ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ ТУНЕЛЕЙ VPN ДЛЯ ОРГАНІЗАЦІЇ СТРИМІНГОВИХ ТЕХНОЛОГІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ»

Виконав: студент 6 курсу, групи БСДМ-62
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Клімов А.О.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

РЕФЕРАТ

Текстова частина магістерської роботи: 68 сторінок, 15 рисунків, 3 таблиці, 22 джерела.

Об'єкт дослідження – процес забезпечення захисту корпоративної інформації за допомогою VPN технологій.

Предмет дослідження – технологія захищених тунелей VPN для організації стрімінгових технологій в корпоративній мережі.

Мета роботи – розробити варіант моделювання та топології Cisco Packet Tracer і застосувати технології та їх захист в компанії.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту інформації за допомогою технологій VPN.

В роботі розроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформації та визначено мета та завдання управління Cisco Packet Tracer.

Проаналізовано існуючі технології управління захисту стримінгових технологій в корпоративних мережах за допомогою захищених тунелей VPN.

Досліджено методи та засоби управління захистом корпоративних мереж наприклад Cisco Packet Tracer. Визначено призначення, основні функції та склад програмного комплексу, принципи робити Cisco Packet Tracer.

На основі досліджень проведених в роботі розроблено варіант топології системи управління захистом використання віртуальних захищених тунелей VPN для організацій стримінгових технологій в корпоративних мережах та застосування технології VPN та їх захист на підприємстві.

Галузь використання – кібербезпека корпоративних мереж.

VPN, СИСТЕМА, БЕЗПЕКА, OPENVPN, ІНТЕРНЕТ, КЛІЄНТ, СЕРВЕР, КРИПТОГРАФІЯ, ЗАХИСТ, МЕТОДИ ЗАХИСТ ІНФОРМАЦІЇ, ПРОТОКОЛИ VPN, МЕРЕЖІ VPN, КОНФІГУРАЦІЯ VPN.

ABSTRACT

Master's thesis: 68 pages, 15 figures, 3 tables, 22 sources.

Object of research – the process of ensuring the protection of corporate information using VPN technologies.

Subject of research – the secure VPN tunnel technology for organizing streaming technologies in the corporate network.

The aim of research – to develop a modeling model and topology of Cisco Packet Tracer and recommendations for the application of technology and their protection in the company.

Research methods – elaboration of literature on this topic, analysis of operational documentation, international standards and their comparison, modeling the process of information protection using VPN technologies.

The paper analyzes the problem of cybersecurity of corporate information and defines the purpose and objectives of Cisco Packet Tracer management.

The existing technologies of management of protection of streaming technologies in corporate networks by means of the protected VPN tunnels are analyzed. Methods and tools for managing the protection of corporate networks such as Cisco Packet Tracer are studied. The purpose, main functions and composition of the software package, principles of making Cisco Packet Tracer are determined.

Based on the research conducted, a variant of the topology of the management system for the protection of the use of virtual secure VPN tunnels for organizations of streaming technologies in corporate networks and recommendations for the use of VPN technology for their protection in the enterprise.

Field of use – cybersecurity of corporate networks.

VPN, SYSTEM, SECURITY, OPENVPN, INTERNET, CLIENT, SERVER, CRYPTOGRAPHY, PROTECTION, INFORMATION PROTECTION METHODS, VPN PROTOCOLS, VPN NETWORKS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IPSec	–	Internet protocol security
L2F	–	Layer-2 forwarding
L2TP	–	Layer-2 tunneling protocol
LAN	–	Local area network
MPLS	–	Multiprotocol label switching
PAP	–	Password authentication protocol
PPTP	–	Point-to-Point Tunneling Protocol
SA	–	Security association
SSL	–	Secure sockets layer
VPN	–	Virtual private network
ІБ	–	Інформаційна безпека
ІТ	–	Інформаційні технології
КМ	–	Корпоративних мереж
НСД	–	Несанкціонований доступ
ОС	–	Операційні системи
ПЗ	–	Програмне забезпечення

ВСТУП

Актуальність дослідження. Розвиток технологій формує сучасні реалії в роботі всіх галузей світу. Кожне підприємство, компанія, фірма підлаштовується під сучасні можливості для комфортної роботи, підвищення якості продуктивності праці, незважаючи на різні чинники, які зумовлені проблематикою дистанційної роботи працівників.

Одно час, корпоративна інформація, яка передається через відкритий доступ мережі Інтернет, має вразливості, вона може бути перехоплена зловмисниками для використання в корисливих цілях, завдяки спеціальним програмам-сніфферів. Також потрібно враховувати, що цією інформацією може бути, засекречені документи, логіни, паролі від особистих кабінетів, і корпоративна пошта. Тому конфіденційність корпоративної мережі виходить на перший план, по захисту інформації.

Потрібно розуміти, що під час передачі даних по каналах зв'язку, шифрування або паролювання документів, не гарантуватиме вам абсолютної безпеки, адже будь-який найскладніших пароль можуть зламати, а використовуючи криптоаналіз, можна зламати і шифрувальний ключ.

Об'єкт дослідження - процес забезпечення захисту корпоративної інформації за допомогою VPN технологій.

Предмет дослідження - технологія захищених тунелей VPN для організації стримінгових технологій в корпоративній мережі.

Мета роботи - розробити варіант моделювання та топології Cisco Packet Tracer і застосування технології та їх захист в компанії.

Наукові завдання:

- дослідити технологію захищених тунелей VPN, як основу в побудові безпечної корпоративної мережі;

- проаналізувати особливості та виявити основні труднощі при технології використання віртуальних тунелей VPN для організації стримінгових технологій в корпоративних мережах;

Методи дослідження - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу захисту інформації за допомогою технологій VPN.

Практичне значення одержаних результатів полягає в дослідженні процесу забезпечення захисту корпоративної інформації за допомогою VPN технологій, а також ефективна робота з віртуальними захищеними тунелями VPN для організації стримінгових технологій в корпоративних мережах.

1 ЗАГАЛЬНІ ВІДОМОСТІ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ ТУНЕЛЕЙ VPN

1.1. Загальні положення VPN

Технології захисту віртуальних захищених тунелей з’явилися відносно давно. Зі створенням мережі Інтернет, виникла і потреба в збереженні даних від будь-яких можливих загроз, адже локальна мережа створювала всі умови для перехоплення даних, створення цензури та крадіжка персональної інформації.

Спеціалісти почали створювати методи захисту Інтернет - безпеки, адже було зрозуміло, що людство буде й далі розвиватися в напрямку інформаційних технологій. Науковці вважають, що початковою точкою відліку в інтеграції VPN відіграв Гурдин Сингх-Полл співробітник корпорації Microsoft в 1996 році, він почав розробку протоколу тунелювання «крапка-крапка» (PPTP), щоб користувачі могли мати безпечне підключення до Інтернет та могли безпечно користуватися всіма перевагами інформаційними технологіями.

Враховуючи реалії сучасного світу, а саме пандемію коронавірусу, коли більшість людства знаходиться на самоізоляції або працює дистанційно, захист персональних даних постає на перше місце. Адже при будь-якому користуванні послугами мережі Інтернет всі ваші дані зчитуються і залишають цифровий слід в файлах cookie, кешу і залишають цифрову адресу (IP-адресу), ваше розташування та історію браузеру. Ці дані можуть використовувати різні треті особи для створення рекомендацій для ваших соціальних мереж (Facebook, Instagram), електронних магазинів, і взагалі для покращення загального доступу до пошукових систем мережі Інтернет[1].

В цьому є позитивні і негативні моменти, оскільки через незахищені мережі Інтернет проходить більша частина конфіденційної інформації, потреба людства у збереженні даних виходить на перше місце під час будь-якої роботи в мережі

Інтернет. І найкращим способом для вирішення цієї проблеми є використання віртуальної приватної мережі VPN.

VPN (Virtual Private Network) - це віртуальна приватна мережа або логічна мережа, яка створюється поверх незахищених мереж (мереж оператора зв'язку або сервіс-провайдера Інтернет).

Також потрібно розуміти, що віртуальна мережа - це окрема загальнодоступна мережа, яка зберігає конфіденційність інформації, що передається за рахунок шифрування, тунелювання та іншого захисту.

Головною ідеєю VPN є забезпечення доступу віддалених користувачів до корпоративних мереж через загальнодоступні мережі, зі збереженням конфіденційності інформації. Як середовище для створення VPN може виступати Frame Relay, та найпоширеніша технологія створення мереж VPN в середовищі Інтернет.

Virtual Private Network (VPN) - віртуальна приватна мережа, котра формується поверх інших мереж із меншим рівнем довіри. VPN, формується між двома вузлами та надає можливість клієнту, який приєднався бути учасником віддаленої мережі та користуватися її сервісами (внутрішніми сайтами, базами даних, принтерами, політиками виходу в Інтернет). Безпека передачі інформації через загальнодоступні мережі реалізуються завдяки шифрування, у результаті формується закритий для сторонніх канал обміну інформацією. Технологія VPN пов'язує мережі в єдину мережу із застосування непідконтрольних каналів. Провайдери пропонують власні послуги для розгортання власної VPN-мережі [2].

У залежності від протоколів та призначень, VPN надає можливість поєднати три види вузлів: вузол-вузол, вузол-мережу та мережу-мережу. Застосування технології із використанням мережі Інтернет як передавача IP-трафіку. Мережі VPN мають вирішувати задачі для підключення кінцевого користувача до віддаленої мережі та поєднання декількох локальних мереж. Структура даної технології включає канали глобальної мережі, захищені протоколи та маршрутизатори.

VPN пристрій знаходиться між внутрішньою мережею та мережею Інтернет на кожному кінці з'єднання. При передачі інформації через VPN, вони потрапляють на вхід VPN та після повного проходження через неї та з'являються у точці призначення. Процес вважається «тунелюванням» - формування логічного тунелю у мережі Інтернет, котрий з'єднує дві точки. За допомогою «тунелювання» особиста інформація є невидимою для інших користувачів мережі Інтернет. Перед попаданням інформації до інтернет-тунелю, дані зашифровуються, і це їм надає додатковий захист.

Протоколи шифрування використовують від якого протоколу тунелювання, який підтримується VPN-рішенням. Характеристика VPN-рішення - це є діапазон підтримуваних протоколів автентифікації. Тобто вдосконалення VPN протоколів автентифікації можна гарантувати її захист та не допустити несанкціонованого доступу. Технологія VPN набрали такої популярності, що це є обов'язковим для побудови комплексної системи захисту інформації, для роботи у державних та недержавних організаціях чи структурах не лише в організації, а й поза нею. У зв'язку з карантинними заходами, велика кількість організацій перейшла на віддалену роботу, тому для захисту даних, які надсилаються через мережу Інтернет чи для підключення до сервісів [3].

VPN мають певні відмінності, у порівнянні з іншими, якщо точніше звернення мережі організації не встановлюючи комутоване з'єднання та уникнення виділених ліній.

Користувач маючи доступ до Інтернету може підключитися до мережі офісу, але загальнодоступність даних не означає, що вони не є незахищеними. Система безпеки VPN - це захист корпоративної інформації від несанкціонованого доступу.

Так як інформація передається у зашифрованому вигляді, доступ до яких має лише їх власник. Алгоритм розповсюджений для зашифрування є Triple DES (притаманне потрійне шифрування - використання 3-х ключів) [4].

Достовірність підтверджується через перевірку цілісності даних та ідентифікації користувачів, які західні в VPN. Це даних можливість отримати інформацію, що дані надійшли до адресата без пошкодження та модифікації.

Алгоритм для перевірки цілісності даних, які найчастіше використовуються - MD5 і SHA1. Наступним кроком, система здійснює перевірку на зміну даних у процесі руху мережею, з'ясовуючи чи це навмисно, чи помилково. Тобто, побудова VPN має на меті формування захищених від сторонніх очей доступу тунелів між кількома локальними мережами чи віддаленими користувачами.

Для формування VPN важливо мати програму шифрування вихідного та вхідного трафіку. При цьому, їх реалізація може бути як програмою так і апаратно-програмною, з будь-якими операційними системами, та не важливо, це комп'ютер чи мобільний пристрій. Тому важливо зробити висновок, що автентифікація чи шифрування даних - є невід'ємними елементами захищеного з'єднання [5].

Потрібно зважати на факт використання каналів Інтернет, що мають загальнодоступний характер, адже це порушує принцип конфіденційності. VPN повинен гарантувати, що направлений через нього Інтернет трафік буде цілком захищений, так само як всередині локальної мережі з урахуванням, того, що фінансові переваги будуть збережені. З урахуванням застосування спеціальних пристроїв і механізмів забезпечується безпека даних технологією VPN, тому завжди потрібно враховувати доцільність встановлення певних захисних механізмів, чи дійсно існує потреба встановлення такої системи безпеки даних. Зрозуміло, що фінансові звіти, таємні переговори та документація потребує підвищеного рівня безпеки, але й потрібно зважати на недоцільність встановлення всіх мір шифрування та тунелювання для робочого чату співробітник нижніх ланок. Вистачить і звичного паролю для їх користувачів.

Розподілення мереж WAN почалися дуже давно, а саме такі технології як Frame Relay і ATM, ці технології давали аналог приватної мережі на основі загального доступу до мережі Інтернет з аналогом побудови віртуальної приватної мережі VPN. Та сьогодення диктує нові можливості використання технологій і Frame Relay, і ATM вже в минулому, зараз використовують Ethernet і IP. На даний момент відомо про два різких підйому ринку послуг. Перший був в 2013 році, спричинений політичними небезпеками, кіберзагрозами та цензурою в деяких країнах Сходу, такі як Китай, Гонконг і т. д.

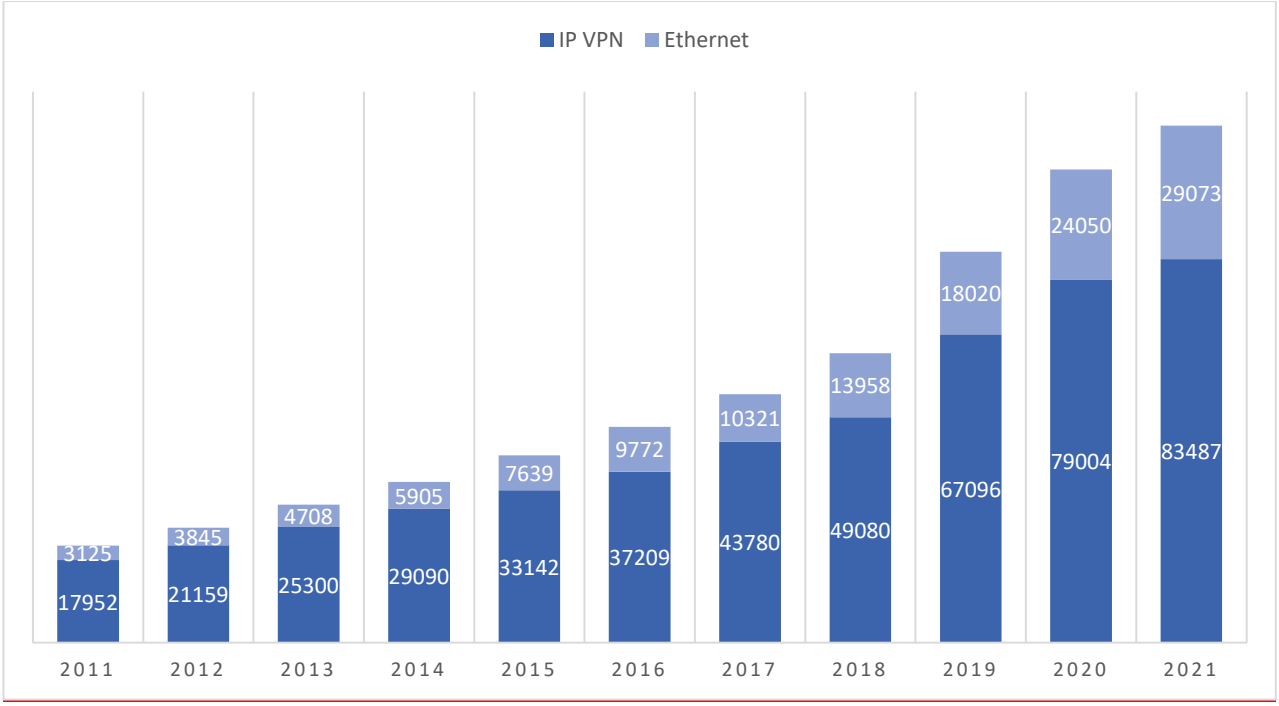

Рис.1.1. Ринок послуги Ethernet та IP в 2010-2021 рр.

