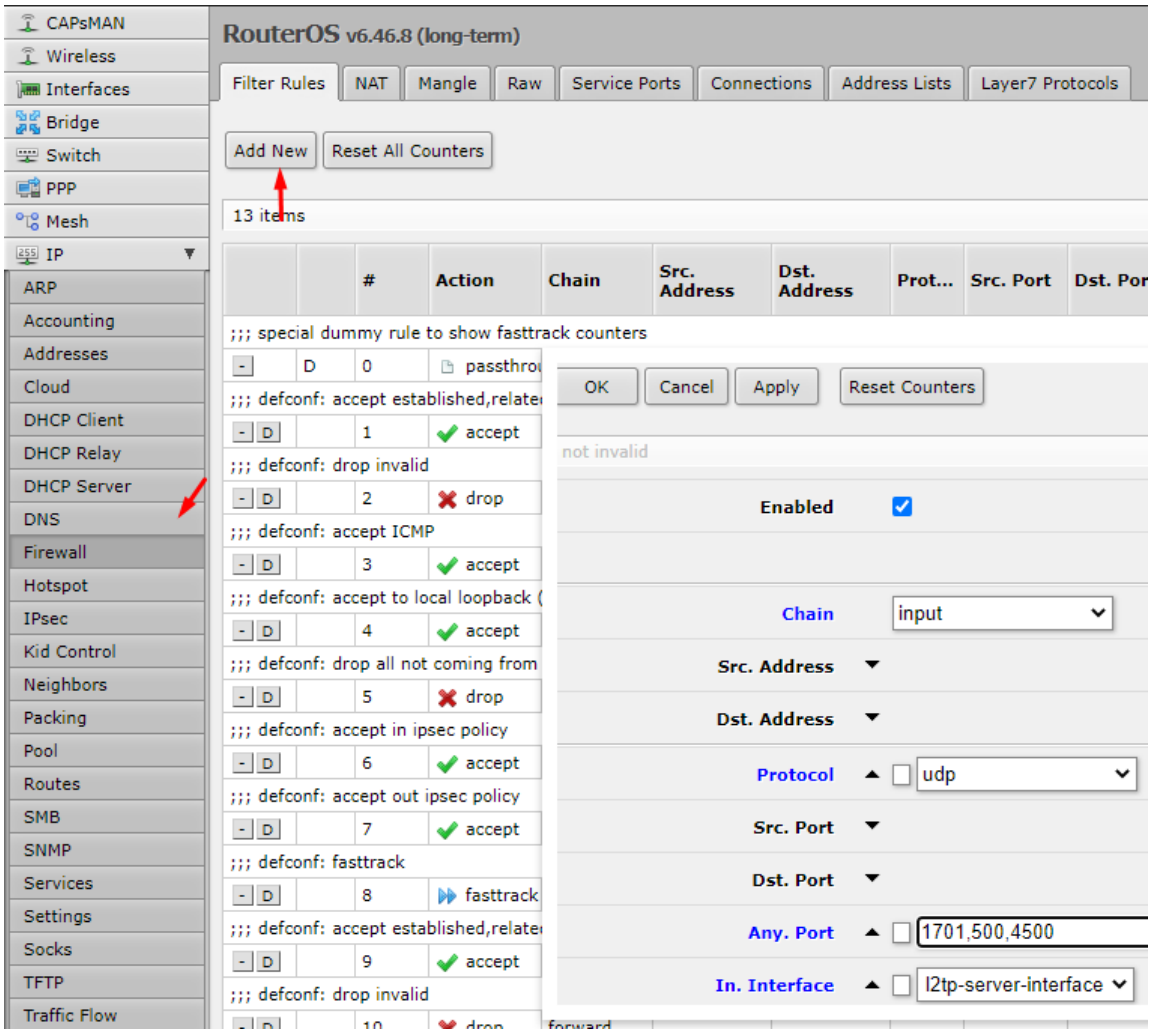

Рисунок 3.7. Налаштування фаєрволу

Настройка сервера закінчена, тепер потрібно налаштувати L2TP на віддаленому маршрутизаторі (рис.3.8).

