Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Технологія побудови захищених комутованих мереж Ethernet

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220179.22.01.20 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Галузинський В.В.
Підпис

Керівник проф., д.т.н, доцент _____ Касянчук М.М.
Підпис

Нормоконтролер старший викладач _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц _____ Кльоц Ю.П.
Підпис

18 грудня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма КІБЕРБЕЗПЕКА

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Галузинському Валерію Валерійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Технологія побудови захищених комутованих мереж Ethernet

Керівник роботи Касянчук Михайло Миколайович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Дослідження стану захисту в сучасних розподілених комутованих мережах Ethernet, визначення та моделювання структури та вразливостей. Формування технології побудови захищених комутованих мереж з віддаленим доступом

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Визначити основні поняття, проаналізувати сучасні методи та засоби побудови комутованих мереж. Дослідити питання захисту в таких мережах. Змоделювати захищену комутовану мережу. Розробити технологію побудови захищених комутованих мереж. Висновки.

5. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

6. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – визначення основних понять, аналіз сучасних методів та засобів забезпечення інформаційної безпеки; постановка задачі	18.09.2023	
4	Робота над розділом 2 – Моделювання необхідних для виконання задачі структур, процесів та забезпечення.	02.10.2023	
5	Робота над розділом 3 – розробка моделей, алгоритмів та методів.	16.10.2023	
6	Робота над розділом 4 – застосування запропонованих рішень.	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент  В.В. Галузинський

Підпис Ініціали, прізвище

Керівник проекту (роботи)  М.М. Касянчук

Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Технологія побудови захищених комутованих мереж Ethernet

Автор роботи: Галузинський Валерій Валерійович

Керівник роботи: д.т.н., професор Касянчук Михайло Миколайович

Загальний обсяг роботи: 93 сторінки, 52 рисунка, 4 таблиці, 2 додатки, 45 посилань.

Ключові слова: комутовані мережі, захищеність мереж, VPN.

Порушення мережної безпеки можуть зупиняти роботу служб електронної комерції, спричиняти втрату бізнес-даних, ставити під загрозу приватність осіб і порушувати цілісність інформації. Ці порушення можуть призвести до втрати корпораціями своїх доходів, крадіжки інтелектуальної власності, судових позовів, ба більше, загрожувати суспільній безпеці.

В роботі розглянуто сучасні підходи до побудови захищених комутованих мереж Ethernet. Визначено основні поняття, методи та засоби для побудови відповідних рішень. Розроблено технологію , що дозволяє проектувати та будувати розподілені мережі із відповідним рівнем захисту.

19.12.2023

ANNOTATION

Theme of qualification work: Technology of building protected switched Ethernet networks

Author of the work: Galuzynskyi Valeriy Valeriyovych

Supervisor: Doctor of Sciences, Professor Kasyanchuk Mykhailo Mykolayovych

Total volume of work: 93 pages, 52 figures, 4 tables, 2 appendices, 45 references.

Keywords: switched networks, network security, VPN.

Network security breaches can disrupt e-commerce services, cause loss of business data, compromise individual privacy and compromise information integrity. These breaches can result in corporations losing revenue, intellectual property theft, lawsuits, and even more, endangering public safety.

The work considers modern approaches to the construction of protected switched Ethernet networks. The main concepts, methods and tools for building appropriate solutions are defined. A technology has been developed that allows designing and building distributed networks with an appropriate level of protection.

19.12.2023

ЗМІСТ

ВСТУП

Наш цифровий світ постійно змінюється. Можливість доступу до Інтернету та корпоративної мережі більше не обмежується фізичним офісом, географічним розташуванням чи часовим поясом. Сучасне глобалізоване робоче місце дозволяє співробітнику отримати доступ до ресурсів чи інформації з будь-якої точки світу в будь-який час і з будь-якого пристрою. Такі вимоги призводять до необхідності створення мереж наступного покоління, які є безпечними, надійними та високодоступними.

Такі новітні мережі повинні не тільки забезпечувати підтримку поточних вимог та обладнання, а й мати можливість інтегрувати застарілі платформи. Підприємства все частіше покладаються на свою мережну інфраструктуру при наданні критично важливих послуг. Ріст і розвиток підприємств зумовлюють збільшення кількості співробітників, відкриття філій та вихід на глобальні ринки. Ці зміни безпосередньо впливають на вимоги до мережі, яка повинна мати можливість масштабування, щоб задовольняти потреби бізнесу.

Мережа повинна підтримувати обмін різними типами мережного трафіку (конвергентна мережа), зокрема файлами даних, електронною поштою, IP-телефонією та відеозастосунками для кількох підрозділів компанії. Всі корпоративні мережі повинні мати можливість:

- Підтримки критично важливих програм.
- Підтримки конвергентного мережного трафіку.
- Підтримки різноманітних потреб бізнесу.
- Забезпечення централізованого адміністративного контролю.

Локальна мережа - це мережна інфраструктура, яка забезпечує для кінцевих користувачів та пристроїв доступ до мережних служб і ресурсів. Кінцеві споживачі та пристрої можуть бути розміщені на одному поверсі або в одній будівлі. Мережа кампусу створюється шляхом об'єднання групи локальних мереж, які займають

невелику географічну територію. Проекти мереж кампусів включають від невеликих мереж з одним комутатором аж до дуже великих мереж з тисячами з'єднань.

Враховуючи зростаючі вимоги до конвергентних мереж, мережу слід розробляти з використанням архітектурного підходу, що вбудовує інтелект, спрощує операції та є масштабованим для задоволення майбутніх потреб.

Мета дослідження. Підвищення безпеки інформаційних потоків в комутованих мережах за рахунок використання захищених каналів

Об'єкт дослідження. Інформаційна безпека та захист даних комутованих мереж.

Предмет дослідження. Технологія побудови захищених комутованих мереж.

Для досягнення мети дослідження необхідно вирішити наступні завдання:

1. Провести аналіз стану безпеки при організації комутованих мереж.

2. Дослідити структурні елементи захищених комутованих розподілених мереж.

3. Розробити модель комутованої розподіленої мережі із впровадженням елементів захисту.

4. Розробити технологію побудови захищених комутованих мереж із відповідними результатами.

Методи дослідження. В дослідженні було використано такі методи дослідження, як аналіз, синтез, математичне моделювання.

Наукова новизна отриманих результатів:

1. Побудована модель комутованої розподіленої мережі із впровадженням елементів захисту

2. Розроблено технологію побудови захищених комутованих мереж, що враховує наявну інфраструктуру та дозволяє впровадити захист передачі даних.

Практична цінність одержаних результатів. Отримані результати дозволяють ефективно реалізувати технологію побудови захищених комутованих мереж.

Перелік публікацій. За темою магістерської роботи опубліковано...

1 ВИЗНАЧЕННЯ ОСНОВНИХ ПОНЯТЬ, АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМУТОВАНИХ МЕРЕЖ

1.1. Основні визначення та поняття мереж VPN

Останнім часом термін VPN з'явився в кожній розмові про захист даних в Інтернеті. І з якоїсь причини. Не так давно технологія VPN була високотехнологічним нововведенням, але сьогодні це необхідний інструмент для безпеки всіх організацій та користувачів, які хочуть приховати свої дані серед інших даних користувачів. Насправді технологія VPN захищає конфіденційність даних у вашій мережі.

Рисунок 1.1 – Загальна структура мережі VPN

Віртуальні приватні мережі (VPN) створюють захищені зашифровані з'єднання в менш захищених мережах, таких як загальнодоступний Інтернет. Просто-VPN використовують тунельні протоколи для шифрування даних в кінці передачі та дешифрування в кінці прийому. Вихідні та вхідні мережеві адреси також зашифровані для забезпечення додаткової безпеки.

Технологія VPN може шифрувати всі дії користувачів або співробітників організації в Інтернеті. Усі дані, які користувач надсилає та отримує. Якщо користувач входить в мережу тільки через VPN, зловмисник не розуміє адресу, за

якою користувач підключається до ресурсу, і бачить тільки 1 з багатьох VPN-маршрутизаторів.

VPN використовуються для надання віддаленим корпоративним працівникам, гігантським корпоративним працівникам та діловим мандрівникам доступу до ресурсів, розміщених у їхній мережі. Щоб отримати доступ до обмежених ресурсів через VPN, користувачеві слід дозволити використовувати додаток VPN та надати 1 або більше елементів автентифікації, таких як пароль, маркер безпеки або біометричні дані.

В даний час використання віддаленого доступу через VPN все частіше використовується в географічно розподілених ресурсах. Ця тема також важлива у відділі автоматизації бізнес-процесів.

Комп'ютерна мережа вимагає сервера VPN, який дозволяє користувачам використовувати всі ресурси приватної захищеної мережі через загальнодоступну мережу. Ви можете використовувати сервер VPN для підвищення безпеки передачі даних через внутрішню мережу та зменшення ймовірності витоку або крадіжки інформації, що передається через Інтернет.

Глобальні тенденції показують, що з моменту появи цієї технології кількість окремих користувачів, що використовують її, зростала високими темпами. У сучасних малих та великих підприємствах VPN є основою всіх комунікацій та збору даних.

Віртуальна приватна мережа-це метод розширення приватної мережі за допомогою загальнодоступної мережі, такої як Інтернет. Назва просто вказує на те, що це віртуальна "приватна мережа". Це означає, що користувач може бути частиною локальної мережі у віддаленому місці. Використовуйте протокол тунелювання для встановлення безпечного з'єднання.

Рисунок 1.2 – Статистика розгортання та використання VPN мереж

І чим більше мережевий відділ компанії, тим більше можливостей у хакерів перехопити незахищену інформацію, тим вище безпека каналів компанії.

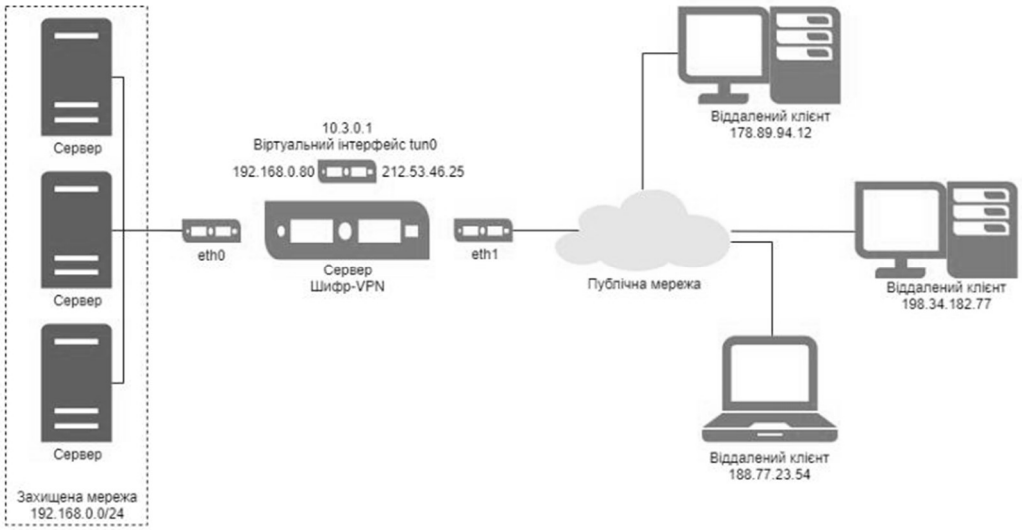

Рисунок 1.3 – Типова архітектура комутованої мережі з VPN

Будь-яка організація неминуче стикається з проблемою передачі інформації між офісами, а також з проблемою захисту цієї інформації. Не кожна організація

може мати свій власний канал доступу. Цю проблему можна вирішити за допомогою технології VPN, залежно від того, чи всі відділи та офіси підключені один до одного. Це також забезпечує гнучкість і високий рівень мережевої безпеки, що забезпечує значну економію коштів при створенні цих мереж.

Віртуальна приватна мережа (VPN - віртуальна приватна мережа) створюється на основі загальнодоступної мережі Інтернет. І якщо в інтернет-комунікаціях є недоліки, головне, щоб вони були схильні до потенційних порушень безпеки та конфіденційності. VPN може гарантувати, що трафік, що надсилається через Інтернет, захищений та передається через локальну мережу. У той же час віртуальні мережі забезпечують значну економію коштів у порівнянні з обслуговуванням власної глобальної мережі.

Однією з найважливіших задач технології VPN є захист потоку корпоративних даних, що передаються по відкритій мережі. Відкриті канали можуть бути надійно захищені тільки методами шифрування.

Так звана виділена лінія не має особливих переваг у порівнянні з загальнодоступною лінією з точки зору інформаційної безпеки. Орендовані лінії можуть бути прокладені в районах, які принаймні частково неконтрольовані і можуть бути пошкоджені або неправильно підключені. Єдина реальна перевага полягає в тому, що гарантується висока пропускна здатність орендованої лінії, а не підвищена безпека.

Принцип роботи VPN узгоджується з основними мережевими протоколами і технологіями. Наприклад, коли встановлено з'єднання віддаленого доступу, клієнт надсилає стандартний потік даних протоколу PPP на сервер. Для віртуальних орендованих ліній між локальними мережами маршрутизатори надсилають пакети PPP. Але принципово новий момент полягає в тому, що дані передаються по захищеному (зашифрованому) тунелю, організованому в загальнодоступній мережі.

Тунелювання дозволяє організувати передачу пакетів протоколу 1 в логічному середовищі з використанням іншого протоколу. В результаті стає можливим розв'язати проблему взаємодії між декількома різними типами мереж,

починаючи з необхідності забезпечення цілісності та конфіденційності переданих даних і закінчуючи подоланням невідповідностей у зовнішніх протоколах або схемах адресації.

Існуючу мережеву інфраструктуру вашої компанії можна підготувати до використання VPN, використовуючи різні варіанти, такі як програмні рішення. Організацію віртуальної приватної мережі можна порівняти з прокладанням кабелю по глобальній мережі.

Найпоширенішим способом створення тунелю VPN є інкапсуляція протоколу IP-мережі в PPP, а потім інкапсуляція згенерованих пакетів у протокол тунелювання. Це називається тунелюванням рівня 2, оскільки 2 це протокол рівня.

Основні функції корпоративної мережі - глобальність і масштабованість підключення - являють собою високий ризик для виконання функціональних завдань. Протокол сімейства TCP / IP був розроблений давно, коли проблеми безпеки були не такі серйозні, як зараз, тому він в основному функціональний і може бути легко переналаштований.

З різким збільшенням кількості домовласників, підключених до Інтернету, і збільшенням кількості великих і малих підприємств, які використовують Інтернет-технології для здійснення своєї діяльності, кількість інцидентів, пов'язаних з інформаційним втручанням, значно збільшилася.

В даний час відомо багато різних загроз різного походження, які приховують різні небезпеки для інформації.

Навмисне походження загрози пов'язане зі зловмисними діями людей, що вживаються для реалізації численних типів загроз. Визначено 2 види загроз: об'єктивна (кількісна або якісна недостатність елемента системи) і суб'єктивна (діяльність іноземних спецслужб, промислове шпигунство, діяльність кримінальних елементів, зловмисні дії недобросовісних співробітників системи).

Причиною загрози можуть бути зловмисники, технічні об'єкти, програми та алгоритми, технічні схеми обробки даних і зовнішнє середовище. Основними причинами витоку інформації є:

– Відповідальна особа не дотримується стандартів безпеки, вимог і правил роботи системи інформаційної безпеки.;

– Є помилка в конструкції захисту системи;

– Проведення технічної розвідки зловмисними сторонами;

Недотримання персоналом стандартів, вимог та експлуатаційних правил може бути навмисним або ненавмисним. Що відрізняє цей інцидент від розвідувальних дій недобросовісних сторін, так це те, що в цьому випадку особа, яка вчинила протиправну дію, керується особистими мотивами. Враховуються 3 типи витоків інформації:

– Розкриття інформації;

– Несанкціонований доступ до даних;

– Отримання інформації, захищеної спецслужбами спецслужб;

Розкриття інформації означає несанкціоновану передачу захищеної інформації споживачам, які не мають права на доступ до захищених даних, а несанкціонований доступ означає Отримання захищеної інформації зацікавленими сторонами в порушення прав або правил доступу до захищених даних, встановлених юридичними документами або власником інформації. При цьому зацікавленими сторонами, які здійснюють несанкціонований доступ до інформації, можуть бути держави, юридичні особи, групи фізичних осіб (у тому числі державні установи), фізичні особи (хакери).

Отримання інформації, захищеної розвідувальною службою, може здійснюватися з використанням технічних засобів (Технічна розвідка) або алгоритмів-посередників (агентурна розвідка).

Канал витоку інформації-це джерело витоку інформації, матеріальний носій або розподільне середовище сигналу, що несе ідентифіковану інформацію, і однією з основних характеристик каналу засобів вилучення інформації з сигналу або носія є розташування засобів вилучення інформації з сигналу або носія. у контрольованій області, що охоплює або виходить за межі системи

Інформація повинна передаватися з пункту а в пункт Б таким чином, щоб зловмисник не міг до неї отримати доступ. Ситуація дуже реальна і часто трапляється на практиці, особливо останнім часом. Окремі вузли або цілі сегменти мережі можуть функціонувати як точки А і В. У разі передачі інформації між мережами приватний канал зв'язку, що належить компанії, може виступати в якості механізму захисту даних. Однак підтримка таких каналів зв'язку обходиться дуже дорого.

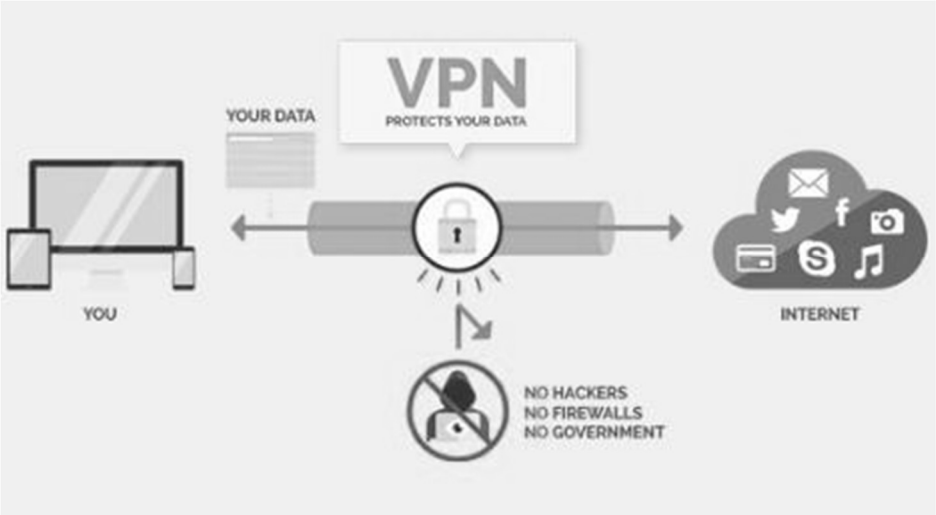

Рисунок 1.4 – Організація захищеного VPN каналу

Передача інформації через традиційні канали зв'язку (наприклад, через Інтернет) простіше і дешевше, але потреба інших компаній, що циркулюють в мережі, в передачі конфіденційних даних виникає тільки в глобальній мережі. Така потреба може виникнути в локальній мережі, де один тип трафіку повинен бути відокремлений від іншого (наприклад, трафік в білінговій системі повинен бути відокремлений від трафіку в системі інформаційних технологій).

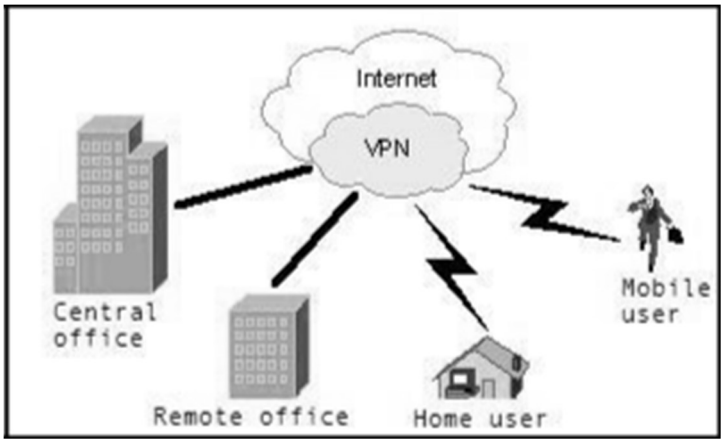

Рисунок 1.5 – Елементи мережі організації

Особливістю технології VPN є те, що організація віддаленого доступу здійснюється через Інтернет.Це набагато дешевше і краще. Вам знадобиться інтернет, ваша реальна IP-адреса та програмне забезпечення, щоб використовувати технологію VPN для організації віддаленого доступу до вашої приватної мережі. І з будь-якої точки світу, якщо ви знаєте дані автентифікації, ви можете увійти в захищену мережу.

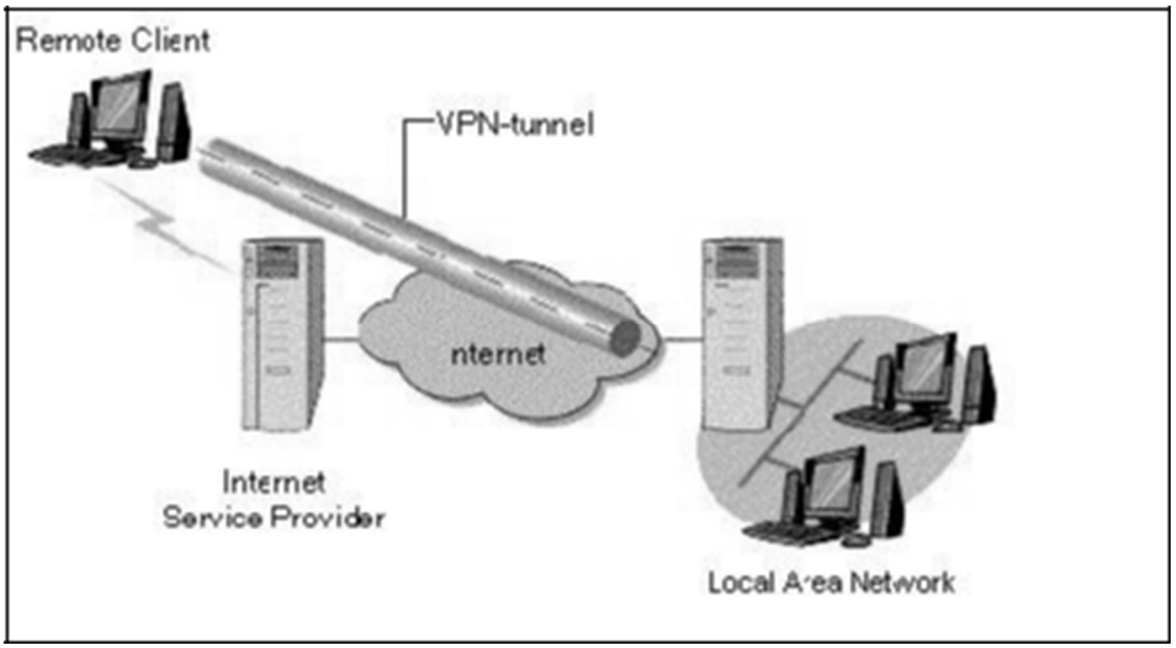

Рисунок 1.6 – Доступ віддаленого користувача до локальної мережі корпорації

Якщо вам потрібна велика кількість ресурсів, розподілених по багатьох мережах, і проблема полягає в конфіденційності переміщення інформації в цих мережах, VPN буде правильним вибором. У цьому перевага VPN - ви можете захистити всю мережу від зловмисників.

Якщо вам потрібен хост, який створює відчуття присутності в одній мережі, VPN - це спосіб реалізувати таке рішення. Ось чому багато людей стурбовані плутаниною щодо IP-адрес для клієнтів, яким потрібен легкий доступ до основних філій, або якщо компанія хоче забезпечити повний і безпечний доступ до своєї локальної мережі. Причини зміни інфраструктури при зміні постачальника? Якщо ви можете використовувати VPN, все, що вам потрібно, це конфігурація маршрутизатора.

Використання VPN є відносно недорогим способом фізичного підключення до віддаленої мережі. При цьому за підключення до глобальної мережі платити не потрібно, так як весь трафік між мережами передається через Інтернет.

1.2. Основні компоненти мережі VPN

VPN базується на 3 основних методах, які використовуються для забезпечення безпеки у вашій мережі:

1. Тунелювання
2. Аутентифікація
3. Шифрування

Тунелювання дозволяє передавати зашифровані дані між 2 точками, гарантуючи, що вся мережева система між цими точками буде прихована для відправника і одержувача даних.

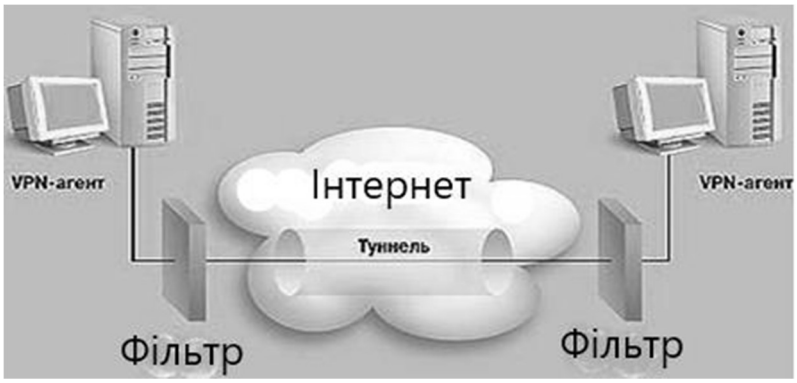

Рисунок 1.7 – Реалізація VPN на базі тунелю

Транспортне середовище тунелю приймає дані мережевого протоколу, що використовуються на вході в тунель, і доставляє їх на вихід без змін. Побудова тунелю достатня для підключення 2 мережевих вузлів, тому з точки зору програмного забезпечення, що працює на ньому, вони виглядали підключеними до однієї (локальної) мережі. Однак на практиці ми не повинні забувати, що "тунель", що містить дані, проходить через безліч проміжних маршрутизаторів відкритої глобальної мережі.

Ця ситуація створює 2 проблеми. По-перше, інформація, що передається через тунель, може бути перехоплена злочинцями.

За допомогою тунелювання пакети даних передаються через загальнодоступну мережу через традиційний двоточковий канал. Між кожною парою "відправник-одержувач даних" встановлюється своєрідний тунель, який є захищеним логічним з'єднанням, що дозволяє інкапсулювати дані з одного протоколу в пакети іншого дека. Основними компонентами тунелю є::

– Відправник (ініціатор з'єднання);
– Мережеві маршрутизатори;
– Тунельний перемикач;
– 1 або більше термінаторів тунелів.

Якщо це конфіденційно (номери банківських карт, фінансова звітність, особиста інформація), загроза компрометації цілком реальна, і це вже неприємно. Що ще гірше, зловмисник може змінити дані, надіслані через тунель, щоб

одержувач не міг перевірити їх справжність. Наслідки можуть бути жахливими. Враховуючи вищесказане, ми прийшли до висновку, що тунель в чистому вигляді підходить тільки для деяких типів мережевих комп'ютерних ігор, і не можна стверджувати, що до нього слід ставитися більш серйозно. Обидві проблеми вирішуються за допомогою сучасних засобів захисту для шифрування інформації. Метод електронного цифрового підпису (EDS) використовується для запобігання несанкціонованим змінам пакетів даних при їх проходженні через тунель. Суть методу полягає в тому, що кожному переданому пакету даних надається додатковий блок інформації, який генерується відповідно до алгоритму асиметричного шифрування і є унікальним для вмісту пакета і закритого ключа ОКТ відправника. Цей інформаційний блок є EDS пакета і дозволяє одержувачу аутентифікувати дані, знаючи відкритий ключ EDS відправника. Використовуйте надійні алгоритми шифрування для захисту даних, що передаються по тунелю, від несанкціонованого сканування.