Збільшення попиту на послуги VPN спричинене не постійною політичною ситуацією, постійними кіберзагрозами на різні державні установи, міжнародні банки, міжнародні компанії, геополітичні конфлікти, високий рівень цензури, блокування різних ресурсів з боку деяких країн.

Потрібно зазначити, що з 2016 року ринок VPN постійно доповнюється, покращується та змінюється, та досягнув суми 31,1 млрл. доларів в 2021 році.

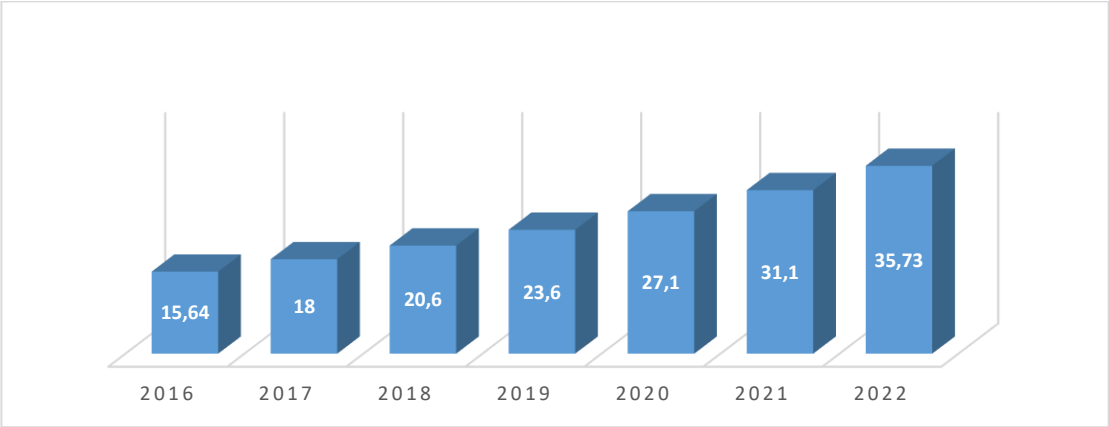

Рис.1.2. Розмір світового ринку VPN

Найбільше розповсюдження VPN – сервіси отримали в країнах Азії, Близького Сходу та Латинської Америки (дані стосовно Китаю підлягають сумніву,

адже з 2017 року в країні відбулася цензура стосовно App Store, Play Store та всіх ресурсів Google, було видалено VPN застосунки). Найменші показники в США та Великобританії.

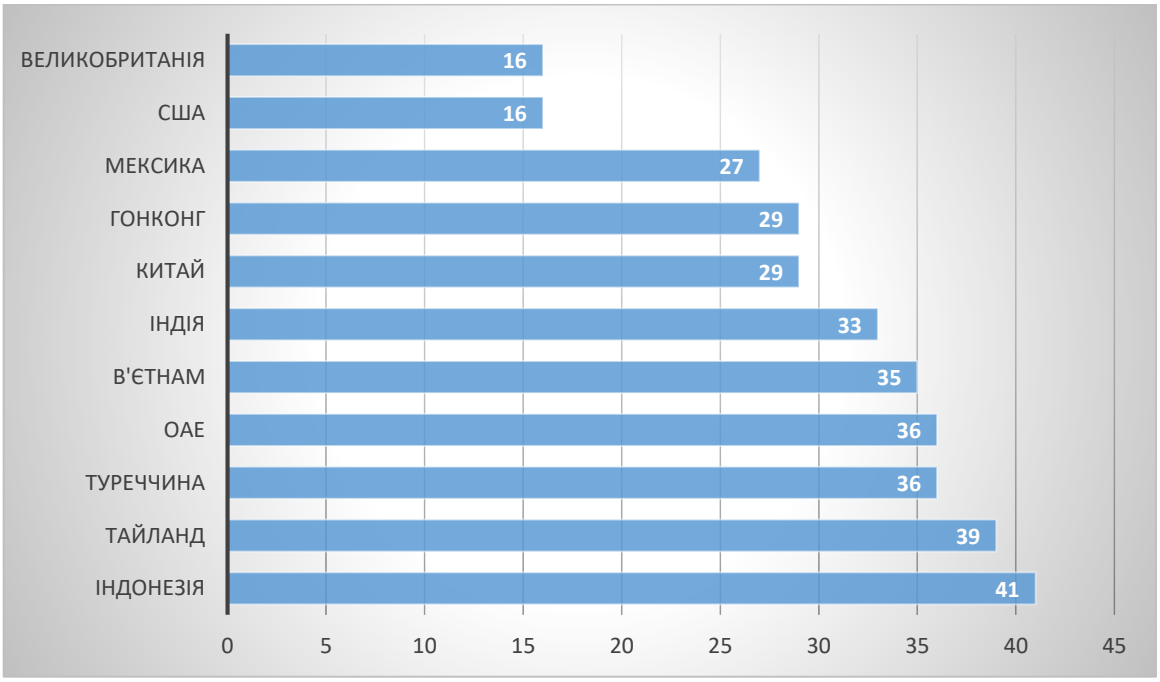

Рис. 1.3. Країни, які найбільше використовують VPN, станом на 2021 рік

Питання популяризації VPN найчастіше виникає з боку звичайних користувачів. В першу чергу занепокоєння власною безпекою персональних даних, з іншого боку можливістю отримувати доступ до всіх заборонених цензурою країн ресурсів Інтернет. Технології VPN сервісів широко використовуються в таких країнах як: Китай, Латинська Америка та країни Індонезії, та Малайзії.

На рис.1.4. приведено перелік цілей, для яких найчастіше використовуються VPN сервіси.

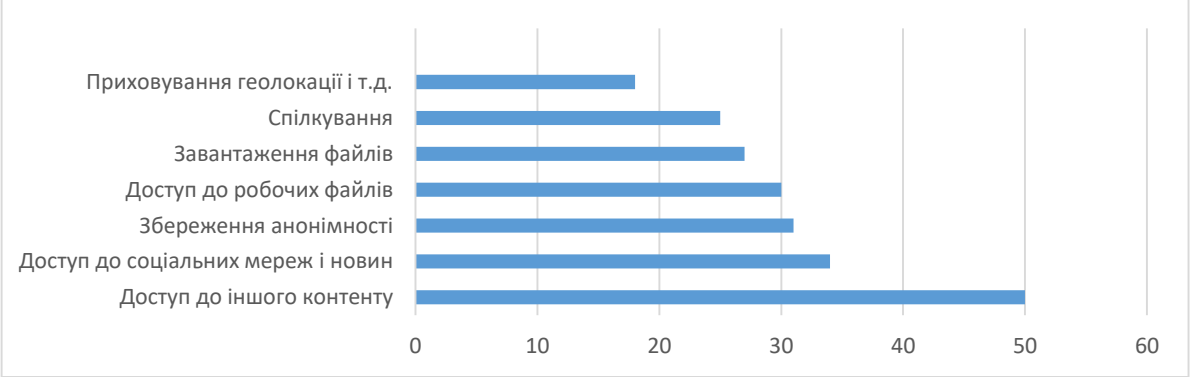

Рис. 1.4. Статистичні дані використання VPN сервісів

Таблиця 1.1.

Переваги і недоліки VPN

Переваги VPN	Недоліки VPN
Ваш особистий трафік зашифрований і надійно передається через Інтернет;	Достатньо висока ціна за платну версію програми;
Використання служби VPN становить хакерів в досить складну ситуацію для доступу до ваших даних;	Залежно від типу послуги VPN, протокол безпеки може бути складним для налаштування;
Можливість користуватися загальнодоступними точками доступу до Wi-Fi, не турбуючись про анонімність ваших персональних даних.	Якщо послуга VPN налаштована неправильно, можуть виникати помилки DNS та IP-адреси, які можуть бути використані у кримінальних цілях хакерів.

1.2. Функціональна складова протоколів VPN

Безпечний віртуальний VPN – це одночасне застосування локальних мереж та комп'ютерів завдяки відкритому зовнішньому середовищі для передачі даних у єдиній віртуальній корпоративній мережі, котра гарантує захист даних, які циркулюють в організації.

У процесі підключення корпоративної локальної мережі до відкритої мережі є такі недоліки:

– НСД до даних компанії, які передаються через відкриту мережу;

– НСД до внутрішніх ресурсів локальної мережі, які перехоплює зловмисник після НСД до мережі.

Таблиця 1.2.

Переваги і недоліки VPN протоколів

Протоколи	Переваги	Недоліки
PPTP	• Висока швидкість; • Вбудований клієнт практично на всіх платформах; • Просте налаштування.	• Протокол зламаний Агенством Національної Безпеки США; • Не гарантує повної безпеки.
L2TP і L2TP/IPsec	• Вважається відносно безпечним; • Доступні в більшості систем і майже на всіх пристроях; • Просте налаштування	• Повільніший ніж OpenVPN; • Захист протоколу порушений Агенством Національної Безпеки США (Наймовірніше послаблює протокол навмисно).
OpenVPN	• Дозволяє обходити більшість файрволів; • Гнучке налаштування; • Відкритий вихідний код, може швидко адаптуватися до нових небезпек; • Сумісний з різними алгоритмами шифрування; • Високій ступінь безпеки.	• Складно налаштувати; • Потрібно стороннє ПО; • Підтримка на мобільних пристроях працює не кращим чином.
SSTP	• Дозволяє обходити більшість файрволів; • Рівень безпеки залежить від обраного шифру; • Взаємодія з ОС Windows та підтримка Microsoft.	• Оскільки протоколом володіє компанія Microsoft, перевірити чи поліпшити його неможливо; • Працює тільки на платформі Windows.
IKEv2	• Високій ступінь безпеки – підтримка різних шифрів, зокрема 3DES, AES, AES 256; • Також підтримує пристрої Blackberry; • Стабільно підключається знову після розриву з’єднання або зміни мереж; • Просто встановити і налаштувати; • Швидше ніж L2TP, PPTP, SSTP.	• Підтримує малу кількість платформ; • Порт UDP 500 блокується простіше, ніж рішення на основі SSL, як, наприклад, SSTP або OpenVPN; • Вихідний код не відкритий; • Встановлення на сервер досить важка, може викликати потенційні проблеми.

Захист інформації у процесі передачі відкритими канали фундаментується на функціях:

– автентифікація взаємодіючих сторін;

– криптографічне шифрування даних, які передаються;

– перевірка правильності та цілісності переданої інформації.

Функції, які характеризуються зв’язком між собою. Реалізація ґрунтується на застосуванні методів КЗІ. Для захисту КСМ від НСД із зовнішнього середовища застосовуються міжмережеві екрани для підтримки безпеки інформаційної взаємодії через фільтрацію повідомлень. Міжмережевий екран знаходиться на інтерфейсі між локальною та відкритою мережами. Для захисту конкретного комп’ютера, який під’єднаний до відкритої мережі, то встановлюється відповідне ПЗ міжмережевого екрану [6].

Протокол тунелювання «точка-точка» — більш відомий як PPTP — є однією з найстаріших версій, які все ще використовуються сьогодні. Силою цього протоколу є його швидкість: він має надзвичайно високі швидкості з’єднання. Однак ця швидкість коштує. PPTP швидкий частково тому, що його рівень шифрування даних слабкий за сучасними стандартами. Це означає, що стороннім користувачам легше зламати шифрування, передбачене цим протоколом. Якщо потрібен більший захист, необхідно дослідити сильнішу форму протоколу.

Протокол тунелювання рівня 2, коли використовується з безпекою протоколу Інтернету, є кроком уперед від базового PPTP. Це тому, що цей рівень протоколу тунелювання пропонує два етапи захисту: частини L2TP і IPSec цього протоколу створюють власне шифрування. Це призводить до двох рівнів захисту ваших онлайн-даних.

Цей тип протоколу тунелювання через два шари шифрування може призвести до зниження швидкості з’єднання в Інтернеті. L2TP/IPSec іноді також блокується брандмауером. Це тому, що цей тип VPN-тунелювання використовує фіксовані порти.

Протокол Secure Socket Tunneling є незвичайним, оскільки він доступний лише в операційних системах Windows. Цей тип протоколу тунелювання дуже

безпечний, що робить його безпечним вибором. Він також не використовує фіксовані порти, тому SSTP легше проходить через брандмауери.

Проблема, звичайно, полягає в тому, що цей протокол недоступний для інших операційних систем, крім Windows. Це закриває багатьох потенційних користувачів.

Якщо користувач шукає найсильніший захист під час роботи в Інтернеті, слід розглянути можливість інвестування в постачальника послуг VPN, який покладається на протокол OpenVPN. Цей протокол працює з усіма основними операційними системами, Linux, Window і Mac, на мобільних операційних системах Android та iOS.

OpenVPN, можливо допоможе, оскільки він працює з такими системами, як FreeBSD, NetBSD, Solaris і OpenBSD.

OpenVPN наразі вважається найкращою формою протоколу тунелювання VPN. Це тому, що його шифрування особливо міцне. Він також вправно обходить брандмауери.

IKEv2 (Internet Key Exchange версії 2) — це протокол шифрування VPN, який обробляє дії запиту та відповіді. Він забезпечує безпеку трафіку, встановлюючи й обробляючи атрибут SA (Security Association) у набірі аутентифікації – зазвичай IPSec, оскільки IKEv2 в основному заснований на ньому та вбудований у нього.

IKEv2 був розроблений Microsoft спільно з Cisco, і він є наступником IKEv1.

Застосування саме VPN має певний набір переваг порівнюючи інші сучасні методи дистанційного доступу. Тобто, користувач, який має доступ до Інтернету, може під’єднатися до мережі організації. Загальнодоступність даних не завжди дорівнює незахищеності. Система безпеки VPN – це можливість для захисту корпоративної інформації від НСД.

Інформація передається лише у зашифрованому виді. Зчитавши дані, їх власник підтверджує чинність та здійснює перевірку цілісності даних та ідентифікацію користувачів, які включають у VPN. Де, перша гарантує, що дані надійшли до адресата у першочерговорму вигляді. Популярні алгоритми перевірки

цілісності даних – MD5 і SHA1. Побудова VPN припускає формування захищених від НСД тунелів між кількома локальними мережами чи користувачами.

Для формування VPN з обох ліній зв’язку програми шифрування вихідного та розшифрованого вхідного трафіку. Які здійснюють роботу на спеціалізованих через ПЗ чи програмно-апаратне забезпечення та з будь-якими операційними системами [7].

VPN включають такі переваги: економічність, гнучкість та зручність застосування. Завдяки VPN мережі організації обмежують зростання кількості модемів, серверів доступу, комутаційних ліній та інших технічних засобів, котрі необхідно впроваджувати для забезпечення віддаленим користувачам доступ до своїх мереж.

Рівень безпеки та анонімності мереж VPN залежить від реалізації та налаштування. Високий рівень конфіденційності здійснюється завдяки ПЗ та правильної реалізації. Налаштування мереж VPN дозволяють користувачам досягти анонімності в віртуальному просторі.

Реалізація VPN представляється як у локальній обчислювальній мережі організації розміщується VPN сервер. Віддалений користувач із застосуванням клієнтського ПЗ, VPN ініціює процедуру зв’язку з сервером. Здійснюється автентифікація користувача, як вступна фаза – встановлення VPN-з’єднання. У випадку підтвердження повноважень настає наступна фаза – між клієнтом та сервером – погодження деталей забезпечення безпеки з’єднання. Далі здійснюється VPN-з’єднання, це забезпечує обмін інформацією між клієнтом та сервером у формі, тоді пакет з даними здійснюється через процедури зашифрування/розшифрування та перевірки цілісності автентифікації даних.

Глобальною проблемою мереж VPN є відсутність встановлених стандартів автентифікації та обміну зашифрованої інформації. Проблема тягне за собою сповільнення розповсюдження VPN, користуючись розробками різних виробників, і це ускладнений процес об’єднання мереж компаній-партнерів.

VPN розгортають на рівнях не вище мережевого. Застосуючи криптографію на таких рівнях надає застосовувати транспортні протоколи (TCP, UDP).