3.3 L2TP клієнт

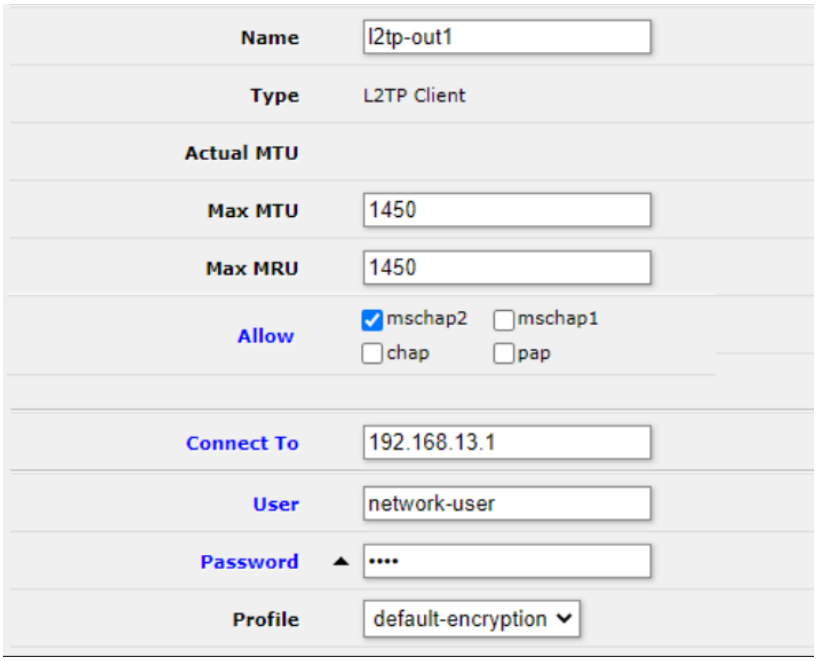

Рисунок 3.8. Створення L2TP клієнту

Додаємо статичний маршрут (рис.3.9), щоб клієнти маршрутизатора знали куди звертатись до абонентів віддаленої локальної мережі через VPN.

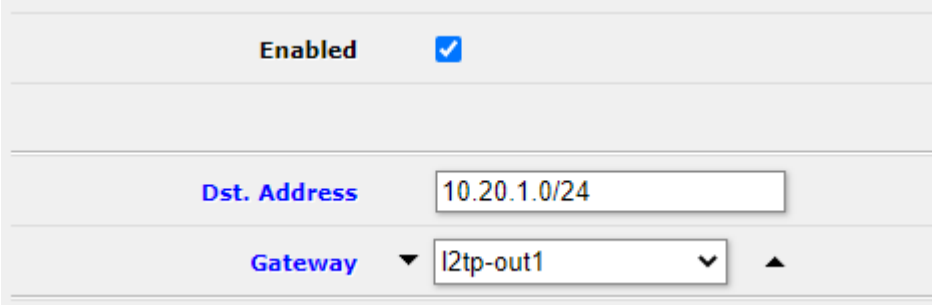

Рисунок 3.9. Створення маршруту для клієнтської частини мережі

На цьому все, дві локальні мережі можуть спілкуватись через L2TP VPN тунель.