Забезпечення безпеки є важливою функцією VPN. Всі дані з клієнтського комп'ютера передаються через Інтернет на VPN-сервер. Такі сервери можуть розташовуватися дуже далеко від клієнтського комп'ютера, а дані по шляху в мережу організації проходять через обладнання багатьох провайдерів. Як переконатися, що дані не були скомпрометовані або змінені. Для цієї мети використовуються різні методи аутентифікації та шифрування.

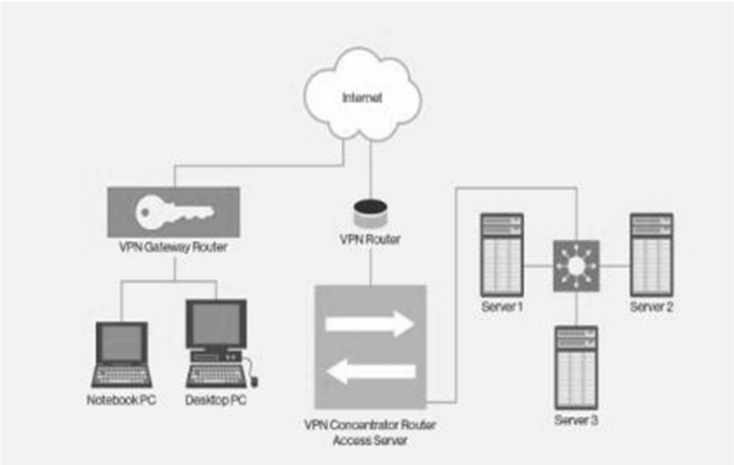

Рисунок 1.8 – Аутентифікація користувача в VPN мережах

Будь-який з протоколів може автентифікувати PPTP-користувача:

– EAP або розширюваний протокол аутентифікації;

– Протокол автентифікації рукостискання Mschap або Microsoft Challenge (версії 1 і 2);

– Протокол аутентифікації рукостискання глави або виклику;

– Протокол аутентифікації SPAP або Shiva;

– Протокол аутентифікації PAP або пароля.

Протокол MSCHAP версії 2 та протокол безпеки транспортного рівня (EAP-TLS) вважаються найкращими, оскільки вони забезпечують взаємну автентифікацію. У всіх інших протоколах лише сервер автентифікує клієнта.

PPTP забезпечує достатній ступінь безпеки, але L2TP по IPSec більш надійний. L2TP по протоколу IPSec не тільки забезпечує аутентифікацію на рівнях "користувач" і "комп'ютер", але також аутентифікує і шифрує всі дані.

Аутентифікація виконується у відкритому форматі (пароль у відкритому тексті) або за наступною схемою: запросіть зворотний зв'язок. Клієнт надсилає пароль на сервер. Сервер порівнює це з таблицею і відхиляє доступ або відповідає підтвердженням. Явної аутентифікації практично немає.

Схема запиту зворотного зв'язку набагато більш здійсненна. Загалом, це виглядає так:

– Клієнт відправляє запит на сервер для перевірки автентичності;

– Повертає зворотний зв'язок з сервером (виклик);

– Клієнт видаляє хеш з пароля (хеш - це хеш, який перетворює вхідну послідовність даних будь-якої довжини в комбінацію перших бітів фіксованої довжини).;

– Сервер зробить те саме і порівняє результат із відповіддю ініціалізатора;

– Якщо зашифрований запит збігається, то процес аутентифікації вважається успішним.

На першому етапі перевірки автентичності VPN-клієнта і сервера L2TP по протоколу IPSec використовує локальний сертифікат, отриманий від служби

сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють безпечне з'єднання ESP ВТС (Security Association). Аутентифікація на рівні користувача виконується після завершення процесу аутентифікації комп'ютера по протоколу L2TP (через IPSec). Ви можете використовувати будь-який протокол для автентифікації, навіть PAP, який надсилає ім'я користувача та пароль незашифрованими. Це дуже безпечно, оскільки L2TP через IPSec шифрує весь сеанс. Однак, коли ви використовуєте MSCHAP для виконання аутентифікації користувача, він використовує інший ключ шифрування для аутентифікації комп'ютера і користувача, що забезпечує додатковий захист.

Шифрування гарантує, що практично ніхто не зможе отримати доступ до пакетів, що надсилаються через Інтернет.

Рисунок 1.9 – Ілюстрація шифрованого каналу VPN мережах

В даний час підтримуються 2 методи шифрування:

1. Протокол шифрування MPPE або Microsoft точка-точка сумісний лише з MSCHAP.

2. EAP-TLS автоматично вибирає довжину ключа шифрування, коли параметри узгоджені між клієнтом і сервером.

MPPE використовує перемикач довжини 32, 40, 56, 64, 72, 128 або 256-біт. Операційна система Windows підтримує шифрування лише з довжиною ключа 32 і 40 біт, тому в гібридному середовищі Windows усі пристрої зашифровані.

Протокол MMPE був розроблений для двоточкових каналів зв'язку, через які пакети надсилаються послідовно, і втрата пакетів неможлива. У цьому випадку значення ключа іншого пакета залежить від результату дешифрування попереднього пакета. При створенні віртуальної мережі через мережу спільного доступу ці умови не можуть дотримуватися, оскільки пакети даних зазвичай надходять одержувачам в іншому порядку, ніж вони були відправлені. Таким чином, PPTP використовує порядковий номер пакета для зміни ключа шифрування. Це дозволяє виконувати дешифрування незалежно від раніше отриманих пакетів.

Обидва протоколи реалізовані як в Microsoft Windows, так і за її межами (наприклад, в операційних системах Linux), і алгоритм VPN може значно відрізнятися.

Таким чином, зв'язка " тунель + автентифікація + шифрування " дозволяє передавати дані між 2 точками через загальнодоступну мережу та моделювати поведінку приватної (локальної) мережі. Іншими словами, розглянутий інструмент дозволяє створити віртуальну приватну мережу.

Додатковим приємним ефектом VPN-мережі є можливість (і навіть необхідність) використання системи адресації, що використовується в локальній мережі.

Справжня реалізація віртуальної приватної мережі виглядає наступним чином: VPN-сервер встановлюється в локальній комп'ютерній мережі офісу вашої компанії. Віддалений користувач (або маршрутизатор, якщо підключено 2 офіси) запускає процедуру підключення до сервера за допомогою клієнтського програмного забезпечення VPN. Відбувається аутентифікація користувача-перший етап налаштування VPN-з'єднання. У разі підтвердження авторизації, 2. Починається етап-між клієнтом і сервером обговорюються деталі безпеки з'єднання. Після узгодження деталей встановлюється VPN-з'єднання для забезпечення обміну інформацією між клієнтами

І сервер у формі-аутентифікація даних, при якій кожен пакет даних проходить процедуру шифрування / дешифрування та перевірки цілісності.

Основна проблема мереж VPN полягає у відсутності встановлених стандартів аутентифікації та обміну зашифрованою інформацією. Ці стандарти все ще розробляються, тому продукти різних виробників не можуть встановлювати VPN-з'єднання та автоматично перемикати Комутатори.

Ця проблема призводить до уповільнення розповсюдження vpn, оскільки важко змусити різні компанії використовувати продукти одного і того ж виробника, і тому процес об'єднання мережі компаній-партнерів у так звану мережу Екстранет є складним.

У цьому розділі ми обговорили загальні методи підключення VPN до мережі передачі даних, Створення розподільної мережі та віддаленого доступу до мережі. Схема віддаленого доступу також може змінюватися залежно від типу послуги, яку підтримує віддалений клієнт. У багатьох випадках віддалений доступ до файлів, баз даних та принтерів використовується у стилі, який користувачі використовують під час роботи у своїй локальній мережі. Цей режим називається режимом віддаленого вузла. Іноді повідомлення електронної пошти обмінюються при віддаленому доступі, наприклад, в центральній мережі, де можна автоматично отримувати запитані корпоративні дані з бази даних.

Особливе місце серед усіх видів віддаленого доступу до комп'ютера займає можливість віддаленого управління комп'ютером так само, як користувач управляє комп'ютером за допомогою локально підключеного терміналу. У цьому режимі він може запускати програму на віддаленому комп'ютері і бачити результати роботи в режимі реального часу. У той же час цей метод доступу прийнято ділити на термінальний доступ і віддалене адміністрування.

1.3 Висновки

Метою VPN є прозорий доступ до мережевих ресурсів, який дозволяє користувачам робити все, що вони зазвичай роблять, незалежно від того, наскільки далеко вони знаходяться. Ось чому VPN набувають популярності серед працівників, які працюють у віддалених деках, та філій, яким потрібно ділитися ресурсами з географічно віддалених офісів.

Основна ідея VPN-захистити весь трафік, що передається через віртуальну приватну мережу. Впровадження VPN значно полегшує роботу та налаштування мережі. Ключ може бути простим і недорогим.

Перевага технології VPN полягає в тому, що організація віддаленого доступу здійснюється через Інтернет, а не по телефонній лінії.Це набагато дешевше і краще. Вам потрібен лише Інтернет та дійсна IP-адреса, Щоб використовувати технологію VPN для організації віддаленого доступу до вашої приватної мережі. Крім того, будь-який користувач у світі може увійти в мережу, якщо знає свою IP-адресу, ім'я користувача та пароль.[1]

По-перше, інформація передається в зашифрованому вигляді. Тільки власник ключа шифрування може прочитати отримані дані. Аутентифікація включає перевірку цілісності даних та ідентифікацію користувачів, які беруть участь у vpn. По-перше, він гарантує, що дані надходять до місця призначення саме в тому форматі, в якому вони були передані.

Переваги VPN очевидні. Дозволяючи користувачам підключатися через Інтернет і збільшуючи пропускну здатність каналів зв'язку при перевантаженні мережі, VPN можуть допомогти заощадити на вартості телефону, оскільки немає необхідності возитися з пулом модемів. Крім того, Vpn надає вам доступ до мережевих ресурсів, що змушує адміністраторів підключатися ззовні за нормальних обставин.

Тому створення захищеної приватної мережі та використання технології шифрування інформації є важливим завданням для всіх компаній.

2 ПОНЯТТЯ VPN, ЇХ КЛАСИФІКАЦІЯ ТА ХАРАКТЕРИСТИКИ В ПРОЦЕСАХ ПОБУДОВИ КОМУТОВАНИХ МЕРЕЖ

2.1 Класифікація VPN і їх характеристика

VPN класифікуються за такими основними параметрами (рис.2.1):

– залежно від ступеня захисту;

– згідно методу застосування;

– за системою бронювання;

– відповідно до використовуваного протоколу;

– залежно від рівня роботи, пов'язаного з роботою стека протоколів OSI.

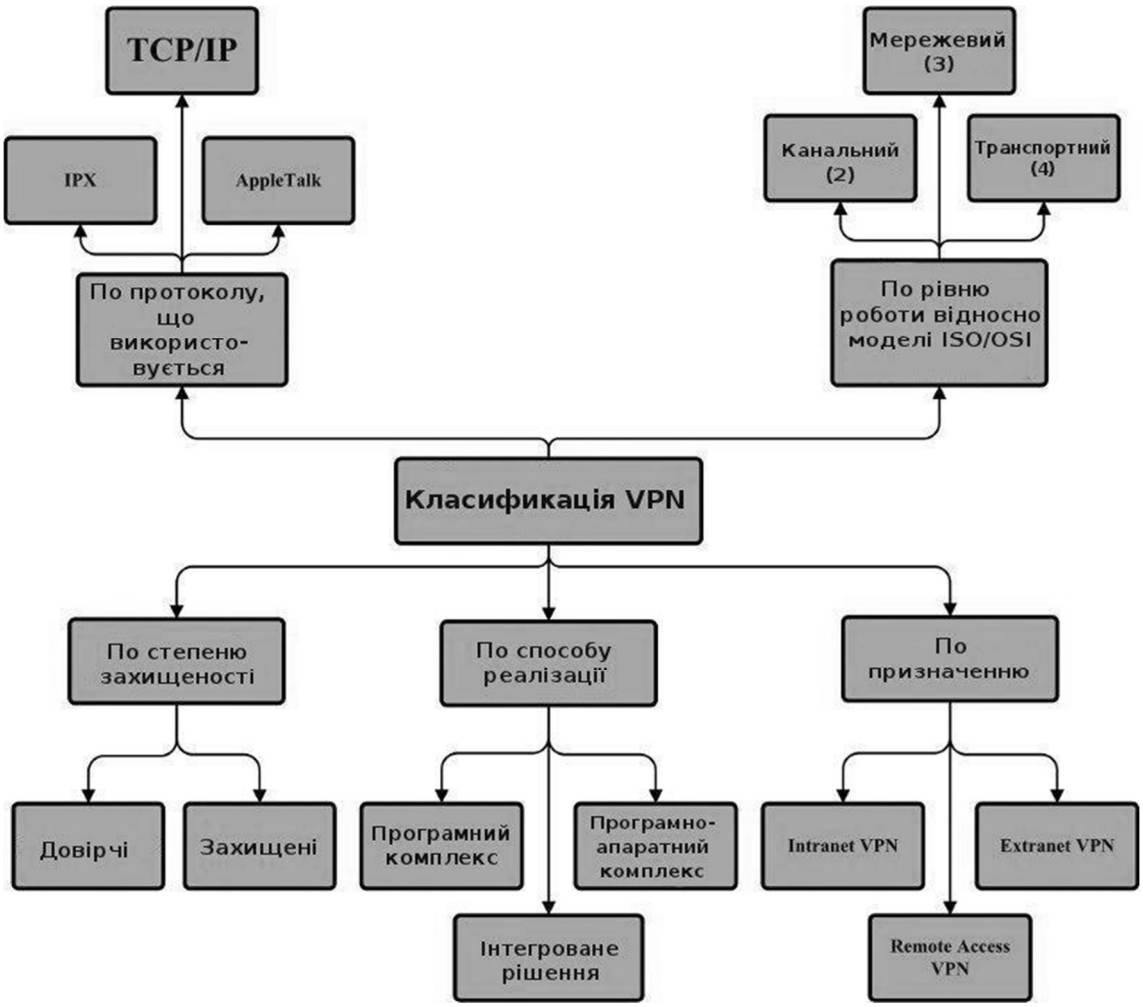

Рисунок 2.1 – Класифікація VPN

Залежно від типу використовуваного середовища вони діляться на захищені і надійні.

a) безпечна мережа VPN. Найпоширеніший варіант приватних мереж. З його допомогою можна створити безпечну та надійну підмережу на основі ненадійної мережі, якою зазвичай є Інтернет. Прикладами захищених VPN є IPSec, OpenVPN та PPTP.

b) надійна мережа VPN. Вони використовуються, коли середовище передачі є надійним, і їх можна вважати необхідними лише для вирішення проблеми створення віртуальної підмережі у більшій мережі. Питання безпеки стали неактуальними. Прикладами таких рішень VPN є MPLS та L2TP. Правильніше сказати, що ці протоколи передають завдання безпеки іншим протоколам. Наприклад, L2TP зазвичай використовується в поєднанні з IPSec.

Залежно від методу використання VPN поділяють на:

a) VPN-мережа у вигляді спеціального програмного і апаратного забезпечення. Реалізація мережі VPN здійснюється з використанням спеціального набору програмного і апаратного забезпечення. Ця програма забезпечує високу продуктивність і, в принципі, високий ступінь безпеки.

b) VPN-мережа у вигляді програмних рішень. Вони використовують персональний комп'ютер зі спеціальним програмним забезпеченням, яке забезпечує функціональність VPN.

c) VPN-мережа з вбудованим рішенням. Функція VPN надає комплекс, який також вирішує проблеми фільтрації мережевого трафіку, організації брандмауерів і забезпечення якості обслуговування.

Відповідно до призначення виділяють наступні види VPN:

a) Інтранет VPN. Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

b) VPN з віддаленим доступом. Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до

корпоративних ресурсів з домашнього комп'ютера або, перебуваючи у відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

c) Екстранет VPN. Використовують для мереж, до яких підключаються "зовнішні" користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому необхідне забезпечення спеціальних «рубежів» захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

За протоколом, що використовується, розрізняють такі VPN:

a) TCP/IP;

b) IPX;

c) AppleTalk.

На сьогоднішній день виробники програмного забезпечення переходять на протокол TCP / IP, і абсолютна більшість VPN рішень підтримує саме його.

Мережі VPN будуються з використаним протоколом тунелювання даних через мережу зв'язку загального користування Інтернет, причому протоколи тунелювання забезпечують шифрування даних і здійснюють їх наскрізну передачу між користувачами. Як правило, на сьогодні VPN використовують наступні рівні моделі OSI:

a) канальний рівень.

b) мережевий рівень.

c) транспортний рівень.

На канальному рівні в якості протоколів тунелювання можуть використовуватися протоколи L2TP і PPTP, в яких присутня авторизація і автентифікація. В найближчий час прогнозується зростання кількості віртуальних приватних мереж, що функціонуватимуть на базі протоколу тунелювання другого рівня L2TP (Layer 2 Tunneling Protocol).

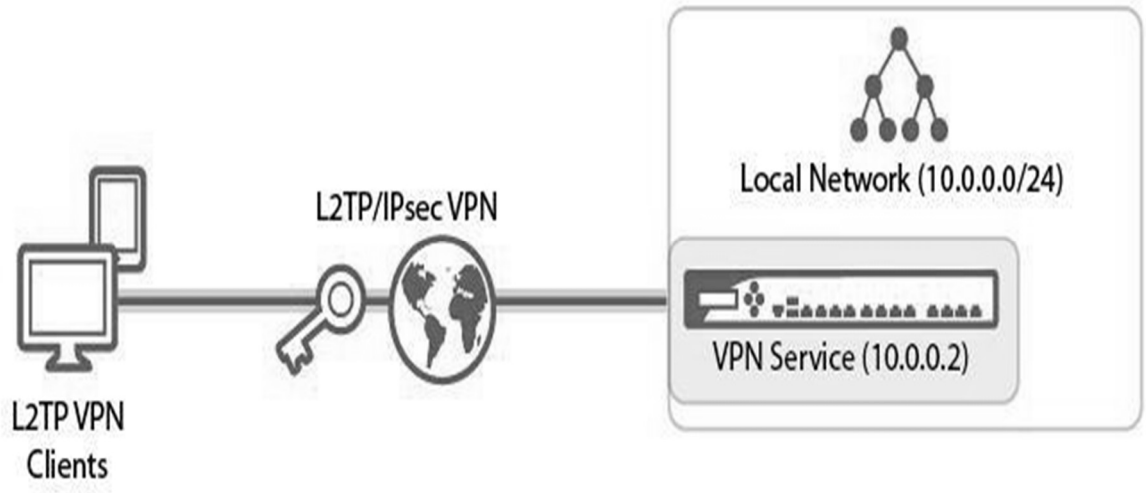

Рисунок 2.2 – Канальний рівень

L2TP з'явився як результат комбінації протоколів PPTP і L2F (Layer 2 Forwarding). PPTP дозволяє відправляти пакети PPP через тунель, а L2F дозволяє відправляти пакети SLIP і PPP. Протокол L2TP ввібрав в себе кращі можливості PPTP і L2F. Найбільш важливою перевагою L2TP є те, що цей протокол дозволяє не тільки мережам IP, а також мережам ATM, X25 та FrameRelay, створювати тунелі. На жаль, реалізація L2TP у Windows 7 та молодших версіях підтримує лише IP.

L2TP використовує протокол udp як транспорт і використовує однаковий формат повідомлень як для управління тунелями, так і для передачі даних. Реалізація Microsoft L2TP використовує UDP-пакети, що містять зашифровані PPP-пакети, в якості керуючих повідомлень. Надійність доставки забезпечує контроль послідовності посилок.

Функції PPTP і L2TP різні. L2TP використовує той самий формат і протокол не тільки в мережі IP, але і в службовому повідомленні для створення тунелю та надсилання даних за його межі. PPTP доступний лише в мережах IP, і для створення та використання тунелю потрібне окреме TCP-з'єднання. L2TP по протоколу IPSec забезпечує більший рівень безпеки, ніж PPTP, і може гарантувати майже 100-відсоткову безпеку критично важливих для вашої організації даних. Можливості

L2TP роблять його дуже перспективним протоколом для створення віртуальних мереж.

Протокол тунелювання другого рівня (L2TP) є галузевим стандартом і є першим протоколом тунелювання на основі RFC, який підтримується операційними системами клієнта та сервера. На відміну від PPTP, L2TP Н не використовує шифрування-двоточкове шифрування (MPPE) - для шифрування блоку даних протоколу точка-точка (PPP). L2TP залежить від безпеки протоколу шифрування IPSec. Комбінація L2TP та ipsec відома як L2TP / IPSec. L2TP / IPSec забезпечує інкапсуляцію та шифрування персональних даних в основній віртуальній приватній мережі (VPN).

L2TP використовує два типи пакетів: інформаційні пакети та контрольні пакети. Блок управління використовується для монтажу та обслуговування тунелів. Інформаційні повідомлення використовуються для інкапсуляції фреймворків PPP, що надсилаються через тунель. Контрольні повідомлення використовують надійний канал управління L2TP для забезпечення доставки. Якщо інформаційні повідомлення втрачені, вони не передаються повторно.

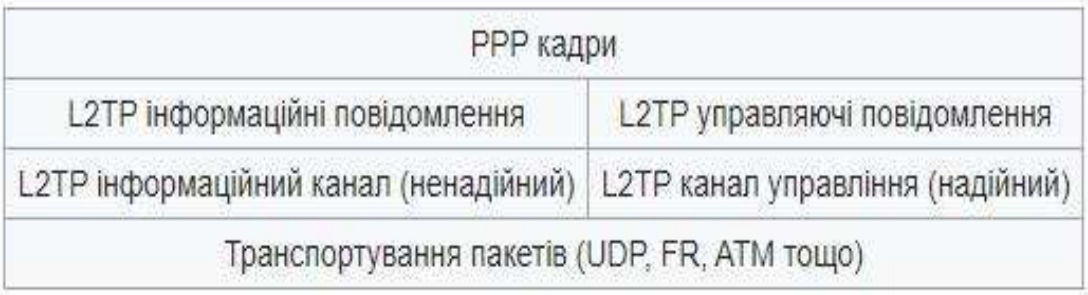

Рисунок 2.3 – Складові протоколу

Рисунок 2.4 – Формат заголовка:

Цей тип біта (T) характеризує тип пакета. Це значення дорівнює 0 для інформаційних повідомлень і 1 для адміністраторів.

Якщо біт довжини (L) дорівнює 1, існує поле довжини. Для керуючих повідомлень цей біт повинен дорівнювати 1.

Біт X зарезервований для майбутніх додатків. Усі біти повинні мати значення 0 для вихідних повідомлень і ігноруватися для вхідних повідомлень.

Також є поля Ns і Nr, якщо порядковий біт S дорівнює 1. В керуючому повідомленні він обов'язково повинен дорівнювати 1.

Якщо біт зсуву (O) дорівнює 1, існує поле значення зміщення. В керуючому повідомленні повинен дорівнювати 0.

Біт пріоритету (P) для всіх керуючих повідомлень повинен бути рівний 0. Для інформаційних повідомлень - якщо цей біт дорівнює 1, це інформаційне повідомлення має пріоритет у черзі.

У полі експорт відображається версія заголовка інформаційного повідомлення L2TP.

Значення 1 зарезервовано для виявлення пакетів L2F в умовах використання пакетів L2TP. Пакети, отримані з невідомим значенням поля експорту, відкидаються.

Поле Довжина (необов'язково) показує загальну довжину повідомлення в октетах.

Ідентифікатор тунелю містить ідентифікатор керуючого каналу. Ідентифікатор тунелю L2TP має лише локальні значення. Тобто різні кінці одного тунелю потребують різних ідентифікаторів. Ідентифікатор тунелю для кожного повідомлення повинен відповідати очікуванням одержувача. Ідентифікатор тунелю вибирається під час створення тунелю.

Ідентифікатор сеансу визначає ідентифікатор сеансу в цьому тунелі. Сеанс L2TP

Вони називаються тільки з використанням ідентифікаторів, що мають власне значення. Ідентифікатор сеансу для кожного повідомлення повинен відповідати очікуванням одержувача. Ідентифікатор сеансу вибирається під час створення сеансу.

У полі визначає порядковий номер інформаційного або контрольного повідомлення, який починається з нуля і збільшується на 1 (по модулю 2 1 6) для кожного відправленого повідомлення.

Поле NR містить очікуваний порядковий номер для наступного повідомлення: отже, NR дорівнює NS останнього отриманого повідомлення плюс 1 (за модулем 2 1 6). В інформаційному повідомленні NR зарезервований і, якщо він існує (це визначається через S-дека), слід ігнорувати при прийомі.

Це поле визначає число октетів після заголовка l2TP, що ініціалізує поле даних, якщо воно існує. Вміст заповнювача зсуву не визначено. Якщо є поле зміщення, відображається заголовок L2TP. Зсув закінчується після останнього октету заповнювача.

Протокольні операції. Щоб налаштувати сеанс тунелювання PPP L2TP, потрібно виконати два кроки:

– Установка каналів управління для тунелів
– Створення сеансу у відповідь на запит вхідного або вихідного дзвінка.

Перед початком вхідного або вихідного дзвінка необхідно створити тунель і відповідний канал управління. Щоб дозволити L2TP надсилати кадри PPP через тунель, вам потрібно реалізувати сеанс L2TP. В одному тунелі може бути кілька сеансів між одним і тим же LAC і LNS.

Контрольне з'єднання. Це основне питання, яке має бути реалізовано між LAC та LNS перед початком сеансу. Налаштування контрольного з'єднання включає в себе безпечну ідентифікацію партнерів, версію L2TP, можливості каналу і прийняття рішень про зміну персоналу. L2TP включає в себе просту і додаткову систему тунельної аутентифікації, подібну CHAP, в процесі налаштування керуючого з'єднання.

Окремі сеанси можуть бути створені після успішної установки керуючого з'єднання. Кожен сеанс відповідає 1 ППС потоку інформації між LAC і LNS. На відміну від налаштувань підключення до елемента керування, Налаштування сеансу асиметричні щодо LAC та LNS. Lac запитує доступ до сеансу LNS для вхідних запитів, а LNS просить LAC ініціювати сеанс для обробки вихідних запитів.

Коли створюється тунель, кадри PPP з віддаленої системи, отримані LAC, передаються з CRC, заголовка каналу тощо. Він інкапсулюється в L2TP і передається через відповідний тунель. LNS приймає пакети L2TP і обробляє інкапсульовану структуру PPP так, ніби вона отримана через власний інтерфейс PPP.

Відправник повідомлення, пов'язаного з певним сеансом і тунелем, поміщає ідентифікатори сеансу і тунелю (зазначені партнером) у відповідні поля заголовка всіх вихідних повідомлень.