Для створення віртуальної мережі застосовується інкапсуляція протоколу PPP в будь-який інший протокол. То даний спосіб використовує реалізацію PPTP чи Ethernet (PPPoE). Технологія VPN використовує не лише для формування приватних мереж, але надання виходу в Інтернет.

При належному рівні застосування одного ПЗ мережа VPN може забезпечити високий рівень шифрування переданої інформації. А за умови правильного налаштування та експлуатації всіх компонентів, технологія VPN забезпечує анонімність в мережі [8].

Заголовки аутентифікації забезпечують безпеку даних та аутентифікацію IP-пакетів:

– Цілісність даних гарантує, що неможлива невиявлена зміна вмісту пакета під час передачі;

– Функції автентифікації дозволяють кінцевим системам або мережевим пристроям автентифікувати користувача або користувача додаток і фільтрація трафіку відповідно;

– Запобігання атак підміни адреси;

– Захист від атак повторного відтворення.

Перші три функції гарантуються хеш-функцією аутентифікації. Код аутентифікації повідомлення функція — це процес аутентифікації в поєднанні із симетричним ключем. Якщо коротко, ці функції обчислити дайджест повідомлення, а потім дайджест шифрується за допомогою спільного секрету між ними господарів.

Дайджест — це результат математичного розрахунку фіксованої довжини. Було доведено, що це дуже малоймовірно відтворіть дайджест, якщо вихідну інформацію було змінено, оскільки це забере занадто багато часу. Такі методи використовуються, наприклад, на загальнодоступних FTP-серверах. Під час публікації файлу на сервері це є корисно також розмістити дайджест файлу на тому ж сервері. Дайджест гарантує, що вихідний файл не має було змінено кимось. Найвідомішим методом розрахунку дайджесту є MD5. Однак, оскільки це також

небезпечний метод, використання безпечного хеш-алгоритму (SHA)-256 тепер рекомендовано.

Необхідним протоколом для АН є хешований код аутентифікації повідомлення (HMAC) SHA 1. Остання функція в АН (anti - replayattack) побудована з механізмом розсувного вікна. Кожен пакет отримує порядковий номер, а різні методи гарантують, що без цього пакет неможливо відтворити повідомлення.

Інкапсуляція корисного навантаження безпеки пропонує дві послуги:

– Шифрування: дані шифруються за допомогою попередньо визначеного протоколу між двома хостами;

– Аутентифікація: у першому випуску RFC щодо IPSec АН використовувався для аутентифікації, а ESP — лише для шифрування. Це подальше дослідження показало, що шифрування без аутентифікації не є безпечним.

Як і старі RFC дозволив використання ESP без АН, було вирішено додати можливість аутентифікації в ESP до нові RFC. Зараз є деяка надмірність. Можна використовувати АН для аутентифікації, а також використовувати ESP для аутентифікації і зашифрувати. Брюс Шнайер, відомий фахівець з криптографії, пропонує використовувати ESP як для, так і для забудь про АГ.

Алгоритми аутентифікації, які використовуються в ESP:

– Стандарт потрійного шифрування даних (3DES) у режимі ланцюжка блоків шифрування (це обов’язкове протокол);

– Розширений стандарт шифрування (AES) у режимі ланцюжка блоків шифрування;

– Режим лічильника AES. DES не підтримується в останній версії протоколу, тому його не можна використовувати. AES тепер є стандартом де-факто, і його слід використовувати для шифрування.

1.3. Мережевий захист тунелів VPN

Зрештою, простий тунель IPSec не пропускатиме багатоадресний трафік, тому оновлення маршрутизації не перетинатимуть тунель, вимагаючи від користувача покладатися на RRI (ін'єкція зворотного маршруту) або статичні маршрути. Отже, потрібно подолати перешкоду, а для цього - прокладається тунель GRE.

Існує кілька способів: перший – запустити тунель GRE через тунель IPSec, у цьому випадку пункт призначення тунелю знаходиться на іншому кінці тунелю IPSec і відповідає ACL тунелю IPSec, однак необхідно переконатися, що трафік між кінцевими точками тунелю зашифрований. Інший спосіб — застосувати профіль IPSec до тунелю GRE.

```
!
crypto keyring LabKeyRing
  pre-shared-key address 172.17.1.1 key LabKey
!
crypto isakmp policy 5
 encr aes
 authentication pre-share
crypto isakmp profile ISAKMP-Profile
   keyring LabKeyRing
   match identity address 172.17.1.1 255.255.255.255
!
!
crypto ipsec transform-set LabTSET esp-aes esp-sha-hmac
!
crypto ipsec profile LabIPSecProfile
 set transform-set LabTSET
 set pfs group2
 set isakmp-profile ISAKMP-Profile
!
```

Рис.1.5. Прокладання тунелю GRE через IPSec

Деякі з цих конфігурацій виглядатимуть знайомими, наприклад, політика ISAKMP та набір трансформації. Однак є кілька відмінностей, наприклад, відсутність криптографії, кількох нових профілів та брелоків (рис 1.5).

```
!
crypto keyring LabKeyRing
  pre-shared-key address 172.17.1.1 key LabKey
!
```

Рис.1.6. IP-конфігурація тунелю

Ця конфігурація дозволяє вкладати певні хости та попередньо спільні ключі до певного брелока, які будуть застосовуватися пізніше (рис. 1.6).

У профілі ISAKMP вказується, які кінцеві точки повинні відповідати цій політиці, а також прив'язуються до ключів, які були створені раніше. В одному профілі ISAKMP можна мати кілька PSK в брелоку та кілька відповідних ідентифікаторів. Профіль ISAKMP просто знайде правильний PSK в брелоку для конкретної відповідної ідентифікаційної адреси в профілі ISAKMP (рис. 1.7).

```
!
crypto ipsec profile LabIPSecProfile
 set transform-set LabTSET
 set pfs group2
 set isakmp-profile ISAKMP-Profile
!
```

Рис. 1.7. Прив'язка ключів до профілю ISAKMP

Тепер наявний профіль IPSec, це дуже близько до того, що зробила крипто-карта. Він пов'язаний з ISAKMP, тому він знає, з якими одноранговими партнерами зіставлятися, а також набір трансформації для фази 2 переговорів. Тут можна встановити рівень досконалої прямої секретності (PFS), якщо це потрібно.

```
!
interface Tunnel1
 description IPSec Tunnel
 ip address 10.1.1.2 255.255.255.252
 ip mtu 1418
 tunnel source FastEthernet0/0
 tunnel destination 172.17.1.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile LabIPSecProfile
end
```

Рис.1.8. Захист командного тунелю ipsec LabIPSecProfile

Дві команди, які роблять це – це режим тунелю ipsec ipv4, який повідомляє тунелю, що він буде працювати в режимі IPSec. Наступний профіль захисту командного тунелю ipsec LabIPSecProfile — це те, як зв’язати профіль IPSec, який було створено раніше (рис. 1.8).

Тепер, коли є GRE із захистом IPSec, тунель GRE захищений від прослуховування в мережі Інтернет. Цей тунель GRE також надає користувачеві транспортний механізм для передачі багатоадресного трафіку, щоб запускати протокол маршрутизації через це з’єднання, надаючи користувачеві масштабоване рішення для керування VPN-сесіями «сайт-сайт» та інфраструктурою маршрутизації.

Асоціації безпеки (SA) в термінології IPSec формують основу для операцій IPSec.SA – це контракти між двома об’єктами , що визначають протоколи IPSec, що використовуються для захисту пакетів, перетворень, ключів і їх тривалість, а також багато іншого.

Перш ніж дві сутності зможуть обмінюватися пакетами за допомогою IPSec, вони повинні спочатку створити SA, які завжди є односторонній (симплекс). Таким чином, якщо хости A і B спілкуються з IPSec, кожен хост матиме два SA: SAin і SAout. Параметри SAin для хоста A і SAout для хоста B будуть мати однакові криптографічні параметри. Аналогічно, SA специфічні для протоколу. Для кожного протоколу є SA: ESP і AH. Кожен хост IPSec тому має вести базу даних (базу даних асоціації безпеки (SADB)) для зберігання всіх SA. Безпека Індекс параметра — це 32-бітовий елемент, який використовується для ідентифікації SA в SADB. SA керуються (створюються та видаляються) вручну або за допомогою протоколу, і в цьому випадку використовується протокол IKE.
Це виходить за рамки цього публікації для опису точного та повного використання SA, але має бути ясно, що SA є основою Фреймворк IPSec. У наведеній вище структурі SA пов’язана з політикою та DOI. SA є зв’язками між поняттями (фреймворк IPSec) і реальність (як реально використовувати всі ці речі в передачі даних).

При побудові захищеної віртуальної мережі VPN в першу чергу є вирішення задачі – забезпечення ІБ. Відповідно визначенням, які вказуються у різних нормативно-правових актах, ІБ характеризується: конфіденційністю, цілісністю та доступністю. Що стосується задач VPN критерії безпеки даних визначаються як [9]:

- конфіденційність – інформація, яка передається доступна лише відправнику та отримувачу. Конфіденційність забезпечується за допомогою різних методів і алгоритмів симетричного і асиметричного шифрування.
- цілісність – інформація, яка має бути доставлена без модифікацій та пошкоджень. Цілісність переданих даних зазвичай досягається завдяки різних варіантів технології КЕП, які ґрунтуються на асиметричних методах шифрування та односторонніх функціях.
- доступність – інформація, має бути доступна лише легальним користувачам.

Автентифікація здійснюється на основі багаторазових та одноразових паролів, кваліфікованих сертифікатів, смарткарт, протоколів суворої автентифікації, який забезпечує встановлення VPN з’єднань лише між легальними користувачами та запобігає доступу до засобів VPN небажаних осіб.

Авторизація надає абонентам доступ лише тим, які довели свою автентичність. Авторизація та керування доступом реалізуються найчастіше одними й тими ж засобами.

Для забезпечення безпеки переданих даних віртуальними захищеними мережами вирішуються наступними задачами [10]:

- взаємна автентифікація абонентів при встановленні з’єднання. Автентифікація абонентів здійснюється тоді, коли дозволяється вхід для легальних користувачів та запобігає доступу до мережі небажаних осіб.
- забезпечення конфіденційності, цілісності та автентичності переданої інформації. Завдання забезпечення конфіденційності інформації полягає в захисті переданих даних від НСД до читання та копіювання. Основний засіб забезпечення конфіденційності інформації є шифрування.

- авторизація та керування доступом. Компонент безпеки VPN це гарантія доступу до комп'ютерних сервісів для авторизованих користувачів, а для неавторизованих – ні.

При побудові програмних засобів авторизації застосовуються централізована (реалізує принцип єдиного входу) та децентралізована схема авторизації.

Часто зустрічається ролеве керування доступом, яке покращує керованість систем. Тобто, розподіляються між користувачами системі чи сервісів ролі, які наділені певними правами, у користувача може бути кілька ролей.

- безпека периметра мережі та виявлення вторгнень. Жорсткий контроль доступу до сервісів та ресурсів мережі, які захищаються, це є важливою функцією мережі. Застосування засобів безпеки, як мережевий екран, системи виявлення вторгнень та аудиту безпеки, антивіруси.

Важливим аспектом є мережевий екран, система виявлення вторгнень IDS (Intuasion Detection System) та системи аналізу захищеності.

- керування безпекою мережі. Мережі VPN інтегрують мережеві пристрої та сервіси управління безпекою та пропускною спроможністю. Для організацій важливим є цілісне управління даними пристроями та сервісами через інфраструктуру VPN, включаючи користувачів віддаленого доступу та засобів extranet. Система управління мережею включає набір засобів для управління політиками безпеки, пристроями та сервісами VPN будь-якого масштабу.

1.4. Структура характеристик корпоративних мереж

Комутатори, маршрутизатори та безпроводові точки доступу є основними елементами мережі. Через них пристрої, підключені до мережі, можуть спілкуватися один з одним та з іншими мережами, як-от Інтернет. Комутатори, маршрутизатори та безпроводові точки доступу виконують дуже різні функції в мережі.

Комутатори. Комутатори є основою більшості бізнес-мереж. Комутатор діє як контролер, з'єднуючи комп'ютери, принтери та сервери до мережі в будівлі чи

кампусі. Комутатори дозволяють пристроям у мережі спілкуватися один з одним, а також з іншими мережами, створюючи мережу спільних ресурсів. Завдяки обміну інформацією та розподілу ресурсів комутатори економлять гроші та підвищують продуктивність.

Є два основних типи комутаторів, які можна обрати як частину мережевих основ: локальні та керовані хмарою.

Локальний комутатор дає змогу конфігурувати та контролювати локальну мережу, забезпечуючи більш жорсткий контроль над мережевим трафіком.

Комутатор, керований хмарою, може спростити керування мережею. Користувач отримує простий користувальницький інтерфейс, багатосайтове керування повним стеком і автоматичні оновлення, що доставляються безпосередньо на комутатор.

Маршрутизатори. Маршрутизатори з'єднують кілька мереж разом. Вони також підключають комп’ютери в цих мережах до Інтернету. Маршрутизатори дозволяють всім комп’ютерам, підключеним до мережі, використовувати єдине підключення до Інтернету, що заощаджує гроші.

Диспетчером виступає маршрутизатор. Він аналізує дані, які надсилаються по мережі, вибирає найкращий маршрут для переміщення даних і відправляє їх у дорозі. Маршрутизатори з’єднують бізнес зі світом, захищають інформацію від загроз безпеці і навіть можуть вирішувати, які комп’ютери мають пріоритет над іншими. Крім цих основних мережевих функцій, маршрутизатори мають додаткові функції, які роблять мережу простішою або безпечнішою. Залежно від потреб у безпеці, наприклад, можна вибрати маршрутизатор з брандмауером, віртуальною приватною мережею (VPN) або системою зв’язку за протоколом Інтернету (IP).

Точки доступу. Точка доступу дозволяє пристроям підключатися до безпроводової мережі без кабелів. Безпроводова мережа дозволяє легко підключати нові пристрої в Інтернет і забезпечує гнучку підтримку мобільним працівникам.

Точка доступу діє як підсилювач для мережі. У той час як маршрутизатор забезпечує пропускну здатність, точка доступу розширює цю пропускну здатність, щоб мережа могла підтримувати багато пристроїв, і ці пристрої могли отримати

доступ до мережі з більшої відстані. Але точка доступу робить більше, ніж просто розширює Wi-Fi. Вона також може надавати корисні дані про пристрої в мережі, забезпечувати активну безпеку та служити багатьом іншим практичним цілям.

Точки доступу підтримують різні стандарти IEEE. Кожен стандарт є поправкою, яка була ратифікована з часом. Стандарти працюють на різних частотах, забезпечують різну пропускну здатність і підтримують різну кількість каналів.

Безпроводова мережа. Щоб створити свою безпроводову мережу, можна вибрати один із трьох типів розгортання: централізоване розгортання, конвергентне розгортання та розгортання в хмарі.

1. Централізоване розгортання. Найпоширеніший тип безпроводової мережі, централізоване розгортання, традиційно використовується в кампусах, де будівлі та мережі знаходяться в безпосередній близькості. Це розгортання консолідує безпроводову мережу, що полегшує оновлення та сприяє розширеній безпроводовій функціональності. Контролери базуються локально і встановлюються в централізованому місці.

2. Конвергентне розгортання. Для невеликих кампусів або філій конвергентні розгортання забезпечують узгодженість безпроводових і проводових з’єднань. Це розгортання об’єднує проводовий та безпроводовий пристрій на одному мережевому пристрої — комутаторі доступу — і виконує подвійну роль комутатора та безпроводового контролера.

3. Хмарне розгортання. Ця система використовує хмару для керування мережевими пристроями, розгорнутими локально в різних місцях. Рішення вимагає хмарних пристроїв Cisco Meraki, які забезпечують повну видимість мережі через свої інформаційні панелі. Рішення для динамічних багато точкових віртуальних приватних мереж DMVPN – це власне рішення Cisco Internetworking Operating System (IOS) для створення IPSec та GRE VPN у масштабований спосіб. Грунтується на двох технологіях Cisco: Next Hop Resolution Protocol (NHRP) і багатоточкові тунельні інтерфейси GRE.