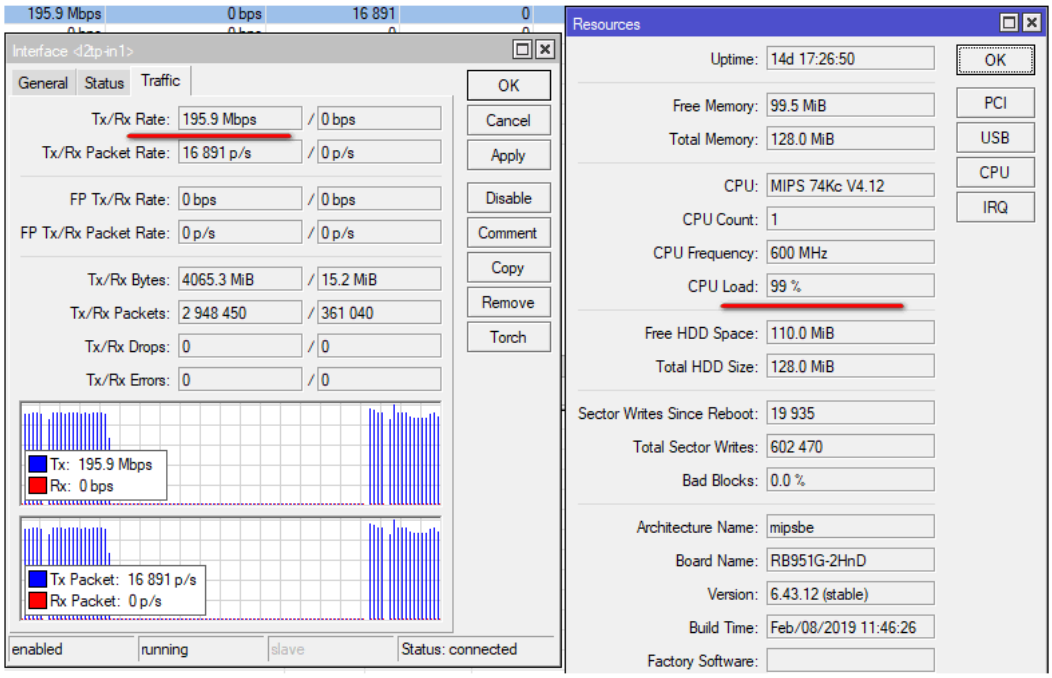

Рисунок 3.10. Апаратна загруженість маршрутизатору при передачі пакетів без шифрування

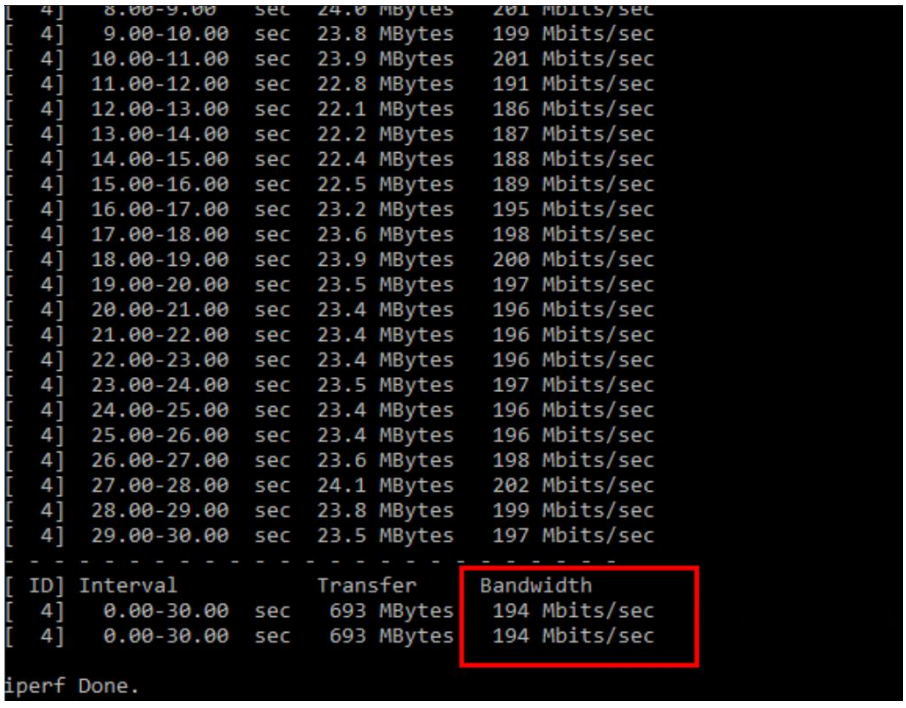

Рисунок 3.11. Заміри швидкості при передачі пакетів без шифрування

Після тестів (рис.3.10, рис.3.11), бачимо що пропускна здатність є досить великою, вузли успішно обмінюються пакетами.