І L2TP, і IPSec повинні підтримуватися як клієнтом VPN, так і сервером VPN. L2TP встановлюється за протоколом TCP / IP. Залежно від вашого вибору під час налаштування серверів маршрутизації та віддаленого доступу, L2TP налаштований на 5 або 128 портів L2TP.

2.2 Концепція побудови комутованих мереж на базі VPN

В даний час найпоширенішим протоколом VPN є протокол тунелювання точка-точка або протокол тунелювання точка-точка (PPTP). PPTP

Він використовує існуючий відкритий стандарт TCP / IP і в основному базується на застарілому протоколі двоточкового зв'язку. Фактично, PPP, RRT залишається протоколом зв'язку для сеансу зв'язку. RRT створює тунель до NT-сервера одержувача через мережу та надсилає його через цей тунель

Пакет RRP для віддаленого користувача. Сервери та робочі колоди використовують віртуальну приватну мережу і не звертають уваги на те, наскільки безпечна або доступна глобальна мережа між ними.

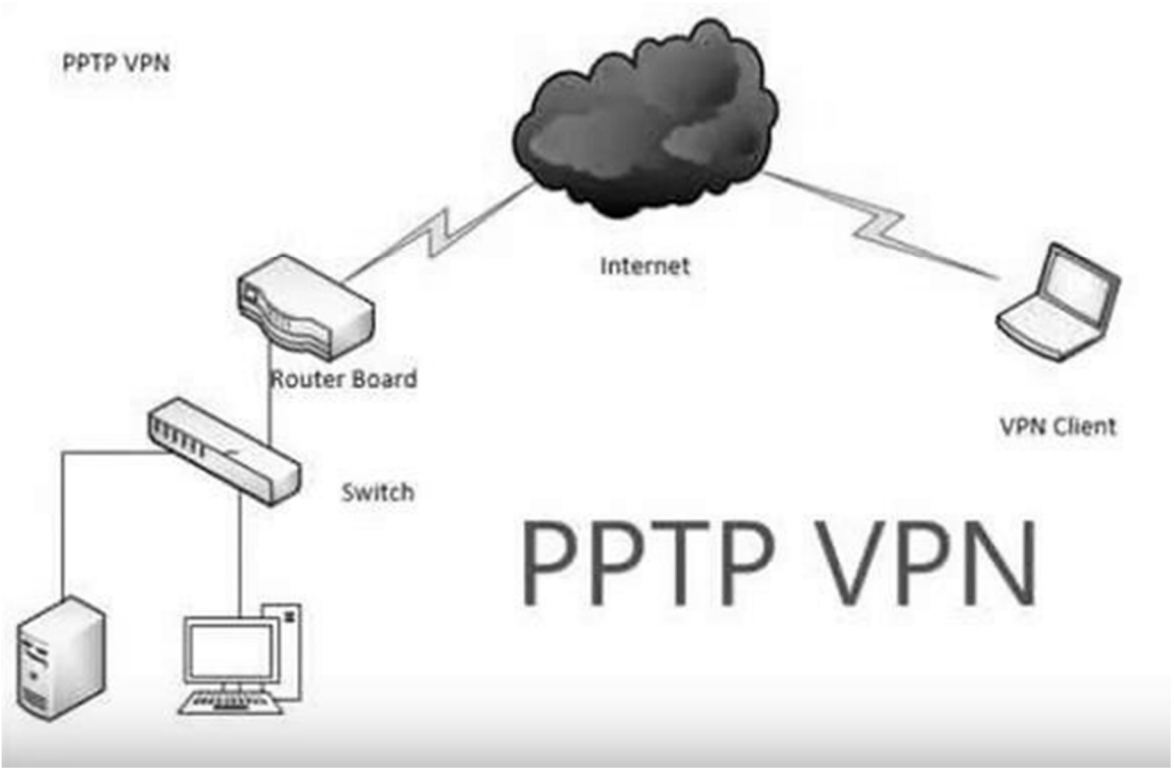

Рисунок 2.5 – Структурна побудова мережі на базі протоколу PPTP

Можливості протоколу RTR застосовуються лише до пристроїв під управлінням Windows, але він надає компаніям можливість взаємодіяти з існуючою мережевою інфраструктурою і не завдавати шкоди власним системам безпеки. Таким чином, віддалений користувач може підключитися до Інтернету за допомогою локального провайдера через аналоговий або ISDN-канал і встановити з'єднання з сервером NT. У той же час компанії не потрібно витрачати багато

грошей на організацію та обслуговування пулу модемів, що надають послуги віддаленого доступу. PPTP -

Комп'ютер може встановити безпечне з'єднання з сервером, створивши приватний тунель у мережі, яка не захищена стандартною безпекою.

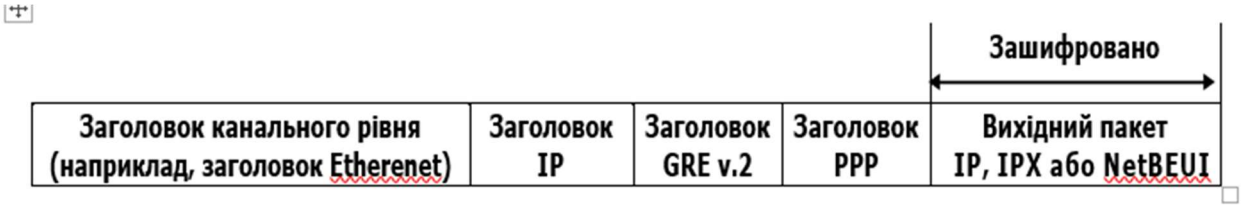

Рисунок 2.6 – Структурна пакета PPTP

PPTP інкапсулює IP-пакети для передачі через IP-мережу. Клієнт PPTP створює з'єднання управління тунелем, використовуючи порт призначення. Цей процес відбувається на транспортному рівні моделі OSI. Після створення тунелю клієнтський комп'ютер і сервер починають обмінюватися пакетами оновлень. На додаток до керуючого каналу PPTP, що забезпечує працездатність каналу, створюється з'єднання для передачі даних по тунелю. Інкапсуляція даних перед відправкою через тунель дещо відрізняється від звичайної передачі. Інкапсуляція даних перед відправкою в тунель включає 2 кроки::

Отримані дані потім надсилаються до моделі OSI та інкапсулюються протоколом вищого рівня.

Отже, 2. під час міграції дані надходять на транспортний рівень. Однак інформація не може бути відправлена в пункт призначення, оскільки за це відповідає канальний рівень OSI. Таким чином, PPTP шифрує завантажувальний простір пакета і зазвичай шифрує 2, який є частиною PPP. успадковує функцію рівня. Іншими словами, він додає заголовок PPP і суфікс до пакету PPTP. Це завершує створення структури канального шару.

Потім PPTP інкапсулює структуру PPP в пакет інкапсуляції глобальної маршрутизації (GRE), що належить до мережевого рівня. GRE інкапсулює мережеві рівні, такі як IPX, AppleTalk та DECnet, щоб забезпечити передачу через IP-мережі. Однак GRE не має можливості створювати сеанси та захищати дані від

зловмисників. Він використовує функцію PPTP для створення з'єднань для управління тунелями. Використання GRE як методу інкапсуляції обмежує охоплення PPTP лише IP-мережами.

Після того, як кадр PPP інкапсулюється в кадр за допомогою заголовка GRE, інкапсуляція виконується в кадр за допомогою заголовка IP. Заголовок IP містить адресу відправника та одержувача пакета. Нарешті, PPTP жовтня додає заголовок та розрив PPP. У Жовтневому додатку 3 показана структура даних, які будуть передаватися через тунель PPTP.

Система передачі передає даних через тунель. Приймаюча система видаляє всі заголовки служб і залишає лише дані PPP.

MPLS VPN-це сімейство методів, що використовуються для створення віртуальних приватних мереж (VPN) за допомогою багатопротокольної комутації тегів (MPLS). MPLS VPN-це гнучкий спосіб передачі та маршрутизації декількох мережевих трафіків по магістралі MPLS. В даний час в мережі розгорнуто 3 типи мереж MPLS VPN:

1. Точка-точка (так званий конвеєр)
2. Рівень 2 (VPLS)
3. Рівень 3 (VPRN)

MPLS-це модель OSI з канальним шаром 3. Його часто називають протоколом канального мережевого рівня, оскільки він працює на рівні, який може бути між канальним та мережевим рівнем. Двоточкова VPN-адреса MPLS використовує віртуальні виділені деки (VLL) для забезпечення зв'язку рівня 2 точка-точка між 2 сайтами. Ці VLL можуть інкапсулювати платформи Ethernet, TDM та ATM.

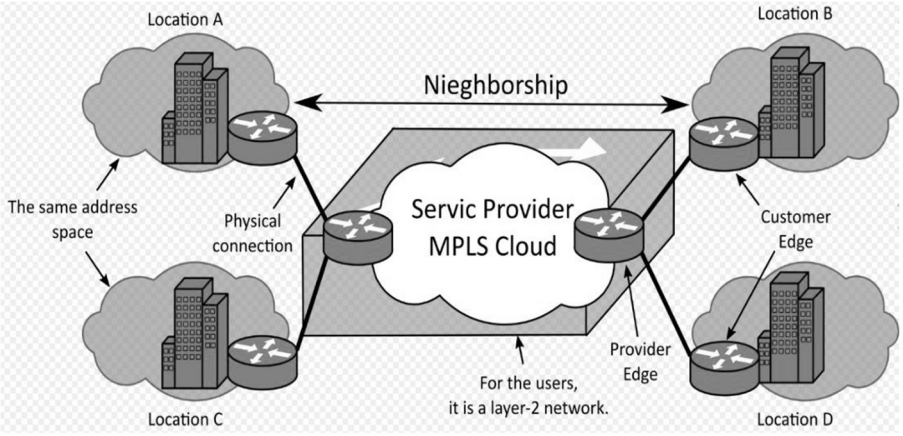

Рисунок 2.7 – Структура MPLS мереж

MPLS VPN працює в двох доменах: клієнтської мережі IP і внутрішніх (магістральних) MPL провайдера, необхідних для підключення до клієнтської мережі.

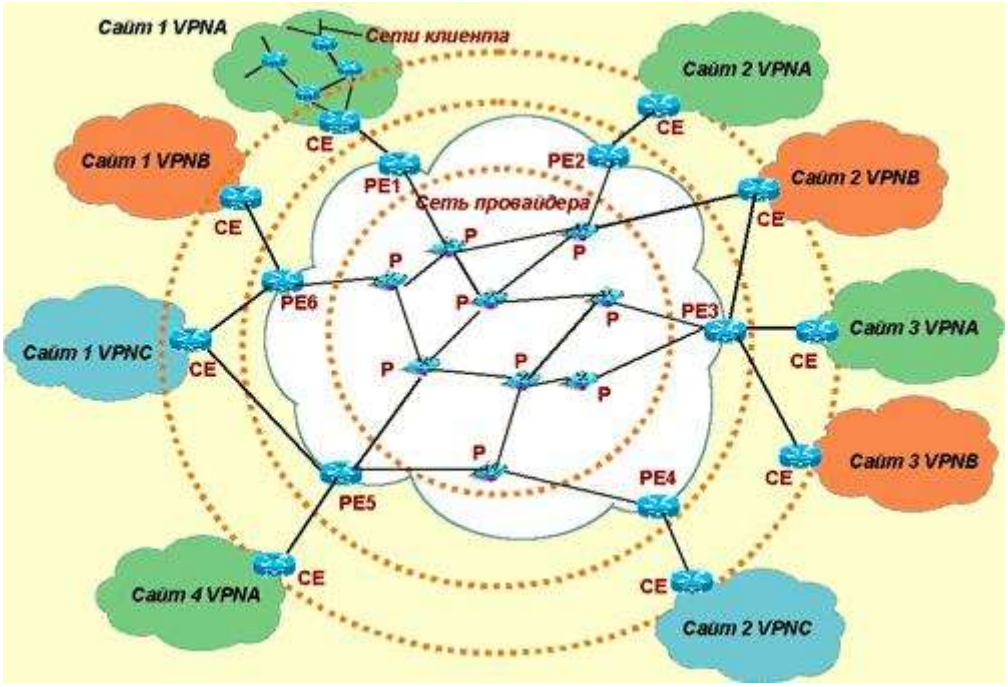

Рисунок 2.8 – Компоненти MPLS VPN

Як правило, якщо кожен клієнт має кілька географічно визначених мережевих IP-адрес, кожен клієнт має кілька підмереж, пов'язаних із маршрутом. Географічно призначені мережеві сегменти корпоративної мережі часто називають сайтами. 1. Сайти, що належать клієнту, обмінюються пакетами з IP-адресами, які надають та створюють віртуальну приватну мережу для цього клієнта.

Наприклад, можна сказати, що це один з 4 сайтів з 1 для корпоративної мережі з центральним відділом, відомим віддаленій філії. Протокол внутрішнього шлюзу (IGP) використовується для обміну інформацією про маршрутизацію на використовуваному веб-сайті (домени, обмежені автономними системами, такими як RIP, OSPF та IS-IS).

2.3 Безпека каналів комутованих мереж

Протокол IPSec використовується на мережевому рівні. IPSec забезпечує шифрування та конфіденційність даних, а також автентифікацію абонентів. Протокол IPSec дозволяє реалізувати повнофункціональний доступ, еквівалентний фізичному підключенню до корпоративної мережі. Щоб налаштувати VPN, кожен учасник повинен встановити певні параметри IPSec. Це означає, що кожному клієнту потрібне програмне забезпечення для реалізації IPsec.

Він призначений для забезпечення високоякісного криптографічного захисту, сумісного з IPSec, Ipv4 та Ipv6. Набір служб безпеки, що надаються, включає контроль доступу, цілісність, автентифікацію джерела даних, захист від відтворення (тип часткової цілісності масиву), шифрування, і ці послуги надаються на рівні IP та забезпечують захист протоколів IP та / або високого рівня.

Ці цілі досягаються за допомогою 2 протоколів безпеки дорожнього руху: заголовок автентифікації (AH) та корисне навантаження інкапсуляції безпеки (ESP), а також використання процедур управління протоколом криптографічного ключа. Набір протоколів IPSec в будь-якому контексті і спосіб їх налаштування можуть бути визначені користувачем, додатком і / або сайтом будь-якої організації.

Якщо ці механізми реалізовані та розгорнуті належним чином, користувачі, які не використовують ці механізми безпеки для захисту трафіку, розміщують ці механізми, а також призначені для того, щоб бути незалежними від алгоритму. Ця модульність дозволяє вибирати різні набори алгоритмів, не впливаючи на інші

частини програми. Наприклад, різні спільноти користувачів можуть при необхідності вибирати інший набір алгоритмів шифрування даних.

За замовчуванням для забезпечення сумісності в глобальному Інтернеті визначено стандартний набір алгоритмів. Реалізація цих алгоритмів

Він розроблений у поєднанні з протоколами захисту трафіку IPSec та управління ключами, щоб дозволити розробникам систем та додатків використовувати високоякісні технології криптографічної безпеки.

Жодна компанія не хоче відкрито ділитися фінансовою чи іншою конфіденційною інформацією з третіми сторонами. Канали VPN захищені надійними алгоритмами шифрування, вбудованими в стандарт протоколу безпеки IPSec. IPSec, або безпека Інтернет-протоколу, є стандартом, обраним міжнародним співтовариством, і група IETF- Internet Engineering Task Force, що всі інші пристрої між ними повинні забезпечувати тільки трафік IP-пакетів.

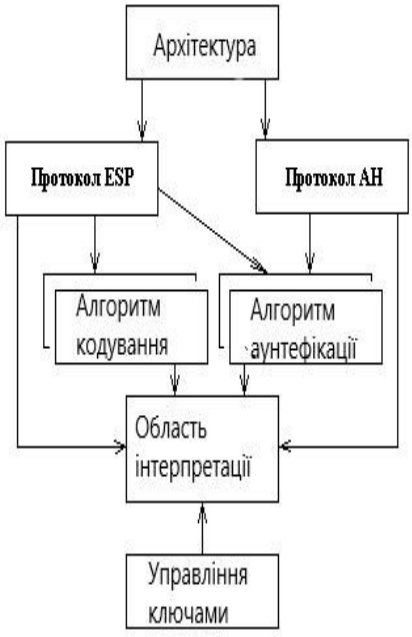

Рисунок 2.9 – Архітектура IPSec.

Стандарт безпеки Інтернет-протоколу (IPSec), який використовується для створення віртуальних приватних мереж (VPN) та Асоціація інтернет-безпеки,

встановив безпечні з'єднання між віддаленими користувачами та приватними корпоративними мережами. Кожне захищене з'єднання називається тунелем. ASA використовує стандарти тунелювання ISAKMP та IPSec для створення та управління тунелями. ISAKMP та IPSec виконують такі дії:

- Налаштування параметрів тунелю
- Встановлення тунелю
- Аутентифікація та дані Користувача
- Управління ключами безпеки
- Шифрування та дешифрування даних
- Контроль передачі даних через тунель
- Управління передачею вхідних і вихідних даних в якості кінцевої точки тунелю або маршрутизатора.

IPSec використовується для підключення VPN до локальної мережі і надає можливість використовувати IPSec для VPN-з'єднань клієнт-локальна мережа. У термінології IPS одноранговий клієнт - це клієнт віддаленого доступу або інший захищений шлюз.

Існують певні розбіжності щодо вибору рівня реалізації захищеного каналу.З іншого боку, вибір більш високого рівня вказує на незалежність від типу передачі (вибір протоколу мережевого і канального рівнів).З іншого боку, для кожного рівня потрібні окремі налаштування та конфігурації. Перевага вибору нижчого рівня полягає в універсальності та оглядовості запропонованого, а недоліком є те, що він залежить від вибору конкретного протоколу (наприклад, PPP або Ethernet). Консенсусним рівнем вирівнювання є IPSec: він розміщується на мережевому рівні з використанням найвищого розширеного протоколу IP цього рівня. Це робить IPSec більш гнучким і може використовуватися для захисту протоколів на основі TCP та UDP. У той час він прозорий для подальших пропозицій.

Коли ви створюєте тунель, у вас є угоди, пов'язані з безпекою, які регулюють автентифікацію, шифрування, інкапсуляцію та управління ключами. Ці правила передбачають 2 етапи: створення тунелю (IKE SA) і управління трафіком в тунелі

(IPSec SA). VPN з локальної мережі в локальну мережу з'єднують мережі, розташовані в різних географічних точках.

Тунель IPSec - це правила, встановлені між точками. SA визначає протоколи та алгоритми, що застосовуються до конфіденційних даних, а також визначає ключі, що втягують відповідні точки. IPSec SA контролює фактичну передачу трафіку користувача. Втиснути IPSec SA в IPSec SA контролює фактичну передачу трафіку користувача. Деки, що використовуються для кожного CA, встановлюються між точками. Кожен SA складається з::

- Набір для перетворення IKEV1 або IKEV2
- Зашифровані дані
- ACL
- Тунельна група
- Політика до фрагментації

Побудова захищеного каналу зв'язку може здійснюватися на різних рівнях OSI.

IPSec – це набір Інтернет-стандартів, свого роду "надбудова". Його ядро складається з 3 протоколів:

- Заголовок автентифікації (AN) забезпечує цілісність вихідних даних, автентифікує історичну інформацію та працює шляхом пересилання вихідних пакетів

- Інкапсуляція безпеки корисного навантаження (ESP) обмежує потік конфіденційного трафіку і забезпечує надійність (шифрування) переданої інформації. Крім того, він може виконувати функцію AH. Він забезпечує транзитивність цільових даних, перевірку історичної інформації та роботу з повторною передачею пакетів. При використанні ESP обов'язково вказати набір служб з підтримкою безпеки. Кожна з його функцій може бути включена за запитом.

- Протоколи атрибуції інтернет-безпеки та управління ключами. (ISAKMP) - це протокол, який використовується для великих підприємств, з'єднань та

взаємної автентифікації, і він підходить для інших приватних ключів та відомих приватних ключів. Цей протокол попередньо включає різні використовувані механізми обміну ключами, включаючи використовувані протоколи, такі як завдання з фіксованим ключем, обмін ключами в Інтернеті, Конвенція про інтернет-ключі KERBERIZE та тип запису DNS IPSECKEY.

Заголовок автентифікації (AH), як правило, є необов'язковим заголовком, який зазвичай розміщується між основним заголовком IP-пакета та полем даних. Наявність АГ не впливає на рівень транспорту або процес передачі інформації на більш високому рівні. це єдина мета.

Існує захист від атак, пов'язаних з несанкціонованими змінами вмісту пакета, включаючи зміну вихідної адреси мережевого рівня. Для перевірки достовірності отриманих даних необхідно змінити більш високий рівень протоколу.

Формат AH дуже простий: він складається з даних змінної довжини, що складаються з 96-розрядних заголовків та 32-розрядних слів. Наступний заголовок вказує наступний заголовок, довжина корисного навантаження представляє довжину пакета, SPI є вказівником на контекст безпеки, а поле порядкового номера містить серійний номер пакета.

IPSec може працювати в 2 режимах: транспортному і тунельному.

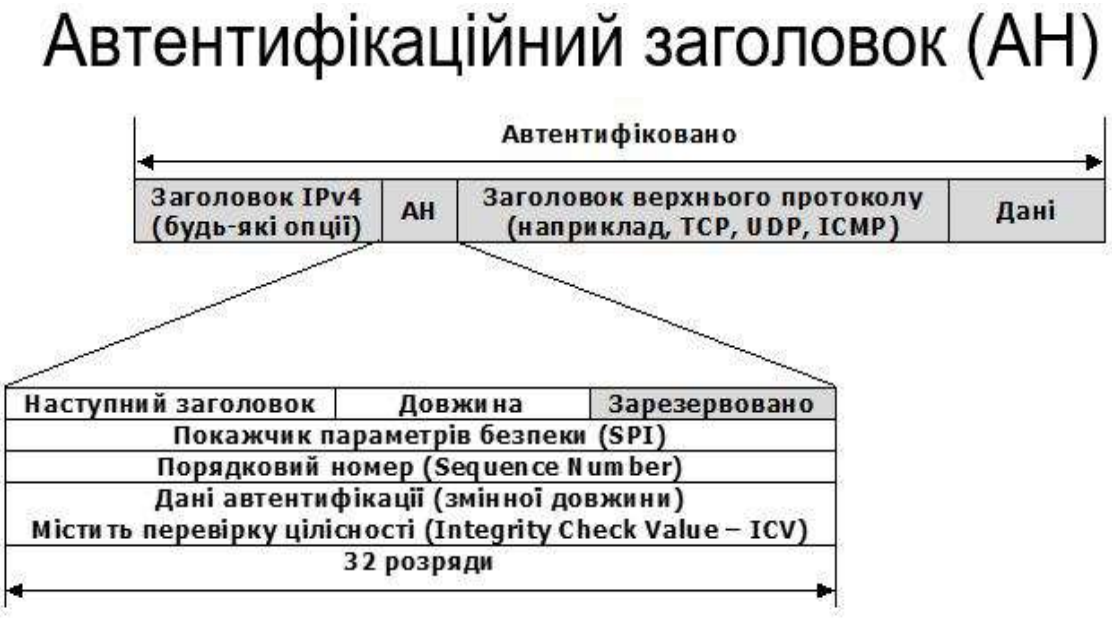

Рисунок 2.10 – Структура заголовка AH

Якщо використовується інкапсуляція зашифрованих даних, заголовок ESP є кінцем набору заголовків параметрів, які "видно" в пакеті. Оскільки основною метою esp є забезпечення конфіденційності даних, для різних типів інформації може знадобитися використання суттєво різних алгоритмів шифрування. Отже, формат ESP може значно відрізнятися залежно від використовуваного алгоритму шифрування. Однак ви можете розрізнити поле SPI, яке визначає контекст безпеки, та Поле порядкового номера, що містить серійний номер пакета. У заголовку ESP поле "дані автентифікації ESP" (контрольна сума) є необов'язковим. Одержувач пакету ESP розшифровує заголовок ESP і використовує параметри та дані алгоритму шифрування, що використовується для дешифрування інформації транспортного рівня.

У режимі передачі шифруються (або підписуються) тільки дані IP-пакета, і вихідний заголовок зберігається. Режим передачі зазвичай використовується для організації з'єднання між хостами. Він також може використовуватися між шлюзами для організації тунелів, розташованих іншими способами (наприклад, L2TP).

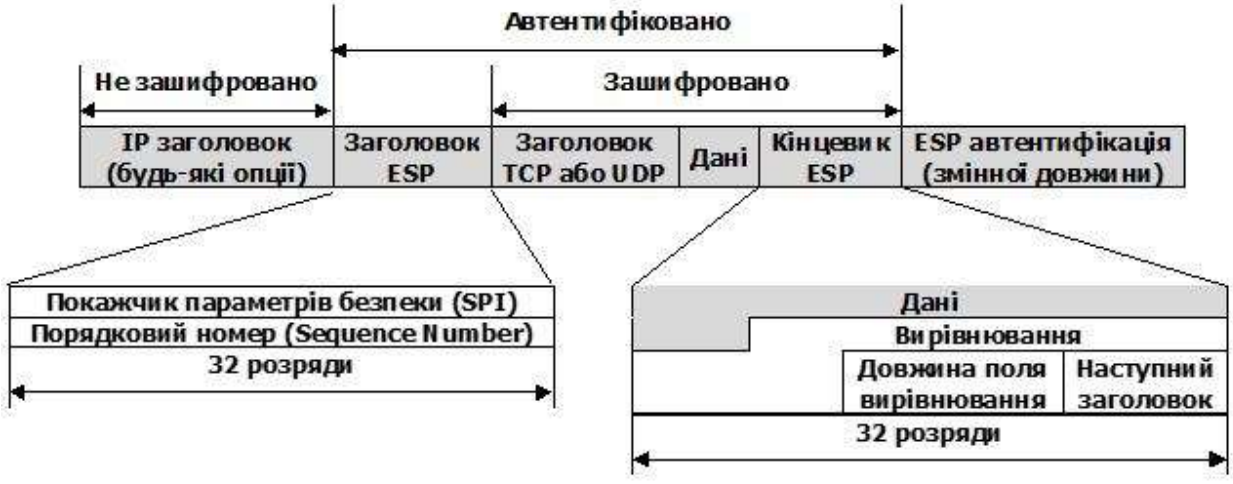

Рисунок 2.11 – Структура заголовка ESP

У режимі тунелювання весь вихідний IP-пакет шифрується: дані, заголовки, інформація про маршрут і додаються в поле даних нового пакета. Тунельний режим можна використовувати для організації безпечної передачі даних через відкриті

канали зв'язку між шлюзами (наприклад, Інтернетом) для підключення віддалених комп'ютерів до віртуальної приватної мережі або для об'єднання різних частин віртуальної приватної мережі. Режим IPSec не є взаємовиключним.

На одному вузлі деякі SA можуть використовувати транспортний режим, а інші - тунельний режим.