DMVPN не змінює засновані на стандартах тунелі IPSec VPN, але він змінює їх конфігурацію. Під час завантаження спицевий маршрутизатор реєструє свою реальну публічну IP-адресу інтерфейсу, а концентратор підтримує NHRP база даних усіх справжніх публічних адрес інтерфейсу спіка. Згодом спицеві маршрутизатори запитують NHRP База даних для реальних адрес маршрутизаторів призначення для динамічного створення прямих тунелів. Багатоточковий Інтерфейс тунелю GRE дозволяє одному інтерфейсу GRE підтримувати декілька тунелів IPSec.

У типовому дизайні IPSec з концентратором і спицями весь трафік VPN проходить через сайт-концентратор, який діє як шлюз. Таким чином, пропускна здатність концентратора та використання ЦП обмежують розмір VPN. У DMVPN dynamic-mesh спицеві маршрутизатори потрібно підтримувати лише тунелі, які використовуються на даний момент, а маршрутизатори-концентратори підтримують лише трафік і переповнення від прямого руху.

У контексті GTS інфраструктура на основі DMVPN була розгорнута як резервна копія для RMDCN у великому масштабі оперативний пілот на початку лютого 2010 року з таких причин:

– Маршрутизатор RMDCN Customer Edge (CE) — це маршрутизатор Cisco під керуванням IOS;

– Перемаршрутизація трафіку між інфраструктурами RMDCN та DMVPN може здійснюватися в швидкий, автоматичний і надійний спосіб. До інфраструктури на основі DMVPN застосовуються такі обмеження:

– Рішення підтримує RMDCN будь-який зв’язок;

– Використання спеціалізованих маршрутизаторів Cisco;

– Використання піднабору маршрутизаторів Cisco під керуванням певних версій IOS для обмеження усунення несправностей та проблем з обслуговуванням;

– Обладнання DMVPN керується локально;

– Використання DMVPN є додатковою опцією до портфоліо доступних резервних копій RMDCN механізми (критично важливі та цифрова мережа з інтегрованими послугами (ISDN)).

Вибрана топологія DMVPN – це «один DMVPN/подвійний концентратор», а вузол спиці, розгорнутий DMVPN маршрутизатор відповідає таким технічним вимогам:

– Маршрутизатор Cisco DMVPN має бути встановлений у тому самому фізичному сегменті LAN/DMZ, що й маршрутизатор RMDCN CE;

– Маршрутизатор DMVPN повинен мати публічну IP-адресу, доступну через Інтернет – без NAT слід розгорнути;

– Маршрутизатор DMVPN повинен мати можливість встановлювати тунелі IPSec до інших сайтів DMVPN RMDCN та надсилати через них зашифрований трафік RMDCN, що дозволить протоколам IPSec приймати пакети с загальнодоступних IP-адрес маршрутизатора DMVPN, тобто ESP, GRE, IKE (UDP 500) і NAT-T (UDP 4500) протоколи.

Забезпечено середовище підключення, що дозволить підключення до кожного маршрутизатора та інше вільне операційне використання VPN через Інтернет, рішення VPN на основі вільно доступного програмного забезпечення (OpenVPN) і була встановлена операційна система Linux.

OpenVPN – це повнофункціональне рішення SSL VPN звідкритим вихідним кодом, яке вміщує широкий спектр конфігурації, включно з віддаленим доступом, мережами VPN типу «сайт-сайт», безпекою Wi-Fi та віддаленим доступом у масштабі підприємства рішення з балансуванням навантаження, перемиканням збоїв і детальним контролем доступу. Починаючи з фундаментальної передумови, що складність є ворогом безпеки, OpenVPN пропонує економічно ефективний, легка альтернатива іншим технологіям VPN.

Легкий дизайн OpenVPN позбавляє від багатьох складнощів, які характеризують інші VPN реалізації. Модель безпеки OpenVPN заснована на SSL, галузевому стандарті безпеки комунікації через Інтернет. OpenVPN реалізує рівень взаємозв’язку відкритих систем 2 або 3 безпечні мережеві розширення за допомогою протоколу SSL/TLS, підтримують гнучкі методи автентифікації клієнта на основі сертифікатів, смарт-карт та/або двофакторної аутентифікації та дозволяє користуватись або групово політики контролю доступу з використанням правил

брандмауера, що застосовуються до віртуального інтерфейсу VPN. OpenVPN не є Інтернетом проксі-сервер програми і не працює через веб-браузер. Було вирішено створити три мережі за допомогою програмного забезпечення OpenVPN для полегшення налаштування та дозволу операція буде більш гнучкою:

– Одне з'єднання базової мережі між трьома регіональними телекомунікаційними хабами (RTH);

– Одна мережа, що охоплює північну частину області;

– Одна мережа, що охоплює південну частину області.

Мережне підключення трьох RTH в регіоні буде називатися базовою мережею. Це буде точка доступу до GTS через систему комутації повідомлень. Кожен RTH розміщуватиме сервери для VPN з'єднання.

Висновки до розділу 1

Досліджено загальні положення та структури використання віртуальних захищених тунелей VPN, та зроблено переваги і недоліки протоколів VPN. Також було досліджено переваги і недоліки функціонально складових VPN протоколів.

Проаналізовано статистичні дані по технологіям VPN, а саме: ринок послуги Ethernet та IP, розмір світового ринку VPN, країни, які найбільше використовують VPN, статистичні дані використання VPN сервісів

Виокремлено інформацію з законодавчої бази захисту персональних даних, а також структуру на основі Cisco Packet Tracer та створено тунель GRE захищений від прослуховування в мережі Інтернет.

Зазначено мережевий захист тунелів VPN та критерії безпеки даних, а саме: конфіденційність, цілісність і доступність інформації.

Отримано результат - аутентифікація здійснюється на основі багаторазових та одноразових паролів, кваліфікованих сертифікатів, смарткарт, протоколів суворої аутентифікації та авторизація та керування надається лише тим, що довели свою автентичність.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ ТУНЕЛЕЙ VPN ДЛЯ ОРГАНІЗАЦІЇ СТРИМІНГОВИХ ТЕХНОЛОГІЙ

2.1. Аналіз технології віртуальних захищених тунелів VPN в корпоративній мережі

VPNaaS може бути включено в складні ланцюжки послуг, які можуть бути автоматично керується та налаштовується для надання складних віртуалізованих послуг. Серед вимоги високого рівня, встановлені документом NFV, запропонованим ETSI, в т.ч. портативність, продуктивність, еластичність, стійкість, безпека, безперервність обслуговування тощо [12]. Нижче наведено вимоги, визначені для надання VPN як VNF:

Портативність. Згідно з документом ETSI, якщо говорити про програмне забезпечення реалізації VPN у віртуалізованому середовищі на апаратному забезпеченні загального призначення можливість переміщення, налаштування та виконання VNF на основі VPN між різними постачальників, але стандартні середовища гіпервізора, стандартні експериментальні інфраструктури, такі як розгортання в XIFI має бути досягнуто. У цьому дослідженні переносимість рішення VPN досягається виконанням того ж самого процедурна модель на різних архітектурах. Це було досягнуто у FIWARE, а також на VMware. Таким чином досягається переносимість між різними гіпервізори та експериментальні платформи вважаються важливим аспектом віртуалізації Віртуальні приватні мережі.

Стабільність і безперервність обслуговування. На додаток до портативності, як зазначено у вимогах віртуалізації NFV, встановлення та забезпечення стабільності та безперервності обслуговування є ще одним важливим фактором для віртуалізація VPN, особливо при переміщенні або переналаштуванні програмного забезпечення реалізації у віртуалізованому середовищі.

Максимальне та мінімальне значення досяжної пропускної спроможності, зафіксовані втрати пакетів коефіцієнт, варіації затримки вказані в цьому дослідженні як ключові показники ефективності до забезпечити безперервність обслуговування в мережі. Втрата пакетів зберігається менше ніж на 1%, до забезпечити стабільність мережі.

Безпека. У цьому звіті питання безпеки регулюється за допомогою впровадження різних алгоритмів шифрування та хешування. Оскільки безпека має першорядне значення під час розгортання VPN як функція віртуалізованої мережі, необхідно встановити вимоги для забезпечення даних цілісність; конфіденційність і автентичність не порушені.

Експлуатаційні вимоги. Відповідальність за створення, розподіл, перерозподіл та припинення VPN ресурсів - є важливими експлуатаційними вимогами, які надають віртуалізовані середовища хмарні орендарі відповідно до норм ETSI. Показники розподілу ресурсів, такі як затримка надання віртуальної машини, коефіцієнт відмов VM. Час роботи VPN-сервісу вимірюється та аналізується в поточному дослідженні. Оскільки робота з VPN вводить додаткові заголовки IP і складну обробку криптографічних операцій, досліджено накладні витрати, що виникають при передачі даних.

Вимірювання пропускної спроможності каналу дає детальну інформацію про продуктивність мережі, яка може бути додатковою вивчається та аналізується з кількістю втрачених пакетів під час передачі та із затримкою зіткнувся.

Пропускна здатність мережі визначається як швидкість, з якою дані передаються через канал зв'язку. На додаток до надання безпечних даних через виділені посилання, надійність встановленого каналу зв'язку також не менш важливий для моделювання прямого підключення.

Надійність мережі значною мірою залежить від пропускної здатності даних в підключення. Таким чином, щоб забезпечити безпечну та надійну передачу даних, пропускна здатність приймається як єдине ціле для важливих параметричних аналізів. Jitter визначається як зміна часу між надходженням пакетів до місця

призначення. Хороша мережа передачі записує значення тремтіння від 1 до 5 мілісекунд.

Низьке тремтіння значення допомагають підтримувати міжпакетну затримку, внесену джерелом, тобто надзвичайно важливий при роботі з пакетами невеликого розміру.

Втрата пакетів має місце, коли пакети, що рухаються через канал, не досягають їх мережу призначення. Щоб забезпечити хорошу якість зв'язку, втрата пакетів у мережі підтримується нижче 1%. Чим вище втрата пакетів в мережі, тим більше буде втрата пакетів.

Повторні передачі сегментів TCP, що в кінцевому підсумку впливають на доступну пропускну здатність мережі.

Показники розподілу ресурсів ВМ, що включають час запуску ВМ, час запуску служби ВМ і VM Failure Ratio вимірюються та оцінюються для визначення надійності та швидкості управління оркеструванням.

Категоризація маршрутизаторів Cisco є хорошим початком для багатьох ситуацій. Однак, коли це може бути складно передбачає створення складного та/або великого рішення VPN. Розгортання правильного маршрутизатора в потрібному місці внесе значний внесок у загальний дизайн VPN з точки зору продуктивності та вартості.

Важливо зазначити, що для всіх пакетів, які потребують, буде потрібна додаткова обробка Cisco IOS служби безпеки. Виявилося, що технологія IPSec повільніша, ніж технологія шифрування Cisco. Однією з причин є розгортання алгоритмів аутентифікації, які вважаються повільно. Тим не менш, література з питань безпеки підкреслює відсутність аутентифікації як вразливість безпеки. Без шкоди для безпеки, IPSec має бути технологією для розгортання. Крім того, IPSec представляє розширення пакетів, що, швидше за все, вимагатиме фрагментації та повторної збірки захищеного IPSec IP дейтаграми.

Зашифровані пакети також будуть аутентифіковані, що означає, що більшість пакетів матиме два криптографічні операції, що виконуються над ними.

Вплив на продуктивність також може виникнути при використанні VPN-з’єднань через супутникові Інтернет-посилання. Досвід від тестування, проведене Meteo France, показало наступне. У деяких комплектаціях, особливо при перетині супутникових зв’язків, максимальна одиниця передачі значно зменшена, і потрібні великі пакети IPSec фрагментований. Якщо встановлено біт Don’t Fragment (DF), такі пакети відкидаються. В результаті виходять невеликі пакети (послідовності аутентифікації) можуть проходити, тоді як великі пакети (передачі даних) відкидаються. Щоб уникнути цього, а рекомендується очистити біт DF (на маршрутизаторі Cisco: «crypto ipsec df-bit-clear»).

Хмарні обчислення пропонують підприємствам можливість отримати доступ до обчислювальних ресурсів на вимогу. Це дозволяє підприємствам економити на капітальних витратах, пов’язаних з періодичним обладнанням оновлення, обслуговування та витрати на енергію.

Крім того, хмарні обчислення дозволяють підприємствам динамічно розподіляти та/або вивільняти ресурси відповідно до їхніх потреб або попиту своїх клієнтів. Багато хмарних провайдерів створили центри обробки даних у різних географічних регіонах місцях та з’єднали їх між собою за допомогою високошвидкісних інтернет-посилань. Це робить це можливим для хмарних орендарів для створення екземплярів послуг поблизу користувачів. Теоретично, а клієнт може орендувати ресурси у кількох хмарних провайдерів і об’єднати їх разом загальний пул, як це буває у федеративній хмарі.

Ресурси в пулі часто є будівельними блоками для служб, як правило, віртуальних машин з пов’язаною пам’яттю, сховищем та мережею. Ці будівельні блоки позначаються як віртуальні Мережеві функції (VNF) або загальні активатори (GE) підключаються до служби ланцюги, які можуть виконувати розширену обробку даних. Розглядаючи сценарій, у якому беруть участь різні хмарні провайдери, кожен надання різних послуг, таких як інтернет-магазини, веб-послуги тощо. Орендарі як а частина будь-якої з хмар, не хочуть, щоб їхні облікові дані картки були скомпрометовані, коли пов’язані з торговими послугами.

Так само не хочуть орендарі з діловими відносинами їх конфіденційні дані можуть бути скомпрометовані під час передачі. З подібних причин у хмарних орендарів немає бажаючи покладатися на послуги хмарного постачальника, можуть побудувати власний приватний VPN-тунель для безпечна передача інформації. У цій ситуації бажано, щоб дані, що обходять ці елементи, залишалися конфіденційна, і що треті сторони не можуть змінити її без виявлення. Крім того, це часто зручно, що елементи ланцюга, створені у різних постачальників, розташовані в спільному простір IP-адрес [13].

Це може спростити реалізацію виявлення служби, балансування навантаження, схеми високої доступності тощо. VPN – це типовий спосіб з'єднання мереж через загальнодоступну мережу інфраструктури. Хоча кілька хмарних провайдерів пропонують доступ до VPN своїм орендарям, це може бути небажано за певних обставин (наприклад, орендар не довіряє постачальнику та/або орендар хоче мати кращий контроль над політикою VPN та генерацією ключів і процес розповсюдження). Метою цього проекту є надання VPN-як-послуги (VPNaaS) використання віртуалізованого програмного забезпечення VPN, що по суті робить VPN ще одним будівельним блоком для а обслуговування.

Реалізовують мережу VPN на маршрутизаторах Cisco у Windows середовище Vista, яке пояснює, як впливає на продуктивність VPN оптимальний підбір різних алгоритмів шифрування.

Серед різних комбінацій шифрування, AES256 і 3DES, і алгоритми хешування, SHA1 і MD5, використовували AES256- Система MD5 показала найкращу продуктивність у порівнянні з іншими. Також AES256 працює краще, ніж 3DES і MD5, перевершуючи SHA-1.

Відображаючи необхідність оптимальної переваги алгоритму для отримання вищої мережі пропускна здатність.

Аналогічно, поточне дослідження дає подібні результати, вказуючи алгоритми AES з різними розмірами блоків працюють краще, ніж 3DES, тоді як M 5 перевершує SHA, але в середовищі на базі Linux на хмарній інфраструктурі.

Беручи до уваги різні комбінації алгоритмів шифрування та хешування, помічено, що AES128-MD5 перевершує в усіх випадках.

Це пов’язано з розробкою AES для ефективної реалізації як в апаратному, так і в програмному забезпеченні демонструючи задовільну ефективність, міцніші криптографічні ключі довжиною 256 біт у порівняння з повторюваними слабкими та повільними клавішами та більшою тривалістю часу для 3DES шифрування. Також ключовий графік для AES128 вважається сильнішим, ніж AES256, коли враховуючи стійкість до атак на пов’язані ключі, оскільки чим довший головний ключ джерела, тим більше потрібен контроль над підключами, що послаблює безпеку в моделях атак на відповідні ключі.

3DES був розроблений для ефективної апаратної реалізації, але він поступається продуктивність з програмним забезпеченням, майже в 3 рази менше, ніж у програмних реалізацій була перевершена AES. MD5 вважається менш інтенсивним процесором у порівнянні з Сімейство SHA і, отже, показало кращу продуктивність у порівнянні з SHA. Хоча SHA є вважається більш безпечним, MD5 працює швидше, а отже, і його продуктивність [14].

