Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»

УДК _____

До захисту допущено
В.о. завідувача кафедри

_____ Явіся В.С.___
(підпис) (ініціали, прізвище)

“___”_____2019_р.

Магістерська дисертація

на здобуття освітнього ступеня «магістр»

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

За освітньо-професійною програмою Інженерія та програмування інфокомунікацій.
на тему: «Дослідження методів захисту інформації в VPN мережах»_____
Виконав: студент _2_ курсу, групи ТЗ –з81мп
(шифр групи)

Репецький Богдан Сергійович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник професор, д.т.н. професор Романов О.І._____ __
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант_____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент к.т.н, доцент Бердников О.М._____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 рік

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____Явіся В.С.
(підпис) (ініціали, прізвище)
«___»_____2019 р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Репецькому Богдану Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема дисертації: «Дослідження методів захисту інформації в VPN мережах»

науковий керівник дисертації Романов Олександр Іванович д.т.н, професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «_07_» «_11_» 2019р. № _3854-с_

2. Строк подання студентом дисертації 04.12.2019

3. Об'єкт дослідження: об'єктом дослідження є віртуальні мережі VPN

4. Предмет дослідження: є методи захисту інформації.

5. Перелік завдань, які потрібно розробити:
1. структура, елементи мережі VPN їх призначення та функції;
2. принципи побудови мережі VPN;
3. протоколи мережі VPN;
4. порівняння ефективності основних протоколів;
5. аналіз методів захисту інформації в мережах VPN.

6. Орієнтовний перелік публікацій _____

7. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

8. Дата видачі завдання 20.10.2018

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Пошук та аналіз літератури	23.10.2018	
1	Принципи побудови мережі VPN. ЇЇ відмінності від традиційних мереж	22.03.2019	
2	Класифікація VPN і їх характеристика. Протоколи мережі VPN	18.06.2019	
3	Принципи структурної побудови мереж VPN	21.09.2019	
4	Порівння методи захисту інформації в мережах VPN	15.11.2019	
5	Вступ. Висновки	28.11.2019	

Студент _____ Репецький Б.С.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Романов О.І.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Тема роботи:Дослідження методів захисту інформації в VPN мережах.

Текстова частина дипомної роботи: с.84, рис.35, табл.6, джерел 19.

На даний момент існує багато варіантів реалізації VPN мереж для різних цілей використання, тому перед споживачами даного продукту постає складне питання вибору необхідної архітектури VPN, яка задовольнятиме вимоги до захисту інформації в цих мережах. Для того, щоб обрати підходящу архітектуру необхідно розуміти принципи роботи, побудови та відмінності у роботі різних реалізацій VPN. В наш час все більшого застосування набирає використання віддаленого доступу за допомогою VPN між територіально рознесеними ресурсами. У підрозділах автоматизації процесів підприємств це питання також важливе. Комп'ютерні мережі мають необхідність в наявності сервера VPN, який буде дозволяти користувачам використовувати всі ресурси приватної захищеної мережі через загальнодоступні мережі. Також VPN мережа може використовуватись для підвищення безпеки передачі даних в внутрішній мережі, знизивши можливість витоку чи крадіжки інформації, яка транспортується через Інтернет.

Метою роботи є підвищення ефективності захисту корпоративних і публічних мереж з використанням нових технології VPN, а також визначення основних способів побудови за рахунок їх систематизації та структуризації з використання інтелектуальних засобів представлення знань шляхом розробки комплексного системного підходу, що базується системі мета описів даних, а також методах інтелектуальної обробки інформації і винесення висновків.

Об'єктом дослідження є віртуальні мережі VPN.

Предметом дослідження є методи захисту інформації.

В даній роботі було проведено дослідження структури і принципів роботи основних VPN протоколів та ефективності їх роботи шляхом

порівняння таких показників, ефективність використання наявної ємності каналів, швидкість передачі інформації, шифрування, а також сумісність з ОС.

З результатів дослідження випливає, що протокол OpenVPN краще задовольнятиме вимоги захисту мережі від зловмисників, ніж інші протоколи, оскільки має вищий поріг шифрування даних, а також швидкий незважаючи на великий рівень безпеки.

Результатами даної роботи можуть керуватись компанії чи окремі користувачі, які планують інтегрувати архітектуру VPN до своєї мережевої інфраструктури.

VPN, TCP/IP, PPTP, тунель, IPSec, пакети, захист інформації, TCP/IP, AES, AH, L2TP, IP.

ABSTRACT

Topic: “The Research of Information Security Methods in VPN environment”

It contents 84 pages, 35 figures, 6 tables and 19 sources.

There are many options for implementing VPN networks for different uses, so consumers of this product face the difficult question of choosing the necessary VPN architecture that will satisfy the information security requirements of those networks. In order to choose the right architecture you need to understand the principles of operation, construction and differences in the operation of different VPN implementations. Nowadays, the use of remote access via VPN between territorially dispersed resources is gaining increasing use. In business process automation units, this issue is also important. Computer networks require a VPN server that allows users to use all of the resources of a private secure network over public networks. A VPN environment can also be used to improve the security of data transmission on the internal network, reducing the possibility of leakage or theft of information being transmitted over the Internet.

The purpose of the work is to increase the efficiency of protection of corporate and public networks with the use of new VPN technologies, as well as to identify the main methods of construction through their systematization and structuring using intelligent means of presentation of knowledge by developing a comprehensive systematic approach based on the system of meta descriptions of data, as well as methods intelligent information processing and inference.

The object of the study is virtual VPNs.

The subject of the study is information security methods.

In this paper, we investigated the structure and principles of the main VPN protocols and their effectiveness by comparing such indicators, the efficiency of the available channel capacity, the speed of information transfer, encryption, as well as OS compatibility.

The results of the study suggest that OpenVPN will better meet the requirements of network security against attackers than other protocols because it has a higher data encryption threshold and is faster despite its high level of security.

The results of this work can be managed by companies or individuals who plan to integrate a VPN architecture into their network infrastructure.

VPN, TCP / IP, PPTP, tunnel, IPSec, packets, information security, TCP / IP, AES, AH, L2TP, IP.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN	Virtual Private Network
ISP	Internet Service Prodiver
OSI	Open System Interconnection
RFC	Request for Comments
IETF	Internet Engineering Task Force
SPF	Shortest Path First
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
ISIS	Intermediate System to Intermediate System
TCP	Transmission Control Protocol
HTTP	HyperText Transfer Protocol
LAN	Local Area Network
IP	Internet Protocol
DNS	Domain Name System
UDP	User Datagram Protocol
OS	Operation System
L2TP	Layer 2 Tunneling Protocol
AES	Advanced Encryption Standard
TLS	Transport Layer Security
SSL	Secure Sockets Layer
PPTP	Point-to-Point Tunneling Protocol
SSTP	Secure Socket Tunneling Protocol

NAT	Network Address Translation
FTP	File Transfer Protocol
PPP0E	Point-to-point protocol over Ethernet
PPP	Point-to-Point Protocol
ESP	Encapsulating Security Payload
WAN	Wide Area Network
ACL	Access Control List
GRE	Generic Routing Encapsulation
ISAKMP	Internet Security Association and Key Management Protocol
ASA	Adaptive Security Appliances

ВСТУП

В наш час все більшого застосування набирає використання віддаленого доступу між територіально рознесеними інформаційними мережами. У підрозділах автоматизації підприємств це питання також важливе. Комп’ютерні мережі мають необхідність в наявності сервера VPN, який буде дозволяти віддаленим абонентам використовувати ресурси приватної мережі через загальнодоступні мережі. Також VPN може використовуватись для підвищення безпеки передачі інформації в локальній мережі, зменшивши можливість витоку чи крадіжки інформації, яка транспортується в мережі.

Дуже часто сучасній людині, розвиваючи свій бізнес, доводиться багато подорожувати. Це можуть бути поїздки у віддалені куточки нашої країни або до країн зарубіжжя. Нерідко людям потрібен доступ до своєї інформації, що зберігається на їх домашньому комп'ютері або на комп'ютері фірми. Цю проблему можна вирішити, організувавши віддалений доступ до нього за допомогою модему і телефонної лінії. Використання телефонної лінії має свої особливості. Недоліки цього рішення в тому, що дзвінок з іншої країни коштує чималих грошей. Є й інше рішення під назвою VPN (VirtualPrivateNetwork– віртуальна приватна мережа). Переваги технології VPN в тому, що організація віддаленого доступу робиться не через телефонну лінію, а через Інтернет, що набагато дешевше і краще. Для організації віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться лише Інтернет і реально діюча IP адреса. І будь-який користувач з будь-якого куточка земної кулі зможе зайти в мережу, якщо він знає IP адресу, логін і пароль [1].

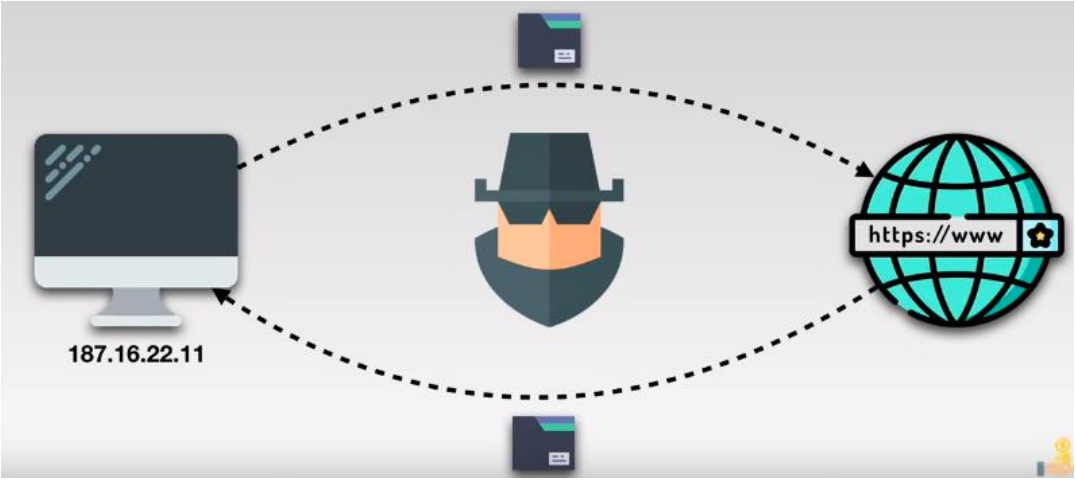

Рисунок 1. Канал без використання VPN.

Технологія VPN. Сьогодні будь-який адміністратор вважає своїм обов'язком організувати VPN-канали для співробітників, що працюють поза офісом. VPN представляє собою об'єднання окремих машин або локальних мереж у віртуальну мережу, яка забезпечує цілісність та безпеку переданих даних. Вона має властивості виділеної приватної мережі й дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад Internet [2].

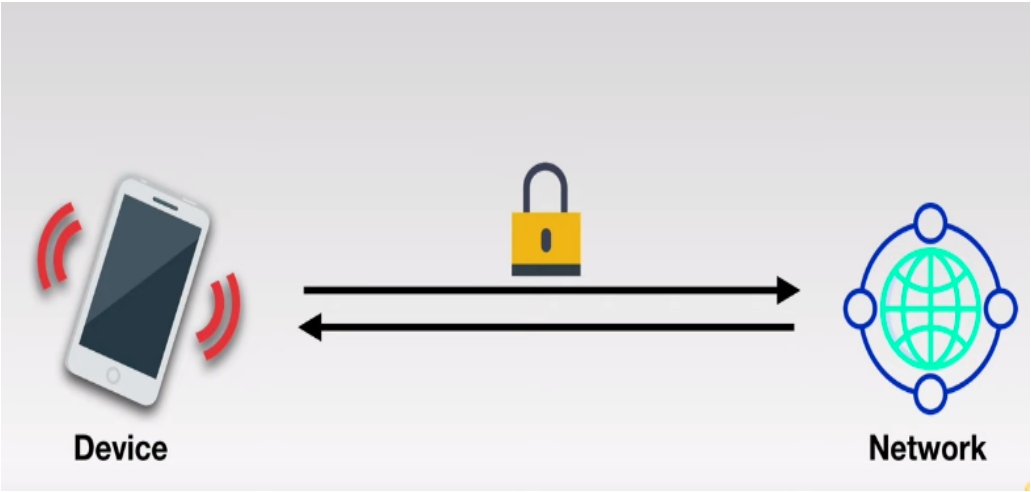

Рисунок 2. Канал з використання VPN.