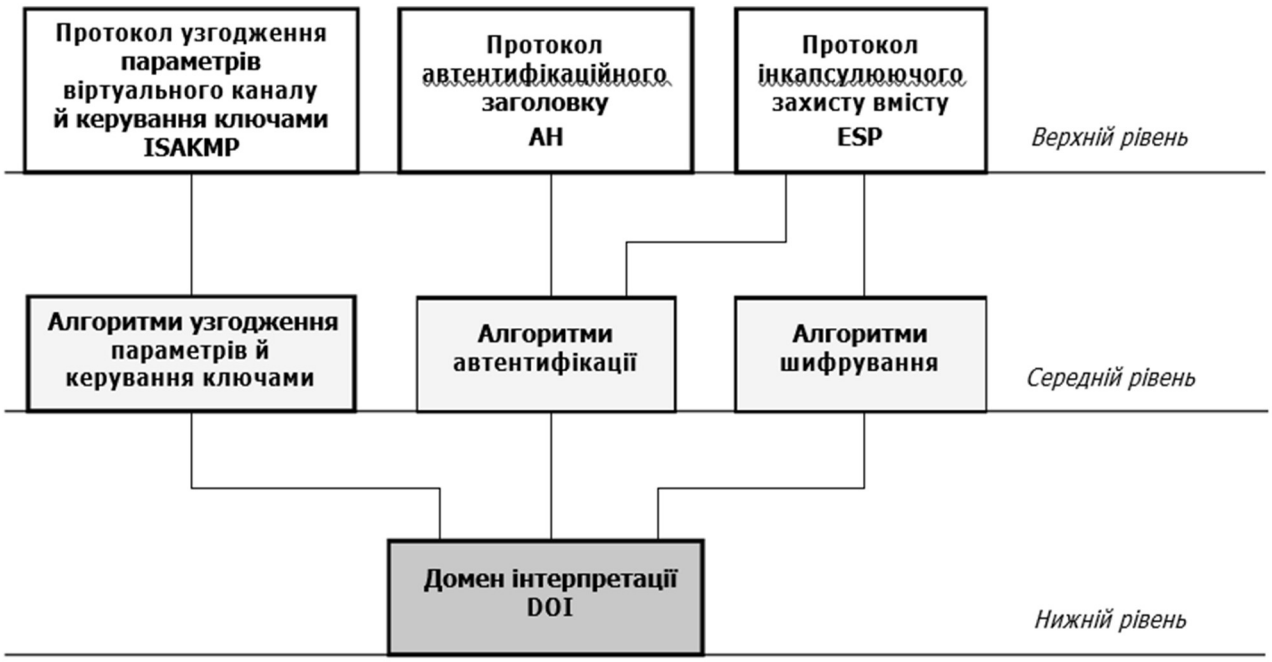

Рисунок 2.12 – Архітектура засобів захисту IPSec.

Транспортний режим використовується для шифрування полів даних в IP-пакетах, що містять протоколи транспортного рівня (TCP, UDP, ICMP). Одним із прикладів використання режиму передачі є надсилання електронного листа. Усі проміжні вузли на шляху пакета від відправника до одержувача використовують лише інформацію відкритого мережевого рівня, а в деяких випадках деякі необов'язкові заголовки пакетів (Ipv6). Недоліками режиму передачі є відсутність механізму для приховування конкретного відправника і одержувача пакета, а також можливість аналізу трафіку. Результатом такого аналізу може стати інформація про обсяг і напрям передачі інформації, що цікавить абонента і місцезнаходження адміністратора.

Тунельний режим дозволяє шифрувати всі пакети, включаючи заголовки мережевого рівня. Тунельний режим використовується, коли необхідно приховати обмін інформацією організації із зовнішнім світом. При цьому адресний простір в заголовку мережевого рівня пакетів, що використовують тунельний режим, вводиться брандмауером організації і не містить інформації про конкретного відправника пакета. Коли ви надсилаєте інформацію ззовні до локальної мережі вашої організації, мережева адреса брандмауера використовується як адреса призначення. Після того, як брандмауер розшифрував перший заголовок мережевого рівня, пакет надсилається одержувачу.

Асоціація безпеки (SA) - це з'єднання, яке надає Служби безпеки для трафіку, що надсилається через ВТС. Два комп'ютери по обидва боки від ВТ підтримують режими, протоколи, алгоритми та перемикачі, що використовуються ВТ. Кожен ВТ використовується лише в одному напрямку. Двосторонній зв'язок вимагає 2 Вт / год. кожен ВТ реалізує 1 режим і протокол, тому, якщо вам потрібно використовувати 2 протоколи (наприклад, AH або ESP) для 1 пакета, вам знадобиться 2 SA.

Політика безпеки зберігається в SPD (базі даних політики безпеки). SPD може вказувати одну з трьох дій: відмовитися від пакета, не використовувати IPSec для обробки пакета або використовувати IPSec для обробки пакета. В останньому випадку SPD також вкаже, який SA слід використовувати (якщо, звичайно, відповідний SA вже створений) або з якими параметрами повинен бути створений новий SA. ВТС також покаже, який SA слід використовувати (якщо, звичайно, відповідний SA вже створений).

IKE є протоколом обміну ключами за замовчуванням для ISAKMP і в даний час є єдиним ключем. IKE знаходиться на вершині ISAKMP і встановлює як ISAKMP SA, так і IPSec SA. IKE підтримує ряд різних примітивних функцій для використання в протоколі. Вибір хеш-функції можна здійснити між хеш-функцією і псевдовипадковою функцією (PRF).

IKE – це протокол, який пов'язує всі компоненти IPSec в єдине ціле. Зокрема, IKE гарантує початкову автентифікацію між учасниками, а також проводить обмін

секретними загальними ключами для цього процесу. Ключ сеансу можна задати вручну. У цьому випадку IKE не використовується. Однак цей варіант не рекомендується і використовується рідко. Традиційно IKE працює через UDP-порт 500.

З IKE з'явилася нова версія протоколу: IKEv2. Існують деякі відмінності в характеристиках та характеристиках цих протоколів. IKEv2 встановлює параметри підключення на одному етапі, що складається з декількох етапів. Процес IKE можна розділити на 2 етапи.

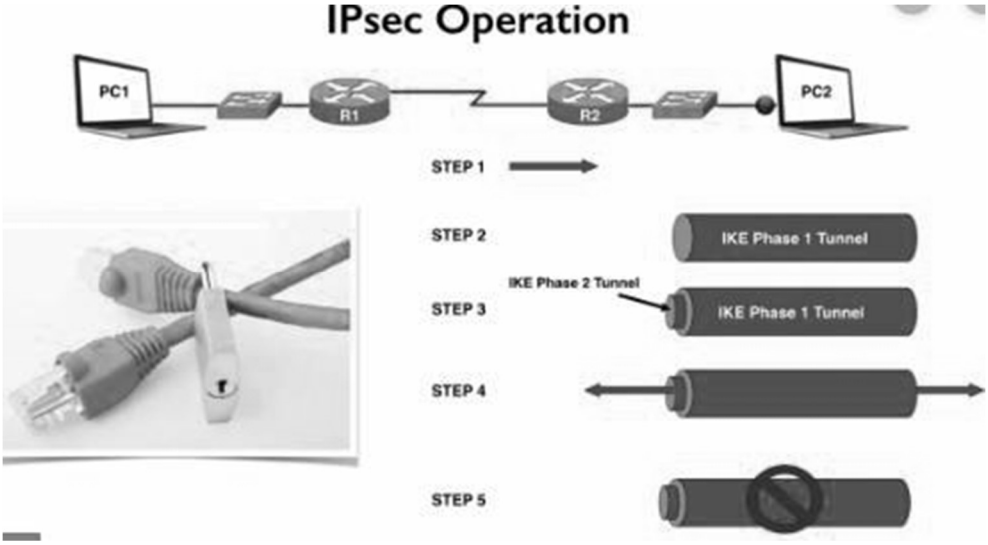

Рисунок 2.13 – Перша фаза IKE.

Перший етап. IKE створює захищений канал між 2 вузлами, що має назву IKE security association (IKE SA). Перший етап IKE може бути виконаний в одному з наступних 2 режимів:

- Базовий режим
- Агресивний режим

Базовий режим складається з трьох двосторонніх обмінів між відправником і одержувачем. При першому обміні алгоритми і хеш-функції, що використовуються для захисту з'єднань IKE, визначаються шляхом зіставлення IKE SA для кожного вузла. Вузли також автентифікують один одного, надсилаючи та перевіряючи набір псевдовипадкових чисел. Особистість іншої сторони перевіряється за допомогою

зашифрованої IP-адреси. В результаті базового режиму створюється захищений канал для подальших обмінів ISAKMP (цей протокол використовується для аутентифікації з'єднань вузлів, створення і управління SA, генерації ключів і запобігання DoS-атак). Вт.

В агресивному режимі менше обмінів і, отже, менше пакетів. Перше повідомлення містить практично всю інформацію, необхідну для встановлення IKE SA. Це відкритий ключ Діффі-Хеллмана для синхронізації пакетів, який підтверджується іншим учасником, ідентифікатором пакета. Покупець відправить назад все необхідне для завершення обміну. Перший вузол просто перевіряє з'єднання. З точки зору безпеки, агресивний режим слабший, оскільки учасники починають обмінюватися інформацією до встановлення безпечного каналу, Отже, можливе несанкціоноване втручання в дані. Однак цей режим працює швидше, ніж основний режим. Відповідно до стандарту IKE, будь-який додаток повинен підтримувати основний режим, і вкрай бажано підтримувати агресивний режим.

Другий етап IKE. На етапі є тільки 1 швидкий режим. Швидкий режим працює тільки після створення захищеного каналу на початковому етапі. Узгодьте загальну політику IPSec, отримайте спільний секретний ключ для алгоритму протоколу IPSec (AH або ESP) та встановіть IPSec SA.

Серійні номери захищають від атак повторної передачі. Крім того, швидкий режим використовується для відображення поточного IPSec SA і вибору нового SA після закінчення терміну служби SA. Стандартна висока швидкість

Мод використовує алгоритм Діффі-Хеллмана з самого першого етапу для оновлення загального секретного ключа.

Для псевдовипадкових функцій хеш-функції в даний час використовуються в конструкціях HMAC замість приватного PRF (HMAC вимагає криптографічної хеш-функції (скажімо, H) та приватного ключа K, щоб визначити, яка хеш-функція HMAC використовується для автентифікації повідомлення. H використовує процедуру стиснення, яка послідовно застосовується до набору блоків даних для стиснення даних. Нехай B - довжина таких блоків в байтах, а L (l <b) - довжина блоку, отриманого з хешу. Якщо ваша програма використовує довший ключ,

спочатку використовуйте h для хешування самого ключа і лише після цього використовуйте отриманий рядок байтів L як ключ у HMAC. В обох випадках мінімальна рекомендована довжина для k дорівнює l байтам.

SPD-це дуже гнучкий механізм управління, який дозволяє дуже добре керувати обробкою кожного пакета. Пакети класифікуються за великою кількістю полів, і SPD може перевірити деякі або всі поля, щоб визначити відповідні дії. Це дозволяє відправляти весь трафік між 2 машинами з використанням одного SA або окремого SA для кожної програми або кожного TCP-з'єднання.

Протокол ISAKMP визначає загальну структуру протоколу, що використовується для налаштування SA та виконання інших основних функцій управління. ISAKMP підтримує кілька областей інтерпретації (DOI), однією з яких є IPSec-DOI. І хоча ISAKMP не визначає точний протокол, він надає "будівельні блоки" для різних протоколів DOI та обміну ключами.

Протокол Oakley – це протокол ідентифікації ключів, який використовує алгоритм перемикання ключів Діффі-Хеллмана. Протокол Oakley підтримує чудову передову безпеку (PFS). Наявність PFS означає, що неможливо розшифрувати весь трафік, якщо ключі в системі скомпрометовані.

Протягом дек. з'єднання, яке називається Асоціацією безпеки (SA), має бути встановлено для ініціювання обміну даними між ними. Концепція BTC є основою і, по суті, суттю IPSec. Це пояснює, як сторони використовують цю послугу для забезпечення безпечного публічного використання. Оскільки з'єднання SA є одностороннім, для втягування сторін має бути встановлено 2 з'єднання. Крім того, оскільки використовується стандартний протокол Вт жовтня, можна реалізувати наступні точки захисту каналу, захищеного як SA, для відправки трафіку з усіх хостів, що взаємодіють по цьому каналу, і створити для нього генератор, що складається з великої кількості захищених асоціацій. Наприклад, в кожному TCP-з'єднанні це дозволяє вибрати необхідні відомості про захист. Встановлення зв'язку починається з взаємної перевірки сторін. За цим слідує вибір параметрів (виконується аутентифікація, шифрування, перевірка цільових даних) і необхідність передачі даних (AH або ESP). Потім певні алгоритми (наприклад,

шифрування, хеш-функції) вибираються з деяких можливих схем, деякі визначені (шифрування-DES, функція - MD5 або SHA-1), інші надаються виробником продукту за допомогою IPSec.

Обробляє вихідні пакети IPSec. Якщо відправляючий модуль IPSec визначає, що пакет пов'язаний з SA, призначеним для обробки ESP, втягується обробка. Залежно від його режиму (режим передачі або тунельний режим) оригінальний IP-пакет обробляється по-різному. У транспортному режимі вихідний модуль IPSec використовує Заголовок ESP (поля індексу параметрів безпеки та порядкового номера в заголовку) та термінал ESP (поле даних - решта полів заголовка, що слідують за даними корисного навантаження) для фільтрації протоколу верхнього рівня (наприклад, TCP або UDP). Для виконання процедури розгортання. У тунельному режимі IP-пакет створюється заголовком ESP і терміналом ESP (інкапсуляція), за яким слідує зовнішній IP-заголовок (вихідний IP se [8], потім виконується шифрування - в режимі передачі шифруються тільки повідомлення протоколу над нижчим рівнем. У тунельному режимі зашифровується весь вихідний IP-пакет (тобто все, що знаходиться після IP-заголовка вихідного пакета). Модуль IPSec, що витікає з реєстру SA, визначає алгоритм шифрування

І закритий ключ. Стандарт IPSec може використовуватися, коли алгоритми шифрування Triple DES, AES і Blowfish підтримуються обома сторонами.

В іншому випадку використовується DES, зазначений у RFC2405. Оскільки розмір відкритого тексту повинен бути кратним певній кількості байтів, наприклад, розмір блоку алгоритму блоку повинен бути додатково виконаний перед шифруванням.

І необхідне додавання зашифрованих повідомлень. Зашифроване повідомлення розміщується в полі даних корисного навантаження. Поле довжина заливки містить довжину заливки. Потім, як і у випадку Н, обчислюється порядковий номер. Потім обчислюється контрольна сума (ICV). На відміну від протоколу АН, він також враховує деякі поля IP при обчисленні контрольної суми-

У ESP обчислюється лише поле в пакеті ESP мінус поле ICV. Перед обчисленням контрольної суми вона заповнюється нулями. Як і протокол АН,

обчислювальний алгоритм ICV відправляє IPSec-модуль дізнається із записів про ВТ, з якими пов'язаний оброблений пакет.

Обробіть вхідні пакети. Після отримання пакета, що містить повідомлення протоколу ESP, модуль IPSec одержувача використовує IP-адресу одержувача, протокол безпеки (ESP) і каталог SPI [8] для пошуку відповідного захищеного віртуального з'єднання (ВТС) в SAD. Якщо відповідний SA не знайдено, пакет втирається. Знайдене безпечне віртуальне з'єднання (ВТС) вказує, чи використовується служба для запобігання повторної пересилання пакетів, тобто для перевірки поля порядкового номера. Якщо служба використовується, поле позначено. Для цього використовується метод розсувних вікон, як у випадку з ah. Лівий край вікна відповідає мінімальному порядковому номеру N правильного отриманого пакета. Пакет з полем порядкового номера містить значення, що починаються з N + 1 і закінчуються на N + W, і витягується правильно. Якщо виявиться, що отриманий пакет знаходиться на лівій межі вікна, він буде знищений. Потім, якщо існує служба аутентифікації, модуль втягування IPSec використовує алгоритм аутентифікації, витягнутий з регістру SA, для обчислення ICV з відповідного поля в отриманому пакеті і порівнює результат зі значенням ICV в поле Значення перевірки цілісності. Якщо обчислене значення ICV відповідає отриманому значенню, отриманий пакет вважається дійсним. Якщо перевірка дає негативний результат, вхідний пакет відкидається. Потім пакет розшифровується. Приймаючий модуль IPSec дізнається із запису SA, який алгоритм шифрування використовується, а також потай від нього ключ. Слід зазначити, що процедура перевірки і дешифрування контрольної суми може виконуватися не тільки послідовно, але і паралельно.

В останньому випадку процедура перевірки контрольної суми повинна бути завершена до процедури дешифрування, а процедура дешифрування також повинна бути зупинена у разі відмови перевірки ICV. Це дозволяє швидше виявляти пошкоджені пакети і підвищує рівень захисту від атак типу "відмова в обслуговуванні" (DoS-атаки). Потім декодоване повідомлення надсилається на основі наступного поля заголовка для подальшої обробки.

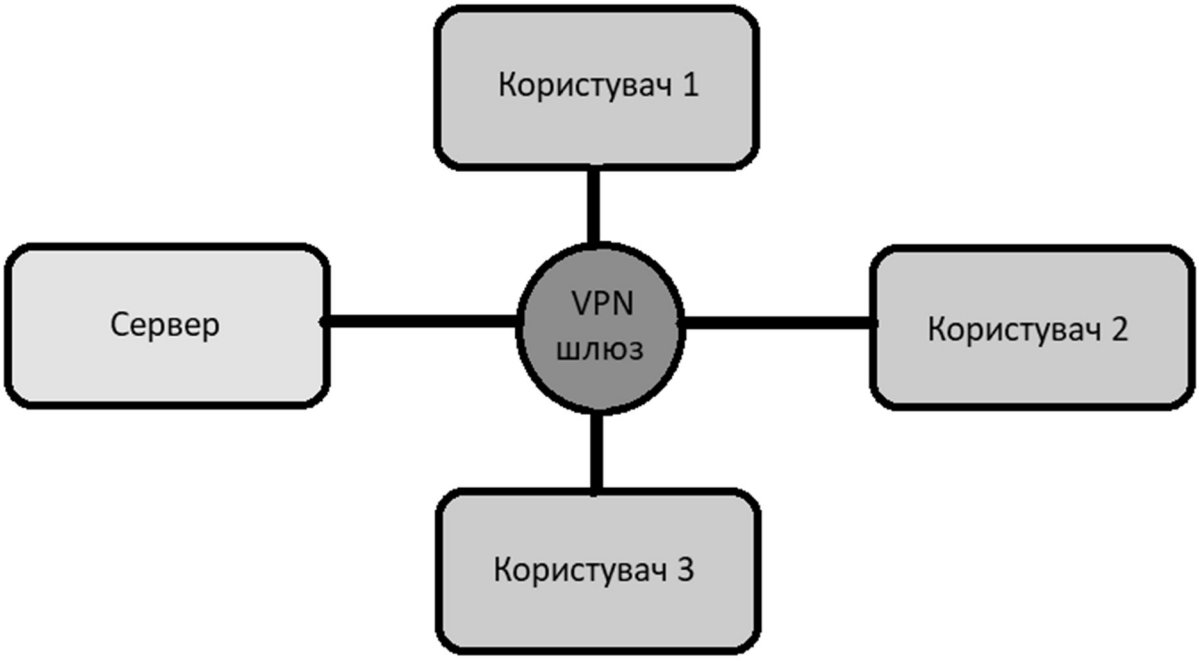

Рисунок 2.14 – Рознесення абонентів за допомогою шлюза.

Протокол IPSec в основному використовується для організації VPN-тунелів. У цьому випадку протоколи ESP та AH працюють у тунельному режимі. Крім того, ви можете використовувати протоколи для створення доступу до мережі, налаштовуючи політики безпеки певним чином. Метою брандмауера є моніторинг та фільтрація пакетів, що проходять через брандмауер, відповідно до зазначених правил. Встановлюється набір правил, і на екрані видно всі, хто проходить повз посилки. Якщо відправлені пакети підпадають під дію цих правил, брандмауер буде обробляти їх відповідним чином[14]. Наприклад, він може відхиляти певні пакети та переривати небезпечні з'єднання. Наприклад, ви можете вимкнути веб-трафік, налаштувавши відповідну політику безпеки. Для цього достатньо заборонити відправку пакетів, що містять повідомлення протоколів HTTP і HTTPS. IPSec також можна використовувати для захисту сервера - тому всі пакети відкидаються, крім тих, які необхідні для правильної роботи функції сервера. Наприклад, для веб-сервера, якщо ви використовуєте HTTPS, ви можете блокувати весь трафік, крім з'єднань через TCP-порт 80 або TCP-порт 443.

IPSec забезпечує безпечний доступ користувача до сервера тут. Коли ви використовуєте протокол ESP, усі запити на сервер та їх відповіді шифруються. Однак відкриті повідомлення надсилаються через шлюз VPN (у домені шифрування). Перетворення - це використання ipsec в режимі передачі для шифрування трафіку між файловим сервером і комп'ютером в локальній мережі або використання ipsec в тунельному режимі для з'єднання 2 офісів.

В даний час існує кілька різних пропозицій щодо інкапсуляції одного протоколу в інший. Для принципових цілей були запропоновані інші типи інкапсуляції для передачі IP по IP. Це дуже схоже на вищезазначену пропозицію, але з більш загальним протоколом GRE.

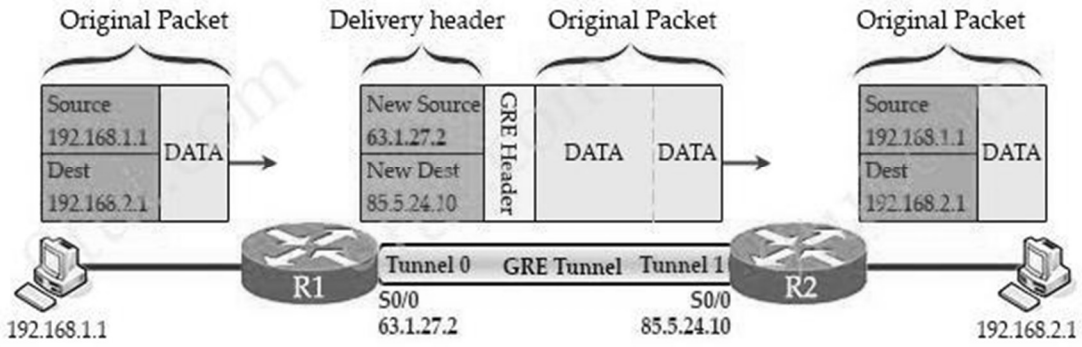

Рисунок 2.15 – Реалізація VPN за допомогою GRE.

Хоча я намагаюся бути більш загальним, у протоколі є багато нюансів. Отже, це твердження може не підходити для ситуацій, в яких описується конкретна інкапсуляція "X над Y". Це спроба створити простий загальний механізм, який зменшує проблеми інкапсуляції цього Протоколу до більш керованого розміру. У найпоширенішому випадку в системі є пакети, які потрібно інкапсулювати та доставити до місця призначення. Це називається пакетом корисного навантаження. Конфігурація корисного навантаження спочатку інкапсулюється в пакет GRE. Отримані пакети GRE інкапсулюються та передаються за іншими протоколами. Цей зовнішній протокол називається протоколом доставки.

Формат інкапсульованого пакету GRE виглядає наступним чином:

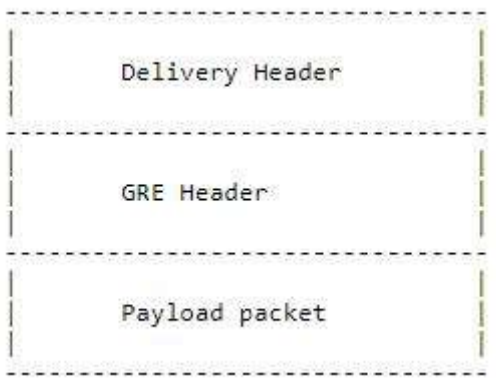

Рисунок 2.16 – Вигляд GRE пакета.

Заголовок пакету GRE має вигляд:

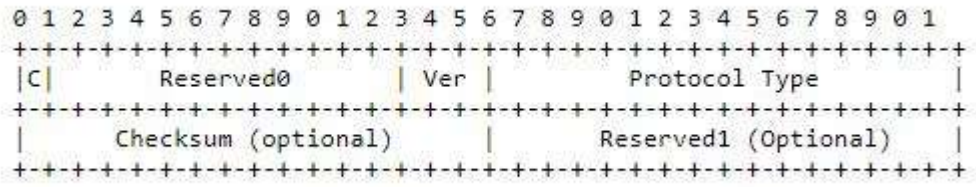

Рисунок 2.17 – Заголовок GRE пакета.

2.4 Принципи побудови структури мережі VPN

Існує кілька варіантів реалізації мережі VPN. Вибираючи рішення, Ви повинні враховувати фактори продуктивності інструменту побудови VPN. Наприклад, якщо маршрутизатор вже працює на межі Жовтневої потужності процесора, ви додаєте VPN-тунель і використовуєте шифрування/дешифрування інформації, вся мережа може перестати працювати через те, що цей маршрутизатор не справляється з навантаженням. Не кажучи вже про VPN-трафік із простим трафіком. Для створення VPN найкраще використовувати спеціалізоване обладнання, але якщо є обмеження за коштами, можна звернути увагу на чисто програмні рішення.

Основні параметри для створення VPN:

– Віддалений доступ до VPN

– VPN з сайту на сайт

VPN з віддаленим доступом-означає, що тунель організований між додатком, встановленим на комп'ютері клієнта (наприклад, Cisci Any Connect), і будь-яким авторизуючим пристроєм (в залежності від вибору вашої організації), яке діє як сервер і організовує з'єднання від різних клієнтів (таких як VPN-концентратори, маршрутизатори і Cisco ASA).).

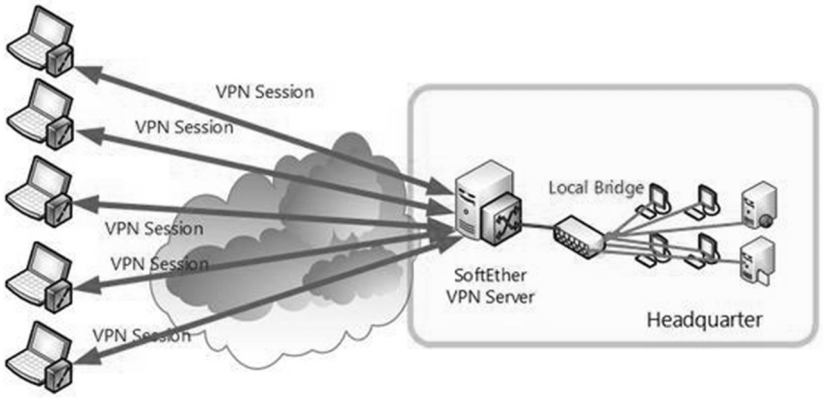

Рисунок 2.18 – Структура Remote access VPN

VPN з віддаленим доступом більш тісно пов'язані з додатками VPN, які використовуються для захисту особистих даних та даних користувачів. VPN з віддаленим доступом спочатку був представлений, щоб дозволити працівникам, які працюють у будь-якій точці світу, безпечно підключатися до віддаленої локальної мережі компанії. Віддалені працівники можуть отримати доступ до захищених ресурсів у локальній мережі компанії з будь-якої точки світу. Як і всі VPN, віддалені VPN призначені для забезпечення безпеки ваших даних. Коли ви використовуєте VPN з віддаленим доступом, пристрій віддаленого користувача відповідає за шифрування та дешифрування надісланих та отриманих даних.

Для віддаленого доступу VPN потрібен NAS (сервер мережевого доступу) або шлюз VPN для перевірки облікових даних пристрою, який намагається увійти в VPN. По суті, це nas, віддалений користувач, до якого вам потрібно підключитися, якщо ви хочете використовувати VPN для віддаленого доступу.