Оскільки VPN імітують конфіденційне з’єднання, пропускна здатність через тунель VPN є на нього часто впливають накладні витрати та використовувані складні алгоритми обробки. Відповідний метод обчислення максимальної пропускної здатності мережі полягає в мінімізації затримки, що вноситься збереження втрат пакетів нижче 1%.

Під час аналізу пакетів TCP з оцінених результатів видно, що найкращий у всьому був представлений AES128-MD5, потім AES256-MD5 і AES128- SHA256. Найгірше працювали 3DES-SHA256 і 3DES-MD5. Причини є неефективна реалізація програмного забезпечення, слабка продуктивність ключа і більший період часу 3DES порівняно з AES. Щоб підтримувати хорошу якість зв’язку, втрати пакетів зберігаються менше ніж на 1% протягом усього часу розрахунковий аналіз. Пакети UDP мали подібну криптографічну продуктивність до TCP.

Аналогічно, AES128-MD5 показав найкращу пропускну здатність, а 3DES-SHA256 – найнижчу продуктивність. Джіттер враховується для різних комбінацій

алгоритмів шифрування та хешування з різними розмірами пакетів. Спостерігається, що тремтіння для тунельного трафіку вище, ніж у нетунельному або трафік відкритого тексту через додаткові витрати, що виникають під час шифрування даних. Додаткові криптографічні витрати на додаток до додаткових заголовків IPSec збільшують мережу складність, що збільшує тремтіння в мережі.

Спостерігається, що DES демонструє максимум тремтіння в порівнянні з іншими комбінаціями через несумісність програмного забезпечення. Пропускна здатність і джиттер розраховуються для різних розмірів MTU. У TCP це так помітив, що в міру збільшення MTU пропускна здатність мережі також збільшувалася. Акцент був зроблений на забезпеченні надійної та безпечної передачі даних та отже, незважаючи на змінні розміри пакетів, втрата пакетів у мережі зберігалася нижче 1%.

Подібна продуктивність спостерігалася в TCP і UDP, пропускна здатність мережі в UDP демонстрував подальшу перевагу, коли втрата пакетів у мережі була скомпрометована та дозволена перевищувати 1%. Але щоб забезпечити хорошу якість посилання, втрати пакетів були зменшені до менш ніж 1%. Так накладні витрати, введені через тунельний трафік, що складається з додаткового заголовка IPSec і складність шифрування погіршує продуктивність мережі як для трафіку TCP, так і для UDP.

Детальне вивчення різних архітектурних реалізацій VPN і детальне вивчення різних механізмів розподілу ключових для безпеки посилення. Також хмарна платформа на базі Linux для полегшення спілкування різні елементи, конфігурація та моделювання рішення IPSec VPN з відкритим вихідним кодом. Далі слідує оцінка діяльності різних алгоритми шифрування для оцінки введених накладних витрат. Серед різноманітних досліджених реалізацій була прийнята архітектура site-to-site забезпечення безпеки мережі, маршрутизації, інкапсуляції та шифрування, які повинні виконуватися маршрутизатори шлюзу, позбавлені участі клієнтів/користувачів, використовуючи IPSec в тунельному режимі.

Інтернет рентабельність IKEv2 і модульна функція strongSwan відрізняє ефективність над іншими доступне програмне забезпечення. Низькі витрати на

інфраструктуру та простота розгортання нової мережі додають до цього можливості масштабованості та гнучкості. Серед різних ключових методів розподілу, у цій реалізації використовуються ключі попереднього видалення, щоб уникнути складних конфігурацій. Архітектура VPN була змодельована та розроблена за допомогою об'єднаної хмарної лабораторії FIWARE і CLI OpenStack.

Один з основних елементів, які необхідно розрахувати, пропонуючи прототип VPN хмара — це вплив моделі на продуктивність. Незважаючи на те, що має важкий введені суми накладних витрат, вагомою причиною для прийняття цієї моделі було б покращити та врахувати характеристики хмари та забезпечити безпечну передачу даних по всьому світу однолітні елементи. Серед різних комбінацій використовуваних алгоритмів шифрування та хешування, AES128-MD5 показав найкращі результати в порівнянні з 3DES-SHA256, який виробляв найменше пропускна здатність.

Показники розподілу ресурсів ВМ також оцінювали максимальну тривалість часу необхідний для запуску та встановлення послуги VPN у віртуалізованому середовищі. Ці показники описують фактори швидкості та надійності, необхідні для запуску та оркестровка хмарних сервісів. Важливою частиною цього дослідження є визначені вимоги щодо пропозиції VPN як віртуалізована мережева функція. Досягнення переносимості через стандартні гіпервізори та експериментальні платформи, що забезпечують стабільність та безперервність обслуговування шляхом аналізу досяжного Важливими факторами є всі значення та значення джиттера, мінімальні втрати пакетів керування послугами VPN на віртуалізованих серверах. Також основною метою створення VPN є забезпечити безпеку в хмарі для безпечного та конфіденційного спілкування [15].

Різні оперативні оцінки проводяться для дослідження швидкості та надійності розподілу ресурсів ВМ, розгортання та керування в хмарному середовищі. Дозволяє низький час обслуговування VPN модель, яка буде використовуватися для безпечних телефонних розмов, при цьому час, необхідний для налаштування тунель до зв'язку лише близько 2 секунд.

Різні архітектури, включно з мережами VPN, між хостом і віддаленим доступом придатні для впровадження віртуальних VPN були вивчені та зазначені разом з кожним переваги та недоліки. Також різні механізми розповсюдження ключів, у тому числі попередньо спільні ключі та цифрові сертифікати вивчені, і для кожного є чіткий опис було згадано.

Розробка та моделювання рішення IPSec VPN на хмарній платформі має було прийнято для реалізації в цій дисертації далі відповідаючи на RQ на основі моделювання хмарного рішення VPN. Також продуктивність впливає на вбудовану модель оцінюються як TCP, так і UDP-трафіком.

Пропускна спроможність мережі, тремтіння і втрати пакетів є вимірювали для різних алгоритмів шифрування та хешування, таким чином вивчаючи вплив найкраща алгоритмічна комбінація для кожного з оцінюваних показників, а також визначення безпеки криптографічні комбінації для конфіденційної передачі інформації, таким чином відповідаючи на четвертий RQ.

2.2. Аналіз та порівняння протоколів реалізації VPN

Спеціальні протоколи. Деякі постачальники VPN вирішують писати власні протоколи замість того, щоб використовувати існуючий. Кілька прикладів — Catapult Hydra від Hotspot Shield, Lightway від ExpressVPN та NordLynx від NordVPN. Ці протоколи відрізняються за своєю продуктивністю та безпекою, і іноді їх код не є загальнодоступним. Ми рекомендуємо використовувати лише протоколи з відкритим кодом.

Деякі користувацькі протоколи створюються з нуля, але багато з них є лише розгалуженнями протоколів з відкритим кодом. NordLynx, наприклад, — це просто Wireguard із системою подвійного NAT для запобігання реєстрації IP-адрес.

Типи VPN: безпечні або надійні. Усі VPN, які ми розглядаємо в Comparitech, вважаються «безпечними» VPN. Це означає, що трафік, який надсилається та отримується через них, зашифрований та аутентифікований. Бути безпечним VPN також означає, що і сервер, і клієнт погоджуються щодо властивостей безпеки, і

ніхто за межами VPN не може впливати на ці властивості. Захищені VPN використовують один із перерахованих вище протоколів.

«Надійна» VPN відрізняється від захищеної VPN. Надійні VPN можуть не використовувати жодне шифрування. Натомість користувачі «довіряють» постачальнику VPN, щоб переконатися, що ніхто інший не може використовувати ту саму IP-адресу та шлях. Ніхто, крім постачальника, не може змінювати дані, вводити дані або видаляти дані на шляху в VPN.

Надійні VPN сьогодні зустрічаються набагато рідше. Зазвичай корпорації використовували їх для віддаленого доступу до внутрішніх ресурсів компанії, а не для підключення до всесвітньої мережі. Але загрози безпеці стали великими для більшості компаній, які ризикували використовувати незашифроване з'єднання.

VPN, які поєднують властивості шифрування безпечної VPN і властивості виділеної лінії надійної VPN, іноді називають «гібридними» VPN. Гібридні VPN є поширеними сьогодні, особливо для корпорацій. Але більшість комерційних провайдерів VPN, які пропонують необмежений доступ до Інтернету, не надають клієнтам виділену IP-адресу, тому вони не вважаються гібридами.

Хмарні обчислення пропонують підприємствам можливість отримати доступ до обчислювальних ресурсів на вимогу. Це дозволяє підприємствам економити на капітальних витратах, пов`язаних з періодичним обладнанням оновлення, обслуговування та витрати на енергію. Крім того, хмарні обчислення дозволяють підприємствам динамічно розподіляти та/або вивільняти ресурси відповідно до їхніх потреб або попиту своїх клієнтів. Багато хмарних провайдерів створили центри обробки даних у різних географічних регіонах місцях та з'єднали їх між собою за допомогою високошвидкісних інтернет-посилань.

Це робить це можливим для хмарних орендарів для створення екземплярів послуг поблизу користувачів. Теоретично, а клієнт може орендувати ресурси у кількох хмарних провайдерів і об'єднати їх разом загальний пул, як це буває у федеративній хмарі. Ресурси в пулі часто є будівельними блоками для служб, як правило, віртуальних машин з пов'язаною пам'яттю, сховищем та мережею.

Ці будівельні блоки позначаються як віртуальні Мережеві функції (VNF) або загальні активатори (GE) підключаються до служби ланцюги, які можуть виконувати розширену обробку даних. У об'єднаній хмарі взаємопов'язані елементи можуть охоплювати величезні географічні відстані, а також кілька автономних Інтернет Системи (АС).

АН (Authentication Header) - управління цілісністю переданих даних і аутентифікацію. призначений для забезпечення аутентифікації відправника, контролю цілісності даних та додатково для запобігання повторному відтворенню пакета - за умови, що приймаюча сторона налаштована на перевірку серійного номера пакета. Поля пакетів IP, які змінюються з часом, не підлягають перевірці цілісності.

АН захищає дані протоколу вищого рівня та ті поля заголовків IP, які не змінюються по маршруту доставки або змінюються передбачувано – кількість полів невелика - це прийом (клас трафіку), мітка потоку та обмеження стрибків. присутній необов'язковий заголовок вихідної маршрутизації).

Надає три види охоронних послуг:

- Забезпечення конфіденційності (шифрування вмісту пакетів IP, а також частковий захист від аналізу трафіку через тунельний режим);

- Цілісність IP-пакетів, аутентифікація джерела даних.

- Забезпечення захисту від відтворення IP-пакетів.

- Функціональність ESP ширша, ніж АН (додано шифрування);

- ESP не повинен надавати всі послуги, але повинен включати або конфіденційність, або автентифікацію.

Розмір заголовка - це не стільки заголовок, скільки код (накладення) кодованого вмісту. Наприклад, наступне заголовкове посилання не можна розмістити на початку відписаної частини, оскільки воно втратить конфіденційність.

ISAKMP (Internet Security Association and Key Management Protocol) - управління установкою з'єднання, взаємну аутентифікації кінцевими вузлами один одного і обмін секретними ключами.

SA (Security Association) - це набір параметрів про те як сторони будуть надалі використовувати ті чи інші властивості протоколів зі складу IPsec.

Віртуальна приватна мережа (VPN) забезпечує підвищену безпеку між двома повторними різні сутності, які обмінюються даними через ненадійні мережі, такі як Інтернет. Системи VPN запобігають різним атакам, таким як підслуховування або повторення. Однак традиційні VPN не підтримують мобільність користувачів.

Дійсно, мережа збої автоматично руйнують безпечні тунелі та призводять до подальшого повторного це необхідно для відновлення розбитих тунелів. Такі переговори передбачає дорогі обчислювальні операції для відновлення тунелів, а також транспортні та прикладні зв'язки. Ця фаза переговорів викликає не тільки значну затримку, але й створює ризики «Людина-посередині» прихватки. Тому традиційні VPN не можуть ефективно працювати в динамічному режимі та/або мобільні середовища.

Мобільна VPN дозволяє, з одного боку, захищати зв'язок і підтримувати відкритими сеанси програми під час зміни місця розташування. З іншого боку, мобільна VPN безкоштовна для повторного узгодження ключа сеансу на етапі відновлення. Ці дві технічні властивості необхідні в безпечних мобільних середовищах.

Незважаючи на свої цікаві властивості, системи, що працюють в автономному і мобільні середовища постійно піддаються деяким проблемам безпеки, як-от DoS і повторні атаки. Щоб запобігти атакам відтворення, пакети MUSeS створюються шляхом додавання порядкових номерів до їхніх заголовків.

Іншими словами, кожен пакет окремо ідентифікується своїм порядковий номер, доданий до його заголовка. Таким чином, коли пакет буде відтворено, це буде буде автоматично виявлено і згодом буде знищено. На етапі відновлення генерується повідомлення Re-hello, яке потім надсилається для того, щоб відновити перерваний сеанс без використання механізму повторного узгодження ключа сеансу. Однак пакет Re-hello може бути відтворений, оскільки він не містить се-номер запиту для виявлення атаки повтору.

Таким чином, зловмисник, який має у ltrated мережа могла б потім відправити послідовність пакетів Re-hello з метою здійснення атак відмови в обслуговуванні (DoS). Крім того, приймач одноранговий партнер не може визначити, який дубець є останнім отриманим серед інших повторних отримані пакети, інакше цю проблему можна було б легко вирішити. Якщо говорити конкретно, при отриманні Re-hello, одноранговий одержувач обробляє його, щоб розв'язати і виклик і перш ніж закінчити, він отримує ще один, знову інший тощо.

Нарешті, цільовий одноранговий буде насичений, а виконання запитів Re-hello. Крім того, HIP може бути вразливим до DoS-атак на етапі відновлення, як показано на стаття, що аналізує безпеку протоколу HIP. Щоб вирішити цю проблему безпеки, MUSeS призначає мітку часу під час надсилання кожен пакет Re-hello, щоб розпізнати найсвіжіший запит серед отриманих запити.

Таким чином, система MUSeS намагається запобігти DoS-атакам, які використовують файл безперервна послідовність пакетів Re-hello. Завдяки своїй мобільності, гнучкість і автономні, VPN-системи на основі P2P, на жаль, не є повністю невразливими до вторгнення зловмисників. Справді, у повністю децентралізованих P2P мережах, кожен одноранговий пристрій може приєднатися та вийти з мережі в будь-який час і зазвичай без жодних аутентифікація. У нашій системі аутентифікація гарантується за допомогою виклику повідомлення.

Як правило, для аутентифікації однорангового вузла в мережі вузол шифрує запущений dom Challenge повідомлення та надсилає його відповідному однорангові. При отриманні цього повідомлення, відповідний одноранговий вузол розшифровує його і надсилає те саме повідомлення до ровесник-ініціатор. Таким чином, однолітка-ініціатор з'ясовує особу кореспондента [16].

Протокол HIP розроблено, щоб бути стійким до відмови в обслуговуванні (DoS) і людина посередині (MitM) атакує, і якщо використовується з увімкненою ESP, вона забезпечує захист від DoS і MitM для протоколів верхнього рівня, таких як TCP і UDP. Однак у N2N і MOBIKE не може бути безпечних тунелів без N2N-Super-Node або MOBIKE-GW.

Іншими словами, коли N2N-супервузли і MOBIKE-GW недоступні, будь-який безпечний зв’язок буде неможливим. Протокол HIP і MUSeS не страждають цими порушеннями. Хоча MUSeS пропонує надійний механізм безпеки у віддаленому спілкуванні, Однак між двома однолітками є слабке місце безпеки в локальному плікативних зв’язків. На відміну від спілкування між двома однолітками MUSeS, локальний зв’язок між MUSeS і програмами не захищений.

Це означає що неавторизована програма користувача, запущена зловмисником, повинна встановити з’єднання з віддаленим чесним MUSeS або підслуховувати обміняний трафік між MUSeS і локальними додатками. Це ненадійне спілкування повинно викликають проблеми з безпекою.

З одного боку, щоб запобігти зовнішнім шкідливим процесам для підключення MUSeS, лише локальні програми мають право підключатися до MUSeS за допомогою петлі зворотна адреса.