VPN відрізняється рядом економічних переваг у порівнянні з іншими методами дистанційного доступу. Маючи доступ в Інтернет, будь-який користувач може без проблем підключитися до мережі офісу своєї фірми. Слід зауважити, що загальнодоступність даних зовсім не означає їхню

незахищеність. Система безпеки VPN – це броня, яка захищає всю корпоративну інформацію від несанкціонованого доступу.

Насамперед, інформація передається в зашифрованому виді. Прочитати отримані дані може лише власник ключа до шифру. Підтвердження справжності містить у собі перевірку цілісності даних і ідентифікацію користувачів, задіяних в VPN.

Суттєвим фактором будь-якої передачі даних є безпека інформації. На сьогодні це - одна з найважливіших складових роботи системного адміністратора. І чим більше мережевий підрозділ компанії , тим більші можливості з’являються у правопорушника щодо перехоплення інформації, тим більше повинна бути безпека каналів підприємства.

Отже, створення віртуальних приватних комп’ютерних мереж, застосування технології шифрування інформації є важливою технічною задачею.

1. ЗАВДАННЯ І ЦІЛІ ВИКОРИСТАННЯ МЕРЕЖ VPN

1.1. Цілі і задавання мереж VPN

Останнім часом термін VPN з'являється в кожній розмові про захист даних в мережі. І не просто так. Не так давно технологія VPN була високотехнологічної новинкою, але сьогодні це необхідний інструмент для кожної організації, чи користувача який бажає приховати свої дані серед інших даних користувачів. По суті, технологія VPN захищає конфіденційність даних в мережі.

Рисунок 1.1. Загальна структура мережVPN

Віртуальна приватна мережа (VPN) - це набір протоколів, який створює безпечне зашифроване з'єднання через менш захищену мережу, наприклад, загальнодоступний Інтернет. VPN використовує протоколи тунелювання для шифрування даних на кінці відправлення та дешифрування на кінці прийому. Щоб забезпечити додаткову безпеку, вихідні та приймаючі мережеві адреси також шифруються.

Технологія VPN може шифрувати всі дії користувача чи працівника організації в інтернеті. Всі дані, що відправляє користувач і отримуєте. Якщо користувач буду входити в мережу лише через VPN, зловмисник не зрозуміє з якої адреси підключився до джерела користувач, а бачитиме лише один із багаточисленних VPN-маршрутизаторів.

VPN використовуються для надання віддаленим корпоративним працівникам, працівникам гігантських корпорацій та бізнес-мандрівникам доступу до ресурсів, розміщених у власних мережах. Щоб отримати доступ до обмеженого ресурсу через VPN, користувач повинен бути уповноважений користуватися додатком VPN та надавати один чи більше факторів аутентифікації, наприклад пароль, маркер безпеки або біометричні дані.

В наш час все більшого застосування набирає використання віддаленого доступу за допомогою VPN між територіально рознесеними ресурсами. У підрозділах автоматизації процесів підприємств це питання також важливе. Комп’ютерні мережі мають необхідність в наявності сервера VPN, який буде дозволяти користувачам використовувати всі ресурси приватної захищеної мережі через загальнодоступні мережі. Також VPN сервер може використовуватись для підвищення безпеки передачі даних в внутрішній мережі, знизивши можливість витоку чи крадіжки інформації, яка транспортується через Інтернет.

Світова тенденція показує, що за роки з часу запуску технології кількість приватних користувачів які нею користуются зростає з великими швидкостями. У сучасних компаніях малого та великого бізнесу VPN є основою всіх комунікацій, та отримання даних.

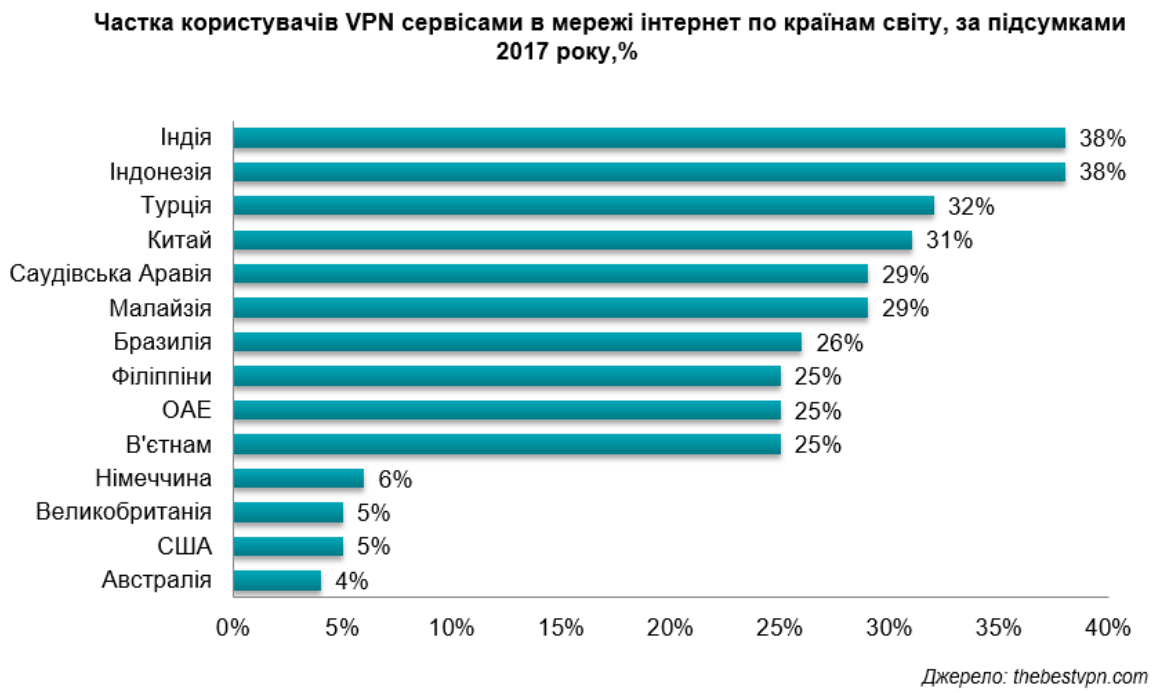

Рисунок 1.2. Тенденція попиту VPN мереж

Віртуальна приватна мережа - це спосіб розширити приватну мережу, використовуючи загальнодоступну мережу, таку як Інтернет. Назва лише підказує, що це віртуальна "приватна мережа", тобто користувач може бути частиною локальної мережі, який сидить у віддаленому місці. Він використовує протоколи тунелювання для встановлення безпечного з'єднання. І чим більший мережевий підрозділ компанії, тим більші можливості з’являються у хакера щодо перехоплення незахищеної інформації, тим більше повинна бути безпека каналів підприємства.

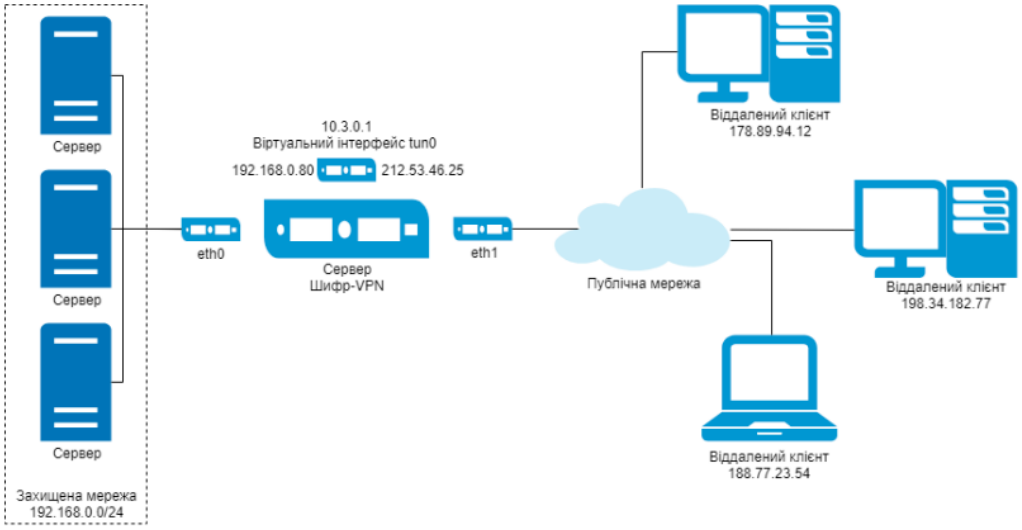

Рисунок 1.3. Структурна схема мережі VPN організацій

Будь-яка організація, обов’язково приходить до питання передачі інформації між своїми офісами, а також з питанням захисту цієї інформації. Не кожна організація може собі дозволити мати власні канали доступу, і це питання дозволяє вирішити технологія VPN, на основі якої і з'єднуються усі підрозділи і офіси, що забезпечує гнучкість і одночасно високу захищеність мережі, а також велику економію витрат на створення цих мереж.

Віртуальна приватна мережа (VPN - Virtual Private Network) створюється на базі загальнодоступної мережі Інтернет. І якщо зв'язок через інтернет має свої недоліки, головним з яких є те, що вона схильна до потенційних порушень захисту і конфіденційності, то VPN можуть гарантувати, що трафік, що направляється через інтернет, захищений, як і передача усередині локальної мережі. У той же час віртуальні мережі забезпечують істотну економію витрат в порівнянні із змістом власної мережі глобального масштабу.

Одним з найважливіших завдань технології VPN є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені лише криптографічним методом .

Так звані виділені лінії не мають особливих переваг перед лініями загального користування в плані інформаційної безпеки. Виділені лінії хоч би частково розташовуватимуться в неконтрольованій зоні, де їх можуть

пошкодити або здійснити до них несанкціоноване підключення. Єдина реальна перевага - це гарантована велика пропускна спроможність виділених ліній, а не підвищена захищеність.

Принцип роботи VPN не суперечить основним мережевим протоколам і технологіям. Наприклад, при установлені з'єднання віддаленого доступа, клієнт посилає серверу потік даних стандартного протокола PPP. У разі організації віртуальних виділених ліній між локальними мережами їх роутери також обмінюються пакетами PPP. Проте, принципіально новим моментом являється пересилка даних через безпечний(зашифрований) тунель, організованний в межах загальнодоступної мережі.

Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, використовуючи інший протокол. В результаті виникає можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Існуюча мережева інфраструктура корпорації може бути підготовлена до використання VPN за допомогою різних варіантів, наприклад програмного рішення. Організацію віртуальної приватної мережі можна порівняти з прокладкою кабелю через глобальну мережу.

Найбільш поширений метод створення тунелів VPN - інкапсуляція мережевого протоколу IP в PPP і подальша інкапсуляція утворених пакетів в протокол тунелювання. Такий підхід називають тунелюванням другого рівня, оскільки тут являється протокол на другому рівні.

Головні особливості корпоративних мереж - глобальність зв'язків і масштабованість - представляють високу небезпеку для виконання ними своїх функціональних обов'язків. Оскільки протоколи сімейства TCP / IP розроблені доволі давно, коли проблема безпеки ще не стяла так гостро, як зараз, то вони, в першу чергу, розроблялися як функціональні і легко переналаштовувані, що допомогло розповсюдитись стеку сімейств TCP/IP на велику кількість комп'ютерних систем. Крім того, в теперішній час при використанні Інтернету

у зловмисників з’являються численні засоби і методи для проникнення і крадіжки даних в корпоративних мережах.

У зв'язку з гігантським ростом численності хостів, підключенних до інтернету, і росту числа великих та малих компаній бізнесу, використовуючих технології інтернету для ведення своєї діяльності, значно збільшилось число інцидентів, пов'язаних з інформаційним втручанням.

До теперішнього часу відома велика кількість різнопланових загроз різноманітного походження, що приховують в собі різну небезпеку для інформації.