Спробуємо тепер підключити шифрування ipsec

3.4 Налаштування ipsec

В налаштуваннях L2TP серверу потрібно ввімкнути ipsec шифрування та вказати пароль (рис.3.12).

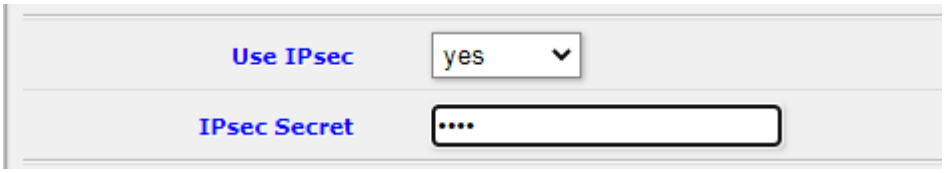

Рисунок 3.12. Додавання ipsec шифрування

Після підключення L2TP клієнту логи серверу видають наступне:

19:17:00 l2tp,ppp,info l2tp-out1: initializing...

19:17:00 l2tp,ppp,info l2tp-out1: connecting...

19:17:03 ipsec,info initiate new phase 1 (Identity Protection): 192.168.13.197[500]<=>192.168.13.1[500]

19:17:04 ipsec,info ISAKMP-SA established 192.168.13.197[500]-192.168.13.1[500] spi:a0f84dc0c7b5d2ab:464e7ffb25495ef3

19:17:07 l2tp,ppp,info l2tp-out1: authenticated

19:17:07 l2tp,ppp,info l2tp-out1: connected

Проведемо тести (рис.3.13, рис.3.14)

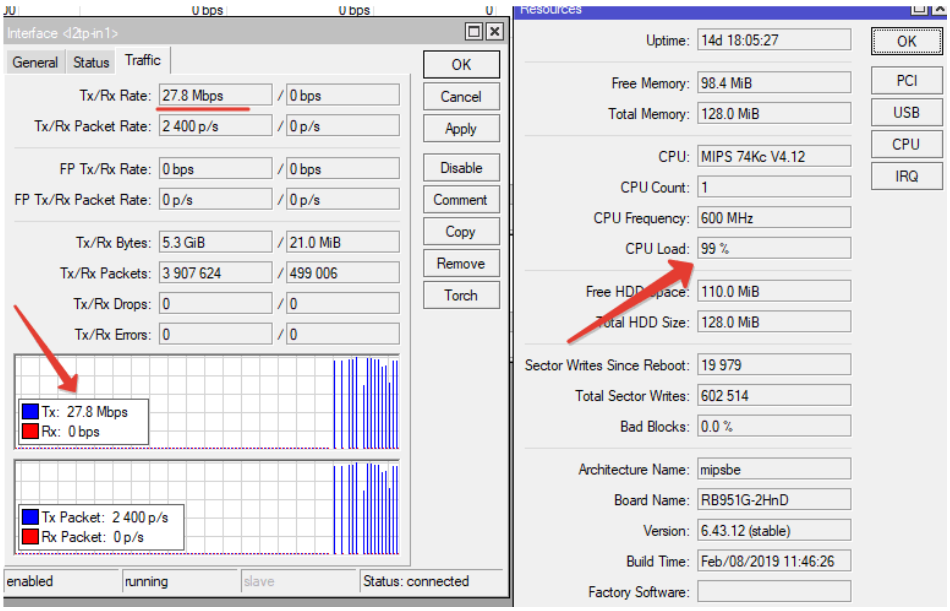

Рисунок 3.13. Апаратна загруженість маршрутизатору при передачі пакетів з шифруванням