З іншого боку, тільки користувач може зловити, використовуючи tcpdump або wireshark, локальний трафік, що проходить від локальних додатків до MUSeS проміжне програмне забезпечення і навпаки. Таким чином, звичайні текстові дані обмінюються між локальними програми та MUSeS захищені.

Мобільні пристрої та динамічні середовища набувають поширення в Інтернеті. Однак, наприклад, традиційні інфраструктури VPN не підтримують сеанс безперервність є результатом зміни розташування або реконструкції мережі. Після кожного розрив з’єднання, для відновлення зламаного потрібен процес повторного узгодження ключа тунеля, щоб усунути збої в мережі, що виникли внаслідок зміни розташування або реконструкції мережі.

На відміну від більшості динамічних систем VPN, ці системи мають перевагу щоб бути досить масштабованим і мати можливість спілкуватися через NAT і стіни. Децентралізована P2P VPN є гнучкі та самоорганізуючі інфраструктури які дозволяють користувачам створювати власні захищені мережі в ненадійній мережі працювати.

Рівень 2 одноранговий VPN, який називається N2N, і ELA топології дуже схожі, незважаючи на те, що N2N базується на рівні OSI 2, тоді як ELA базується

на рівні OSI 3. Однак використання супервузлів у N2N обмежує його повну масштабованість, оскільки ці вузли відіграють важливішу роль, ніж інші вузли, і, таким чином, вони можуть послабити загальну силу мережі N2N і навіть можуть порушити його підключення, якщо вони не вдаються.

Freelan –це багатоплатформна однорангова VPN з відкритим вихідним кодом, яка розтягує локальну мережу через Інтернет. На основі протоколу UDP FreeLAN Протокол безпечного каналу (FSCP) розроблено, щоб бути безпечним та ефективним, і намагається зменшити витрати мережі. Крім того, системи Freelan можуть бути підключені діяти відповідно до моделі клієнт/сервер, однорангової або гібридної моделі підходить найкраще.

Щоб оцінити ці чотири технології VPN у сценарії мобільності, ми маємо використовував розроблений інструмент під назвою Network Emulator For Mobile Universes (NEmu) Вінсента Отефажа. Був проведений експеримент із зазначеною реалізацією в динамічному середовищі, що складається з одного мобільного вузла.

Мобільний вузол всередині цього середовище має можливість залишити одну мережу (один віртуальний маршрутизатор) у порядку приєднатися до іншого (іншого віртуального маршрутизатора). Ця подія спричиняє збій мережі- під час переміщення до можливого наступного підключення. Цей зрив є прозорим для програми і не заважає системі MUSeS від продовження роботи, незважаючи на те, що мобільний вузол відключено на хвилинку.

Технічно рухливість вузла складається у спричиненні штучного збою у віртуальному мережевому інтерфейсі. Від’єднуємо, а віртуальний провід від віртуального комутатора та повторно підключіть його до іншого віртуального комутатора. Система MUSeS приховує цю зміну мережі не лише для програми користувача але також до віддаленого відповідного вузла. показати еволюцію пропускної спроможності між двома коридорами відповідно на заявки з часом. Для всіх систем переривання мережі відбувається на 40-й секунді після початку експерименту та пропускної здатності миттєво падає до нуля в інтервалах часу [17].

Це означає, що тривалість розриву 20 секунд. З’єднання в мережі відновлюється і рівень CLOAK на 60-й секунді. Однак через затримку пропускну

здатність залишається на нулі після 60-ї секунди до ефективного відновлення. Ця затримка змінюється від однієї системи до іншої. Дійсно, тоді як проміжне програмне забезпечення MUSeS має а затримка 3 секунди, протоколи MOBIKE, N2N і HIP мають відповідно затримки 12 секунд, 51 секунду і 13 секунд. Порушення мережі як через неякісні пристрої, так і через відсутність технічних навиків. Повністю поширені в країнах, що розвиваються, особливо в Африці.

Для подолання безпеки та продуктивності необхідні захищені стійкі сеанси. проблеми, пов’язані з перебоями з’єднання. Представлено чотири мобільні VPN-рішення з відкритим вихідним кодом надали детальний технічний аналіз ysis цих систем і порівняли їх з точки зору функціональності та продуктивність. Результати показують, що MUSeS є конкурентоспроможним рішенням для надання безпечний і мобільний зв'язок.

2.3. Методи використання стримінгових технологій віртуальних захищених тунелей

Для полегшення спілкування різні елементи, конфігурація та моделювання рішення IPSec VPN з відкритим вихідним кодом за допомогою сильногоЛебідь було досягнуто. Далі слідує оцінка діяльності різних алгоритми шифрування для оцінки введених накладних витрат. Серед різноманітних досліджених реалізацій була прийнята архітектура site-to-site забезпечення безпеки мережі, маршрутизації, інкапсуляції та шифрування, які повинні виконуватися маршрутизатори шлюзу, позбавлені участі клієнтів/користувачів, використовуючи IPSec в тунельному режимі. IKEv2 і модульна функція strongSwan відрізняє ефективність над іншими доступне програмне забезпечення.

Низькі витрати на інфраструктуру та простота розгортання нової мережі додають до цього можливості масштабованості та гнучкості. Серед різних ключових методів розподілу, які вивчаються в У розділі 3 у цій реалізації використовуються ключі попереднього видалення, щоб уникнути складних

конфігурацій. Архітектура VPN була змодельована та розроблена за допомогою об’єднаної хмарної лабораторії FIWARE і CLI OpenStack.

Один з основних елементів, які необхідно розрахувати, пропонуючи прототип VPN хмара — це вплив моделі на продуктивність. Незважаючи на те, що має важкий введені суми накладних витрат, вагомою причиною для прийняття цієї моделі було б покращити та врахувати характеристики хмари та забезпечити безпечну передачу даних по всьому світу однолітні елементи.

Серед різних комбінацій використовуваних алгоритмів шифрування та хешування, AES128-MD5 показав найкращі результати в порівнянні з 3DES-SHA256, який виробляв найменше пропускна здатність.

Показники розподілу ресурсів ВМ також оцінювали максимальну тривалість часу необхідний для запуску та встановлення послуги VPN у віртуалізованому середовищі. Ці показники описують фактори швидкості та надійності, необхідні для запуску та оркестровка хмарних сервісів. Важливою частиною цього дослідження є визначені вимоги щодо пропозиції VPN як віртуалізованої мережевої функції. Досягнення переносимості через стандартні гіпервізори та експериментальні платформи, що забезпечують стабільність та безперервність обслуговування шляхом аналізу досяжного [18].

Важливими факторами є всі значення та значення джиттера, мінімальні втрати пакетів керування послугами VPN на віртуалізованих серверах. Також основною метою створення VPN є забезпечити безпеку в хмарі для безпечного та конфіденційного спілкування. Різні оперативні оцінки проводяться для дослідження швидкості та надійності розподілу ресурсів ВМ, розгортання та керування в хмарному середовищі. Дозволяє низький час обслуговування VPN модель, яка буде використовуватися для безпечних телефонних розмов, при цьому час, необхідний для налаштування тунель до зв'язку лише близько 2 секунд.

Різні архітектури, включно з мережами VPN, між хостом і віддаленим доступом придатні для впровадження віртуальних VPN були вивчені та зазначені разом з кожним переваги та недоліки. Також різні механізми розповсюдження

ключів, у тому числі попередньо спільні ключі та цифрові сертифікати вивчені, і для кожного є чіткий опис було згадано.

Розробка та моделювання рішення IPSec VPN на хмарній платформі було прийнято для реалізації в цій дипломній роботі, що додатково відповідає RQ на основі моделювання хмарного рішення VPN. Також продуктивність впливає на вбудовану модель оцінюються як TCP, так і UDP-трафіком.

Пропускна спроможність мережі, тремтіння і втрати пакетів є вимірювали для різних алгоритмів шифрування та хешування, таким чином вивчаючи вплив найкраща алгоритмічна комбінація для кожного з оцінюваних показників, а також визначення безпеки криптографічні комбінації для конфіденційної передачі інформації, таким чином відповідаючи на четвертий RQ.

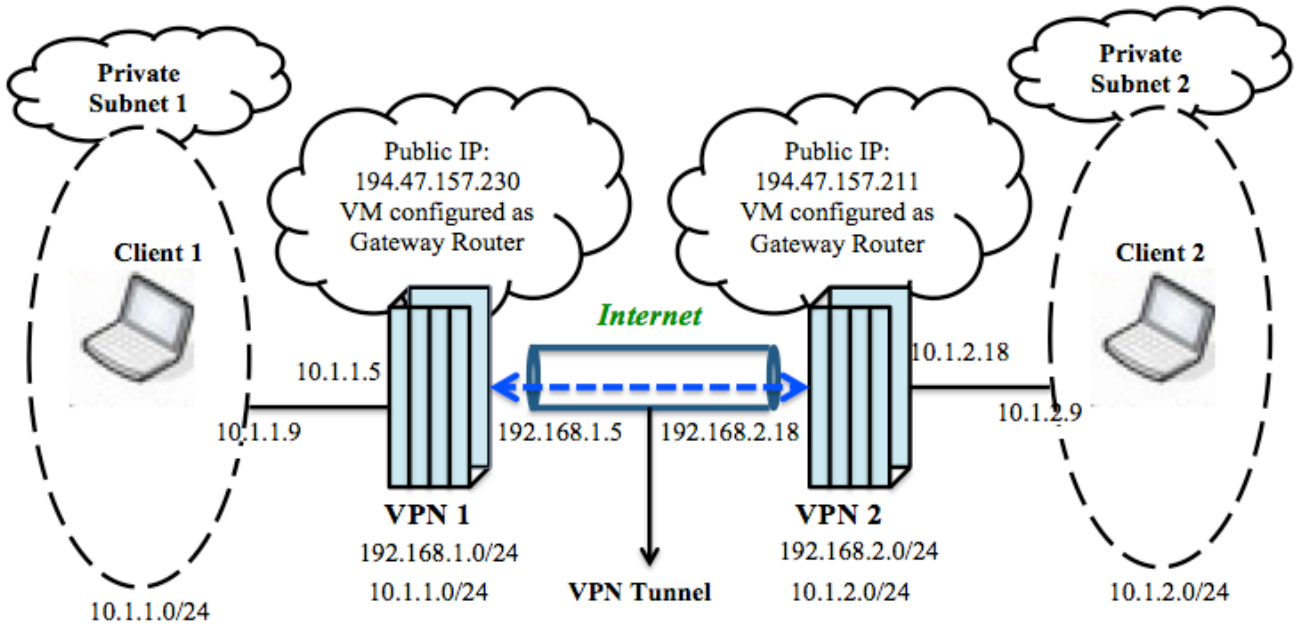

Рис.2.1. VPN архітектура

У мережах VPN типу «site-to-site» хости/клієнти/користувачі, які працюють через тунель VPN, не вимагають окремого встановлення клієнтського програмного забезпечення VPN на кожному, надсилання або отримання TCP/IP трафік увімкнено через VPN-шлюзи. Шлюз на одному кінці відповідає за інкапсуляція, шифрування та аутентифікація вихідного трафіку, надсилання його одноранговій VPN шлюз на іншому кінці через публічну інфраструктуру до цільового сайту.

VPN-сервіс інший кінець від’єднує IP-заголовок, розшифровує дані та пересилає пакети даних до цільовий хост у його приватній мережі. Найпоширеніший безпечний протокол, який використовується при налаштуванні між сайтом VPN — це протокол IPSec. Через те, що VPN в основному розгортаються за допомогою протоколу IPSec здатність підвищувати продуктивність і комунікацію, таким чином підвищуючи гнучкість мережі [19].

Перевага: VPN типу «site-to-site» пропонують більшу масштабованість та гнучкість, оскільки лише шлюз VPN повинен підтримувати функціональність IPSec, а отже, встановлення і витрати на керування між розгорнутими шлюзами мінімальні. Також це розвантажує обробку накладні витрати від окремих систем до маршрутизатора шлюзу, що звільняє пам’ять споживання і швидкість обробки.

Недолік: Однак накладні витрати, якими керують маршрутизатори шлюзу, збільшуються Таким чином, використання ЦП погіршує продуктивність користувача з точки зору швидкості зв’язку.

StrongSwan — одне з найвідоміших рішень на основі IPSec-VPN з відкритим кодом реалізовано на кросплатформних платформах. Основна мотивація вибору strongSwan над іншим програмним забезпеченням для реалізації IPSec, таким як OpenSwan тощо, є широким адаптивність до різних дистрибутивів Linux, реалізація ключа IKEv1 і IKEv2 протоколи обміну, можливість розширення до багатьох плагінів і розширені звіти про документацію. strongSwan IKEv2 за своєю суттю є багатопоточним, тоді як OpenSwan є однопотоковим, таким чином дозволяючи першому обробляти тисячі одночасних тунелів IPSec на шлюзах VPN.

StrongSwan також забезпечує кращу підтримку аутентифікації, механізмів безпеки та є модульна в порівнянні з монолітною поведінкою OpenSwan. Щоб створити тунельну архітектуру між одноранговими шлюзами, програмне забезпечення strongSwan встановлено всередині двох віртуальних машин, які діють як VPN-шлюзи, як пояснювалося в попередньому розділі.

StrongSwan — це повне рішення IPSec, що забезпечує шифрування та аутентифікацію серверів і клієнтів.

Нижче наведено кілька його переваг:

- StrongSwan підтримує сумісність IKEv2, що є однією зі своїх ефективних переваг перед інші.
- Численні тунелі здатності обробки strongSwan IKEv2, що є властиво багатопотоковий перевершує OpenSwan, який є однопотоковим.
- StrongSwan є модульним і пропонує окремі плагіни, що покращують його функціональність.

StrongSwan — використовує протоколи IKEv1 або IKEv2 для встановлення SA через однолітків.

Мета IKE — забезпечити надійну аутентифікацію як однорангових, так і похідних унікальні криптографічні ключі сеансу. Ці сеанси IKE, позначені IKE_SA, забезпечують означає обмін інформацією про конфігурацію та узгодження IPSec SA, позначених як CHILD_SA. Ці IPSec SA визначають зацікавлений трафік, який буде надіслано через тунель і як дані шифруються та аутентифікуються.

CHILD_SA складається з двох елементів, фактичний IPSec SA, що описує шифрування, алгоритм хешування та ключі, необхідні для шифрування та аутентифікація трафіку та політики, щоб визначити, який трафік буде використовувати такий SA.

Політики працюють у обох напрямках, тобто буде доступний лише трафік, який відповідає вхідній політиці розшифровано на іншому кінці. Експериментальна установка для досягнення VPN-з’єднання «site-to-site». Налаштування маршрутизаторів шлюзу, VPN1 і VPN2, можна переглянути в Додатку А.

Як згадувалося в розділі IPSec VPN асоціації, функціональні можливості, функціонування та продуктивність чітко зображує прозорість додатків, здатність захищати трафік у реальному часі та компетентність IPSec VPN для високобезпечного з’єднання «site-to-site». StrongSwan є одним із більшість проектованих реалізацій IPSec VPN на Linux платформи в порівнянні з вже існуюче програмне забезпечення OpenVPN, OpenSwan тощо.

У тунельному режимі IPSec VPN створюються та керуються через наскрізні шлюзи. Як згадувалося в попередніх розділах, тунельний режим захищає будь-яку

внутрішню маршрутизацію інформації шляхом шифрування IP-заголовка всього пакета, а потім інкапсуляція нового заголовка IP у вихідний заголовок. Накладні витрати через шифрування значно знижують пропускну здатність мережі міра.

За оцінкою, AES128-MD5 демонструє чудову продуктивність з точки зору пропускної здатності. Причина в тому, що, порівняно з іншим алгоритмом хешування, виробляє SHA256, MD5 128-розрядний вихід, а SHA256 видає 256-бітний вихід, що додатково приносить додатковий накладні витрати, що призводять до погіршення продуктивності. Також MD5 вважається менш ЦП інтенсивний у порівнянні з сімейством SHA. Хоча SHA вважається більшим безпечний, MD5 працює швидше, а отже, і його продуктивність.

У порівнянні з іншим алгоритмів шифрування, 3DES спочатку був розроблений для апаратних моделей і, отже, його низька ефективність у програмних реалізаціях, де AES була розроблена як для програмного забезпечення і апаратних реалізацій, а отже, і його чудову продуктивність. У порівнянні з AES128 і AES256, залежно від довжини криптографічного ключа, чим довший накладні вводить.