Навмисне походження загрози обумовлюється зловмисними діями людей, що здійснюється з метою реалізації виликої кількості видів загроз. Відмічені дві різновидності появи загроз: об'єктивні (кількісна або якісна недостатність елементів системи) і суб'єктивні (діяльність розвідувальних служб іноземних держав, промисловий шпіонаж, діяльність кримінальних елементів, зловмисні дії недобросовісних співробітників системи).

Джерелом загроз можуть бути зловмисники, технічні об’єкти, програми і алгоритми, технологічні схеми обробки даних і зовнішнє середовище.

Основними причинами витоку інформації є:

- недотримання персоналом норм безпеки, вимог, правил експлуатації ситсем захисту інформації;
- помилка в проектуванні захисту систем;
- ведення зловмисною стороною технічної розвідки.

Недотримання персоналом норм, вимог, правил експлуатації може бути як умисним, так і ненавмисним. Від ведення зловмисною стороною розвідки цей випадок відрізняє те, що в данному разі обличчям, що здійснює несанкціоновані дії, рухають особисті мотиви. Причини витоку інформації достатньо тісно пов'язані з видами витоку інформації. Розглядаються три види витоку інформації:

- розголошення інформації;
- несанкціонований доступ до даних;
- отримання захищеної інформації розвідками спецслужб.

Під розголошенням інформації розуміється несанкціоноване доведення захищеної інформації до споживача, які не мають права доступу до захищених даних, а також під несанкціонованим доступом розуміється отримання захищенної інформації зацікавленим суб'єктом з порушенням установлених правовими документами або власником інформації прав або правил доступа до захищених даних. При цьому зацікавленим суб’єктом, що здійснює несанкціонований доступ до інформації, може бути держава, юридична особа, група фізичних осіб (у тому числі громадська організація), окрема особа(хакер).

Отримання захищеної інформації розвідками може здійснюватися за допомогою технічних засобів (технічна розвідка) або агентурними алгоритмами (агентурна розвідка).

Канал витоку інформації - сукупність джерел витоку інформації, матеріального носія або середовища росповсюдження несучого зазначену інформацію сигналу і засоби виділення інформації з сигналу або носія. Однією з основних властивостей каналу є місце розташування засобів виділення інформації з сигналу або носія, які можуть розташовуватись в межах контролюємої зони, охоплюючи систему, або поза нею.

З пункту А в пункт Б необхідно передати інформацію таким чином, щоб до неї зловмисник не зміг отримати доступ. Цілком реальна і часто виникаюча на практиці ситуація, особливо в останній час. Як пункти А і Б можуть виступати окремі вузли або цілі сегменти мереж. У випадку з передачею інформації між мережами в якості захисту може виступати виділений канал зв'язку, що належить компанії, інформація якої вимагає захисту. Однак підтримка таких каналів зв'язку – дуже дороге задоволення.

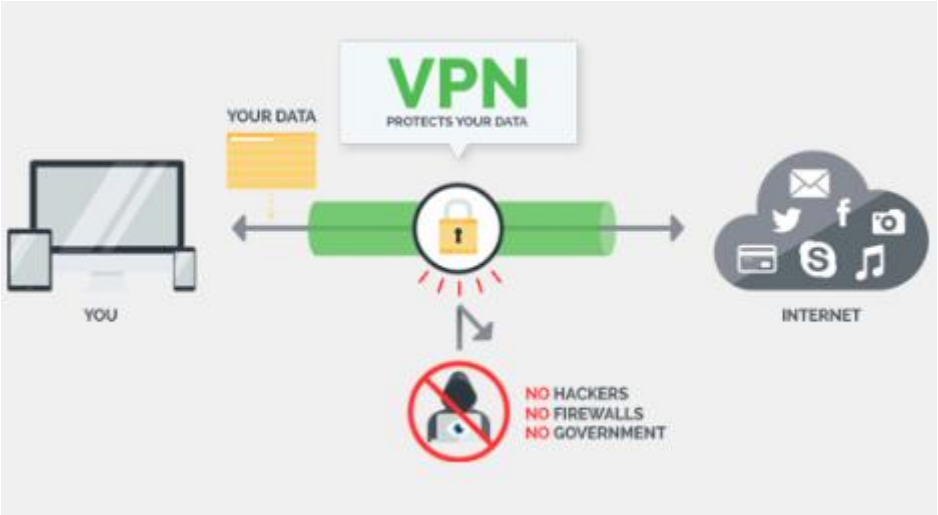

Рисунок 1.4. Ілюстрація захищеного каналу VPN

Легше й дешевше, якщо інформація буде передаватися по звичайним каналам зв'язку (наприклад, через Інтернет), але яким способом буде віддалена або прихована від трафіку інших компаній, циркулюючого в мережі. Потреба в конфіденційній передачі даних виникає лише в глобальних мережах. Така потреба може виникнути і в локальних мережах, де потрібно відділити один тип трафіку від іншого (наприклад, трафік білінг систем від трафіку інформаційної-технологічної системи).

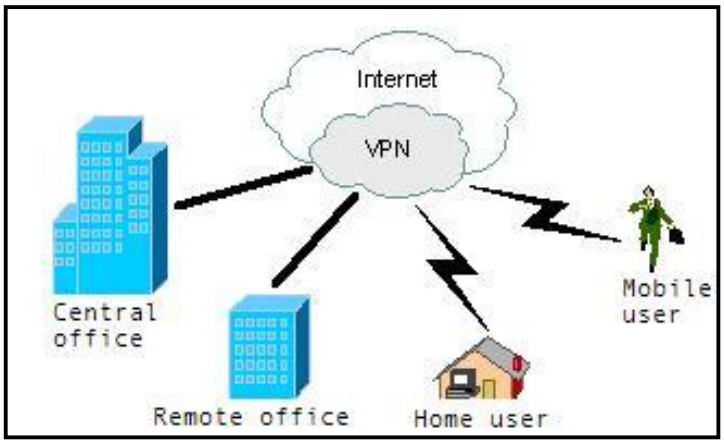

Рисунок 1.5. Елементи мережі організації

Особливість технології VPN в тому, що організація віддаленого доступу робиться через Інтернет, що набагато дешевше і краще. Для організації віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться Інтернет і реальна IP-адреса а також програмне забезпечення. І

будь-який користувач з будь-якої точки земної кулі зможе зайти в захищену мережу, якщо він знає дані авторизації.

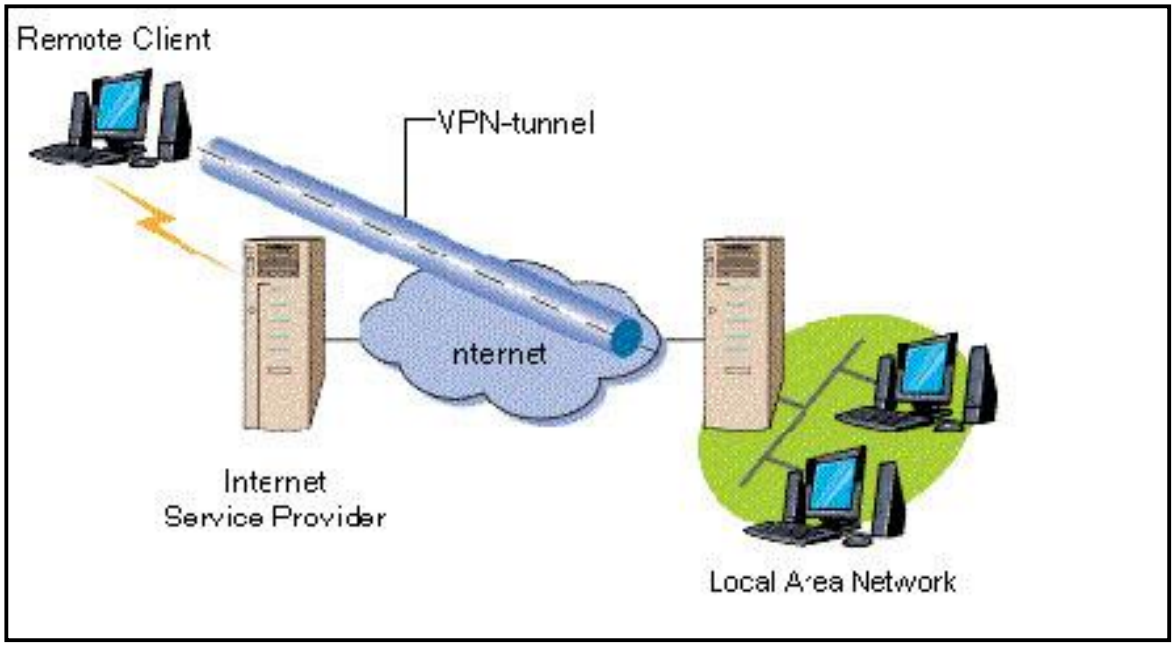

Рисунок 1.6 Доступ віддаленого користувача до локальної мережі корпорації

Якщо є потреба великої кількості ресурсів, розподілених в багатьох мережах, і проблемою являється конфіденційність переміщення інформації в цих мережах, то VPN буде потрібним вибором. В цьому заключається перевага VPN – можна просто захистити від зловмисників всю мережу.

Якщо необхідні хости, які створюють відчуття, що вони знаходяться в одній мережі, VPN - це спосіб реалізувати подібне рішення. Це дійсно зручно, якщо ви працюєте з клієнтами, яким необхідний простий доступ до головних філіалів, або якщо компанія хоче отримати повний и безпечний доступ до локальної мережі. Навіщо турбуватися про плутанину з великою кількістю IP – адрес? Навіщо змінювати інфраструктуру при зміні провайдера? Якщо можна використовувати VPN, то необхідна всього-на-всього конфігурація маршрутизатора.

Використання VPN – це відносно дешевий спосіб з’єднання фізично віддалених мереж. При цьому немає необхідності в оплаті WAN-конектів, так як весь трафік між мережами передається за допомогою інтернету.

1.2. Основні складові VPN мереж

VPN базується на трьох основних методах, які застосовуються при реалізації заходів безпеки в мережах:

1.Тунелювання.

2. Аутентифікація.

3.Шифрування.

1.2.1. Тунелювання

Тунелювання забезпечує передачу шифрованих даних між двома точками - таким чином, що для выдправника і приймача даних виявляється прихованою вся мережева система, що лежить між ними цими точками.

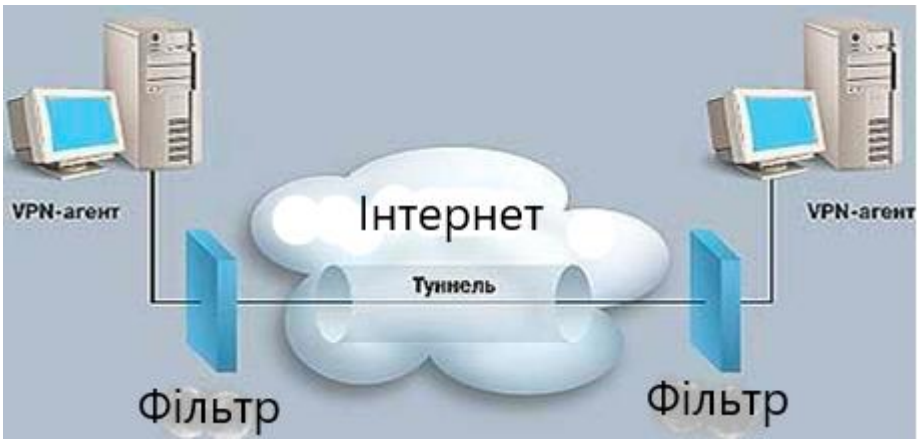

Рисунок 1.7 Реалізація VPN на базі тунелю

Транспортне середовище тунелю, підхоплює дані використовуваного мережевого протоколу на вході в тунель і без змін доставляє їх до виходу. Побудови тунелю достатньо для того, щоб з'єднати два мережевих вузла так, що з точки зору працюючого на них програмного забезпечення вони виглядали підключеними до однієї (локальної) мережі. Однак не можна забувати, що насправді “тунель” з даними проходить через безліч проміжних маршрутизаторів відкритої глобальної мережі.

Такий стан справ таїть в собі дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена правопорушниками.