Як правило, віддалений доступ до VPN вимагає, щоб пристрій був оснащений клієнтським програмним забезпеченням. Це клієнтське програмне забезпечення VPN взаємодіє зі шлюзом VPN, аутентифікує користувача як віддаленого користувача і створює безпечний "віртуальний" тунель між локальною мережею і шлюзом.

Після створення тунелю дані, які ви надсилаєте з цього пристрою, інкапсулюються та шифруються VPN віддаленого доступу та надсилаються на шлюз VPN, розташований поблизу віддаленої локальної мережі. Потім шлюз VPN розшифровує трафік і передає дані в локальну мережу.

Захищений не тільки весь трафік, що надсилається через віртуальний тунель, але й весь трафік, який користувач отримує з локальної мережі (або своїх серверів), також захищений шляхом зворотного проходження через цей тунель. Шлюз VPN шифрує вхідний трафік (користувача) і перехоплюється клієнтом VPN.

VPN Site-To-Site – означає, що в схемі є 2 пристрої (наприклад, маршрутизатор), і між ними є тунель. У цьому випадку користувач не вимагає установки спеціального програмного забезпечення на задній панелі пристрою, в локальній мережі, на комп'ютері.

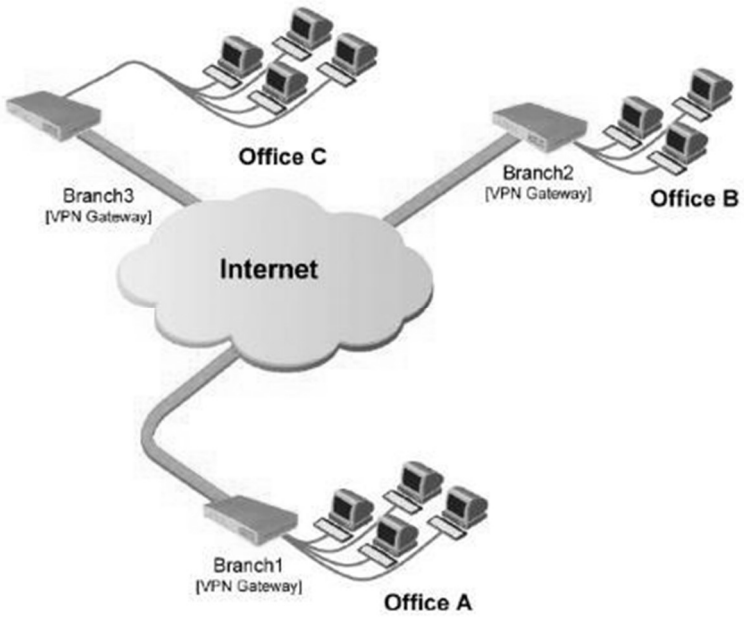

Рисунок 2.19 – Структура Site-to-site VPN

VPN з віддаленим доступом надійно підключає окремі пристрої. Використовуючи віддалену локальну мережу, VPN Site-To-Site дозволяє підключати 2 або більше локальних мереж у різних фізичних місцях. VPN від сайту до сайту використовують загальнодоступний Інтернет для розширення мережі компанії на кілька офісних приміщень.

Існує 2 поширені типи міжсайтових VPN: інтрамережа та екстрамережа. VPN на основі внутрішньої мережі використовувався для об'єднання декількох офісних локальних мереж в одну приватну мережу, пізніше названу глобальною мережею (WAN).1

З іншого боку, VPN на основі екстранети дозволяють компаніям використовувати загальнодоступний Інтернет для підключення своїх локальних мереж до мереж інших компаній, клієнтів або спільнот. Це дозволяє обмінюватися інформацією зі своїми діловими партнерами, зберігаючи при цьому локальну мережу (інтрамережу).

У міжсайтовій vpn шлюз VPN у віддаленій локальній мережі взаємодіє зі шлюзом в іншій локальній мережі (або мережі штаб-квартири) для створення безпечного тунелю. На відміну від VPN з віддаленим доступом, віддалені пристрої не потребують клієнта VPN і надсилають Звичайний трафік через шлюз VPN.

Якщо клієнт VPN недоступний, шлюз VPN відповідає за автентифікацію, шифрування та цілісність даних користувача та мережі. Шлюз приймає зашифровані дані, розшифровує їх, а потім надсилає дані на цільовий пристрій у мережі. Тунелі, створені службами VPN "сайт-сайт", дозволяють компаніям ділитися мережами та ресурсами між своїми розподіленими та віддаленими офісами незалежно від відстані. Пристрої в одній локальній мережі можуть взаємодіяти з пристроями в іншій локальній мережі так, ніби вони є частиною тієї ж мережі.

Існує 2 основних способи створення VPN між сайтами: Інтернет-VPN і MPLS (мультифокусна комутація) VPN.

2.5 Висновки

Суть полягає в тому, що існують різні реалізації мереж VPN, кожна з яких може забезпечити надійний захист даних, але існують відмінності в структурі та логіці роботи.

З точки зору забезпечення всебічного захисту корпоративних інформаційних систем від атак з відкритих мереж, VPN на моїй основі є найбільш підходящим варіантом. Сьогодні практично всі провідні виробники маршрутизаторів та інших мережевих пристроїв заявляють про підтримку різних протоколів VPN у своїх продуктах. Під контролем єдиної системи управління і аудиту об'єднання можливостей шлюзів DOE і VPN в одній точці є не тільки технічно грамотним, але і зручним рішенням для адміністрування.

3 МОДЕЛІ ТА ТЕХНОЛОГІЯ ПОБУДОВИ ЗАХИЩЕНИХ КОМУТОВАНИХ МЕРЕЖ

3.1 Модель захищеної комутованої мережі з використанням VPN

VPN на основі брандмауера. Брандмауери більшості виробників підтримують тунелювання та шифрування даних. Усі ці продукти базуються на тому, що трафік, що проходить через брандмауер, зашифрований. Модуль шифрування залежить від самого програмного забезпечення брандмауера. Недоліком цього методу є залежність продуктивності від обладнання, на якому працює брандмауер.

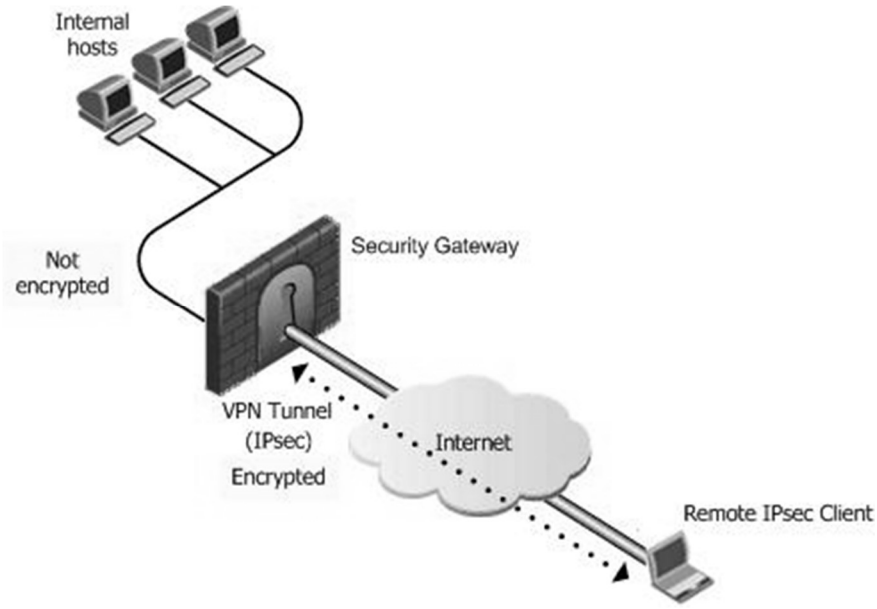

Рисунок 3.1 – VPN на основі брандмауерів

При використанні брандмауера на базі ПК слід пам'ятати, що таке рішення можна використовувати тільки для невеликого обсягу інформації, що передається по невеликій мережі.

Як приклад VPN на основі брандмауера, ви можете вказати брандмауер-1 у Check Point software technology. FairWall-1 використовує стандартний підхід на

основі IPSec для створення VPN. Трафік, що надходить у брандмауер, розшифровується, а потім застосовуються стандартні правила контролю доступу.

VPN на основі маршрутизатора. Інший спосіб створення VPN-це використання Програми для створення безпечного каналу маршрутизатора. Оскільки вся інформація в локальній мережі передається через маршрутизатор, рекомендується призначити цьому маршрутизатору завдання шифрування.

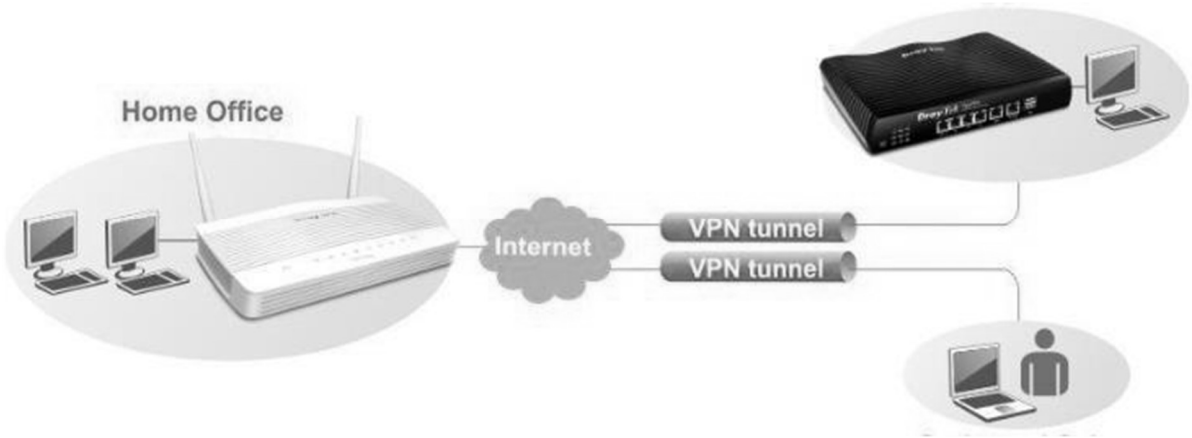

Рисунок 3.2 – VPN на основі маршрутизаторів

Прикладом пристрою для створення VPN на маршрутизаторі є пристрій Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3, маршрутизатори Cisco підтримують протоколи L2TP та IPSec. Окрім простого шифрування переданої інформації, Cisco також підтримує наступні функції жовтня:

Існують інші функції VPN, такі як Ідентифікація та обмін ключами під час налаштування тунельного з'єднання.

Ви можете використовувати додаткові модулі шифрування ESA для підвищення продуктивності вашого маршрутизатора. Крім того, Cisco Systems випустила спеціальний VPN-пристрій під назвою Cisco 1720vpn Access Router, призначений для встановлення в офісах малого бізнесу та великих організацій.

Програмне забезпечення VPN. Наступний підхід до створення VPN-це суто програмне рішення. При реалізації такого рішення найчастіше використовується спеціальне програмне забезпечення, що виконує роль проксі-сервера, що працює

на виділеному комп'ютері. Комп'ютер з таким програмним забезпеченням може знаходитися за брандмауером.

Рисунок 3.3 – VPN на основі програмного забезпечення

Прикладом такого рішення є програмне забезпечення Digital AltaVista Tunnel97. Під час використання цього програмного забезпечення клієнт підключається до сервера Tunnel97, автентифікується на цьому сервері та обмінюється ключами. Шифрування виконується на основі 56 - або 128-бітного ключа, отриманого в процесі встановлення з'єднання. Потім зашифрований пакет інкапсулюється в інші IP-пакети, що надсилаються на сервер. Крім того, програмне забезпечення значно підвищує безпеку з'єднання, створюючи новий ключ кожні 30 хвилин жовтня.

Чудова річ у AltaVista Tunnel97-це простота установки та експлуатації. Недоліками цієї системи можна вважати нестандартну архітектуру (власний алгоритм обміну ключами) і низьку продуктивність.

3.2. Топологія та особливості мережі VPN

Зазвичай, коли ви створюєте VPN, використовується двоточкове з'єднання з певним сервером або встановлюється тунель Ethernet з певним сервером, якому призначена певна підмережа для тунелю. У той же час сервер VPN виконує функцію маршрутизації та фільтрації трафіку для доступу до локальної мережі через VPN.

Навіть якщо ви використовуєте цей підхід, у вас є можливість фільтрувати трафік залежно від того, як ви підключаєтесь (наприклад, використовуючи різні фільтри для локальної мережі та віддалених користувачів), але вам більше не потрібно налаштовувати маршрутизацію, а віддалений комп'ютер безпосередньо підключений до локальної мережі та віддаленої мережі. машина підключена до локальної мережі. Ви можете переглядати ресурси і навіть використовувати широкосмугові пакети без додаткової настройки. Через такі VPN вони показують усі комп'ютери в локальній мережі Windows, усі доступні сервери xdmcp із трансляцією xdmcp.

VPN завжди складається з двоточкового каналу, також відомого як тунель. Тунелі створюються в незахищеній мережі, найчастіше в Інтернеті. Двоточкове з'єднання означає, що воно завжди встановлюється між 2 комп'ютерами, званими вузлами або одне деки. Кожен одноранг несе відповідальність за шифрування даних перед входом у тунель та розшифровку цих даних після виходу з тунелю.

VPN жовтень груд завжди налаштовується між 2 точками, але кожен одноранговий вузол може налаштувати додатковий тунель з іншими вузлами. Наприклад, якщо 3 віддалені станції повинні бути підключені до одного офісу, в цьому офісі створюються 3 окремі тунелі VPN. У всіх тунелях однорангові вузли на стороні офісу можуть бути однаковими. Це можливо, оскільки вузли можуть шифрувати та розшифровувати дані, а не всю мережу, як показано на рис.3.4:

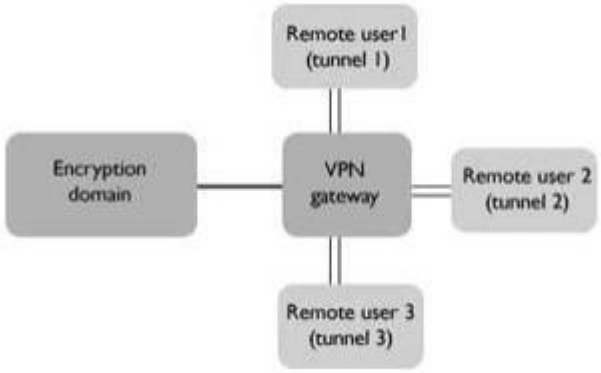

Рисунок 3.4 – Рознесення користувачів за допомогою шлюза

У цьому випадку вузол VPN називається шлюзом VPN, а Мережа за ним-доменом шифрування. Використання шлюзу корисно з кількох причин. По-перше, всі користувачі повинні пройти через один пристрій. Це спрощує завдання управління політикою безпеки та моніторингу вхідного та вихідного мережевого трафіку. По-друге, персональний тунель, що веде до кожної робочої станції, до якої користувач повинен отримати доступ, якщо є дуже швидкий шлюз (оскільки тунель є двоточковим каналом), користувач підключається до шлюзу, а потім користувач відкриває доступ до мережі (область шифрування). Ви можете це зробити.

Цікаво відзначити, що саме шифрування в домені не зашифровано. Це пов'язано з тим, що ця частина мережі вважається безпечною і знаходиться під прямим контролем, на відміну від інтернету. Це також вірно, якщо ви використовуєте шлюз VPN для підключення свого офісу. Це шифрує лише інформацію, що передається через небезпечні канали між офісами. розподіляє дані, що передаються по небезпечних каналах між офісами. На наступному рисунку показано VPN, що з'єднує 2 офіси.

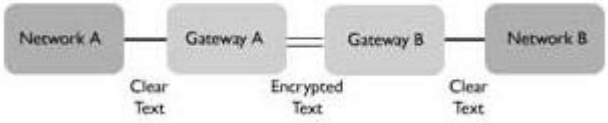

Рисунок 3.5 – VPN на основі незахищеної мережі.

Мережа a вважається областю шифрування VPN-шлюзу a, A мережа b вважається областю шифрування VPN-шлюзу B відповідно. Коли користувач мережі A висловлює бажання відправити дані в мережу b, VPN-шлюз a шифрує їх і відправляє через VPN-тунель. Шлюз VPN B розшифровує інформацію та надсилає її одержувачу в мережі B.

Використовуйте режим тунелювання, коли мережеве з'єднання забезпечується шлюзом VPN. Це означає, що після шифрування всього пакета IP додається новий заголовок IP. Новий заголовок містить IP-адреси 2 VPN-шлюзів і відображається, коли їх перехоплює Датчик пакетів. Я встановив оригінальний комп'ютер першого домену шифрування та 2. Неможливо ідентифікувати комп'ютер-одержувач домену.

За допомогою тунелювання пакети даних передаються через загальнодоступну мережу через звичайний канал. Між кожною парою даних "відправник-одержувач" встановлюється своєрідний тунель - безпечне логічне з'єднання, яке дозволяє інкапсулювати дані з одного протоколу в інший у пакетах. Основним компонентом є тунель:

- Ініціатор;
- Мережеві маршрутизатори;
- Тунельний перемикач;
- 1 або більше термінаторів тунелів.

Сам по собі принцип роботи VPN суперечить основним мережевим технологіям і протоколам. Наприклад, під час налаштування підключення віддаленого доступу клієнт надсилає серверу потік стандартних пакетів протоколів PPP. Для віртуальних орендованих ліній між локальними мережами маршрутизатор інкапсулює пакети PPP. Однак принципово новим моментом є те, що пакети передаються через захищений тунель, організований у загальнодоступній мережі. Тунелювання дозволяє передавати пакети з одного протоколу в логічне середовище за допомогою іншого протоколу. В результаті стає можливим вирішити проблему взаємодії між декількома різними типами мереж,

починаючи з необхідності забезпечення цілісності та конфіденційності даних і закінчуючи подоланням невідповідностей у зовнішніх протоколах або схемах адресації.

Існуюча мережева інфраструктура вашої компанії може бути підготовлена до використання VPN, використовуючи як програмне, так і апаратне забезпечення. Організацію віртуальної приватної мережі можна порівняти з прокладанням кабелю по глобальній мережі.

Як правило, пряме з'єднання встановлюється між віддаленим маршрутизатором і кінцевим пристроєм тунелю по протоколу PPP.

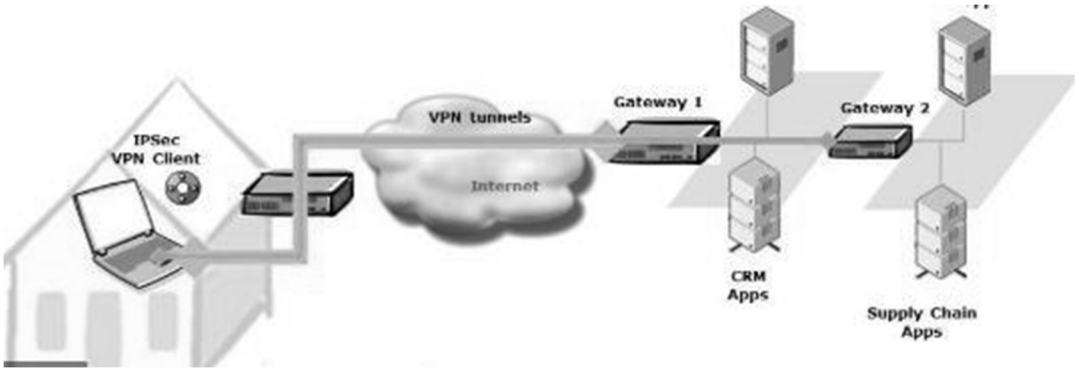

Рисунок 3.6 – Типове використання VPN за допомогою VPN агента

На рисунку показано загальне використання VPN, які дозволяють віддаленим користувачам ноутбуків та користувачам, які працюють вдома, отримувати доступ до офісної мережі. Щоб цей план працював, користувач повинен мати встановлене клієнтське програмне забезпечення VPN. За сценарієм використовується тунельний режим, оскільки користувач хоче отримати доступ до ресурсів у домені, а не до самого шлюзу. Єдиний випадок, коли ввімкнено режим передачі, - це коли один комп'ютер повинен безпосередньо отримати доступ до іншого.

Існує безліч варіантів VPN-шлюзів і VPN-клієнтів. Це може бути апаратне або програмне забезпечення, встановлене на вашому маршрутизаторі або ПК. Наприклад, ОС FreeBSD постачається з програмним забезпеченням для створення шлюзів VPN та налаштування клієнтів VPN. Існує також рішення VPN для програмного забезпечення Microsoft.

Залежно від програмного забезпечення, яке ви використовуєте, усі VPN працюють за такими принципами::

1. Кожен вузол ідентифікує один одного перед створенням тунелю, щоб переконатися, що зашифровані дані надсилаються на правильний вузол.

2. Обидва вузли вимагають попередньо налаштованої політики та визначають протоколи, які можна використовувати для шифрування та забезпечення цілісності даних.

3. Вузол порівнює політику таким чином, щоб вона відповідала використовуваному алгоритму;

Якщо це не вдається, тунель не встановлюється.

4.As після узгодження алгоритму створюється ключ, який використовується для шифрування / дешифрування даних за допомогою симетричного алгоритму.

3.3 Висновки

Реалізація мережі VPN здійснюється з використанням спеціального набору програмного і апаратного забезпечення. Ця програма забезпечує високу продуктивність і, в принципі, високий ступінь безпеки.

У вигляді програмних рішень персональні комп'ютери використовуються в спеціальному програмному забезпеченні, інтегрованих рішеннях, що забезпечують функції VPN, а функції VPN забезпечують комплекс, що вирішує проблеми фільтрації мережевого трафіку, організації брандмауерів і забезпечення якості обслуговування.

4 РЕАЛІЗАЦІЯ ЗАХИЩЕНИХ КОМУТОВАНИХ МЕРЕЖ З ВИКОРИСТАННЯМ VPN

4.1 Модель захищеної мережі з віддаленим доступом

Для реалізації моделі скористаємось фрагментом мережі організації. На рис. 4.1 наведена топологія мережі, що забезпечує захищений доступ до серверів компанії, які розташовані у одному місті, для співробітників віддалених офісів у інших містах. Для реалізації цієї задачі був організований тунель між офісами, що побудований на основі IPsec VPN. Доступ до серверів обмежено за технологією Client SSL VPN (Cisco AnyConnnect).

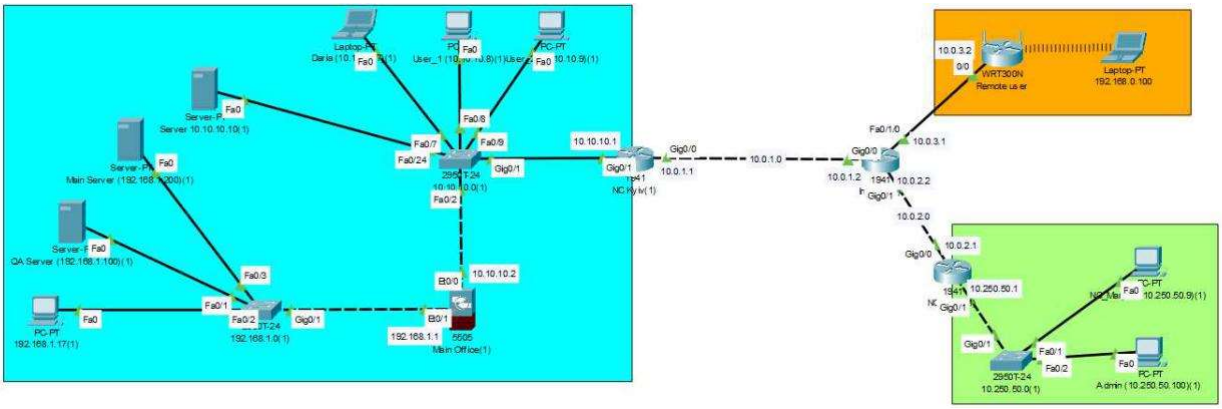

Рисунок 4.1 – Схема IPsec VPN та SSL VPN для віддаленого офісу та віддаленого співробітника

У додатку В наведено лістинги конфігураційних файлів для основних пристроїв. Використання цих команд підходить для серверів ASA та AAA, до яких звертається ASA, коли працівник компанії намагається підключитися до захищеного сервера за допомогою Cisco AnyConnect, тоді як тунель IPSec встановлюється за допомогою конфігурації маршрутизатора обмеження корпоративного офісу.

4.2 Реалізація технології IPsec VPN та SSL VPN для віддаленого офісу за допомогою Cisco Packet Tracer

Модель віддаленого доступу була реалізована за допомогою Cisco Packet Tracer. Але враховуючи особливості та обмеження даної програми, насамперед додавання SSL клієнта, неможливо показати Client SSL (Anyconnect VPN), а також IPsec VPN для віддаленого офісу та SSL VPN для віддаленого співробітника в одній схемі. Тому було побудовано дві моделі:

– IPsec VPN та SSL VPN для віддаленого офісу
– Clientless SSL VPN для віддаленого співробітника

На рис. 4.2 наведена схема захищеного доступу до серверів компанії, які розташовані у одному місті, для співробітників віддалених офісів у інших містах. Тунель між офісами побудований на основі IPsec VPN. Доступ до серверів обмежується за технологією SSL VPN.

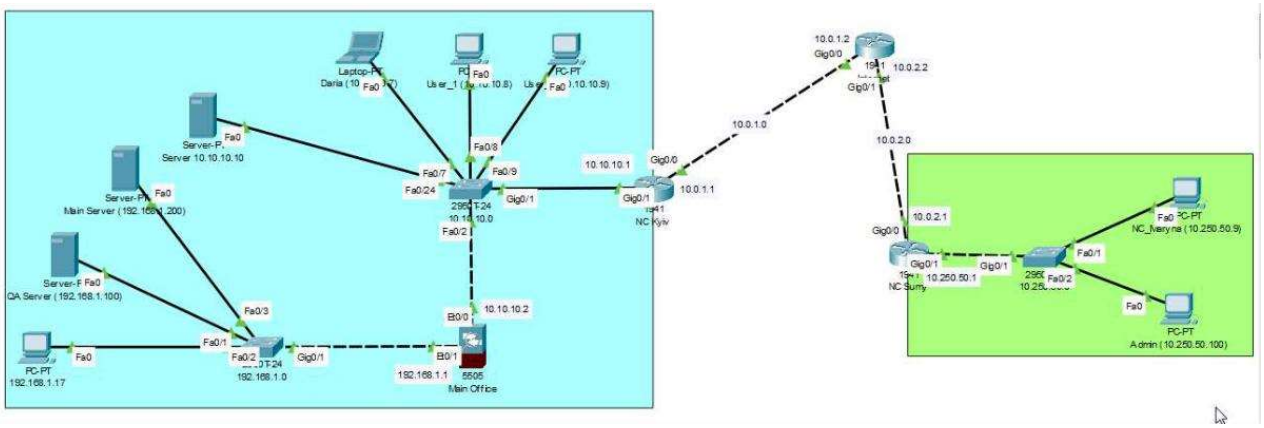

Рисунок 4.2 – Схема IPsec VPN та SSL VPN для віддаленого офісу

В таблицях 4.1 та 4.2 представлено IP-адреси для основних пристроїв та права доступу користувачів до ресурсів мережі.