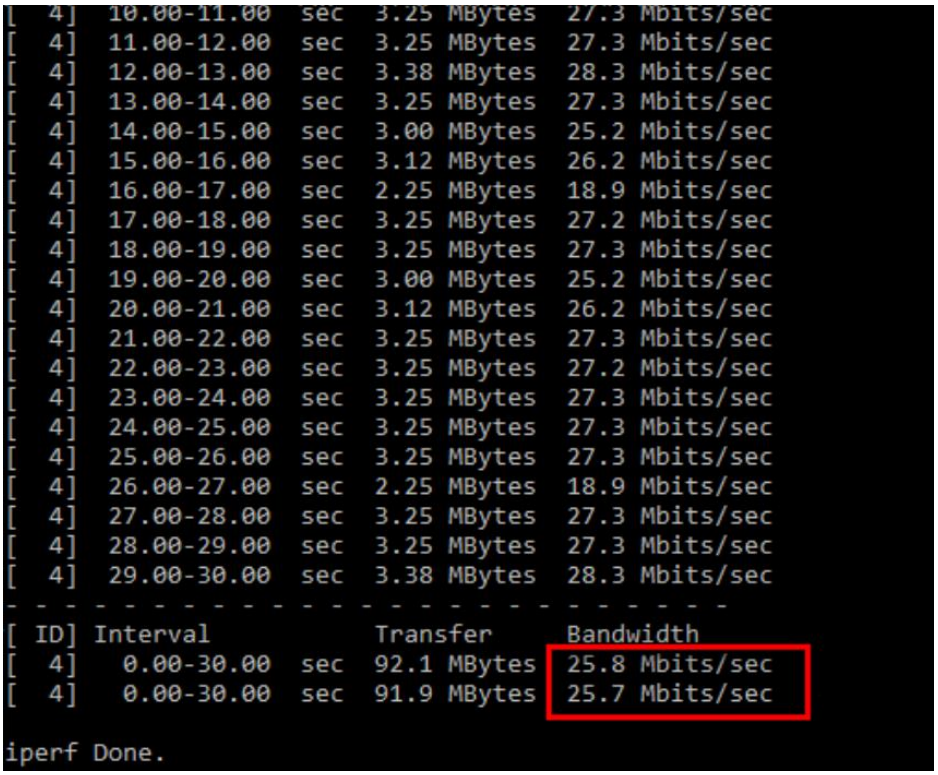

Рисунок 3.14. Заміри швидкості при передачі пакетів з шифруванням

Висновки до третього розділу

Що лишній раз підтверджує роботу шифрування, спосіб дійсно притуплює швидкість передачі, проте тепер з’єднання є зашифрованим.

За замовчуванням використовується алгоритм SHA1 та шифрування AES. Ці параметри можна змінити.

Потрібно пам’ятати, що даний клас маршрутизаторів класифікується як «домашній», тому очікувати від нього швидкості та продуктивності серверного рівня не варто.

Середня швидкість 26 Мбіт/с. При цьому процесор загружений на 100%. В даному тесті маршрутизатор не нагружений нічим окрім тестів, в реальних же випадках швидкість буде набагато менше.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Під час виконання магістерської роботи при розробці тестової корпоративної мережі необхідно було створити фізичне середовище для її функціонування. На основі «ВДОП 5.2.00-5.05-97. Типова інструкція з охорони праці при прокладанні кабелю кабелеукладачем (40863)» було досліджено, сформовано та дотримано наступних положень, затверджених керівництвом.

Загальні положення

1) До виконання робіт з монтажу силових та освітлювальних кабельних мереж допускаються робітники, які досягли 18 років та пройшли:

- навчання та перевірку знань з електробезпеки;
- навчання в закладах освіти для виконання робіт з підвищеною небезпекою
- спеціальне навчання та атестацію з питань пожежної безпеки;
- вступний інструктаж у службі охорони праці;
- первинний інструктаж безпосередньо на робочому місці.

2) Допущені мають виконувати тільки ті роботи, про безпечне виконання яких вони проінструктовані безпосередньо керівником.

3) Палити дозволяється тільки в спеціально відведених місцях, обладнаних урнами або ємностями з водою.

4) Роботи на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів.

До початку роботи

1) перевірити ступінь готовності будівельних робіт;

2) оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР);

3) узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

4) ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Вимоги безпеки під час виконання роботи

1) Прокладання кабелів слід виконувати тільки в рукавицях.

2) Працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

3) Протягувати кабель через отвори в стінах та через міжповерхові перекриття дозволяється за умов, коли робітники знаходяться по обидва боки, при цьому відстань від входу кабелю в трубу до крайнього положення рук робітника повинна бути не менше .

4) Не дозволяється перекладати кабель, який знаходиться під напругою.

Вимоги безпеки після закінчення роботи

1) Не залишати робоче місце до закріплення кабелю на кабельних конструкціях.

2) Упорядкувати робоче місце.

3) Прибрати інструмент та пристрої у відведене для них місце.

4) Зняти спецодяг, засоби індивідуального захисту, очистити від пилу, скласти у відведене для них місце, помити руки, обличчя з милом; при можливості, прийняти душ.

5) Доповісти керівникові робіт про всі недоліки, які мали місце під час виконання робіт.

Висновок

Під час виконання робіт було дотримано усіх зазначених пунктів та відзвітовано про виконання роботи. Проведення робіт було успішним та без пригод. Керівництво залишилось задоволеним.

4.2 Безпека в надзвичайних ситуаціях. Забезпечення електробезпеки користувачів персональних комп'ютерів

Небезпека ураження електричним струмом існує завжди, якщо є контакт з пристроєм, що живиться напругою 36 В і вище, тим більше від електричної мережі 220 В. Це може статися через помилку в разі дотику до відкритих струмоведучих частин, але частіше за все через різних причин (перевантаження, не зовсім якісна ізоляція, механічні пошкодження та ін.). В процесі експлуатації може погіршити ізоляція струмоведучих частин, в тому числі і кабелі живлення, в результаті чого вони можуть виявитися під напругою, і випадковий дотик до них загрожує електротравми, а у важких випадках - і загибеллю людини.

Зоною підвищеної електронебезпеки є місця підключення електроприладів і установок. Нерідко підключають розетки розташовують на підлозі, що неприпустимо. Часто відбувається інша помилка - перевантаження розеток по потужності, і, як наслідок, відбувається порушення ізоляції, що приводить до короткого замикання.

Значна потенційна небезпека від ураження електрострумом полягає в нездатності органів чуття людини виявити на відстані наявність електричної напруги.

Для виключення, а точніше - для зведення до мінімуму потенційну небезпеку електротравмування необхідно дотримуватися вимог, встановлених "Правилами експлуатації електроустановок споживачів" і "Правилами техніки безпеки при експлуатації електроустановок споживачів" (ПЕ і ПТБ електроустановок споживачів), а також "Правилами влаштування електроустановок" (ПУЕ).

Електричні обчислювальні машини (ЕОМ), периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем

захисту мають відповідати класу зони за ПУЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, перейти на негорючу ізоляцію.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПУЕ.

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ (ПЕОМ), на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

ПЕОМ, периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні підключатися до електромережі тільки з допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників повинні мати спеціальні контакти для підключення нульового захисного провідника. Конструкція їх має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має

бути зворотним. Необхідно унеможливити з'єднання контактів фазових провідників з контактами нульового захисного провідника.

Неприпустимим є підключення ПЕОМ та периферійних пристроїв ПЕОМ до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення ПЕОМ, периферійних пристроїв слід виконувати за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 36 В за своєю конструкцією повинні відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В і мають бути пофарбовані в колір, який візуально значно відрізняється від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Індивідуальні та групові штепсельні з'єднання та електророзетки необхідно монтувати на негорючих або важкогорючих пластинах з урахуванням вимог ПУЕ та Правил пожежної безпеки в Україні.

Електромережу штепсельних розеток для живлення ПЕОМ, периферійних пристроїв ПЕОМ при розташуванні їх уздовж стін приміщення прокладають по підлозі поряд зі стінами приміщення, як правило, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

При розташуванні в приміщенні за його периметром до 5 ПЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

Електромережу штепсельних розеток для живлення ПЕОМ при розташуванні їх у центрі приміщення, прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не дозволяється застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, що містять сірку. Відкрита прокладка кабелів під підлогою

забороняється. Металеві труби та гнучкі металеві рукави повинні бути заземлені. Заземлення повинно відповідати вимогам НПАОП 40.1-1.21-98.