За допомогою тунелювання пакети даних транслюються через загальнодоступну мережу як по звичайному з'єднанню “точка-точка”. Між кожною парою “відправник-отримувач даних” встановлюється своєрідний тунель - безпечне логічне з'єднання, що дозволяє инкапсулировать дані одного протоколу в пакети іншого. Основними компонентами тунелю є:

• відправник(ініціатор з'єднання);

• маршрутизатор мережі;

• тунельний комутатор;

• один або кілька тунельних термінаторів.

Якщо вона конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже неприємно. Гірше того, зловмисники мають можливість модифікувати передаються через тунель дані так, що одержувач не зможе перевірити їх достовірність. Наслідки можуть бути жахливими. Враховуючи сказане, ми приходимо до висновку, що тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий пакет даних забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакета і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

1.2.2.Аутентифікація

Забезпечення безпеки є основною функцією VPN. Всі дані від комп'ютерів-клієнтів проходять через Internet до VPN-сервера. Такий сервер може знаходитися на великій відстані від клієнтського комп'ютера, і дані на шляху до мережі організації проходять через обладнання безлічі провайдерів. Як переконатися, що дані не були перехоплені або змінені? Для цього застосовуються різні методи аутентифікації і шифрування.

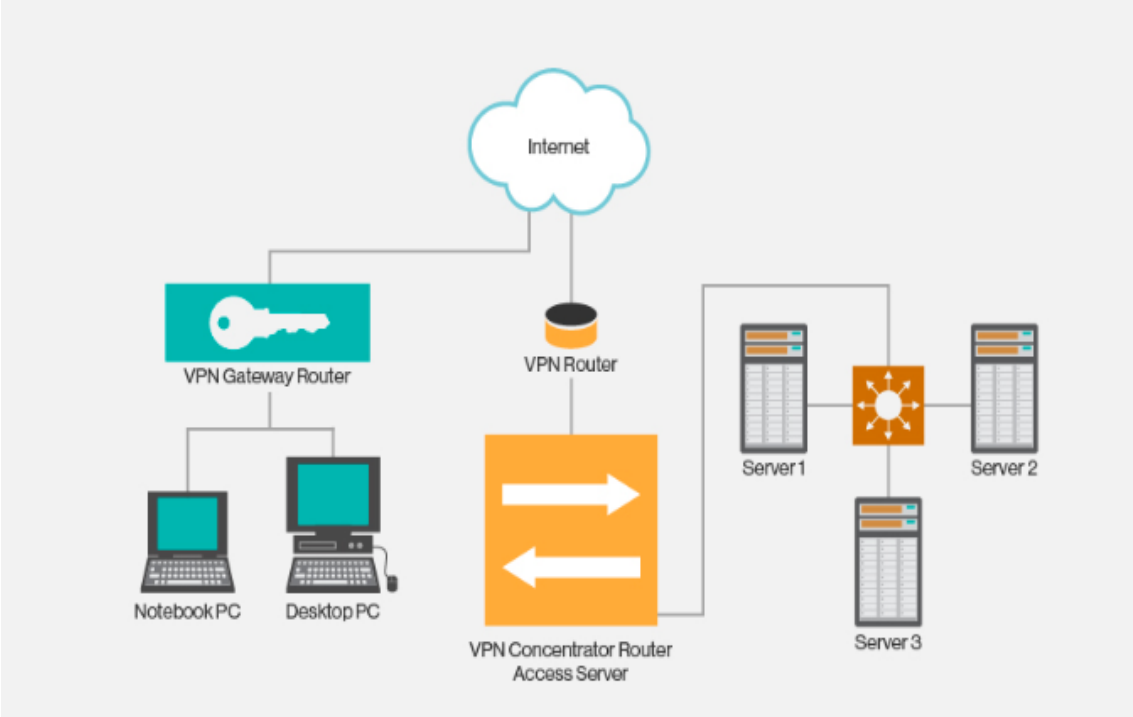

Рисунок 1.8 Аутентифікація користувача в VPN мережах

Для аутентифікації користувачів PPTP може використовувати будь-який з протоколів:

- EAP або Extensible Authentication Protocol;
- MSCHAP або Microsoft Challenge Handshake Authentication Protocol (версії 1 і 2);
- CHAP або Challenge Handshake Authentication Protocol;
- SPAP або Shiva Password Authentication Protocol;
- PAP або Password Authentication Protocol.

Кращими вважаються протоколи MSCHAP версії 2 і Transport Layer Security (EAP-TLS), оскільки вони забезпечують взаємну аутентифікацію,

тобто VPN-сервер і клієнт ідентифікують один одного. У всіх інших протоколах тільки сервер проводить аутентифікацію клієнтів.

Хоча PPTP забезпечує достатній ступінь безпеки, але все ж L2TP поверх IPSec надійніше. L2TP поверх IPSec забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування всіх даних.

Аутентифікація здійснюється або в відритому вигляді (clear text password), або за наступною схемою: запит-відгук. Клієнт посилає серверу пароль. Сервер порівнює це з своєю таблицею і або забороняє доступ, або відповідає підтвердженням. Відкрита аутентифікація практично не зустрічається.

Схема запит-відгук набагато більш застосована. В загальному вигляді вона виглядає так:

- клієнт посилає серверу запит (request) на аутентифікацію;
- сервер повертає свій відгук (challenge);
- клієнт знімає зі свого пароля хеш (хешем називається результат хеш-функції, яка перетворює вхідний масив даних довільної довжини в вихідну бітову комбінацію фіксованої довжини), шифрує їм challenge і передає його серверу;
- те ж саме проробляє і сервер, порівнюючи отриманий результат з відповіддю ініціатора;
- якщо зашифрований запит збігається, аутентифікація вважається успішною.

На першому етапі аутентифікації клієнтів і серверів VPN, L2TP поверх IPSec використовує локальні сертифікати, отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищений коннект ESP SA (security association). Після того як L2TP (поверх IPSec) завершує процес аутентифікації комп'ютера, виконується аутентифікація на рівні користувача. Для аутентифікації можна задіяти будь-який протокол, навіть PAP, що передає ім'я користувача та пароль у незашифрованому вигляді. Це цілком безпечно, так як L2TP поверх IPSec шифрує всю сесію. Проте

проведення аутентифікації користувача при допомоги MSCHAP, що застосовує різні ключі шифрування для аутентифікації комп'ютера і користувача, може посилити захист.

1.2.3. Шифрування

Шифрування гарантує, що майже ніхто не зможе отримати доступ до пакетів при пересиланні через Internet.

Рисунок 1.9 Ілюстрація шифрованого каналу VPN мережах

В даний час підтримуються два методи шифрування:

1. Протокол MPPE шифрування або Microsoft Point-to-Point Encryption сумісний тільки з MSCHAP.
2. EAP-TLS автоматично вибирає довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером.

MPPE працює з ключами довжиною 32, 40, 56, 64, 72, 128 або 256 біт. Операційні системи Windows підтримують шифрування з довжиною ключа тільки 32 та 40 біт, тому в змішаному середовищі Windows слід вибирати довжину ключа яка підтримується усіма пристроями.

Протокол MMPE розроблявся для каналів зв'язку точка-точка, в яких пакети передаються послідовно, і втрата пакетів неможлива. У цій ситуації значення ключа для чергового пакета залежить від результатів дешифрування попереднього пакета. При побудові віртуальних мереж через мережі

загального доступу цих умов дотримуватися неможливо, так як пакети даних часто приходять до одержувача не в тій послідовності, в якій були відправлені. Тому PPTP використовує для зміни ключа шифрування порядкові номери пакетів. Це дозволяє виконувати дешифрацію незалежно від попередніх прийнятих пакетів.

Обидва протоколи реалізовані як в Microsoft Windows, так і поза нею (наприклад, в операційній системі Linux), на алгоритми роботи VPN можуть істотно відрізнятися.

Таким чином, зв'язтунелювання + автентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу.

Додатковим приємним ефектом VPN-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі.

Реалізація віртуальної приватної мережі на практиці виглядає таким чином. У локальній обчислювальній мережі офісу фірми встановлюється сервер VPN. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) з використанням клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером. Відбувається аутентифікація користувача - перша фаза встановлення VPN-з'єднання. У разі підтвердження повноважень настає друга фаза - між клієнтом і сервером виконується узгодження деталей забезпечення безпеки з'єднання. Після цього організується VPN-з'єднання, що забезпечує обмін інформацією між клієнтом і сервером у формі, коли кожен пакет з даними проходить через процедури шифрування / дешифрування та перевірки цілісності - аутентифікації даних.

Основною проблемою мереж VPN є відсутність установлених стандартів аутентифікації і обміну шифрованого інформацією. Ці стандарти все ще знаходяться в процесі розробки і тому продукти різних виробників не можуть встановлювати VPN-з'єднання і автоматично обмінюватися ключами. Дана проблема тягне за собою уповільнення розповсюдження VPN, так як

важко змусити різні компанії користуватися продукцією одного виробника, а тому ускладнений процес об'єднання мереж компаній-партнерів в, так звані, extranet-мережі.

У даному розділі було розглянуто загальну технологію організації VPN підключення до мережі передачі даних, побудову розподільної мережі та віддалений доступ до мережі. Схеми віддаленого доступу можуть відрізнятися також і типом служб, які підтримуються для видаленого клієнта. Найчастіше використовується віддалений доступ до файлів, баз даних, принтерів в тому ж стилі, до якого користувач звик при роботі в локальній мережі. Такий режим називається режимом віддаленого вузла (remote node). Інколи при віддаленому доступі реалізується обмін з центральною мережею повідомленнями електронної пошти, за допомогою якого можна в автоматичному режимі отримати запрошувані корпоративні дані, наприклад з бази даних.

Особливе місце серед всіх видів віддаленого доступу до комп'ютера є спосіб, при якому користувач має можливість віддалено працювати з комп'ютером таким самим чином, ніби він управляв їм за допомогою локального підключеного терміналу. У цьому режимі він може запускати виконання програми на віддаленому комп'ютері і бачити результати роботи у прямому часі. При цьому прийнято розділяти такий спосіб доступу на термінальний доступ і віддалене управління.

Висновки до розділу 1

Мета VPN - прозорий доступ до ресурсів мережі, де користувач може робити все те, що він робить зазвичай незалежно від того, наскільки він віддалений. З цієї причини VPN придбав популярність серед д працівників які працюють віддалено і філіалів, які потребують спільному використанні ресурсів територіально розділених офісів.

Головна ідея VPN - це захист всього трафіку який передається по віртуальним приватним мережам . Реалізація VPN значно спрощує

експлуатацію мережі, її конфігурацію. Комутатори можуть бути простими і дешевими.

Переваги технології VPN в тому, що організація віддаленого доступу робиться не через телефонну лінію, а через Інтернет, що набагато дешевше і краще. Для організації віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться лише Інтернет і реально діюча IP адреса. І будь-який користувач з будь-якого куточка земної кулі зможе зайти в мережу, якщо він знає IP адресу, логін і пароль [1]

Насамперед, інформація передається в зашифрованому виді. Прочитати отримані дані може лише власник ключа до шифру. Підтвердження справжності містить у собі перевірку цілісності даних і ідентифікацію користувачів, задіяних в VPN. Перша гарантує, що дані дійшли до адресата саме в тому виді, у якому послані.

Переваги VPN очевидні. Надавши користувачам можливість з’єднуватися через Інтернет, масштабованість досягається в основному збільшенням пропускної здатності каналу зв’язку, коли мережа стає перевантаженої. VPN допомагає заощадити на телефонних витратах, оскільки вам не потрібно мати справу з пулом модемів. Крім того, VPN дозволяють отримати доступ до мережевих ресурсів, які в звичайній ситуації адміністратори змушені виносити на зовнішнє з’єднання.

Отже, створення захищених приватних мереж, застосування технології шифрування інформації є важливим завданням для кожного підприємства.