Кілька недоліків функціональності 3DES полягають у використанні слабкіших і коротші ключі в порівнянні з AES, використовувані повторювані ключі шифрування та довший час тривалість порівняно з AES. Всі ці фактори підвищують ефективність роботи AES128-MD5. Тому AES128-MD5 працює найкраще, за ним слідують AES256-MD5 і AES128-SHA256.

Оскільки робота з VPN вводить додаткові заголовки IP і складну обробку криптографічних операцій, досліджено накладні витрати, що виникають при передачі даних.

Вимірювання пропускної спроможності каналу дає детальну інформацію про продуктивність мережі, яка може бути додатковою вивчається та аналізується з кількістю втрачених пакетів під час передачі та із затримкою зіткнувся. Пропускна здатність мережі визначається як швидкість, з якою дані передаються через а канал зв’язку.

На додаток до надання безпечних даних через виділені посилання, надійність встановленого каналу зв’язку також не менш важливий для моделювання прямого підключення. Надійність мережі значною мірою залежить від пропускної здатності даних в підключення. Таким чином, щоб забезпечити безпечну та надійну передачу даних, пропускна здатність приймається як єдине ціле для важливих параметричних аналізів. Jitter визначається як зміна часу між надходженням пакетів до місця призначення. Хороша мережа передачі записує значення тремтіння від 1 до 5 мілісекунд. Низьке тремтіння значення допомагають підтримувати міжпакетну затримку, внесену джерелом, тобто надзвичайно важливий при роботі з пакетами невеликого розміру.

Втрата пакетів має місце, коли пакети, що рухаються через канал, не досягають їх мережу призначення. Щоб забезпечити хорошу якість зв’язку, втрата пакетів у мережі підтримується нижче 1% у цьому дослідженні. Чим вище втрата пакетів в мережі, тим більше буде втрата пакетів Повторні передачі сегментів TCP, що в кінцевому підсумку впливають на доступну пропускну здатність мережі. Показники розподілу ресурсів ВМ, що включають час запуску ВМ, час запуску служби ВМ і VM Failure Ratio вимірюються та оцінюються для визначення надійності та швидкості управління оркеструванням.

В порівнянні з звичайними локальними мережами, VPN-мережі мають ряд основних переваг, до яких можна віднести:

Безпека – це один із головних факторів та аспектів роботи VPN-сервісів. Адже навіть якщо третя особа має змогу втрутитися в роботу VPN мережу та прослуховувати трафік, що передається по ній. Без змоги його розшифрувати вся отримана інформація буде набором незрозумілих даних. Без знання ключа, це зробити не має можливості, а на підбір ключа може піти не одна тисяча років, ці фактори можуть залежати від виду шифру, довжини ключа.

Економність – при використанні VPN-мереж на підприємстві є можливість частково обмежити кількість проміжного обладнання (маршрутизаторів, свічів, серверів доступу, тощо), та розхідних матеріалів (кабелів, ліній зв’язку та інших технічних засобів), а головне суттєво зменшити витрати фізичне на обладнання та

його обслуговування. Але при цьому не жертвуючи жодним із аспектів безпеки, навіть якщо користувач має змогу з’єднатися з мережею з будь якої точки земної кулі маючи лише дані для підключення та налаштований клієнт для встановлення зв’язку з мережею через приватний VPN-канал.

Підхід використання саме VPN-мереж є доцільним в наш час, адже кожний вповноважений користувач моє змогу за допомогою мережі Інтернет отримати доступ до потрібних даних, мережевих ресурсів. Це робить використання подібної технології конкурентно спроможним та актуальним в наш час [20].

Тому як подібні властивості важко досягти при використанні звичайних, традиційних приватних мереж, тому як підприємства, які бажають та мають змогу використовувати мережеву ресурси, та мати до них доступ, інколи можуть мати не сумісні мережі, що суттєво ускладнює процес налаштування мережі такого типу. Особливо гостро це питання може виникати коли велика кількість організацій, бажають працювати разом через одну мережу.

Висновки до розділу 2

Досліджено методи використання віртуальних захищених тунелів VPN в стримінгових технологіях в корпоративних мережах мається висновок, що використанням, на прикладі різних реалізацій VPN тунелей і сервісів, допомагає налаштовувати корпоративні мережі більш безпечно.

Проаналізовано дати та детальний аналіз різних конструкцій із зазначенням плюсів і мінусів кожного, щоб визначити найбільш підходящий. Порівняльний аналіз за різними режимами також досліджено експлуатацію, включаючи тунельний і транспортний вид, з зазначенням кожного з них переваги та недоліки для кращої ефективності та придатності.

Виокремлено, що для подолання безпеки та продуктивності необхідні захищені стійкі сеанси. проблеми, пов’язані з перебоями з’єднання.

Зазначено чотири мобільні VPN-рішення з відкритим вихідним кодом надали детальний технічний аналіз ysis цих систем і порівняли їх з точки зору функціональності та продуктивність.

Отримано результат, що MUSeS є конкурентоспроможним рішенням для надання безпечний і мобільний зв'язок.

3 ДОСЛІДЖЕННЯ ЗАХИЩЕНИХ ТУНЕЛЕЙ VPN ДЛЯ ОРГАНІЗАЦІЇ СТРИМІНГОВИХ ТЕХНОЛОГІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1. Побудова захищеної корпоративної мережі на основі технологій VPN

В даній роботі використано схему з наявністю трьох маршрутизаторів Cisco 1841. Cisco 1841 – це маршрутизатори які орієнтовані на малі та великі підприємства. Простота та легке налаштування зробили дані моделі популярним рішенням для реалізації підключення до корпоративних мереж та Інтернету.

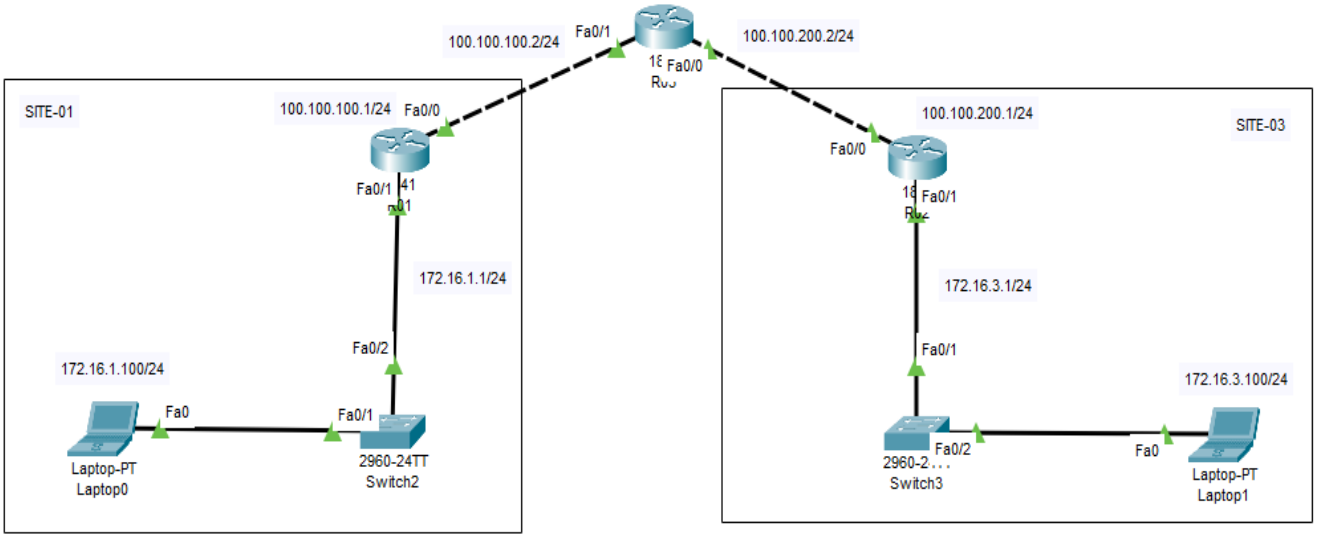

Рис.3.1. Модель організації віртуальних захищених тунелей VPN

В даній роботі було змодельовано спосіб інкапсуляції пакетів у транспортному протоколі. Тунелювання реалізовано як віртуальний інтерфейс Cisco Packet Tracer для забезпечення найбільш простішого інтерфейсу для налаштування. Тунельний інтерфейс не прив’язаний до конкретних протоколів, а скоріше є архітектурою, розробленою для надання послуг, необхідних для реалізації схеми інкапсуляції «точка-точка». Оскільки тунелі являються зв’язками «точка-точка», треба налаштувати окремий тунель для кожного посилання.

Три основні компоненти тунелювання:

• Пасажирський протокол, який є протоколом, який ви інкапсулюєте (AppleTalk, Banyan VINES, IP або обмін пакетами в мережі).

• Протокол перевізника, такий як протокол інкапсуляції загальної маршрутизації або протокол IPSec.

• Транспортний протокол, такий як IP, який є протоколом, який використовується для передачі інкапсульованого протоколу.

GRE здатний обробляти транспортування багатопротокольного та багатоадресного IP-трафіку між двома сайтами, які мають лише одноадресне підключення IP. Важливість використання тунелів у середовищі VPN заснована на тому факті, що шифрування IPSec працює лише для одноадресних кадрів IP. Тунелювання дозволяє шифрувати і передавати багатопротокольний трафік через VPN, оскільки тунельні пакети відображаються в IP-мережі як одноадресний IP-кадр між кінцевими точками тунелю.

Якщо всі підключення повинні проходити через маршрутизатор Cisco серії 1841, тунелі також дозволяють використовувати приватну мережеву адресацію через магістраль постачальника послуг без необхідності запускати функцію трансляції мережевих адрес (NAT).

Надлишковість мережі є важливим фактором при прийнятті рішення про використання тунелів GRE, IPSec або тунелів, які використовують IPSec замість GRE. GRE можна використовувати разом з IPSec для передачі оновлень маршрутизації між сайтами на IPSec VPN.

GRE інкапсулює пакет із відкритим текстом, потім IPSec (у транспортному або тунельному режимі) шифрує пакет. Цей потік пакетів IPSec через GRE дозволяє передавати оновлення маршрутизації, які зазвичай є багатоадресними, передавати через зашифроване посилання. IPSec сам по собі не може цього досягти, оскільки він не підтримує багатоадресну передачу.

Використовуючи резервні тунелі GRE, захищені IPSec, від віддаленого маршрутизатора до резервних маршрутизаторів штаб-квартири, протоколи маршрутизації можна використовувати для розмежування «основних» і «вторинних» центральних маршрутизаторів. Після втрати з’єднання з основним

маршрутизатором протоколи маршрутизації виявлять збій і маршрутизують до вторинного маршрутизатора серії Cisco 1841, забезпечуючи таким чином резервування мережі [21].

Важливо відзначити, що для забезпечення стійкості в штаб-квартирі необхідно використовувати більше одного маршрутизатора. Для стійкості VPN на віддаленому сайті має бути налаштовано два тунелі GRE, один до основного маршрутизатора HQ VPN, а інший до резервного маршрутизатора HQ VPN.

IPSec треба налаштувати в певному порядку: транспортному або тунельному режимі. Тунельний режим IPSec використовується як альтернатива тунелю GRE або в поєднанні з тунелем GRE. Але в тунельному режимі IPSec всі вихідні IP-датаграми шифруються. У цьому режимі мережевий пристрій, наприклад маршрутизатор, може діяти як проксі-сервер IPSec. Це може означати тільки одне - шифрування маршрутизатора від імені хостів.

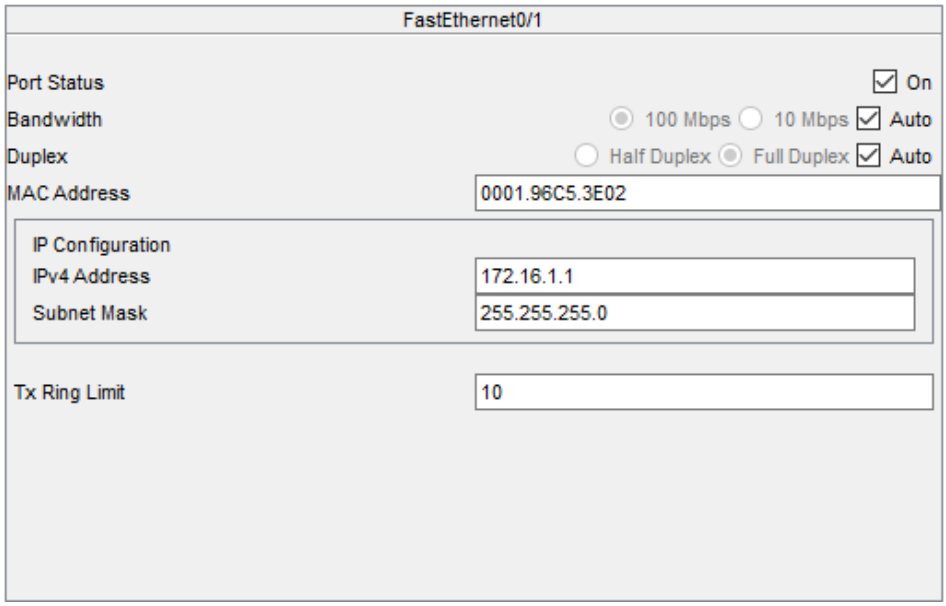

Рис.3.2. Налаштування маршрутизатора Cisco 1841 R01

Маршрутизатор джерела робить шифрування пакетів і пересилає їх через тунель IPSec. Маршрутизатор призначення розшифровує вихідну IP-датаграму і пересилає її цільовій системі. Тунельний режим захищає від аналізу трафіку; у тунельному режимі зловмисник може ідентифікувати лише кінцеві точки

конкретного тунелю, а не справжнє джерело та призначення пакетів, що проходять через цей тунель, якщо навіть відбувається збіг з кінцевими точками тунелю [22].

У транспортному режимі IPSec шифрується тільки корисне навантаження IP, а вихідні IP пакети залишаються недоторканими. Пріоритет цього режиму в тому, що до кожного пакету додається лише кілька байтів.

Це також дозволяє пристроям у загальнодоступній мережі бачити кінцеве джерело та призначення пакету. За допомогою цієї можливості можна ввімкнути спеціальну обробку в проміжній мережі на основі інформації в заголовку IP. Тому заголовок рівня 4 буде зашифрований, що обмежує перевірку пакета. На жаль, передаючи IP-заголовок у чистому режимі транспортування, зловмисник може виконати деякий аналіз трафіку.

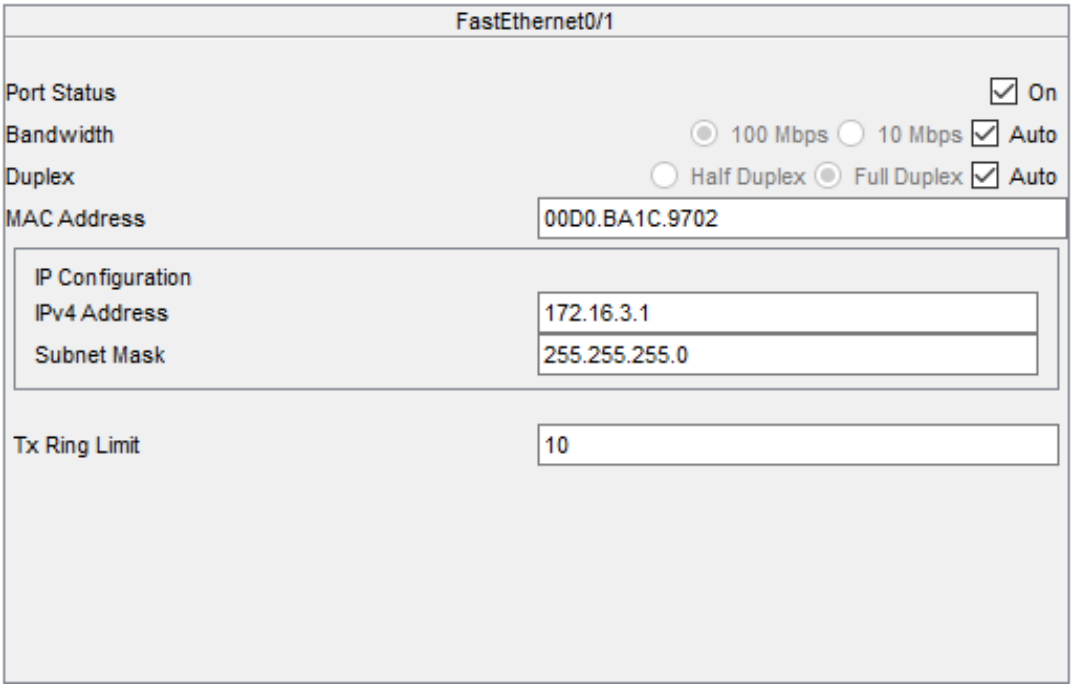

Рис.3.3. Налаштування маршрутизатора Cisco 1841 R03

3.2. Методи та дослідження реалізації захищеної стримінгової технології в корпоративній мережі

Етап 1

1) Для цієї топології використовується маршрутизатори 1841 Cisco та ПК Laptop-PT.