Для підключення переносної електроапаратури застосовують гнучкі проводи в надійній ізоляції.

Тимчасова електропроводка від переносних приладів до джерел живлення виконується найкоротшим шляхом без заплутування проводів у конструкціях машин, приладів та меблях. Доточувати проводи можна тільки шляхом паяння з наступним старанним ізолюванням місць з'єднання.

Є неприпустимими:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Для запобігання уражень електричним струмом під час роботи з комп'ютером слід встановити додаткові захисні пристрої, що забезпечують недоступність струмопровідних частин для дотику; з метою зменшення небезпеки можна використовувати розділовий трансформатор для розв'язки з основною мережею, і обов'язковим у всіх випадках є наявність захисного

заземлення або занулення (захисного відключення) електрообладнання. Для якісної роботи комп'ютерів створюється окремий заземлюючий контур.

Орієнтовний розподіл нещасних випадків внаслідок дії електричного струму в промисловості за вказаними видами травм: місцеві електротравми — 20%; електричні удари — 25%; змішані травми, тобто одночасно місцеві електротравми та електричні удари — 55%.

При важкому стані потерпілого (втрата свідомості, відсутній пульс, дихання переривчасте) необхідно терміново почати робити штучне дихання за способом "з рота в рот" з частотою 12-15 вдування в хвилину і непрямий масаж серця з частотою одне натискання в секунду і продовжувати ці дії до поліпшення стану хворого (діаметр зіниць відновлюється, т. е. зменшується до нормального, пульс повертається, дихання нормалізується). Коли людина приходить до тями, треба продовжувати надавати допомогу ще 5-10 хвилин, потім укласти його в теплі і давати всередину рясне пиття у вигляді теплого чаю. У будь-якому випадку має бути забезпечено надання кваліфікованої медичної допомоги.

Дотримання правил і вимог електробезпеки дозволяє максимально забезпечити захист користувача від ураження електричним струмом. Однак, якщо стався нещасний випадок, в першу чергу необхідно будь-яким способом негайно припинити дію струму, для чого треба вимкнути рубильник, відкинути електропровід від потерпілого сухим ціпком або чимось подібним і обов'язково викликати лікаря. Якщо потерпілий у свідомості і відчуває деяке нездужання, до приходу лікаря слід забезпечити йому спокій, свіже повітря, тепло.

Найбільш небезпечним видом електротравм є електричний удар — раптове збудження живих тканин організму внаслідок дії електроструму, яке супроводжується судомним скороченням м’язів.

У всіх випадках ураження електричним струмом виклик лікаря є обов'язковим незалежно від стану потерпілого.

Висновок

Забезпечення електробезпеки користувачів є однією з найважливіших задач перед побудовою мережі з декількох ПЕОМ. При дотриманні "Правил експлуатації електроустановок споживачів", "Правил техніки безпеки при експлуатації електроустановок споживачів", а також "Правил влаштування електроустановок" можна убезпечитись від нещасних випадків та захистити життя працівників.

ВИСНОВКИ

Домашні маршрутизатори можуть підтримувати VPN мережі, створені вручну, проте такі мережі є переважно повільні. Для розгортання швидких, захищених мереж рекомендується використовувати спеціалізоване обладнання, або ж маршрутизатори вищої категорії (залежить від кількості користувачів).

Проте факт можливості створення локального захищеного середовища вказує на простоту такого методу. Запропонований спосіб створення локального PPP тунелю з шифруванням IPsec є найбільш поширеним, проте не є найбільш актуальний. З поступовою адаптацією технологій VPN, можливо, спільнота і дійде до стандартизації протоколів взаємодії, проте на даний момент це справа тестування та аналізу.