2. КЛАСИФІКАЦІЯ VPN І ЇХ ХАРАКТЕРИСТИКА

2.1.Класифікація VPN і їх характеристика

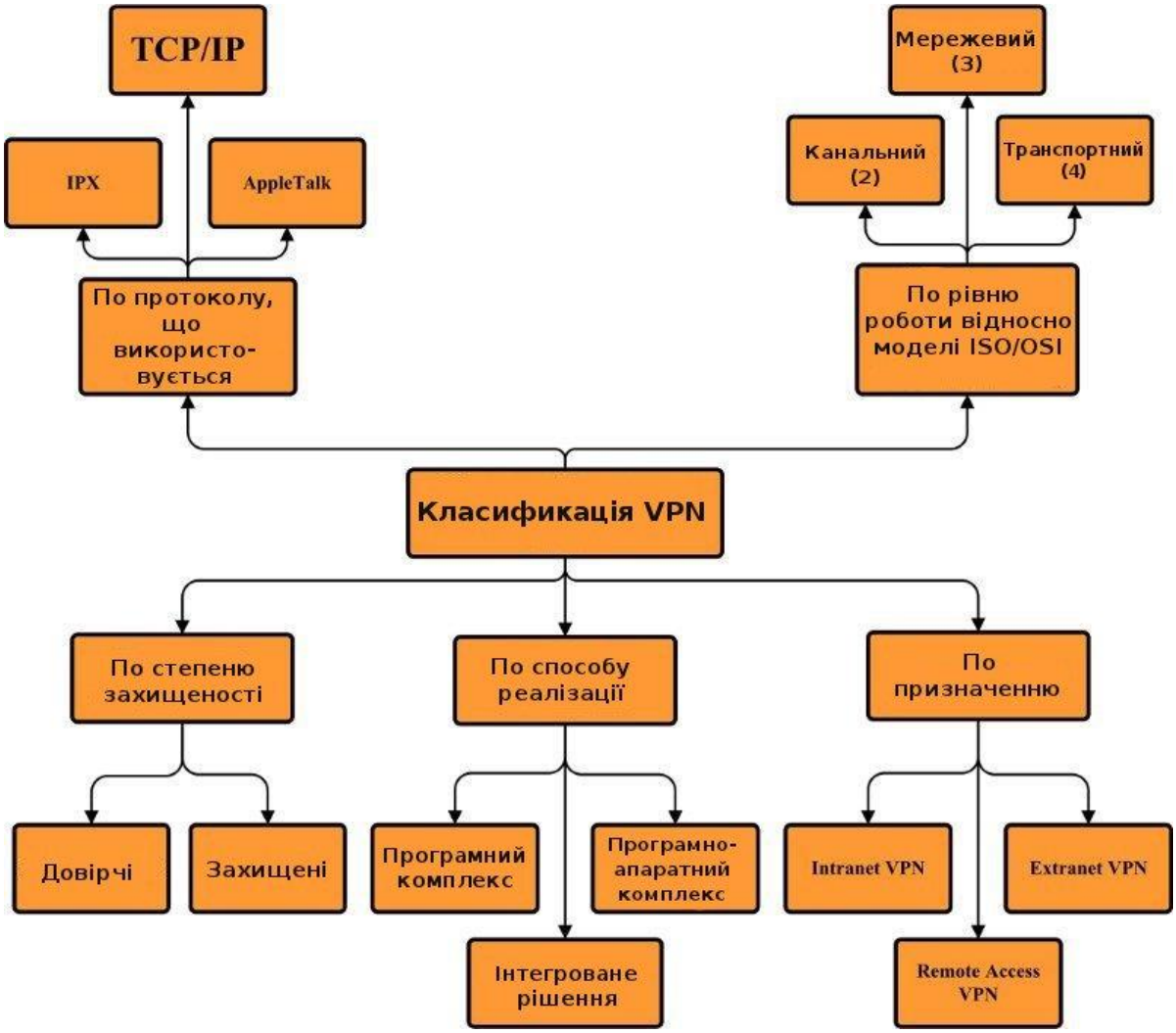

Рисунок 2.1 Класифікація VPN

VPN класифікують по наступним основним параметрам:

1.По степеню захищеності.

2. По способу реалізації

3. По призначенню

4. По протоколу, що використовується

5. По рівню роботи відносно роботи стека протоколів OSI

2.1.1. За типом використовуваного середовища

За типом використовуваного середовища поділяються на захищені і довірчі.

a)Захищені VPN мережі. Найбільш поширений варіант приватних мереж. За його допомогою можливо створити захищену і надійну підмережу на основі ненадійної мережі, як правило, інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

b)Довірчі VPN мережі. Використовуються у випадках, коли передавальне середовище можна вважати надійним і необхідним для вирішення лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN вирішенні є: MPLS і L2TP. Коректніше сказати, що ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec.

2.1.2 За способом реалізації

a)VPN мережі у вигляді спеціального програмно-апаратного забезпечення. Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

b)VPN мережі у вигляді програмного рішення. Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

c)VPN мережі з інтегрованим рішенням. Функціональність VPN забезпечує комплекс, вирішальний також завдання фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

2.1.3 За призначенням

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

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

2.1.4 По протоколу, що використовується

Існують наступні реалізації віртуальних приватних мереж: TCP/IP, IPX і AppleTalk. На сьогоднішній день виробники програмного забезпечення переходять на протокол TCP / IP, і абсолютна більшість VPN рішень підтримує саме його.

2.1.5. По рівню роботи відносно роботи стека протоколів OSI

Мережі VPN будуються з використанням протоколів 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 сьогоднішній день для побудови мереж VPN використовуються протоколи наступних рівнів:

1)канальний рівень.

2)мережевий рівень.

3)транспортний рівень.

2.1.5.1.Канальний рівень

На канальному рівні можуть використовуватися протоколи тунелювання даних L2TP і PPTP, які використовують авторизацію і аутентифікацію.

L2TP. У найближчому майбутньому очікується зростання кількості віртуальних приватних мереж, розгорнутих на базі протоколу тунелювання другого рівня Layer 2 Tunneling Protocol - L2TP.

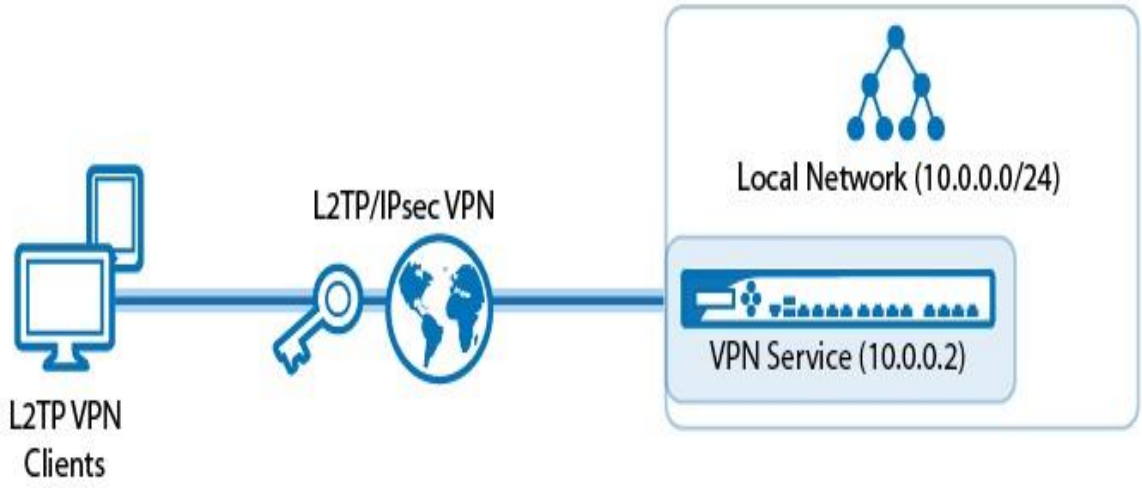

Рисунок 2.2. Канальний рівень

L2TP з'явився в результаті об'єднання протоколів PPTP і L2F (Layer 2 Forwarding). PPTP дозволяє передавати через тунель пакети PPP, а L2F-пакети SLIP і PPP. Протокол L2TP увібрав в себе кращі риси PPTP і L2F. Головне достоїнство L2TP в тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay. На жаль, реалізація L2TP в Windows 2000 підтримує тільки IP.

L2TP застосовує в якості транспорту протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилання даних. L2TP в реалізації Microsoft використовує в якості контрольних повідомлень пакети UDP, що містять шифровані пакети PPP. Надійність доставки гарантує контроль послідовності пакетів.

Функціональні можливості PPTP і L2TP різні. L2TP може використовуватися не тільки в IP-мережах, службові повідомлення для створення тунелю і пересилання за нього даних використовують однаковий формат і протоколи. PPTP може застосовуватися тільки в IP-мережах, і йому необхідно окреме з'єднання TCP для створення і використання тунелю. L2TP поверх IPSec пропонує більше рівнів безпеки, ніж PPTP, і може гарантувати майже 100-відсоткову безпеку важливих для організації даних. Особливості L2TP роблять його дуже перспективним протоколом для побудови віртуальних мереж.

Протокол тунелювання другого рівня (L2TP) - протокол тунелювання на основі RFC, який є галузевим стандартом і вперше підтримується в клієнтських та серверних операційних системах. На відміну від PPTP, L2TP н не використовує Encryption-Point-to-Point-Encryption (MPPE) для шифрування дейтаграм протоколу «точка-точка» (PPP). L2TP покладається на безпеку протоколу шифрування IPSec. Комбінація L2TP та IPSec відома як L2TP/IPSec. L2TP/IPSec надає послуги первинної віртуальної приватної мережі (VPN) інкапсуляції та шифрування приватних даних.

L2TP використовує два види пакетів: інформаційні та керуючі пакети. Керуючі пакети використовуються при встановленні, підтримці тунелів. Інформаційні повідомлення використовуються для інкапсуляції PPP-кадрів, що надсилаються через тунель. Керуючі повідомлення використовують надійний контрольний канал в межах L2TP, щоб гарантувати доставку. Інформаційні повідомлення при втраті не будуть пересилатися повторно.

Таблиця 2.1.Структура протоколу:

PPP кадри	
L2TP інформаційні повідомлення	L2TP управляючі повідомлення
L2TP інформаційний канал (ненадійний)	L2TP канал управління (надійний)
Транспортування пакетів (UDP, FR, ATM тощо)	

Таблиця 2.2. Формат заголовка:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16						31
T	L	x	x	S	x	O	P	x	x	x	x	Версія				Довжина(опц)						
ID тунелю																ID сесії						
Ns (опц)																Nr (опц)						
Offset Size (опц)																Offset Pad (опц).....						
Payload data																						

- Біт тип (T) характеризує різновид пакета.
- Він встановлюється рівним 0 для інформаційних повідомлень і 1 - для управляючих.
- Якщо біт довжини (L) дорівнює 1, поле довжина присутнє.
- Для керуючих повідомлень цей біт повинен бути рівний 1.
- Біти x зарезервовані для майбутніх застосувань.
- Всі зарезервовані біти повинні бути встановлені рівними 0 для вихідних повідомлень і ігноруватися для вхідних.
- Якщо біт послідовності (S) дорівнює 1, присутні поля Ns і Nr.
- Біт S для керуючих повідомлень повинен бути рівний 1.
- Якщо біт зсуву (O) дорівнює 1, поле величини зміщення присутнє.
- Біт O для керуючих повідомлень повинен бути рівний 0.
- Біт пріоритету (P) повинен бути рівний 0 для всіх керуючих повідомлень. Для інформаційних повідомлень - якщо цей біт дорівнює 1, це інформаційне повідомлення має пріоритет в черзі.
- Поле Ver вказує версію заголовка інформаційного повідомлення L2TP.

- Значення 1 зарезервовано для детектування пакетів L2F в умовах, коли вони приходять упереміш з L2TP-пакетами. Пакети, отримані з невідомим значенням поля Ver, відкидаються.

- Поле Довжина (опціонально) вказує загальну довжину повідомлення в октетах.

- ID-тунелю містить ідентифікатор керуючого з'єднання. Ідентифікатори тунелю L2TP мають тільки локальне значення. Тобто, різні кінці одного тунелю повинні мати різні ID. ID-тунелю в кожному повідомленні має бути тим, яке очікує отримувач. ID-тунелю вибираються при формуванні тунелю.

- ID-сесії визначає ідентифікатор для сесії даного тунелю. Сесії L2TP іменуються за допомогою ідентифікаторів, які мають тільки локальне значення. ID-сесії в кожному повідомленні має бути тим, яке очікує отримувач. ID-сесії вибираються при формуванні сесії.