Таблиця 3.1.

Топологія пристроїв Cisco Packet Tracer

Пристрій	Інтерфейс	IP-адрес	Маска підмережі
R01	Fa0/1	172.16.1.1	255.255.255.0
	Fa0/0	100.100.100.1	255.255.255.0
R02	Fa0/1	100.100.200.2	255.255.255.0
	Fa0/0	100.100.100.2	255.255.255.0
R03	Fa0/1	172.16.3.1	255.255.255.0
	Fa0/0	100.100.200.1	255.255.255.0
Laptop0	Fa0/0	172.16.1.100	255.255.255.0
Laptop1	Fa0/0	172.16.3.100	255.255.255.0

2) З'єднання пристроїв методом прямого кабельного з'єднання і налаштування початкової конфігурації маршрутизатора. Налаштування IP-адреси інтерфейсу на маршрутизаторах і маршрут за замовчуванням на R01 і R03, вказує на маршрутизатор R02. Маршрутизатор R02 діє як інтернет-провайдер і не розпізнає інших мереж, крім безпосередньо підключеної мережі (Додаток 1).

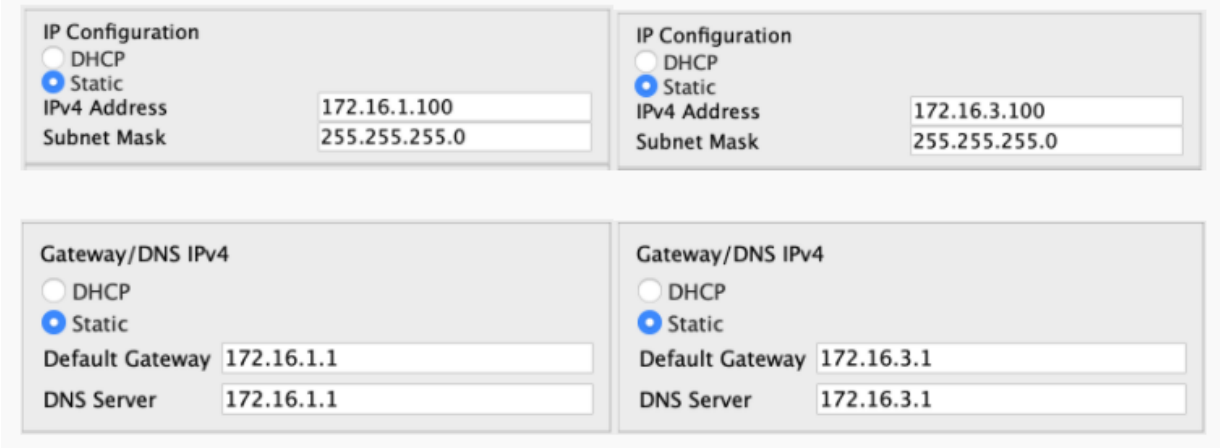

Рис. 3.4. Налаштування IP-адрес для Laptop0 та Laptop1

На ноутбуках налаштовано статичні IP-адреси. Laptop0 повинен мати IP 172.16.1.100/24. Laptop1 повинен мати 172.16.3.100/24. Протестовано пінг з Laptop0

на Laptop1. Це призведе до збою в пересиланні пакетів, оскільки R02 не знає, як маршрутизувати цей трафік.

3) Активація ліцензування на граничних маршрутизаторах, а також активація безпеки на R01 і R03 здійснюється шляхом прописування та конфігурування обладнання (Додаток 1).

Етап 2: 1) Для появи тунелю IPSec, конфігурація на обох кінцях має відповідати (фаза 1 і фаза 2 повинні бути успішними). Тунель буде сформований між R01 і R03.

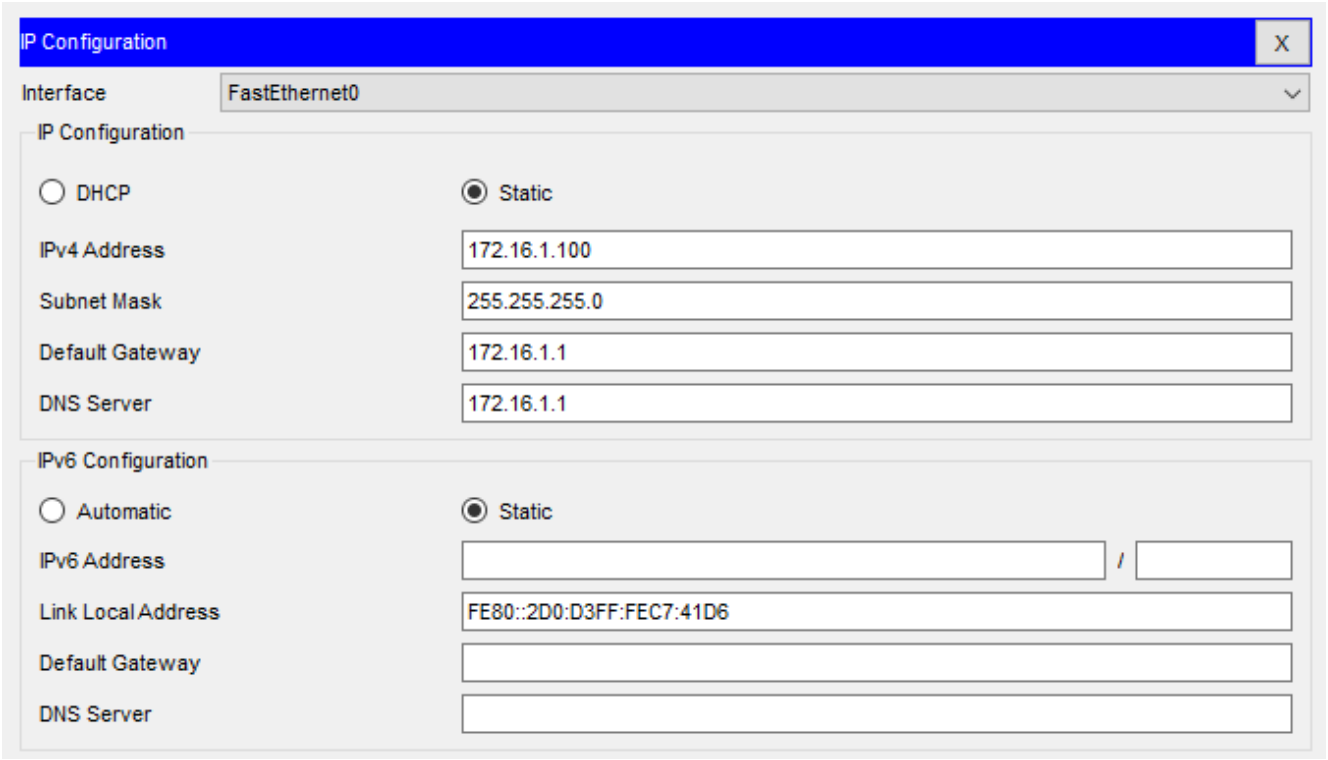

Рис. 3.5. Налаштування IP-адреси Laptop0

2) Фаза налаштування 1 тунелю IPSec. У цій частині визначається політика ISAKMP і вказується інформація щодо використання спільного ключа (Додаток 1).

3) Фаза налаштування 2 тунелю IPSec. На цьому етапі відбувається побудова комунікації IKE. Використовується 256-бітове шифрування AES з кодом аутентифікації хеш-повідомлення (Додаток 1).

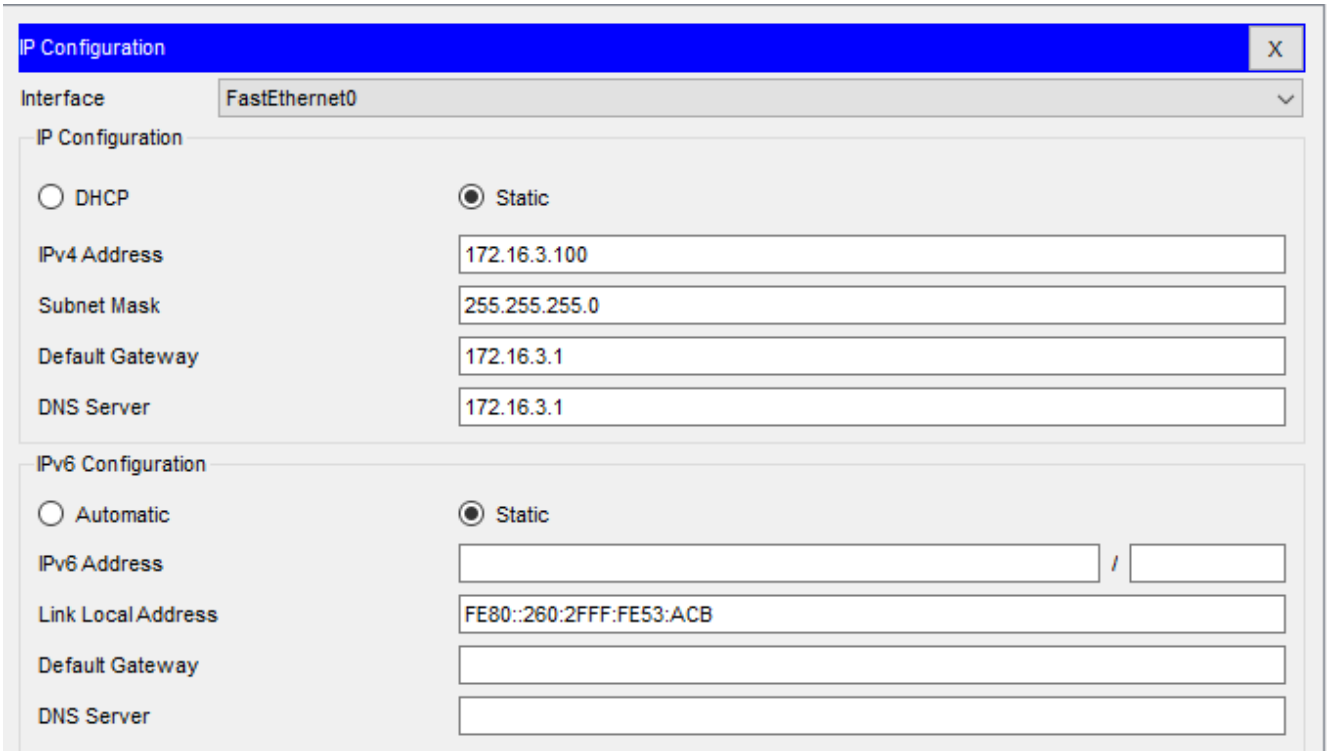

Рис.3.6. Налаштування IP-адреси Laptop1

4) Об’єднання фаз налаштування. Для того щоб отримати позитивний результат, потрібно зв’язати Фазу 1 і Фазу 2 разом, визначивши криптокарту (Додаток А).

5) Активація IPSec на вихідному інтерфейсі. Здійснюється шляхом застосування криптокарти до інтерфейсу (Додаток А).

6) Пінг через тунель. Щоб тунель повернувся також потрібно почати пінг через тунель, тому пінг зроблено з Laptop0 на Laptop1. Спершу пінги можуть бути невдалими але якщо вся конфігурація вірна, пінги мають бути успішними після кількох спроб (Додаток А).

7) Тестування алгоритму дій. Тестуючи правильність послідовності дій отримується результат - тунель активовано та протестовано (Додаток А).

Висновки до розділу 3

Досліджено використання схеми з наявністю трьох маршрутизаторів Cisco 1841 та було змодельовано спосіб інкапсуляції пакетів в транспортному протоколі.

Тунелювання реалізовано як віртуальний інтерфейс Cisco Packet Tracer для забезпечення найбільш простішого інтерфейсу для налаштування.

Проаналізовано, що тунельний інтерфейс не прив’язаний до конкретних протоколів, а скоріше є архітектурою, розробленою для надання послуг, необхідних для реалізації схеми інкапсуляції «точка-точка».

Виокремлено захищені тунелі VPN, було отримано змодельовану схему організації стримінгових технологій в корпоративних мережах та впроваджено політику безпеки щодо захисту каналів стримінгової платформи. Результатом отримано модель топології в Cisco Packet Tracer і наглядно було продемонстровано з’єднання фаз та захищеність тунелів VPN.

Зазначено, що маршрутизатор джерела робить шифрування пакетів і пересилає їх через тунель IPSec, та враховуючи, що у транспортному режимі IPSec шифрується тільки корисне навантаження IP, а вихідні IP пакети залишаються недоторканими. Пріоритет цього режиму в тому, що до кожного пакету додається лише кілька байтів.

Отримано результат, що передаючи IP-заголовок у чистому режимі транспортування, зловмисник може виконати деякий аналіз трафіку.

ВИСНОВКИ

В даній магістерській роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено загальні положення та структури використання віртуальних захищених тунелей VPN, методи використання віртуальних захищених тунелів VPN в стримінгових технологіях в корпоративних мережах мається висновок, що використанням, на прикладі різних реалізацій VPN тунелей і сервісів, допомагає налаштовувати корпоративні мережі більш безпечно та зроблено аналіз переваг і недоліків протоколів VPN. Використання схеми з наявністю трьох маршрутизаторів Cisco 1841 та було змодельовано спосіб інкапсуляції пакетів в транспортному протоколі. Тунелювання реалізовано як віртуальний інтерфейс Cisco Packet Tracer для забезпечення найбільш простішого інтерфейсу для налаштування.

2. Проаналізовано статистичні дані по технологіям VPN, а саме: ринок послуги Ethernet та IP, розмір світового ринку VPN, країни найбільшого використання VPN, статистичні дані використання VPN сервісів. Проблеми забезпечення кібербезпеки корпоративної інформації та існуючі технології управління захисту стримінгових технологій в корпоративній мережі за допомогою захищених тунелей VPN. Порівняльний аналіз за різними режимами також досліджено експлуатацію, включаючи тунельний і транспортний вид, з зазначенням кожного з них переваги та недоліки для кращої ефективності та придатності.

3. Виокремлено інформацію з законодавчої бази захисту персональних даних, а також структуру на основі Cisco Packet Tracer та створено тунель GRE захищений від прослуховування в мережі Інтернет. Для подолання безпеки та продуктивності необхідні захищені стійкі сеанси. Захищені тунелі VPN, було отримано змодельовану схему організації стримінгових технологій в корпоративних мережах та впроваджено політику безпеки щодо захисту каналів

стримінгової платформи. Результатом отримано модель топології в Cisco Packet Tracer і наглядно було продемонстровано з’єднання фаз та захищеність тунелів VPN.

4. Зазначено мережевий захист тунелів VPN та критерії безпеки даних, а саме: конфіденційність, цілісність і доступність інформації. Чотири мобільні VPN-рішення з відкритим вихідним кодом надали детальний технічний аналіз усіх цих систем і порівняли їх з точки зору функціональності та продуктивність. Маршрутизатор джерела робить шифрування пакетів і пересилає їх через тунель IPSec, та враховуючи, що у транспортному режимі IPSec шифрується тільки корисне навантаження IP, а вихідні IP пакети залишаються недоторканими. Пріоритет цього режиму в тому, що до кожного пакету додається лише кілька байтів.

5. Отримані результати можуть бути використані фахівцями з інформаційної безпеки підприємств для правильного використання віртуальних захищених тунелей VPN, який має забезпечити додатковий рівень захищеності стримінгових тунелей в корпоративних мережах, а також надасть більшої мережевої безпеки для взаємодії користувачів.