Переваги ж використання методу L2TP + IPsec:

- Простота та комфорт налаштування;
- Надійне шифрування;
- Підтримка L2TP з’єднань майже усіма сучасними системами та пристроями. Немає необхідності додаткового програмного забезпечення;
- Може об’єднувати як офісі так і віддалених співробітників – site-to-site і site-to-client з’єднання.

Тут можна додати, що використаний був маршрутизатор середнього цінового класу. Не зважаючи на це з роботою він справився та підтримувати «робоче» з’єднання VPN він цілком може. Маршрутизатори ціновою категорією нижче не зможуть охопити мінімальні вимоги ні апаратно, ні програмно. До вибору такої апаратури необхідно підходити дуже ретельно, а бажано консультуватись у спеціалістів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Безпека інформаційних та комунікаційних систем», л.14, Носов В.В.
2. Росляков А.В. Классификация потоковых моделей VPN // Шестая Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникаций». - Уфа, 2005. - С. 34-35.
3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. 1994. № 31. С. 286.
4. Постанова Кабінету міністрів України від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»
5. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).
6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).
7. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. (Нормативний документ системи технічного захисту інформації).
8. Політика безпеки для Internet. [Електронний ресурс]. – Режим доступу : https://lektsii.org/8-12435.html – Загол. з екрана. – Дата звернення 12.11.2019.
9. «Сравнительный обзор реализаций технологии VPN: что выбрать?» URL: https://1cloud.ru/help/network/comparevpntypes#lt2p
10. Файловий архів студентів. URL: https://studopedia.su/17_16565_problemibezpeki-suchasnih-korporativnih-merezh.html (02.06.2020)
11. Леонов С. «Реальная виртуальность». URL: http://www.computeiTa.ru/offline/1998/237/1149

12. Олифер В.Г., Олифер Н.А. «Компьютерные сети. Принципы, технологии, протоколы». - СПб.: Издательство «Питер», 1999. - 672 с
13. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.
14. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.
15. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах / М. П. Карпінський, Я. І. Кінах, О. С. Войтенко, В. Р. Паславський, І. З. Якименко, М. М. Касянчук // Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій", 16-17 листопада 2017 року. — Т. : ТНТУ, 2017. — Том 2. — С. 81–82. — (Комп'ютерно-інформаційні технології та системи зв'язку).
16. Удосконалення методології сумісного використання ресурсів комп'ютерних мереж для дистанційної форми навчального процесу / М. П. Карпінський, Я. І. Кінах, Л. В. Стратійчук, В. Р. Паславський, І. З. Якименко, М. М. Касянчук // Збірник тез доповідей VII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій", 28-29 листопада 2018 року. — Т. : ТНТУ, 2018. — Том 2. — С. 72–73. — (Комп'ютерно-інформаційні технології та системи зв'язку).
17. Програмний моніторинг комп'ютерних мереж для освітніх систем / М. Карпінський, Я. Кінах, У. Яциковська, В. Паславський, Л. Стратійчук // Матеріали XXI наукової конференції ТНТУ ім. І. Пулюя, 16-17 травня 2019 року. — Т. : ТНТУ, 2019. — С. 54. — (Сучасні технології на транспорті).
18. Архіпович Ю.О., Іщук О.Р., Ткаченко М.І. Функціонування корпоративних інформаційних мереж в управлінні фінансовими установами на регіональному рівні:Науково-практичне видання/За ред. Ткаченка І.С.-Тернопіль:Економічна думка,2001 .-70 с.-966-654-046-0
19. Антонюк Я.М., Шияк Б.А., Антонюк М.І. Оцінювання затримки передачі даних за фіксованими протоколами у сегментах комп'ютерних кампусних

мереж//Телекомунікаційні та інформаційні технології.-2019.-№4 .-с.111-119

20. Д.О. Стьопа, О.М. Ярема / Методи захисту інформаційно-телекомунікаційних систем та мереж від несанкціонованого доступу з використанням технології VPN – Матеріали IX науково-технічної конференції «Інформаційні моделі, системи та технології»: ТНТУ, Тернопіль 2021