- Поле Ns визначає порядковий номер інформаційного або керуючого повідомлення, починаючи з нуля і збільшуючись на 1 (по модулю 216) для кожного посланого повідомлення.

- Поле Nr містить порядковий номер, який очікується для наступного повідомлення. Таким чином, Nr робиться рівним Ns останнього по порядку отриманого повідомлення плюс 1 (по модулю 216). В інформаційних повідомленнях, Nr зарезервовано і, якщо присутній (це визначається S-бітом), повинно ігноруватися при отриманні.

- Поле величина зсуву (Offset Size), якщо є, специфікує число октетів після заголовка L2TP, де має починатися поле даних. Вміст заповнювача зсуву не визначено. Якщо поле зміщення присутній, заголовок L2TP завершується після завершального октету заповнювача зсуву.

Протокольні операції:

Необхідна процедура встановлення PPP-сесії тунелювання L2TP включає в себе два етапи:

- Встановлення керуючого каналу для тунелю
- Формування сесії відповідно до запиту вхідного або вихідного виклику.

Тунель і відповідний керуючий канал повинні бути сформовані до ініціалізації вхідного або вихідного виклику. L2TP-сесія повинна бути реалізована до того, як L2TP зможе передавати PPP-кадри через тунель. В одному тунелі можуть існувати кілька сесій між одними і тими ж LAC і LNS.

Керуюче з'єднання. Є первинним, яке має бути реалізовано між LAC і LNS перед запуском сесії. Встановлення керуючого з'єднання включає в себе безпечну ідентифікацію партнера, а також визначення версії L2TP, можливостей каналу, кадрового обміну. L2TP включає в себе просту, опціонну, CHAP-подібну систему аутентифікації тунелю в процесі встановлення керуючого з'єднання.

Встановлення сесії. Після успішного встановлення керуючого з'єднання можуть формуватися індивідуальні сесії. Кожна сесія відповідає одному PPP інформаційного потоку між LAC і LNS. На відміну від встановлення керуючого з'єднання, встановлення сесії є асиметричним щодо LAC і LNS. LAC запитує LNS доступ до сесії для вхідних запитів, а LNS запитує LAC запустити сесію для роботи з вихідними запитами.

Коли тунель сформований, PPP-кадри від віддаленої системи, одержувані LAC, звільняються від CRC, канальних заголовків і т. ін., інкапсульованих в L2TP, і переадресовуються через відповідний тунель. LNS отримує L2TP-пакет і обробляє інкапсульований PPP-кадр, як якщо б він був отриманий через локальний інтерфейс PPP.

Відправник повідомлення, асоційований з певною сесією і тунелем, поміщає ID сесії і тунелю (специфіковані партнером) у відповідні поля заголовка всіх вихідних повідомлень.

І L2TP, і IPSec повинні підтримуватися як клієнтом VPN, так і сервером VPN. L2TP встановлюється за допомогою протоколу TCP / IP. Залежно від вибору під час настройки сервера маршрутизації та віддаленого доступу, L2TP налаштовано на п'ять або 128 портів L2TP.

В даний час найбільш поширеним протоколом VPN є протокол “точка точка” тунельної зв'язку або Point-to-Point Tunnelling Protocol - PPTP. PPTP використовує існуючі відкриті стандарти TCP / IP і багато в чому покладається на застарілий протокол двухточечной зв'язку PPP. На практиці PPP так і залишається комунікаційним протоколом сеансу з'єднання PPTP. PPTP створює тунель через мережу до NT-сервера одержувача і передає по ньому PPP-пакети віддаленого користувача. Сервер і робоча станція використовують віртуальну приватну мережу і не звертають уваги на те, наскільки безпечною або доступною є глобальна мережа між ними.

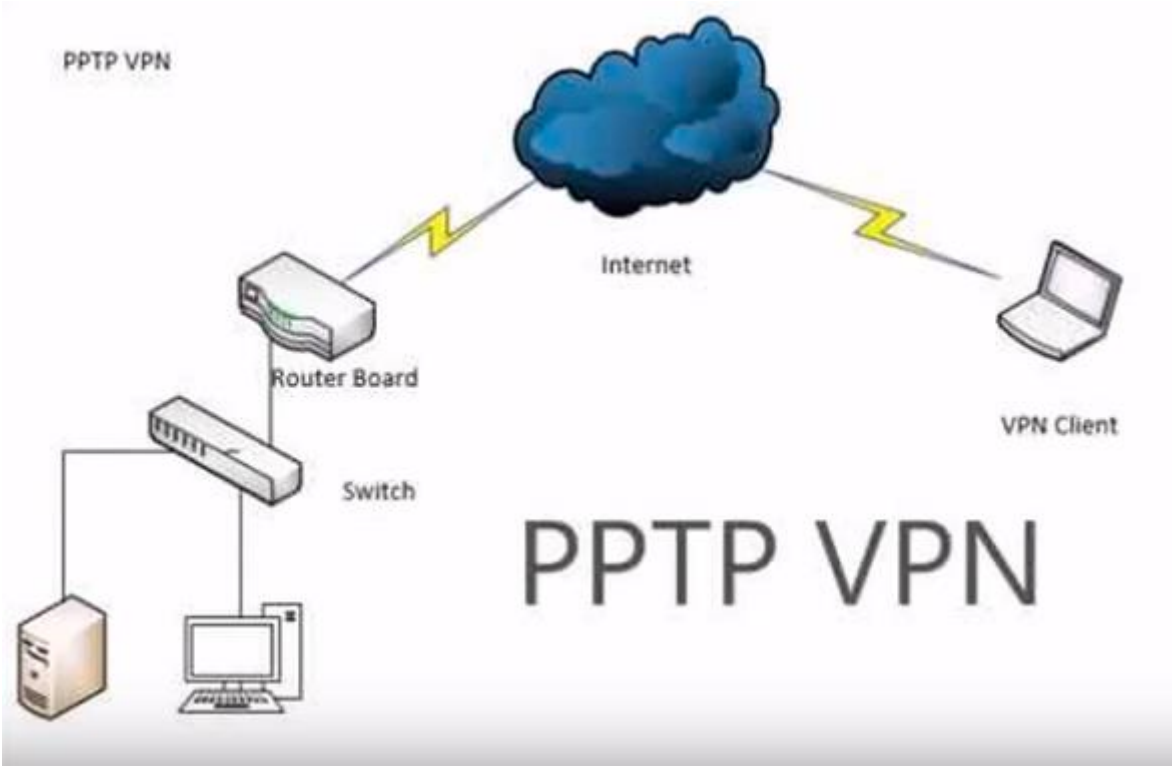

Рисунок 2.3. Структурна побудова мережі на базі протоколу PPTP

Хоча компетенція протоколу PPTP поширюється лише на пристрої, що працюють під управлінням Windows, він надає компаніям можливість взаємодіяти з існуючими мережевими інфраструктурами і не завдавати шкоди

власній системі безпеки. Таким чином, віддалений користувач може підключитися до Інтернету за допомогою місцевого провайдера за допомогою аналогового або каналу ISDN і встановити з'єднання з сервером NT. При цьому компанії не доводиться витрачати великі суми на організацію і обслуговування пулу модемів, що надає послуги віддаленого доступу. PPTP - тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі.

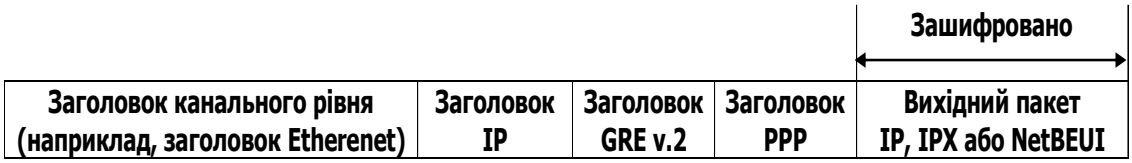

Рисунок 2.4. Структурна пакета PPTP

PPTP інкапсулює пакети IP для передачі по IP-мережі. Клієнти PPTP використовують порт призначення для створення керуючого тунелем з'єднання. Цей процес відбувається на транспортному рівні моделі OSI. Після створення тунелю комп'ютер-клієнт і сервер починають обмін службовими пакетами. На додаток до керуючого з'єднанню PPTP, що забезпечує працездатність каналу, створюється з'єднання для пересилання по тунелю даних. Інкапсуляція даних перед пересиланням через тунель відбувається дещо інакше, ніж при звичайній передачі. Інкапсуляція даних перед відправкою в тунель включає два етапи:

Потім отримані дані відправляються вгору по моделі OSI і инкапсулируются протоколами верхніх рівнів.

Таким чином, під час другого проходу дані досягають транспортного рівня. Однак інформація не може бути відправлена за призначенням, так як за це відповідає канальний рівень OSI. Тому PPTP шифрує поле корисного навантаження пакета і бере на себе функції другого рівня, зазвичай належать PPP, тобто додає до PPTP-пакету PPP-заголовок і закінчення. На цьому створення кадру канального рівня закінчується.

Далі, PPTP інкапсулює PPP-кадр в пакет Generic Routing Encapsulation (GRE), який належить мережевого рівня. GRE инкапсулирует мережевий рівень, наприклад IPX, AppleTalk, DECnet, щоб забезпечити можливість їх передачі по IP-мереж. Однак GRE не має можливості встановлювати сесії і забезпечувати захист даних від зловмисників. Для цього використовується здатність PPTP створювати з'єднання для управління тунелем. Застосування GRE в якості методу інкапсуляції обмежує поле дії PPTP тільки мережами IP.

Після того як кадр PPP був інкапсулює в кадр з заголовком GRE, виконується інкапсуляція в кадр з IP-заголовком. IP-заголовок містить адреси відправника і одержувача пакету. На закінчення PPTP додає PPP заголовок і закінчення. На додатку 3 показана структура даних для пересилання по тунелю PPTP.

Система-відправник посилає дані через тунель. Система-одержувач видаляє всі службові заголовки, залишаючи тільки дані PPP.

MPLS VPN - це сімейство методів використання мультипротокольних комутацій міток (MPLS) для створення віртуальних приватних мереж (VPN). MPLS VPN - це гнучкий метод транспортування та маршрутування декількох типів мережевого трафіку за допомогою магістралі MPLS. Сьогодні в мережах розгорнуто три типи VPN-мереж MPLS:

1. Точка-точка (псевдопровід)

2. рівень 2 (VPLS)

3. рівень 3 (VPRN)

MPLS працює на рівні, який можна було б розташувати між канальним і третім мережевим рівнями моделі OSI, і тому його зазвичай називають протоколом канально-мережевого рівня. Точкові MPLS VPN-адреси використовують VLL (віртуальні орендовані лінії) для забезпечення зв’язку Layer2 «точка-точка» між двома сайтами. Кадри Ethernet, TDM та ATM можуть бути інкапсульовані в межах цих VLL.