Таблиця 4.1 – IP-адреси пристроїв

Пристрій	Інтерфейс	IP - адреса	Мережна маска	Шлюз
Filia_1 router	g0/1	10.101.50.1	255.255.255.0	N/A
	g0/0	10.1.2.1	255.255.255.0	N/A
Internet router	g0/1	10.1.2.2	255.0.0.0	N/A
	g0/0	10.1.1.2	255.0.0.0	N/A
Filia_2 router	g0/1	10.102.10.1	255.0.0.0	N/A
	g0/0	10.1.1.1	255.0.0.0	N/A
Main office ASA	vlan 1	192.168.1.1	255.255.255.0	N/A
	vlan 2	10.100.10.2	255.255.255.0	N/A
PC NC_User_1	Fa0	10.250.50.9	255.0.0.0	10.250.50.1
PC Admin	Fa0	10.250.50.100	255.0.0.0	10.250.50.1
PC-PT	Fa0	192.168.1.17	255.255.255.0	192.168.1.1
Laptop PT-User_2	Fa0	10.10.10.7	255.255.255.0	10.10.10.1
PC-PT User1	Fa0	10.10.10.8	255.255.255.0	10.10.10.1
PC-PT User2	Fa0	10.10.10.9	255.255.255.0	10.10.10.1

Таблиця 4.2 – Права доступу користувачів до серверів

Обліковий запис користувача	Пароль	Ресурс для доступу
Admin	999777555	Main Server
User_1	123123123	Main Server
User_2	12345678	N/A

Для вирішення поставленої задачі були виконані наступні налаштування на пристроях мережі.

Конфігурація IPsec на Filia_1 router:

Configure terminal

Задаємо IP адреси інтерфейсам: interface g0/1

ip address 10.250.50.1 255.255.255.0 no shut

interface g0/0

ip address 10.0.2.1 255.255.255.0 no shut

Додаємо на роутер необхідний модуль безпеки: license boot module c1900 technology-package securityk9 exit

Зберігаємо налаштування:

copy running-config startup-config

reload

show version

Configure terminal

Налаштовуємо IPSec тунель:

access-list 100 permit ip 10.250.50.0 0.0.0.255 10.10.10.0 0.0.0.255

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

exit

crypto isakmp key password address 10.0.1.1

crypto ipsec transform-set NC_Sumy-to-NC_Kyiv esp-aes 256 esp-sha-hmac

crypto map IPSEC 10 ipsec-isakmp

set peer 10.0.1.1

set pfs group5

set security-association lifetime seconds 86400 set transform-set NC_Sumy-to-NC_Kyiv match address 100

Перевіряємо роботу сконфігурованого IPSec шлюзу (рис. 4.3): interface GigabitEthernet0/0

crypto map IPSEC

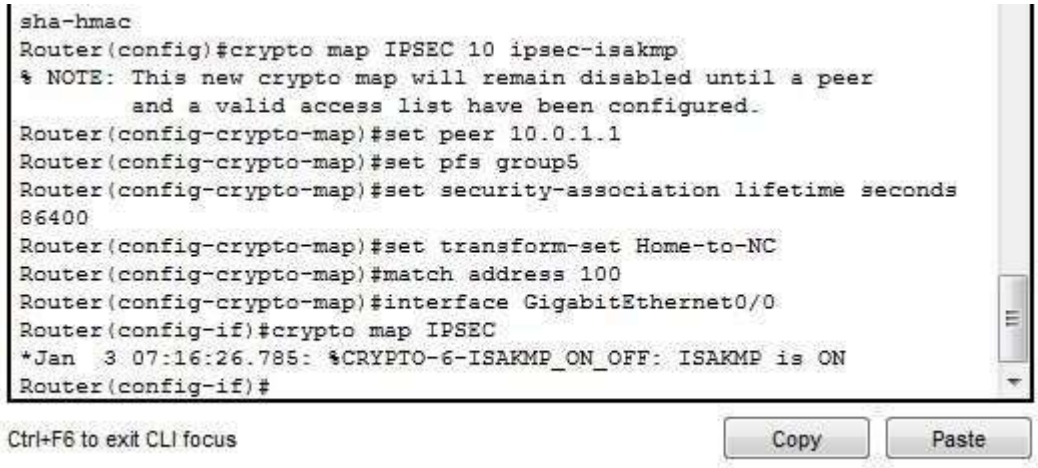

Рисунок 4.3 – Перевірка стану IPSec на Filia_1 router

Конфігуарція Internet router:

Задаємо IP адреси інтерфейсам: Configure terminal

interface g0/1 ip address 10.0.2.2 255.0.0.0 no shut

interface g0/0 ip address 10.0.1.2 255.0.0.0 no shut

Конфігурація Ip sec на Filia_2 router:

Задаємо IP адреси інтерфейсам: Configure terminal

interface g0/1 ip address 10.10.10.1 255.0.0.0

no shut

interface g0/0 ip address 10.0.1.1 255.0.0.0

no shut

conf t

Додаємо на роутері необхідний модуль безпеки: license boot module c1900 technology-package securityk9 exit

Зберігаємо налаштування (рис.4.4):

copy running-config startup-config

reload

show version

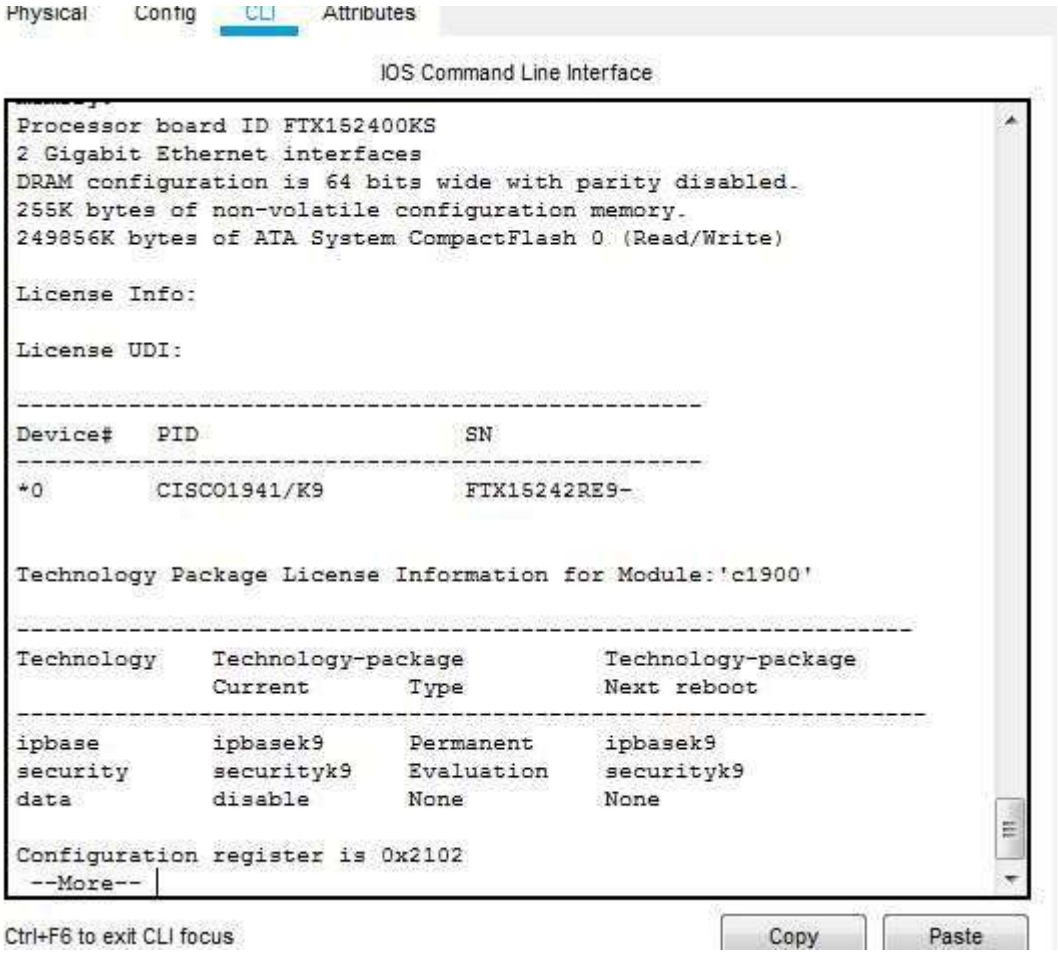

Рисунок 4.4 – Перевірка підключення додаткових модулів безпеки

Configure terminal

Налаштовуємо IPSec тунель:

access-list 100 permit ip 10.10.10.0 0.0.0.255 10.250.50.0 0.0.0.255

crypto isakmp policy 10 encryption aes 256 authentication pre-share group 5 exit

crypto isakmp key password address 10.0.2.1

crypto ipsec transform-set NC_Kyiv-to-Home esp-aes 256 esp-sha-hmac

crypto map IPSEC 10 ipsec-isakmp

set peer 10.0.2.1

set pfs group5

set security-association lifetime seconds 86400 set transform-set NC-to-Home match address 100

Перевіряємо роботу сконфігурованого IPSec шлюзу (рис. 4.5): interface GigabitEthernet0/0

crypto map IPSEC

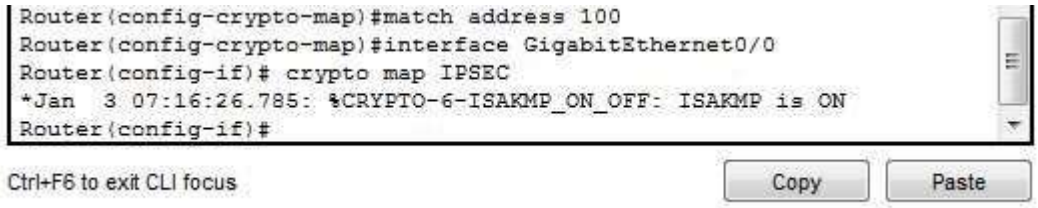

Рисунок 4.5 – Перевірка стану IPSec на Filia_2 router

Конфігурація Main office ASA:

Configure terminal

Встановлюємо IP адреси Vlan-ів: Hostname ASA1

Interface vlan 1

Nameif inside

Security-level 100

Ip address 192.168.1.1 255.255.255.0

exit

Interface vlan 2

Nameif outside

Security-level 0

Ip address 10.10.10.2 255.255.255.0

Exit

Вмикаємо функцію Webvpn для роботи віддалених користувачів:

Webvpn Enable outside Object network lan

Subnet 192.168.1.0 255.255.255.0 Exit

Додаємо дані користувачів:

username Admin password 999777555

username User_1 password 123123123

username User_2 password 12345678

Конфігуруємо адреси серверів (рис. 4.6):

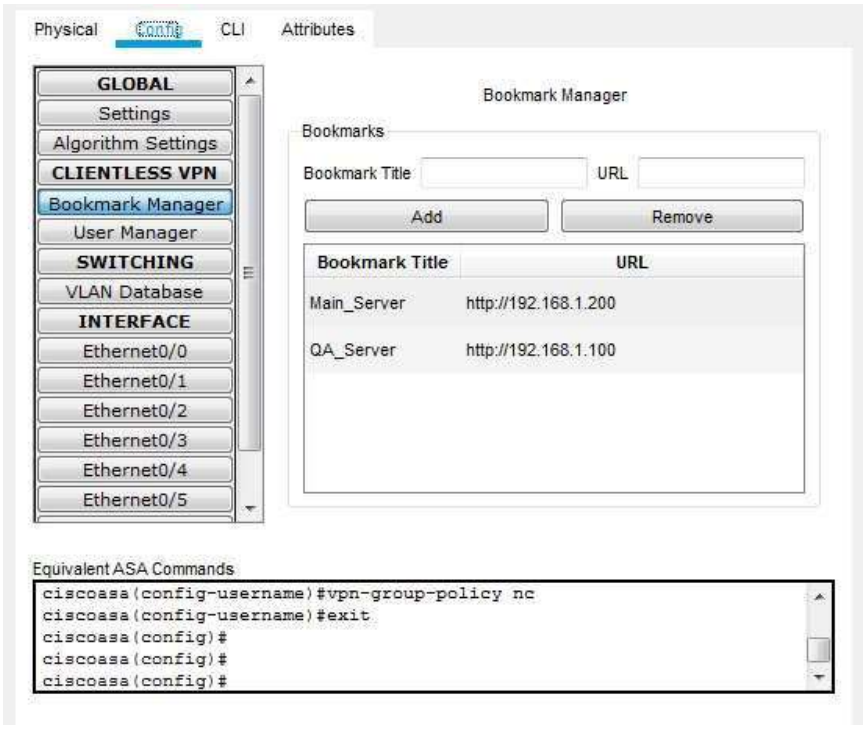

Рисунок 4.6 – Налаштування адрес серверів на Main office ASA

Налаштовуємо доступ для користувачів (рис. 4.7):

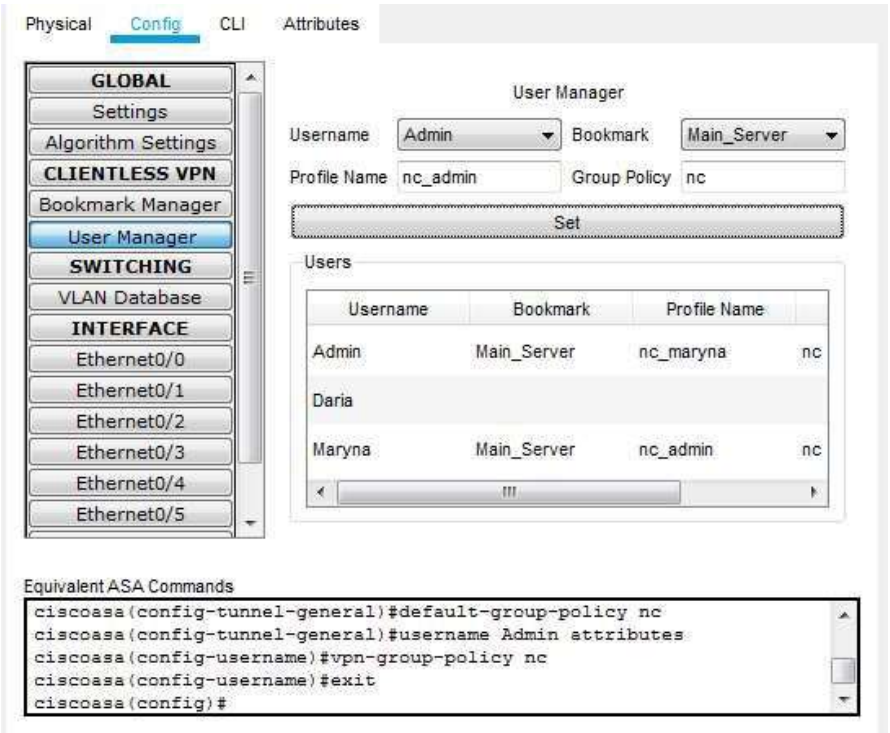

Рисунок 4.7 – Налаштування доступу для користувачів на Main office ASA

Перевіримо шифрування трафіку за допомогою команди show crypto ipsec sa (рис. 4.8):

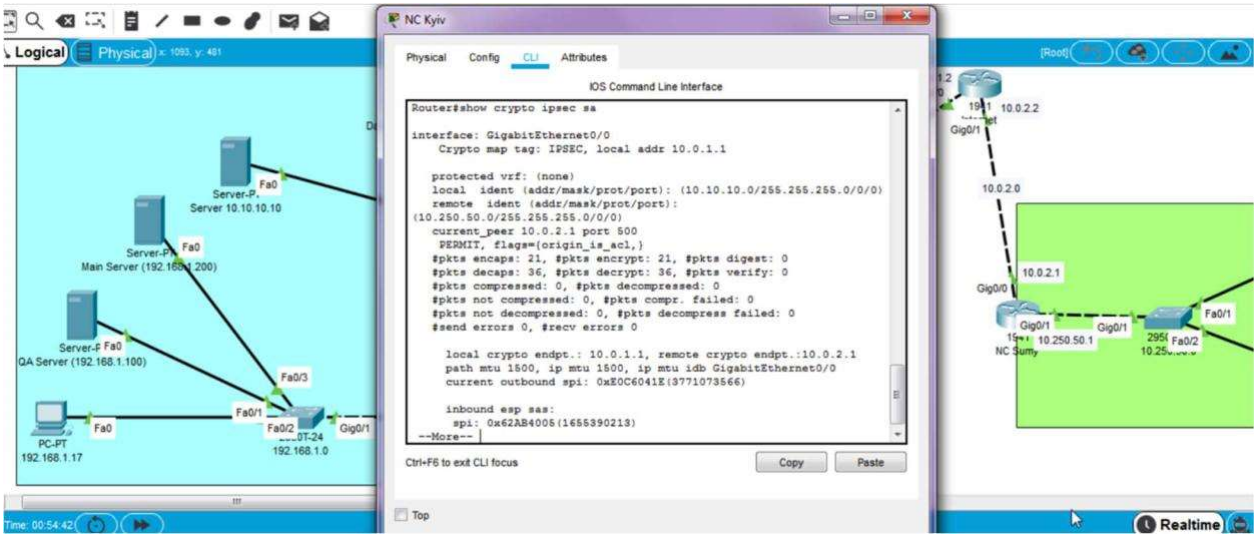

Рисунок 4.8 – Перевірка шифрування трафіку за технологією IPsec

Після налаштування IPsec та SLL можна протестувати доступи користувачів до серверів. Користувач User_1 має доступ до Server 10.10.10.10 без необхідності введення пароля, тільки через IPsec (рис. 4.9).

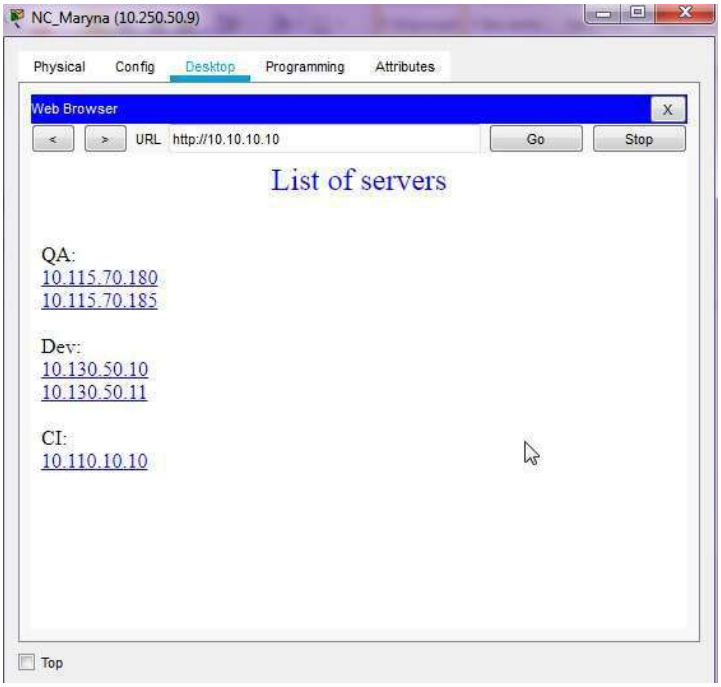

Рисунок 4.9 – Доступні сервери для користувача User_1

Але при намаганні зайти на сервери за межами ASA, система запитає вже логін та пароль для входу (рис. 4.10). При цьому користувач зможе зайти лише на ті сервери, до яких у нього є доступ (рис. 4.11).

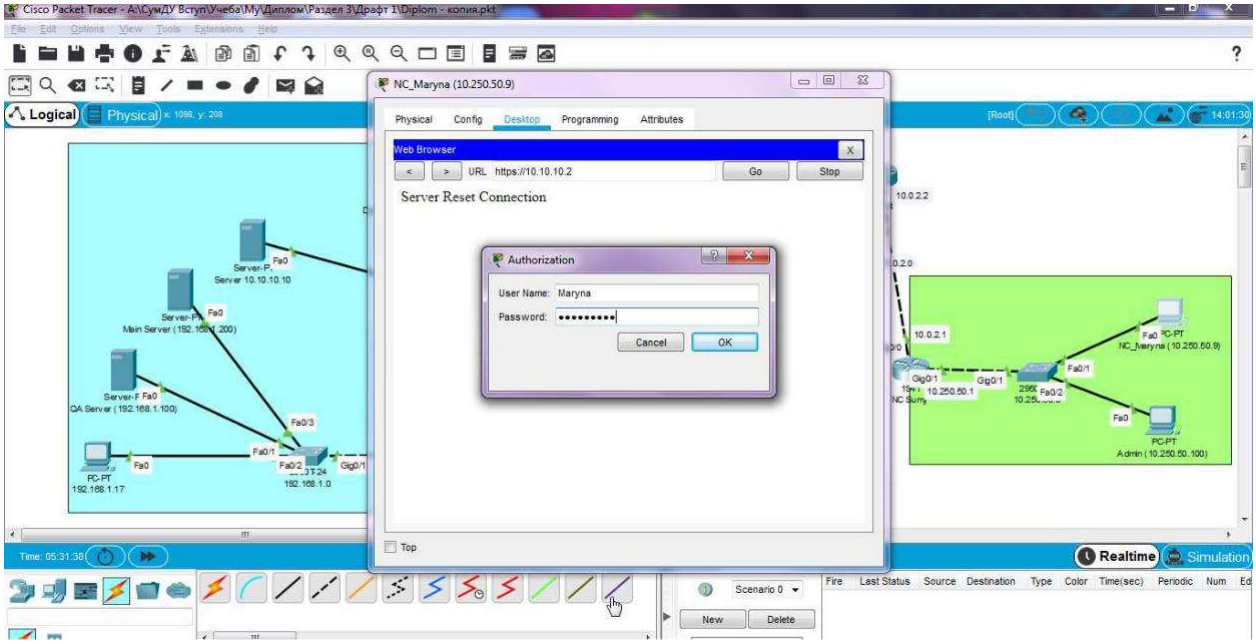

Рисунок 4.10 – Вікно авторизації користувача

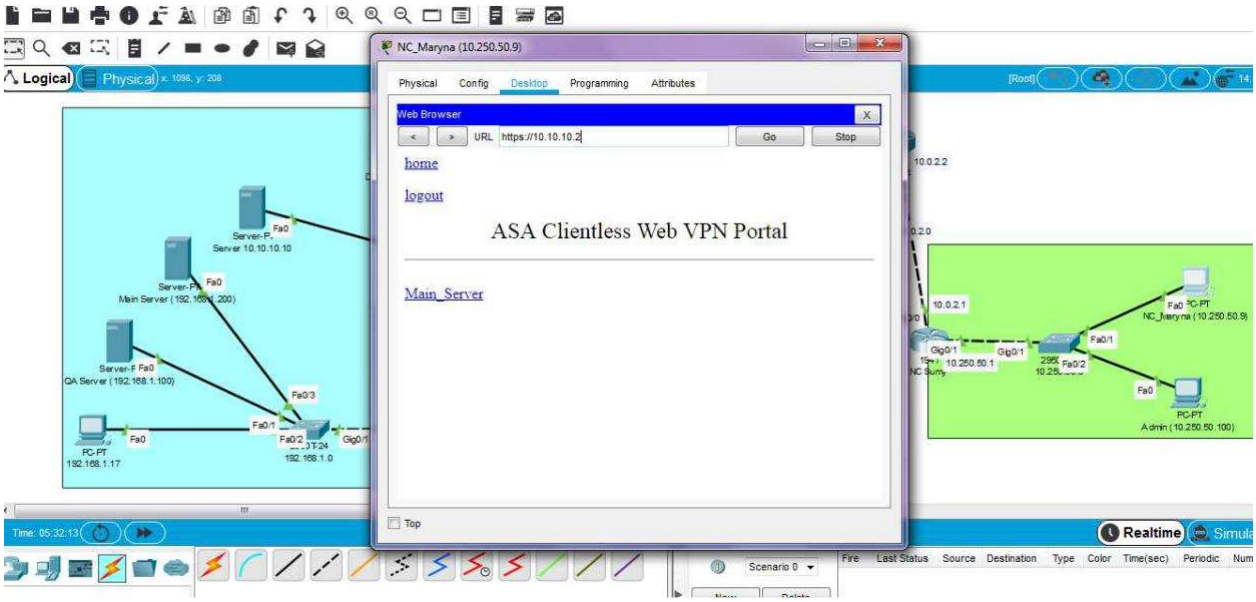

Рисунок 4.11 – Доступні сервери для користувача User_1

Користувач User_2 немає доступу на серверів за межами ASA (рис. 4.12, рис.4.13):

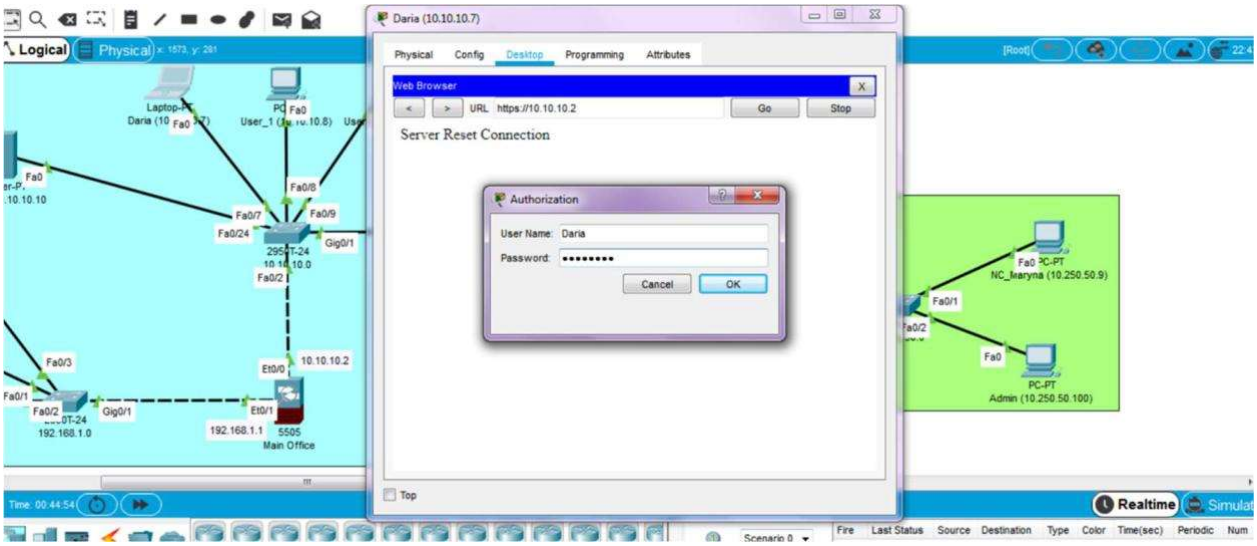

Рисунок 4.12 – Вікно авторизації користувача

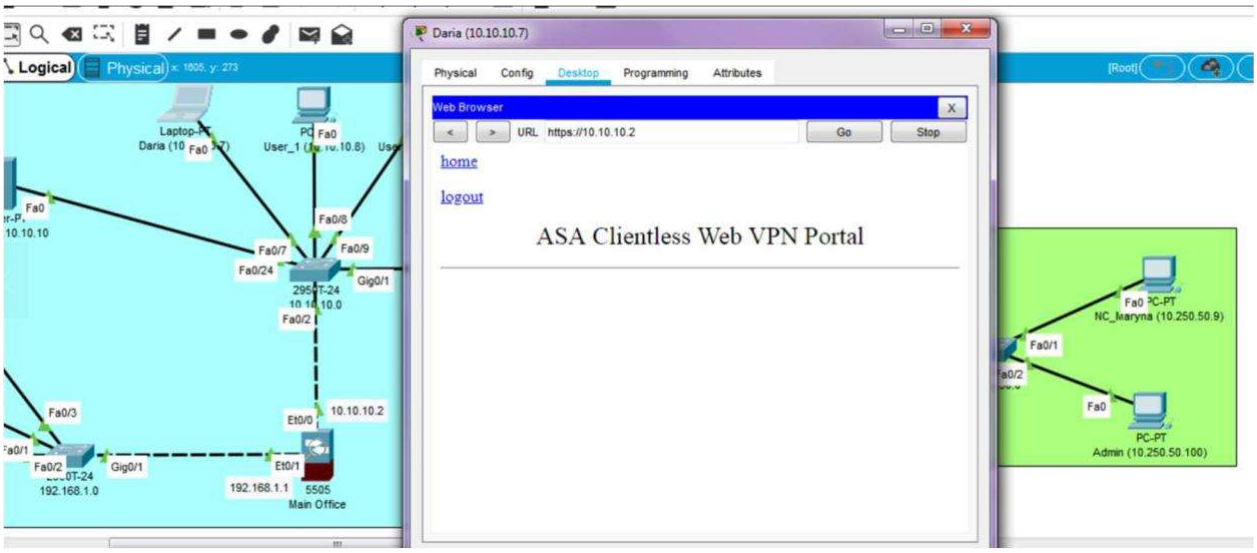

Рисунок 4.13 – Доступні сервери для користувача User_2

Користувач PC-PT має доступ до всіх серверів за межами ASA (рис. 4.14):