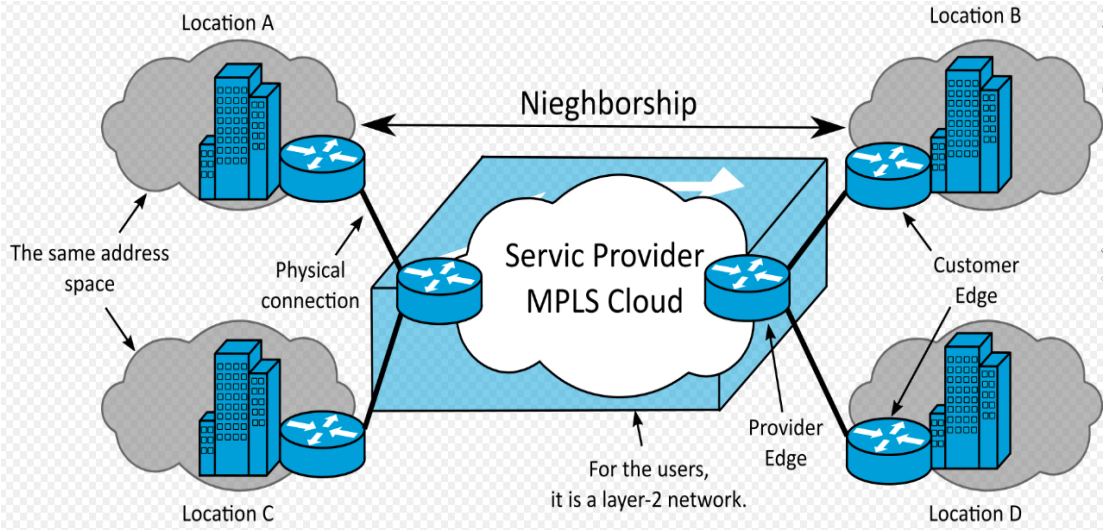

Рисунок 2.5. Структура MPLS мереж

MPLS VPN працює на двох областях: мережі IP-клієнтів і внутрішня (магістральна) MPLS провайдера, необхідна для об'єднання сетей клієнтів

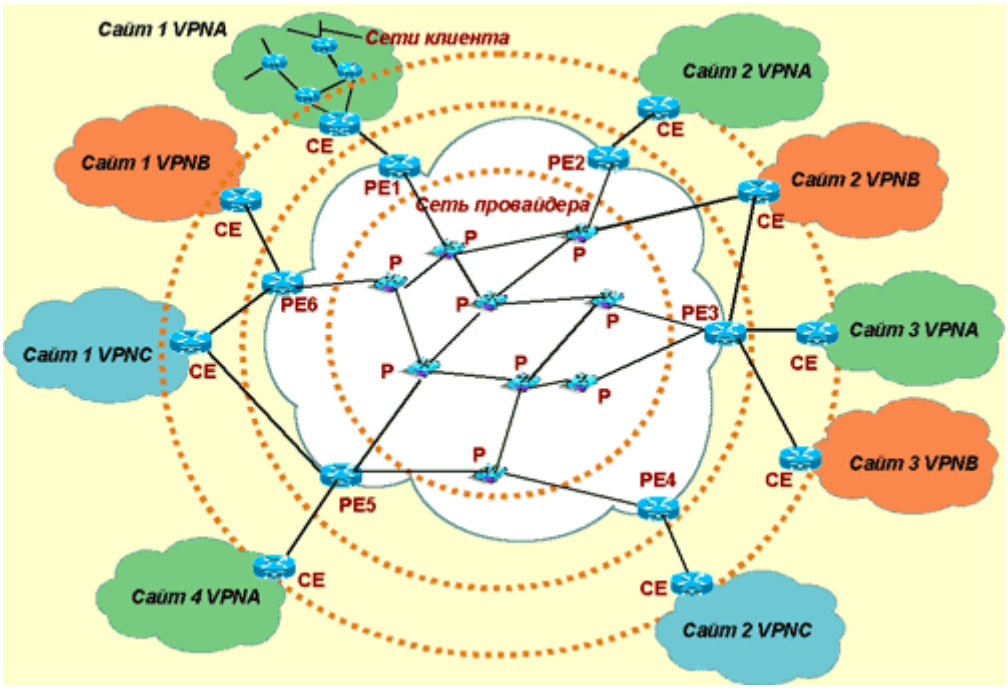

Рисунок 2.6. Компоненти MPLS VPN

У загальному випадку, коли кожен клієнт може бути декількома територіально обумовленими мережевими IP-адресами, кажна з яких може містити кілька підсетей, пов'язаних з маршрутами. Такі територіально виділені мережеві ділянки корпоративної мережі прийняті називати сайти. Сайти які належать одному клієнтові обмінюються пакетами IP-адреси, через які вони пропонують і створюють віртуальну приватну мережу цього клієнта.

Наприклад, про корпоративні мережі, в яких є центральний відділ, відомий з віддаленими філіалами, можна сказати, що вона є з чотирьох сайтів. Для обміну маршрутною інформацією на веб-сайті, що використовується, використовується внутрішній протокол маршрутизації (Internal Gateway Protocol, IGP), область, яка обмежена автономною системою: RIP, OSPF або IS-IS.

2.1.2.2.Мережевий рівень

На мережевому рівні використовується протокол IPSec за допомогою IPSec реалізується шифрування і конфіденційність даних, а також аутентифікацію абонентів. Застосування протоколу IPSec дозволяє реалізувати повнофункціональний доступ еквівалентний фізичній підключенню до корпоративної мережі. Для встановлення VPN кожен з учасників повинен конфігурувати певні параметри IPSec, тобто кожен клієнт повинен мати програмне забезпечення яке буде реалізувати IPSec.

IPsec розроблений для забезпечення сумісного, високоякісного криптографічного захисту для IPv4 та IPv6. Набір пропонованих служб безпеки включає контроль доступу, цілісність без зв'язку, автентифікацію джерела даних, захист від повторів (форма часткової цілісності послідовності), шифрування та обмежену конфіденційність всього потоку трафіку. Ці послуги надаються на рівні IP, забезпечуючи захист протоколів IP та / або верхнього рівня.

Ці цілі досягаються за допомогою використання двох протоколів безпеки руху, заголовка автентифікації (AH) та корисного навантаження інкапсуляції безпеки (ESP), а також за допомогою використання криптографічного ключа

процедури управління протоколами. Набір протоколів IPsec у будь-якому контексті та способів їх налаштування, буде визначатися безпекою та системними вимогами користувачів, додатками та/або сайтами будь-якої організації.

Якщо ці механізми правильно впроваджені та розгорнуті, вони не повинні негативно впливати на користувачів, хостів та інші мережеві Інтернет компоненти, які не використовують ці механізми безпеки для захисту свого трафіку. Ці механізми також розроблені як незалежні від алгоритму. Ця модульність дозволяє вибирати різні набори алгоритмів, не впливаючи на інші частини реалізації. Наприклад, різні спільноти користувачів при необхідності можуть вибрати різні набори алгоритмів шифрування даних.

Стандартний набір алгоритмів за замовчуванням визначений для полегшення сумісності в глобальному Інтернеті. Застосування цих алгоритмів у поєднанні із протоколами захисту трафіку IPsec та протоколами управління ключами покликане дозволити розробникам систем та додатків розгорнути високоякісну технологію криптографічної безпеки.

Жодна компанія не хотіла б відкрито третім особам передавати фінансову або іншу конфіденційну інформацію. Канали VPN захищені потужними алгоритмами шифрування, закладеними в стандарти протоколу безпеки IPsec. IPSec або Internet Protocol Security - стандарт, обраний міжнародним співтовариством, групою IETF - Internet Engineering Task Force, створює основи безпеки для Інтернет-протоколу (IP / Протокол IPSec забезпечує захист на мережевому рівні і вимагає підтримки стандарту IPSec тільки від людей, що спілкуються між собою пристроїв по обидві боку з'єднання. Всі інші пристрої, розташовані між ними, просто забезпечують трафік IP-пакетів.

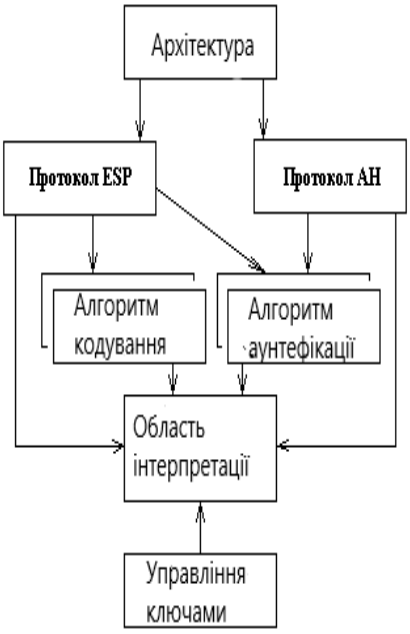

Рисунок 2.7. Архітектура IPSec.

Стандарт безпеки протоколу Інтернету (IPsec) та стандарт Асоціації безпеки в Інтернеті та протоколу управління ключами (ISAKMP), які використовуються для побудови віртуальних приватних мереж (VPN). Створені захищені зв’язки між віддаленими користувачами та приватною корпоративною мережею. Кожне захищене з'єднання називається тунелем. ASA використовує стандарти тунелювання ISAKMP та IPsec для побудови та управління тунелями. ISAKMP та IPsec здійснюють наступне:

• узгодження параметрів тунелю

• встановлення тунелю

• аутентифікацію користувачів і дані

• управління ключами безпеки

• шифрувати і дешифрувати даних

• управління передачею даних через тунель

• Управління передачею даних на вході і виході в якості кінцевої точки тунелю або маршрутизатора.

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

В питаннях вибору рівня реалізації захищеного каналу є кілька аргументів: з однієї сторони, за вибор верхніх рівнів говорить про свою незалежність від видів транспортування (вибору протоколу мережевого та канального рівня), з іншої сторони, для кожного рівня необхідні окремі налаштування та конфігурація. Плюсом у виборі нижчих рівнів є їх універсальність і огляд для запропонованого, мінус - залежність від вибору конкретного протоколу (наприклад, PPP або Ethernet). Компромісним рівнем вирівнювання є IPsec: він розміщений на мережевому рівні, використовуючи найвищий розширений протокол цього рівня - IP. Це робить IPsec більш гнучким, так що він може використовуватись для захисту будь-яких протоколів, заснованих на TCP та UDP. У той час, він прозоро для більшої кількості пропозицій.

Під час створення тунелю йде домовленість про асоціацію безпеки, яка керує автентифікацією, шифруванням, інкапсуляцією та управлінням ключами. Ці домововленості передбачають дві фази: перша, встановити тунель (IKE SA) і другий, керувати трафіком всередині тунелю (IPsec SA). VPN від локальної мережі до локальної мережі з'єднує мережі в різних географічних місцях. У підключеннях IPsec LAN-LAN до IPsec,

Тунелі IPsec - це набори, які встановлюється між точками. SA визначають протоколи та алгоритми, що застосовуються до конфіденційних даних, а також вказують ключі, які використовують відповідні точки. IPsec SA контролюють фактичну передачу трафіку користувача. Між точками узгоджується налаштування, які слід використовувати для кожного CA. Кожен SA складається з наступного:

• набори перетворень IKEv1 або IKEv2

• криптодані

• ACL

• Тунельні групи

• Політика передфрагментації

Побудову захищеного каналу зв'язку може бути реалізовано на різних рівнях OSI.

IPsec є набором стандартів Інтернету та свого роду «надстройкою» над IP-протоколом. Його ядро складають три протоколи:

- Заголовок аутентифікації (AH) забезпечує цілісність передаваних даних, аутентифікацію історичної інформації та функціонування за допомогою повторної передачі пакетів передачі
- Інкапсуляція безпеки корисного навантаження (ESP) забезпечує достовірність (шифрування) передавальної інформації, обмеження потоку конфіденціальної трафіки. Крім цього, він може виконувати функції AH: забезпечувати цільову перехідність даних, аутентифікацію історичної інформації та функціонування за допомогою повторної передачі пакетів. Застосовуючи ESP в обов'язковому порядку, потрібно вказати набір послуг, забезпечених безпекою: каждая з його функцій може включати в себе опціонально.
- Протокол асоціації Інтернет-безпеки та керування ключами (ISAKMP) - протокол, використовуваний для первинної справи, з'єднання, взаємна аутентифікація, котрі підходять іншим та помітним секретним ключам. Протокол попередньо містить використані різні механізми обміну ключовими ключами, включаючи завдання фіксованих ключів, використаних таких протоколів, як Інтернет-обмін ключами, керберизовані Інтернет-переговори ключів або запис DNS типу IPSECKEY.

Аутентифицирующей заголовок (AH) є звичайним опціональним заголовком і, як правило, розташовується між основним заголовком пакету IP

і полем даних. Наявність АН ніяк не впливає на процес передачі інформації транспортного і більш високого рівнів. Основним і єдиним призначенням АН є забезпечення захисту від атак, пов'язаних з несанкціонованою зміною вмісту пакета, і в тому числі від підміни вихідного адреси мережевого рівня. Протоколи вищого рівня повинні бути модифіковані з метою здійснення перевірки автентичності отриманих даних.

Формат АН достатньо простий і складається з 96-бітового заголовка і даних змінної довжини, що складаються з 32-бітових слів. Назви полів достатньо ясно відображають їх вміст: Next Header указує на наступний заголовок, Payload Len представляє довжину пакета, SPI є покажчиком на контекст безпеки і Sequence Number Field містить послідовний номер пакету.