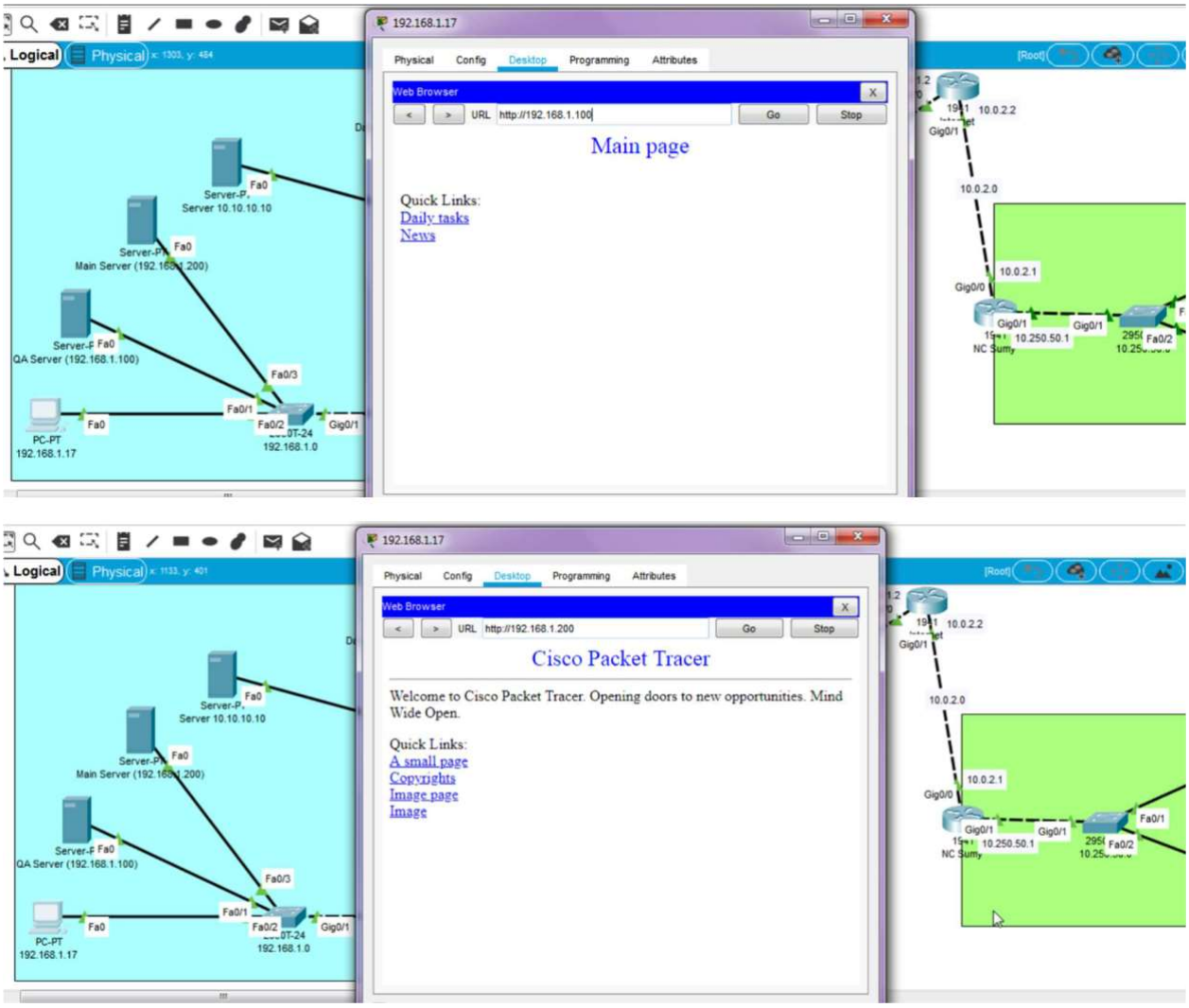

Рисунок 4.14 – Доступні сервери для користувача PC-PT

4.3 Реалізація технології Clientless SSL VPN для віддаленого співробітника за допомогою Cisco Packet Tracer

На рис. 4.15 наведена схема захищеного доступу до серверів офісу в для віддаленого співробітник. Доступ до серверів обмежується за технологією SSL VPN.

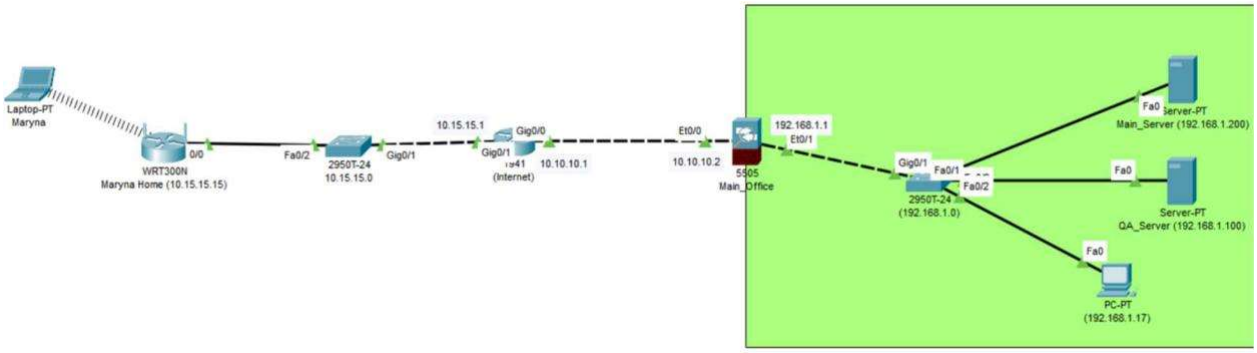

Рисунок 4.15 – Схема SSL VPN для віддаленого співробітника

У табл. 4.3 та табл. 4.4 наведено IP адреси пристроїв та права доступу користувачів до серверів

Таблиця 4.3 – IP адреси пристроїв

Пристрій	Інтерфейс	IP - адреса	Мережна маска	Шлюз
(Internet) router	g0/1	10.15.15.1	255.0.0.0	N/A
	g0/0	10.10.10.1	255.0.0.0	N/A
Main office ASA	vlan 1	192.168.1.1	255.255.255.0	N/A
	vlan 2	10.10.10.2	255.255.255.0	N/A
User_1 Home router	0/0	10.15.15.15	255.255.255.0	10.15.15.1
Laptop User_1	Fa0	192.168.0.100	255.255.255.0	192.168.0.1

Таблиця 4.4 – Права доступу користувачів до серверів

Обліковий запис користувача	Пароль	Ресурс для доступу
User_1	123123123	Main Server

Для вирішення поставленої задачі були виконані наступні налаштування на пристроях мережі.

Конфігурація (Internet) router:

Налаштовуємо IP адреси для інтерфейсів: Configure terminal

interface g0/1 ip address 10.15.15.1 255.0.0.0 no shut

interface g0/0 ip address 10.10.10.1 255.0.0.0 no shut

Конфігурація Main office ASA: Configure terminal

Налаштовуємо IP адреси для Vlan-ів: Hostname ASA1

Interface vlan 1 Nameif inside Security-level 100

Ip address 192.168.1.1 255.255.255.0 exit

Interface vlan 2 Nameif outside Security-level 0

Ip address 10.10.10.2 255.255.255.0 Exit

Вмикаємо функцію Webvpn для віддалених користувачів:

Webvpn Enable outside Object network lan

Subnet 192.168.1.0 255.255.255.0

Exit

Додаємо дані користувачів: username User_1 password 123123123

Задаємо конфігурацію серверів (рис. 4.16):

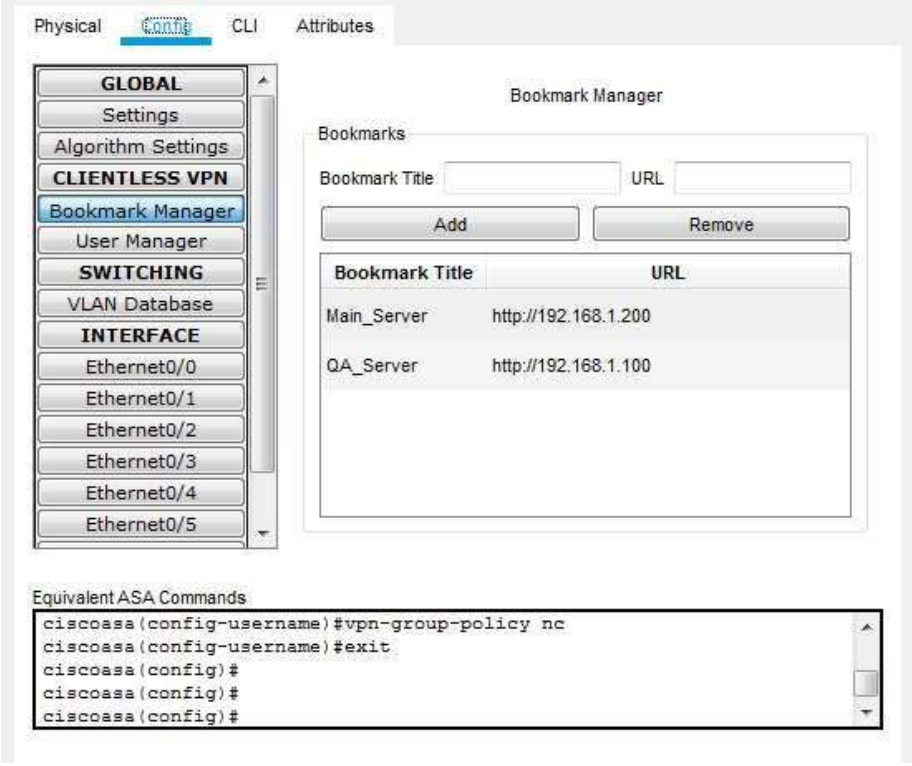

Рисунок 4.16 – Налаштування адрес серверів на Main office ASA

Конфігуруємо доступ для користувачів (рис. 4.17):

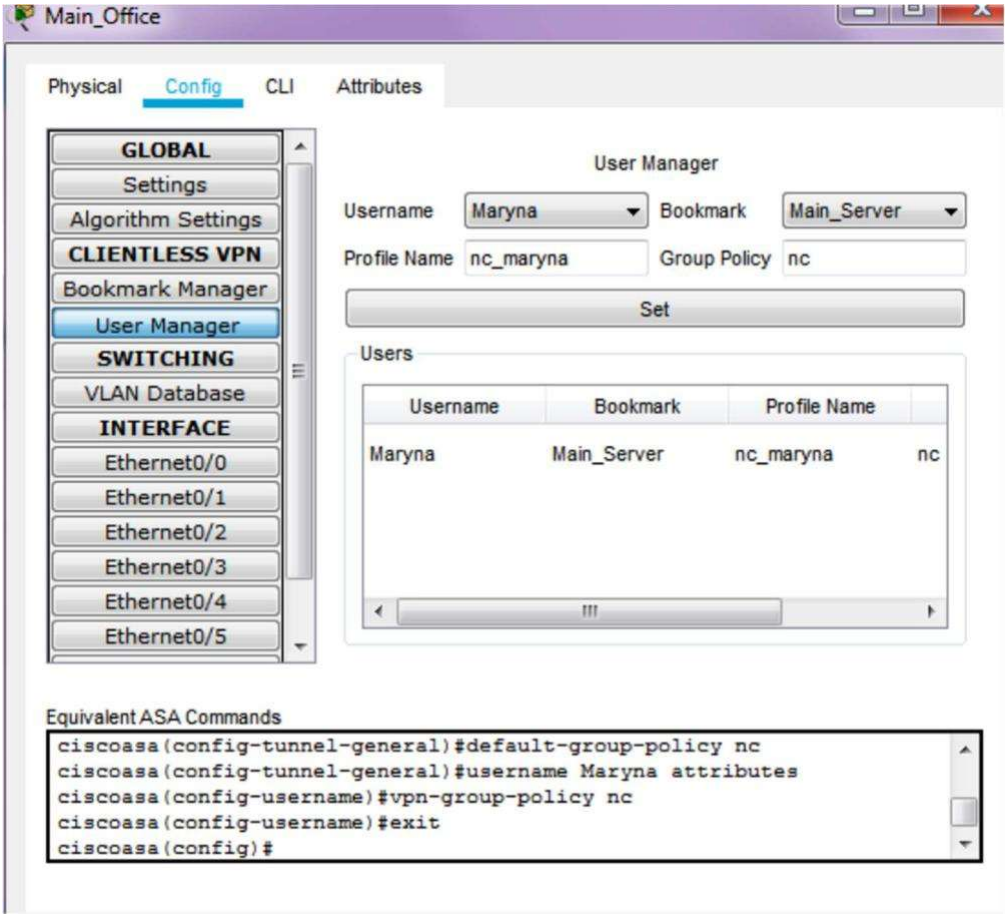

Рисунок 4.17 – Налаштування доступу для користувачів на Main office ASA

Після налаштування SLL можна протестувати доступ користувача до серверів. У користувач User_1 при намаганні зайти на сервери за межами ASA, система запитає логін та пароль для входу. При цьому користувач зможе зайти лише на ті сервери, до яких у нього є доступ (рис. 4.18).

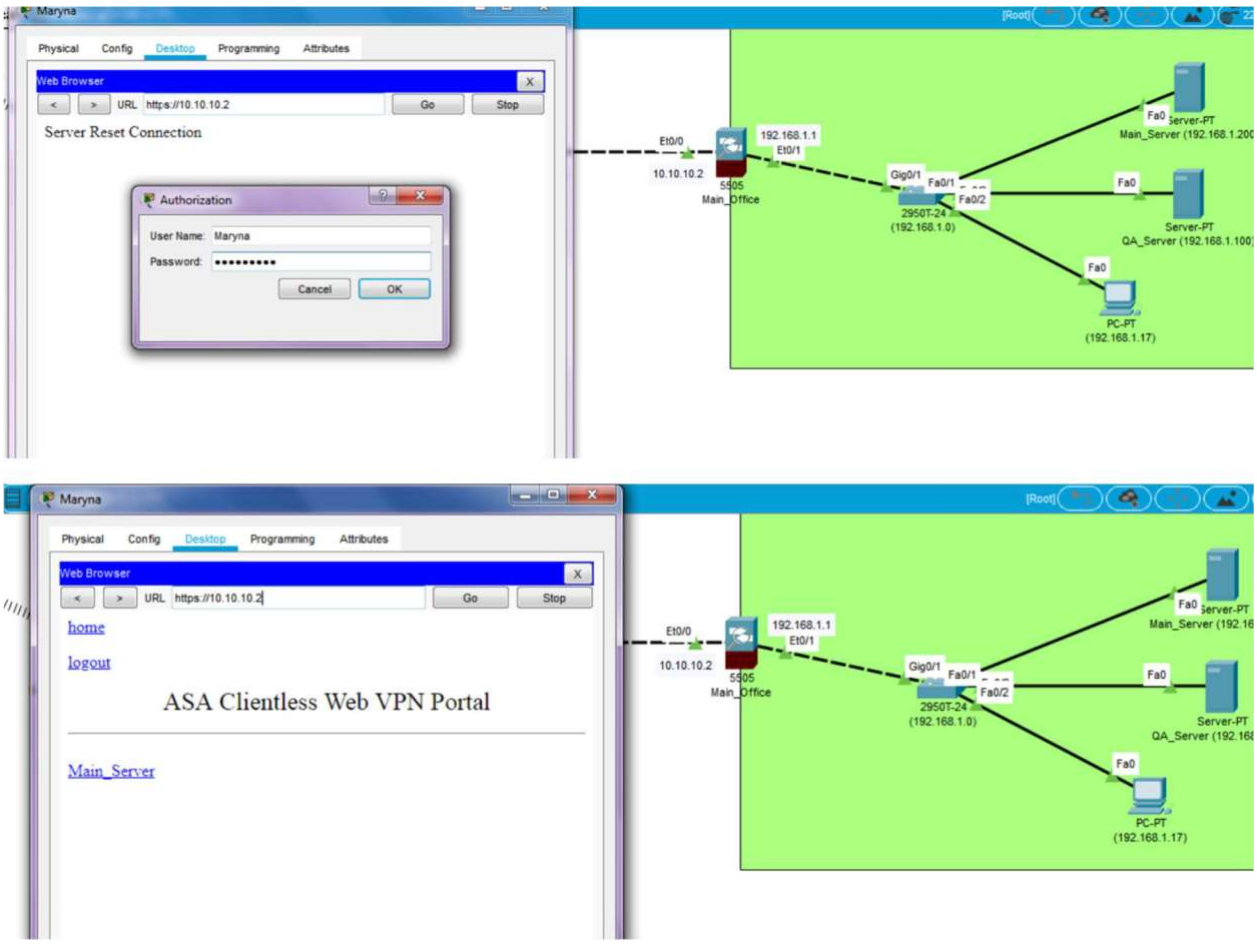

Рисунок 4.18 – Доступ до серверів для користувача User_1

4.4 Висновки

Таким чином, в розділу була реалізована модель комутованої мережі із захищеним доступом до ресурсів мережі з віддалених філіалів. Для моделювання було використане середовище Cisco Packet Tracer. Було проведено тестування мережі на різні варіанти підключення. При цьому було виявлено, що при використанні IPsec VPN відбувається шифрування пакетів та при цьому за допомогою SSL VPN можна обмежити доступ до ресурсів компанії для певних груп користувачів.

ВИСНОВКИ

В магістерській роботі розглянуто питання побудови захищених розподілених комутованих мереж. Дане питання є критично важливим, оскільки в останні роки спостерігається стрімкий розвиток мережних сервісів, що працюють в розподілених системах через відкриті загальнодоступні мережі. В роботі були отримані наступні результати, які відрізняються науковою та технічною новизною:

1. Побудована модель комутованої розподіленої мережі із впровадженням елементів захисту

2. Розроблено технологію побудови захищених комутованих мереж, що враховує наявну інфраструктуру та дозволяє впровадити захист передачі даних.

Такий підхід дозволяє обрати необхідні засоби для побудови захищених комутованих мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. A Framework for IP Based Virtual Private Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/rfc/rfc2764.txt

2. Bollapragada V., Mohamed Kh., Wainner S. IPSec VPN Design. Cisco Press. (2005). 384 p.

3. Douglas Crawford. OpenVPN over TCP vs. UDP: what is the difference, and which should I choose? [Електронний ресурс] – Режим доступу до ресурсу: https://www.bestvpn.com/blog/7359/openvpn-tcp-vs-udp-differencechoose/

4. Harsh Kupwade Patil. Wireless Sensor Network Security: The Internet of Things [Електронний ресурс] / Harsh Kupwade Patil, Thomas M.Chen // Computer and Information Security Handbook. – 2017. – Third Edition, Chapter 18. – P. 317-337. – Режим доступу: https://www.sciencedirect.com/science/article/pii/B9780128038437000181.

5. IPSec – протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.shtml

6. Mabrook Al-Rakhami. Saleh Almowuena Wireless Sensor Networks Security: State of the Art [Електронний ресурс] / Mabrook Al-Rakhami, Saleh Almowuena. – 2018. – Режим доступу: https://arxiv.org/abs/1808.05272.

7. Pure hardware VPNs uale high-availability tests [Електронний ресурс] – Режим доступу до ресурсу: https://web.archive.org/web/20070923013848/http://www.networkworld.com/reviews/2000/1211rev.html

8. Security of Cyber-Physical Systems from Concept to Complex Information Security System / V. Dudykevych, G. Mykytyn, T. Kret, A. Rebets //Advances in Cyber-Physical Systems. – Volume 1, Number 2 (2016). – C. 67-75.

9. Tebogo Kgogo. Software defined wireless sensor networks security challenges // Tebogo Kgogo, Bassey Isong, Adnan M. Abu-Mahfouz // IEEE AFRICON. – 2017. – P. 1508-1513.

10. Tomic I. A Survey of Potential Security Issues in Existing WirelessSensor Network Protocols / I. Tomić, J.A. McCann // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 6. – P. 1910-1923.

11. Virtual private network (VPN) [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Virtual_private_network

12. VPN протоколы [Електронний ресурс] – Режим доступу до ресурсу: https://www.cactusvpn.com/ua/beginners-guide-to-vpn/vpn-protocol/

13. Waleed Al Shehri. A Survey On Security In Wireless Sensor Networks // International Journal of Network Security & Its Applications (IJNSA). – 2017. – Vol. 9, No. 1. – P. 25-32.

14. Wassim Itani. Wireless Body Sensor Networks: Security, Privacy, and Energy Efficiency in the Era of Cloud Computing / Wassim Itani, Ayman Kayssi, Ali Chehab // International Journal of Reliable and Quality E-Healthcare (IJRQEH). – 2016. – Vol. 5, Issue 2. – P. 1-30.

15. Wireless Sensor Network Security for Cyber-Physical Systems / Saqib Ali, Taiseera Al, BalushiZia, NadirOmar, Khadeer Hussain // Cyber Security for Cyber Physical Systems. Studies in Computational Intelligence. – 2018. – Vol. 768. – P. 35-63.

16. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах / О.Г. Корченко, М.Б. Алєксандер, Р.С. Одарченко, А. Алі Наджі, О.Ю. Петренко // Захист інформації. – 6 – 2016. – Том 18. – № 1. – С. 48-56.

17. Базова реалізація бібліотек для роботи з IPsec для Unix-подібних систем [Електронний ресурс] – Режим доступу до ресурсу: http://ipsectools. sourceforge.net/99

18. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с

19. Василина А.В, Яловий М.М., Цибуляк Б.З. Захист кваліфікованих каналів зв'язку за допомогою систем віртуальних приватних мереж. Міжнародна науково-практична конференція «Проблеми та перспективи забезпечення цивільного

захисту». Збірник матеріалів. (Харків, 3-4 квітня 2013). Харків: Вид-во НУЦЗ України. (2013). С. 266- 268.

20. Волошко С.В. Інформаційна безпека в безпроводових сенсорних мережах [Електронний ресурс] / С.В. Волошко, Д.О. Курца // Новітні інформаційні системи і технології. – 2018. – Випуск 9. – Режим доступу: http://journals.pntu.edu.ua/mist/article/view/1039/869.

21. Галкін В.В., Пархоменко І.І. «Використання VPN-технологій для захисту інформації в каналах корпоративних мереж» // Проблема кібербезпеки інформаційно-телекомунікаційних систем: матеріали наук.-техніч. конф.,(КНУ, Київ, Україна, 10 – 11 березня 2016). – К.: КНУ, 2016. – С. 66

22. Дудикевич В.Б. Квінтесенція безпеки кіберфізичних систем / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець // Інформаційні системи і мережі. – 2018. – № 887. – С. 58-69.

23. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

24. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т «Харків. політехн. ін-т». – Харків: НТУ «ХПІ», 2014. – 251 с.

25. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. (Нормативний документ системи технічного захисту інформації).

26. Інформаційна безпека в середовищі безпроводових сенсорних мереж: монографія / М.Б. Александер, С.М. Балабан, М.П. Карпінський, С.А. Райба, В.М. Чиж. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 160 с.

27. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

28. Комплексні системи захисту інформації [Текст] : навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.] ; Вінницький національний технічний університет. − Вінниця : ВНТУ, 2018. − 118 с

29. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

30. Кулаков Ю.А., Луцкий Г.М. Локальные сети, - К.: Юниор, 2008. – 336с.

31. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие. – Киев: Издательство Интуит, 2010. − 608 с.

32. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Медведев Н. Г., Пархоменко І.І., Галкін В.В., «Захист транзакцій в каналах корпоративних мереж за допомогою VPN технологій» // Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні: матеріали наук.-техніч. конф.,(НУБіП, Київ, Україна, 23 – 24 червня 2016). – К.: НУБіП, 2016. – С.47 – 48.

33. Політика безпеки для Internet. [Електронний ресурс]. – Режим доступу: https://lektsii.org/8-12435.html

34. Постанова Кабінету міністрів України від 29 березня 2006 р. N373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

35. Построение защищенного узла доступа в интернет с применением технологии VPN и тунеллирования [Електронний ресурс]. Режим доступу: http://www.opennet.ua/docs/UAS/vpn_solution/.

36. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. 1994. № 31. С. 286.

37. Проект Концепції інформаційної безпеки України. – [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

38. Райан Норманн Выбираем протокол VPN [Електронний ресурс] – Режим доступу до ресурсу: http://www.osp.ua/win2000/2001/07/175027/

39. Романов В.О. Вимоги до забезпечення функціональної та інформаційної безпеки бездротових сенсорних мереж / В.О. Романов, І.Б. Галелюка, В.О. Остапенко // Комп'ютерні засоби, мережі та системи. – 2017. – № 16. – С. 106-117.

40. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 1999.04.28]. К.: ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

41. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: НД ТЗІ 3.6-001-2000. [Чинний від 2000.12.30]. К.: ДСТСЗІ СБУ, 2000. № 60. (Нормативний документ системи технічного захисту інформації).

42. Что такое SSL? [Електронний ресурс]. Режим доступу: http://www.ods.com.ua/win/uas/security/ssl.html.__

43. Трояновська Т. І. Побудова швидкісних мультисервісних мереж / Т. І. Трояновська, Л. А. Савицька, М. О. Максюта, Д. М. Поліщук // «Smart and Young». Київ, 2016. – №8, с. 72–78.

44. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах / М. П. Карпінський, Я. І. Кінах, О. С. Войтенко, В. Р. Паславський, І. З. Якименко, М. М. Касянчук // Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій", 16-17 листопада 2017 року. — Т. : ТНТУ, 2017. — Том 2. — С. 81–82. — (Комп'ютерно-інформаційні технології та системи зв'язку).

45. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. (Нормативний документ системи технічного захисту інформації).

ДОДАТОК А

Копії наукових публікацій

УДК 004.056.53
DOI:

ТІТОВА ВІРА
Хмельницький національний університет
ORCID ID: 0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ ЮРІЙ
Хмельницький національний університет
ORCID ID: 0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
НАГРЕБЕЦЬКИЙ ОЛЕКСІЙ
Хмельницький національний університет
e-mail: nagrebeckiy01@gmail.com
ГАЛУЗИНСЬКИЙ ВАЛЕРІЙ
Хмельницький національний університет
e-mail: Haluzynskyi.Valerii @khmnu.edu.ua

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

У даній статті авторами було проаналізовано існуючі на сьогоднішній день підходи до управління ризиками в інформаційних системах. За результатами аналізу було зроблено висновки, що більшість підходів не враховують концепції та вимоги різних стандартів інформаційної безпеки, що може викликати недовіру до застосовуваних підходів у експертів, які проводять аналіз ризиків, та ускладнити можливу сертифікацію організації. Для реалізації вдосконаленого підходу до управління ризиками авторами було проаналізовано розподілену інформаційну систему з точки зору інформаційної безпеки компаній, а також були описані особливості об'єкта, який розглядається. Також було побудовано модель загроз згідно з керівними документами, проведено збір експертної інформації для визначення імовірності кожної з ідентифікованих загроз та проведено розрахунок ризиків для системи, що розглядається.

Ключові слова: модель загроз, інформаційна безпека, управління ризиками, розподілені інформаційні системи.

VIRA TITOVA, YURII KLOTS, OLEKSII NAHREBETSKYI
Khmelnitskyi National University

INFORMATION SECURITY RISK MANAGEMENT IN DISTRIBUTED INFORMATION SYSTEMS OF PERSONAL DATA PROCESSING

A distributed information system is a set of interactive software modules that have a single system of users. In fact, any system that jointly processes data between two or more computers is a distributed computing system. It is used to reduce the load on the server and ensure the normal operation of the remote department.

In this work, a distributed information system was developed on the example of a free private company with a staff of 150 employees and an economy and finance department, which includes two automated workplaces that process personal data and a server for storing personal data, which, in turn, are included in the general local network of the enterprise, which has access to the Internet. The authors conducted an analysis of methodological and risk prevention documents, as well as the existing object of information activity from the point of view of information protection.

A threat model has been built, according to regulatory documents. The most likely threats to the selected organization were identified and the attack vector for these threats was determined. At the next stage, expert information was collected to determine the probability of the identified threats and risk calculations were carried out for the systems under consideration. As a result, the goal of the work, namely the implementation of a more advanced approach to risk management and, accordingly, IS in distributed information systems for personal data processing, was achieved.

Keywords: threat model, information security, risk management, distributed information systems.

Постановка проблеми

Розподілена інформаційна система – це набір інтерактивних програмних модулів, які мають єдину систему користувачів. Фактично будь-яка система, яка спільно обробляє дані між двома або більше комп'ютерами, є розподіленою обчислювальною системою. Вона використовується для зниження навантаження на сервер та забезпечення нормальної роботи віддаленого відділу.

Кожен вузол розподіленої системи має бути незалежним або автономним. Локальна незалежність означає, що вузли розподіленої системи мають рівні права, тобто вважаються рівними. Це означає, що немає потреби викликати так званий центральний вузол або головний вузол для доступу до будь-яких централізованих служб.

Особливості з погляду захисту персональних даних під час їх обробки у розподілених системах полягають у наступному. Оператор при обробці персональних даних зобов'язаний вживати необхідних правових, організаційних та технічних заходів або забезпечувати їх прийняття для захисту персональних даних від неправомірного або випадкового доступу до них, знищення, зміни, блокування, копіювання, розповсюдження персональних даних, а також від інших неправомірних дій щодо персональних даних. Тобто роботу оператора при обробці персональних даних з точки зору інформаційної безпеки можна звести до вирішення задачі управління ризиками інформаційної безпеки.

Огляд існуючих рішень

Питанням аналізу підходів управління інформаційною безпекою (ІБ) присвячено велику кількість наукових праць, більшість із яких або містять велику кількість наявність математичних формул і моделей; або не містять взагалі ніяких математичних складових; або мають схильність в сторону якої-небудь із двох вище наведених груп підходів. Проаналізуємо змістовні аспекти кожної групи [1-3].

Підходи першої групи, як правило, використовують різні розділи вищої математики. В якості ядра підходів вибирають принципи, засновані на теорії імовірності або корисності (надійності), або нечітких множинах, неперервному чи дискретному розподілі, тощо. Роботи, що відносяться до першої групи підходів, досить часто не враховують реальні вимоги організацій, що займаються аналізом ризиків; вимагають від експертів в області ІБ достатньої математичної підготовки, що часто негативно відображається на практиці застосування даних підходів. Друга група підходів у більшій мірі розвинена зарубіжними авторами. Статті авторів із США, Англії мають перш за

все рекомендаційний характер для модернізації на основі стандартів ІБ: ISO, BS, які вже зарекомендували себе, не вимагаючи глибоких знань вищої математики [4-6].

Третя група підходів у багатьох випадках поєднує в собі експертні оцінки та оцінки ризиків, що базуються на визначенні їх за наявними статистичними даними. Подібні підходи можна успішно застосовувати в практичній діяльності (не дивлячись на ряд мінусів), так як використання бази статистики дозволяє звести до мінімуму суб'єктивну точку зору експерта на вирішувану задачу і проводити роботу за оцінкою ризиків ІБ-спеціалістів без великого досвіду та кваліфікації.

Формулювання цілей статті

За результатами аналізу можна зробити наступні висновки: більшість підходів не враховують концепції та вимоги різних стандартів ІБ, що може викликати недовіру до застосовуваних підходів у експертів, які проводять аналіз ризиків ІБ, ускладнює можливу сертифікацію організації. Багато підходів, в основах яких лежить мета отримати кількісну оцінку ризиків з використанням математичних формул, моделей, заглиблених в математичні теорії, не мають практичний зв'язок з оцінкою ризиків, реальними вимогами бізнесу. Ряд підходів не забезпечує повного процесу оцінки, управління ризиками ІБ, реалізуючи лише деякі його компоненти. Враховуючи сильні та слабкі сторони існуючих підходів авторами було прийнято рішення реалізації більш досконалого підходу до управління ризиками та, відповідно, ІБ в розподілених інформаційних системах обробки персональних даних.

Виклад основного матеріалу

Як об'єкт дослідження було обрано довільне приватне підприємство. Штат підприємства складає 150 працівників. У компанії є кілька відділів, кожен з яких здійснює свою діяльність. У цій роботі нас буде цікавити відділ економіки та фінансів, який включає 2 автоматизованих робочих місця, на яких відбувається обробка персональних даних, та сервер для зберігання персональних даних (рис. 1), які в свою чергу включені в загальну локальну мережу підприємства, що має вихід в мережу Internet. Саме на цьому відділі проводилися зазначені дослідження.

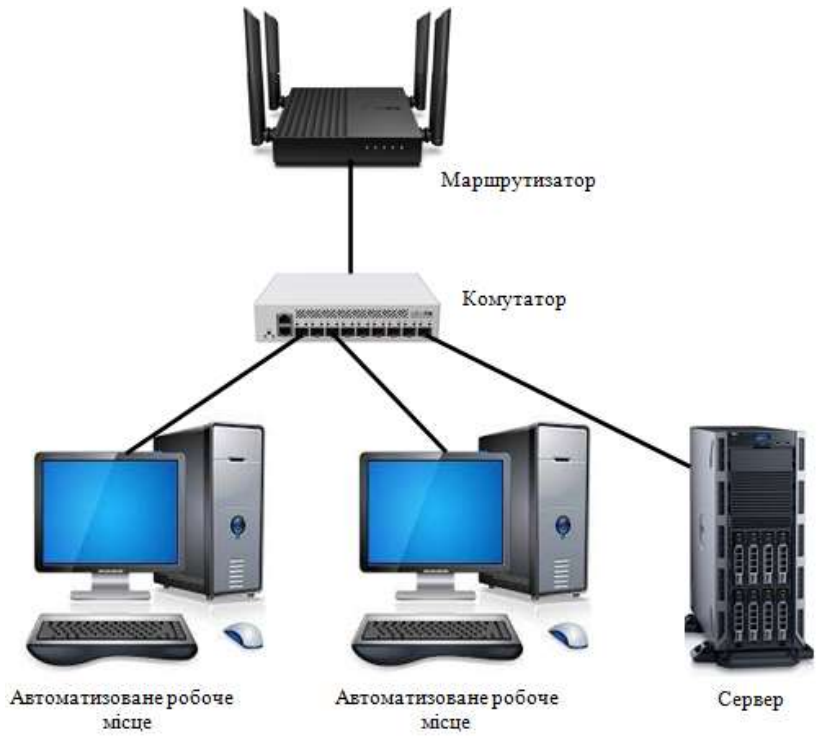

Рис. 1. Схема відділу для дослідження

Діяльність компанії пов'язана з використанням обчислювальної техніки та інформаційних технологій, до неї входить: тестування на відповідність вимогам захищеності від несанкціонованого доступу до інформації; аналіз

уразливостей та контроль відсутності недекларованих можливостей у програмному забезпеченні; розробка та впровадження систем захисту інформації, що становить державну таємницю, на основі сертифікованих базових інформаційних захищених комп'ютерних технологій.

До переліку активів організації входить: обладнання – оцінна вартість 750 тис. грн., статутний капітал – 570 тис. грн., персональні дані працівників – оціночна вартість 250 тис. грн., будівлі, споруди – оціночна вартість 1850 тис. грн., програмні продукти – оціночна вартість 600 тис. грн.

Для досягнення поставленої мети в рамках компанії доцільно використовувати метод розрахунку ризиків, представлений в NIST 800-30 [7]:

$$R = P(t) * S, \tag{1}$$

де R – значення ризику; $P(t)$ – ймовірність реалізації загрози ІБ (застосовується якісна та кількісна шкали); S – ступінь впливу загрози на інформаційний актив (вартість активу в якісній та кількісній шкалі).

Визначимо усі можливі загрози інформаційним активам в розподілених інформаційних системах обробки персональних даних (табл.1).

Для розрахунків значення ризиків R необхідно мати значення $P(t)$ – визначимо його шляхом експертної оцінки за шкалою 1-9. Причому 1 означає, що загрози рівнозначні, 2-9 – що одна загроза є більш імовірною ніж інша у зазначену кількість разів. Отримаємо зведену таблицю порівнянь загроз (табл.2).

Таблиця 1

Модель загроз ІБ

№	Тип загрози		Можливі наслідки
1	Аналіз мережного трафіку		Визначення характеристик мережного трафіку, перехоплення даних, що передаються, в тому числі ідентифікаторів та паролів користувачів
2	Сканування мережі		Визначення протоколів, доступних портів мережних служб, правил формування з'єднань, активних мережних сервісів, ідентифікаторів та паролів користувачів
3	«Парольна» атака		Виконання деструктивних дій, пов'язаних з отриманням несанкціонованого доступу
4	Підміна довіреного об'єкту мережі		Зміна маршруту проходження повідомлень, несанкціонована зміна маршрутно-адресних даних, несанкціонований доступ до мережних ресурсів, нав'язування недостовірної інформації.
5	Нав'язування хибного маршруту		Несанкціонована зміна маршрутно-адресних даних, аналіз та модифікація даних, що передаються, нав'язування хибних повідомлень
6	Впровадження хибного об'єкта мережі		Перехват та перегляд трафіку, несанкціонований доступ до мережних ресурсів, нав'язування недостовірної інформації.
7 7	Відмова в обслуговуванні	Часткове вичерпання ресурсів	Зниження пропускної здатності каналів зв'язку, продуктивності мережних пристроїв, продуктивності серверних додатків
		Повне вичерпання ресурсів	Неможливість передачі повідомлень через відсутність доступу до середовища передачі, відмова у встановленні з'єднання, відмова в наданні сервісів (файловий сервер, пошта, тощо)
		Порушення логічних зв'язків між атрибутами, даними, об'єктами	Неможливість передачі повідомлень через відсутність коректних маршрутно-адресних даних, неможливість отримання послуг в зв'язку з несанкціонованою модифікацією ідентифікаторів, паролів, тощо.
		Використання помилок в програмах	Порушення робото здатності мережних пристроїв

8 7	Віддалений запуск додатків	Розсилання файлів з деструктивним кодом, вірусне зараження	Порушення конфіденційності, цілісності, доступності інформації
		Переповнення буферу	
		Використання можливостей віддаленого керування системою через приховані програмні/ апаратні закладки або штатними засобами	Приховане керування системою

Таблиця 2

Зведена таблиця порівнянь загроз

	З1	З2	З3	З4	З5	З6	З7	З8	$\sum$
З1	1	1	1	1/7	1/7	1/7	1/5	1/3	**3,96**
З2	1	1	1	1/7	1/7	1/7	1/5	1/3	**3,96**
З3	1	1	1	1/7	1/7	1/7	1/5	1/3	**3,96**
З4	7	7	7	1	1	1	3	3	**30**
З5	7	7	7	1	1	1	3	3	**30**
З6	7	7	7	1	1	1	3	3	**30**
З7	5	5	5	1/3	1/3	1/3	1	1	**18**
З8	3	3	3	1/3	1/3	1/3	1	1	**12**
									131,88

Провівши розрахунок вагового коефіцієнту кожної загрози шляхом нормування, отримаємо значення імовірності кожної загрози З1-З8.

$P_1(t)$ (З1 – Аналіз мережного трафіку) = 0,03; $P_2(t)$ (З2 – Сканування мережі) = 0,03; $P_3(t)$ (З3 – «Парольна» атака) = 0,03; $P_4(t)$ (З4 – Підміна довіреного об'єкту мережі) = 0,23; $P_5(t)$ (З5 – Нав'язування хибного маршруту) = 0,23; $P_6(t)$ (З6 – Впровадження хибного об'єкта мережі) = 0,23; $P_7(t)$ (З7 – Відмова в обслуговуванні) = 0,14; $P_8(t)$ (З8 – Віддалений запуск додатків) = 0,09.

При цьому З1-З6 становлять загрозу для персональних даних працівників та програмних продуктів; З7 – становить загрозу для обладнання та програмних продуктів; З8 – тільки для програмних продуктів. Розрахуємо кількісне значення ризику для кожної загрози.

$R_1 = 25500$ грн.; $R_2 = 25500$ грн.; $R_3 = 25500$ грн.; $R_4 = 195500$ грн.; $R_5 = 195500$ грн.; $R_6 = 195500$ грн.; $R_7 = 189000$ грн.; $R_8 = 54000$ грн.

Ризики, які становлять менше 5% від статутного капіталу відкинемо, як такі, що не несуть суттєвих збитків та з легкістю можуть бути скомпенсовані. В нашому випадку таких ризиків, якими можна було б знехтувати, немає. Для всіх існуючих загроз З1-З8 слід застосувати заходи протії, щоб мінімізувати значення ризиків, які вони несуть. Найбільшої уваги потребують загрози З4-З7 (підміна довіреного об'єкту мережі, нав'язування хибного маршруту, впровадження хибного об'єкта мережі, відмова в обслуговуванні). При цьому вартість засобів та заходів захисту не повинна перевищувати суму ризику, який вони мінімізують.

Висновки

В даній роботі було розглянуто розподілену інформаційну систему на прикладі довільної приватної компанії зі штатом 150 працівників та відділом економіки та фінансів, який включає 2 автоматизованих робочих місця, на яких відбувається обробка персональних даних, та сервер для зберігання персональних даних, які в свою чергу включені в загальну локальну мережу підприємства, що має вихід в мережу Internet.

Авторами було проведено аналіз методичних документів із запобігання ризикам, а також наявного об'єкту інформаційної діяльності з погляду захисту інформації. Побудовано модель загроз, згідно з регламентуючими документами. Було визначено найбільш ймовірні загрози для обраної організації та визначено вектор атак для цих загроз. На наступному етапі було проведено збір експертної інформації для визначення імовірності кожної з ідентифікованих загроз та проведено розрахунок ризиків для системи, що розглядається.

В результаті мету роботи, а саме реалізацію більш досконалого підходу до управління ризиками та, відповідно, ІБ в розподілених інформаційних системах обробки персональних даних, було досягнуто.

Література

1. Методи якісного аналізу підприємницьких ризиків [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_50_49235071.pdf

2. Методичні основи оцінки ризиків підприємницької діяльності [Електронний ресурс] – Режим доступу: http://www.vestnikdnu.com.ua/archive/201154/171-176.pdf

3. Методичне забезпечення оцінки ризиків підприємства [Електронний ресурс] – Режим доступу: https://periodicals.karazin.ua/soceconom/article/download/4813/4366/#:~:text

4. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST [Електронний ресурс] – Режим доступу: https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2(9)_09.pdf

5. Stango, Antonietta & Prasad, Neeli & Kyriazanos, Dimitris. (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. 262-267. 10.1109/SECURWARE.2009.47.

6. Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: Guizzardi, R., Ralyté, J., Franch, X. (eds) Research Challenges in Information Science. RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_39

7. Risk Management Guide for Information Technology Systems [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800- 30/archive/2002-07-01

References

1. Metody yakisnoho analizu pidpryiemnytskykh ryzykiv [Elektronnyi resurs] – Rezhym dostupu: http://www.dut.edu.ua/uploads/l_50_49235071.pdf

2. Metodychni osnovy otsinky ryzykiv pidpryiemnytskoi diialnosti [Elektronnyi resurs] – Rezhym dostupu: http://www.vestnikdnu.com.ua/archive/201154/171-176.pdf

3. Metodychne zabezpechennia otsinky ryzykiv pidpryiemstva [Elektronnyi resurs] – Rezhym dostupu: https://periodicals.karazin.ua/soceconom/article/download/4813/4366/#:~:text

4. Realizatsiia protsesnoho pidkhodu do keruvannia ryzykamy informatsiinoi bezpeky v dokumentakh NIST [Elektronnyi resurs] – Rezhym dostupu: https://ela.kpi.ua/bitstream/123456789/23949/1/ITS2017.5.2(9)_09.pdf

5. Stango, Antonietta & Prasad, Neeli & Kyriazanos, Dimitris. (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. 262-267. 10.1109/SECURWARE.2009.47.

6. Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: Guizzardi, R., Ralyté, J., Franch, X. (eds) Research Challenges in Information Science. RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham. https://doi.org/10.1007/978-3-031-05760-1_39

7. Risk Management Guide for Information Technology Systems [Elektronnyi resurs] – Rezhym dostupu: https://csrc.nist.gov/publications/detail/sp/800- 30/archive/2002-07-01

ДОДАТОК Б

Конфігурація обладнання для дослідження

Конфігурація NC Filia_1 router:

```
Configure terminal
interface g0/1
ip address 10.250.50.1 255.255.255.0
no shut
interface g0/0
ip address 10.0.2.1 255.255.255.0
no shut
license boot module c1900 technology-package securityk9
exite
copy running-config startup-config
reload
show version
Configure terminal
access-list 100 permit ip 10.250.50.0 0.0.0.255 10.10.10.0 0.0.0.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key password address 10.0.1.1
crypto ipsec transform-set NC_Sumy-to-NC_Kyiv esp-aes 256 esp-sha-hmac
crypto map IPSEC 10 ipsec-isakmp
set peer 10.0.1.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set NC_Sumy-to-NC_Kyiv
match address 100
interface GigabitEthernet0/0
crypto map IPSEC
```

Конфігурація Internet router:

```
Configure terminal
interface g0/1 ip address 10.0.2.2 255.0.0.0
no shut
interface g0/0 ip address 10.0.1.2 255.0.0.0
no shut
```

Конфігурація NC Main router:

```
Configure terminal
```

```
interface g0/1 ip address 10.10.10.1 255.0.0.0
no shut
interface g0/0 ip address 10.0.1.1 255.0.0.0
no shut
conf t
license boot module c1900 technology-package securityk9
exite
copy running-config startup-config
reload
show version
Configure terminal
access-list 100 permit ip 10.10.10.0 0.0.0.255 10.250.50.0 0.0.0.255
crypto isakmp policy 10 encryption aes 256 authentication pre-share group 5
exit
crypto isakmp key password address 10.0.2.1
crypto ipsec transform-set NC_Kyiv-to-Home esp-aes 256 esp-sha-hmac
crypto map IPSEC 10 ipsec-isakmp
set peer 10.0.2.1
set pfs group5
set security-association lifetime seconds 86400
set transform-set NC-to-Home
match address 100
interface GigabitEthernet0/0
crypto map IPSEC
```

Конфігураці AAA серверу за допомогою інтерфейсу:

```
Configure terminal
Hostname ASA1
Interface vlan 1
Nameif inside
Security-level 100
Ip address 192.168.1.1 255.255.255.0
exit
Interface vlan 2
Nameif outside
Security-level 0
Ip address 10.10.10.2 255.255.255.0
hostname firewall1
names
name 192.168.1.100 QA_Server name 192.168.1.100 QA_Server
name 192.168.1.200 Main_Server name 192.168.1.200 Main_Server
name 10.1.1.10 OUT_DB_server name 10.10.10.10. Server
object-group network Privat_servers
network-object host QA_Server
```

```
network-object host Main_Server
access-list OUT_IN remark ***ftp traffic to Privat servers***
access-list OUT_IN extended permit tcp any object-group Privat_servers eq ftp
access-list OUT_IN extended permit tcp any object-group Privat_servers eq ftp-data
access-list OUT_IN remark ***DB traffic between DB servers***
access-list OUT_IN remark ***Virtual Telnet for Authentication***
access-list OUT_IN extended permit tcp any host 10.50.10.10 eq https
access-list OUT_IN extended deny ip any any log
logging enable
logging buffered informational
static (outside) 10.50.10.10 10.50.10.10 netmask 255.255.255.255
access-group OUT_IN in interface outside
route outside 0.0.0.0 0.0.0.0 10.10.10.254 1
timeout xlate 4:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 4:00:00 absolute
aaa-server ACS_1 protocol tacacs+
aaa-server ACS_1 host 10.10.10.10
key password
aaa authentication serial console ACS_1 LOCAL
aaa authentication enable console ACS_1 LOCAL
aaa authentication ssh console ACS_1 LOCAL
aaa authentication include ip outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ACS_1
aaa authentication exclude tcp/1526 outside OUT_DB_server 255.255.255.255 ACS_1
aaa authorization include ip outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ACS_1
aaa authorization exclude tcp/1526 outside OUT_DB_server 255.255.255.255 ACS_1
aaa authentication include https outside 10.50.10.10 255.255.255.255 0.0.0.0 0.0.0.0
ACS_1
aaa proxy-limit 128
aaa authentication listener https outside port 1443 redirect
virtual telnet 10.50.10.10
telnet timeout 5
ssh 10.10.10.0 255.255.255.0 outside
ssh timeout 5
ssh version 2
console timeout 5
no threat-detection basic-threat
no threat-detection statistics access-list
ssl encryption des-sha1 rc4-md5
username Maryna password PaSsWoRd privilege 15
username Admin password PaSsWoRd privilege 15
Exit
```

```
Webvpn
Enable outside
Object network lan
Subnet 192.168.1.0 255.255.255.0
exit
crypto key generate rsa label ssl-anyconnect
crypto ca trustpoint localtrust
enrollment self
fqdn sslvpn. nc.com
subject-name CN=sslvpn.nc.com
keypair ssl-anyconnect
crypto ca enroll localtrust noconfirm
ssl trust-point localtrust outside
copy tftp://10.150.81.50/anyconnect-win-2.0.0343-k9.pkg flash
webvpn
svc image disk0:/anyconnect-win-2.3.0254-k9.pkg 1
enable outside
svc enable
ip local pool SSLClientPool 10.0.3.1-10.0.3.50 mask 255.255.255.0
group-policy SSLCLient internal
group-policy SSLCLient attributes
dns-server value 10.10.10.10
vpn-tunnel-protocol svc
default-domain value nc.com
address-pools value SSLClientPool
sysopt connection permit-vpn
tunnel-group SSLClientProfile type remote-access
tunnel-group SSLClientProfile general-attributes
default-group-policy SSLCLientPolicy
tunnel-group SSLClientProfile webvpn-attributes
group-alias SSLVPNClient enable
webvpn
tunnel-group-list enable
access-list 100 extended permit ip any 10.0.3.2 255.255.255.0
nat (inside) 0 access-list 100
username Maryna password 123123123 privilege 0
username Maryna attributes
username Admin password 999777555 privilege 0
username Admin attributes
service-type remote-access
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Галузинського Валерія Валерійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.12.2023
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 124303 Назва: Технологія побудови захищених комутованих мереж Ethernet Додано в БД: 2023-12-21 Автора: Галузинський В.В. Керівники: Касянчук М.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	75669	1147	956 (1%)	13 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016029025

Дата перевірки:
21.12.2023 16:40:27 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
21.12.2023 16:41:57 EET

ID користувача:
100008300

Назва документа: **Галузинський_плагіат**

Кількість сторінок: **79** Кількість слів: **12585** Кількість символів: **96781** Розмір файлу: **4.42 MB** ID файлу: **1015718313**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

9.96%
Схожість

Найбільша схожість: **4.88%** з Інтернет-джерелом (https://www.essuir.sumdu.edu.ua/bitstream-download/123456789/822.

9.4% Джерела з Інтернету	180	Сторінка 81
0.9% Джерела з Бібліотеки	46	Сторінка 82

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування	20 сторінок

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод захисту корпоративних інформаційних систем від комплексних деструктивних впливів

Автор: Галузинський Валерій Валерійович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Касянчук Михайло Миколайович, д.т.н, професор
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 9,96%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 1%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ М.М. Касянчук

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Магістр Галузинський Валерій Валерійович
Тема: Технологія побудови захищених комутованих мереж Ethernet

Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека денної форми навчання

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 93 ;

1. Короткий зміст КР та прийнятих рішень У кваліфікаційній роботі розглянуто питання побудови захищених комутованих мереж Ethernet. Проаналізовано сучасні підходи до вирішення цього питання, розглянуто моделі захищених мереж. Розроблено технологію побудови таких мереж з врахуванням наявної інфраструктури.

2. Висновок про відповідність КР завданню Магістерська робота у повній мірі відповідає поставленому завданню як у теоретичній, так і практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми дослідження; її зв'язок із науковими програмами, планами, темами та сформульовано мету та основні завдання дослідження. У першому розділі було досліджено завдання та можливості сучасних комутованих мереж, описано відомі підходи до побудови таких мереж. У другому розділі розглянуто моделі захищених комутованих мереж. У третьому розділі запропоновано технологію для забезпечення безпеки сучасних комутованих мереж Ethernet. У четвертому розділі представлено модуль захищеної мережі, що враховує наявну топологію та дозволяє передавати корпоративні дані через незахищені канали. Також проведено необхідні тести, що показують високий рівень захищеності даних.

4. Позитивні сторони проекту полягають в підвищенні захисту корпоративних інформаційних систем від комплексних деструктивних впливів за рахунок адаптивної оптимізації конфігурації системи захисту

5. Негативні сторони проекту: У роботі недостатньо висвітлено шляхи розгортання системи та оновлення її компонентів в процесі експлуатації.

6. Оцінка графічного оформлення та пояснювальної записки роботи.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки, однак має незначні зауваження

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) д.т.н., проф.
Мартинюк Валерій Володимирович .
Завідувач кафедри АКІТР, доктор технічних наук, професор .

« 18 » грудня 2023 . (підпис)