IPsec може функціонувати в двох режимах: транспортному і тунельному.

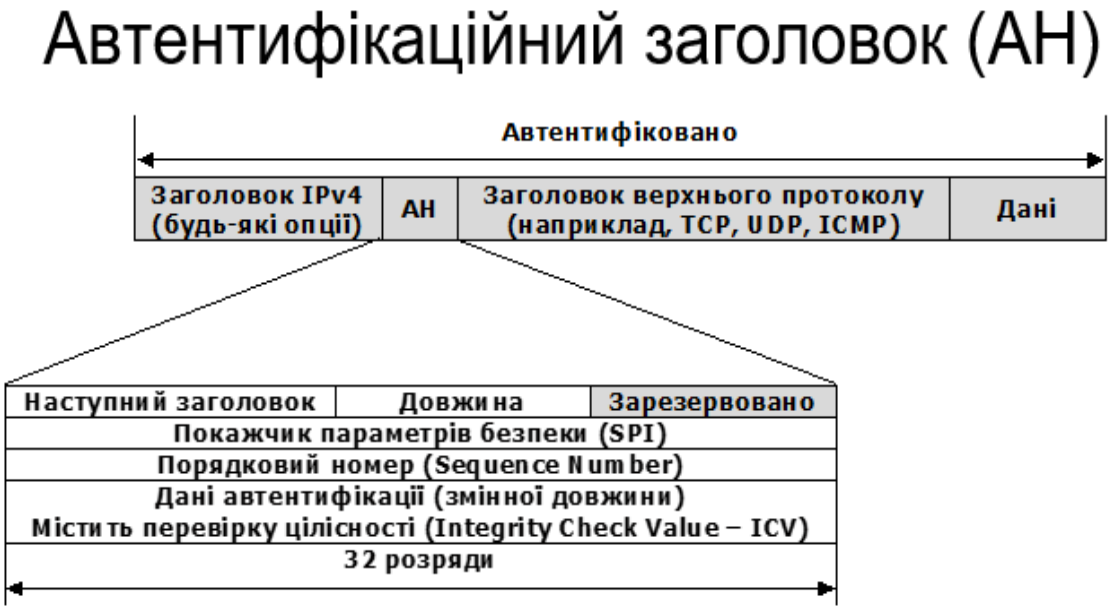

Рисунок 2.8.Структура заголовка АН.

У разі використання інкапсуляції зашифрованих даних заголовок ESP є останнім в ряду опціональних заголовків, "видимих" в пакеті. Оскільки основною метою ESP є забезпечення конфіденційності даних, різні види інформації можуть вимагати застосування істотно різних алгоритмів шифрування. Отже, формат ESP може зазнавати значних змін в залежності від

використовуваних криптографічних алгоритмів. Проте, можна виділити наступні обов'язкові поля: SPI, яке вказує на контекст безпеки і Sequence Number Field, що містить послідовний номер пакету. Поле "ESP Authentication Data" (контрольна сума), не є обов'язковим в заголовку ESP. Одержувач пакету ESP розшифровує ESP заголовок і використовує параметри і дані вживаного алгоритму шифрування для декодування інформації транспортного рівня.

У транспортному режимі шифруються (або підписуються) тільки дані IP-пакета, вихідний заголовок зберігається. Транспортний режим, як правило, використовується для встановлення з'єднання між хостами. Він може також використовуватися між шлюзами для захисту тунелів, організованих яким-небудь іншим способом (Наприклад, L2TP).

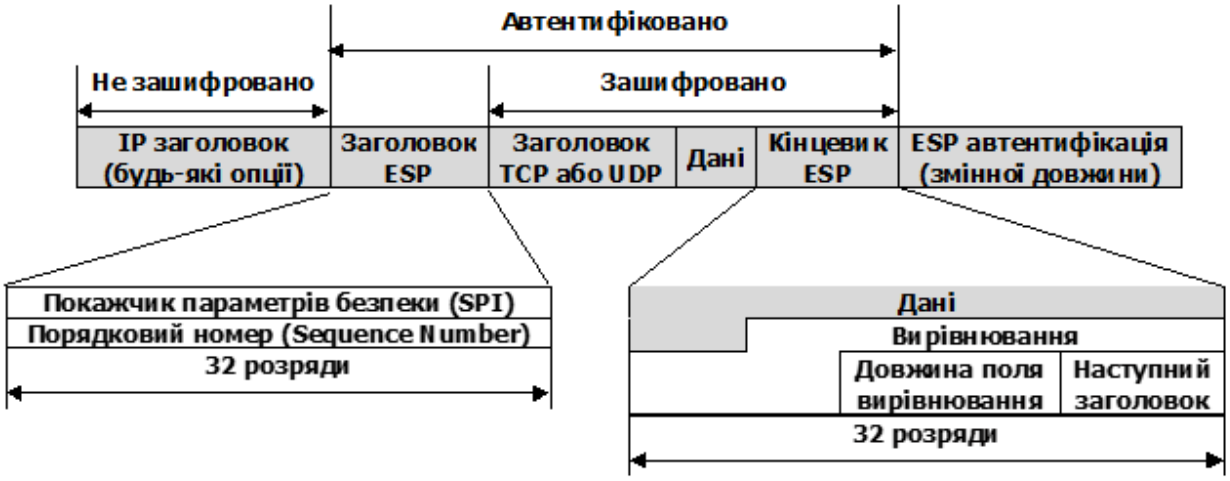

Рисунок 2.8.Структура заголовка ESP.

У тунельному режимі шифрується весь вихідний IP-пакет: дані, заголовок, маршрутна інформація, а потім він вставляється в поле даних нового пакета, тобто відбувається інкапсуляція. Тунельний режим може використовуватися для підключення віддалених комп'ютерів до віртуальної приватної мережі або для організації безпечної передачі даних через відкриті канали зв'язку (наприклад, Інтернет) між шлюзами для об'єднання різних частин віртуальної приватної мережі. Режими IPsec не є взаємовиключними.

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

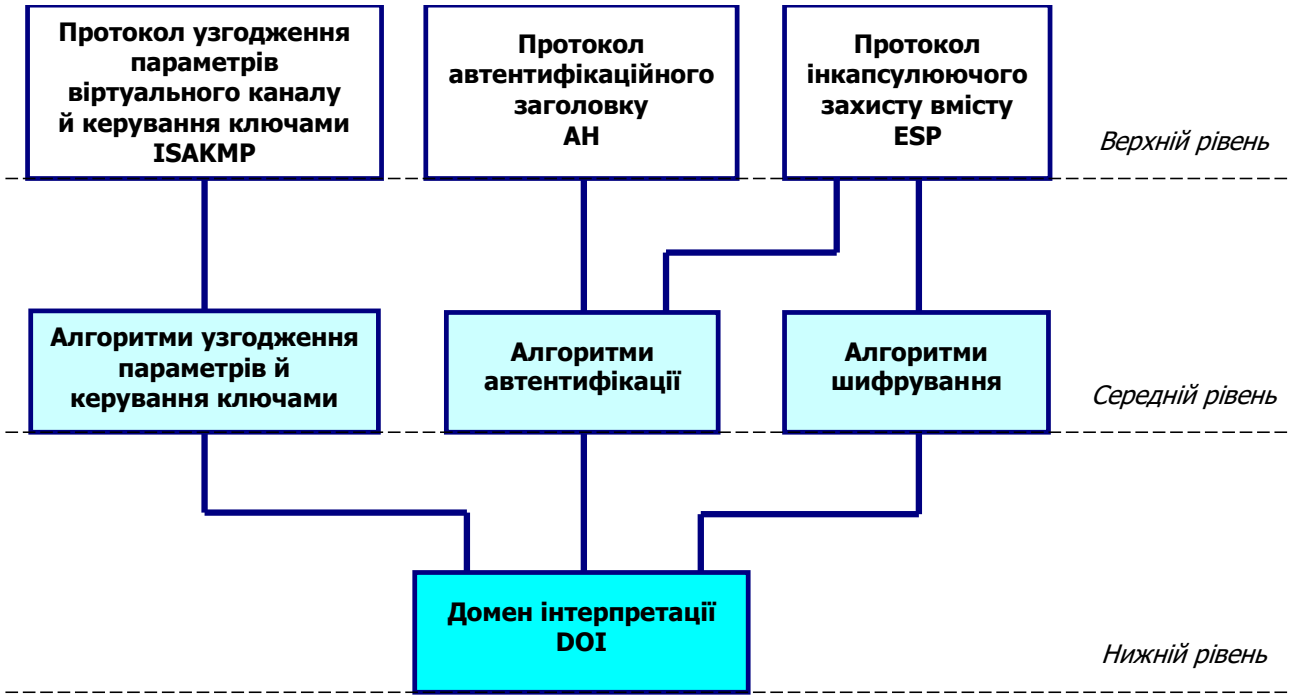

Рисунок 2.10. Архітектура засобів захисту IPSec.

Транспортний режим використовується для шифрування поля даних IP пакету, що містить протоколи транспортного рівня (TCP, UDP, ICMP), яке, в свою чергу, містить інформацію прикладних служб. Прикладом застосування транспортного режиму є передача електронної пошти. Всі проміжні вузли на маршруті пакету від відправника до одержувача використовують тільки відкриту інформацію мережевого рівня і, можливо, деякі опціональні заголовки пакету (в IPv6). Недоліком транспортного режиму є відсутність механізмів приховування конкретних відправника і одержувача пакету, а також можливість проведення аналізу трафіку. Результатом такого аналізу може стати інформація про обсяги і напрямки передачі інформації, області інтересів абонентів, розташування керівників.

Тунельний режим передбачає шифрування всього пакету, включаючи заголовок мережевого рівня. Тунельний режим застосовується у разі необхідності приховування інформаційного обміну організації із зовнішнім світом. При цьому, адресні поля заголовка мережевого рівня пакета, що

використовує тунельний режим, заповнюються фаєрволом організації і не містять інформації про конкретний відправника пакета. При передачі інформації з зовнішнього світу в локальну мережу організації в якості адреси призначення використовується мережева адреса брандмауера. Після розшифровки фаєрволом початкового заголовка мережевого рівня пакет направляється одержувачу.

Security Association (SA) - це з'єднання, яке надає служби забезпечення безпеки трафіку, який передається через нього. Два комп'ютери на кожній стороні SA зберігають режим, протокол, алгоритми і ключі, які використовуються в SA. Кожен SA використовується тільки в одному напрямку. Для двобічної зв'язку потрібно два SA. Кожен SA реалізує один режим і протокол; таким чином, якщо для одного пакету необхідно використовувати два протоколи (як наприклад AH і ESP), то потрібно два SA.

Політика безпеки зберігається в SPD (База даних політики безпеки). SPD може вказати для пакета даних одне з трьох дій: відкинути пакет, не обробляти пакет за допомогою IPSec, обробити пакет за допомогою IPSec. В останньому випадку SPD також вказує, який SA необхідно використовувати (якщо, звичайно, відповідний SA вже був створений) або вказує, з якими параметрами повинен бути створений новий SA.

IKE - протокол обміну ключами за замовчуванням для ISAKMP, на даний момент є єдиним. IKE знаходиться на вершині ISAKMP і виконує, власне, встановлення як ISAKMP SA, так і IPSec SA. IKE підтримує набір різних примітивних функцій для використання в протоколах. Серед них можна виділити хеш-функцію і псевдослучайную функцію (PRF).

IKE - протокол, що зв'язує всі компоненти IPsec в працююче ціле. Зокрема, IKE забезпечує початкову аутентифікацію сторін, а також їх обмін загальними секретними ключами.Існує можливість вручну встановити ключ для сесії. В цьому випадку IKE не використовується. Однак цей варіант не

рекомендується і використовується рідко. Традиційно, IKE працює через порт 500 UDP.

Існує IKE і більш нова версія протоколу: IKEv2. У специфікаціях та функціонуванні цих протоколів є деякі відмінності. IKEv2 встановлює параметри з'єднання за одну фазу, що складається з декількох кроків. Процес роботи IKE можна розбити на дві фази.

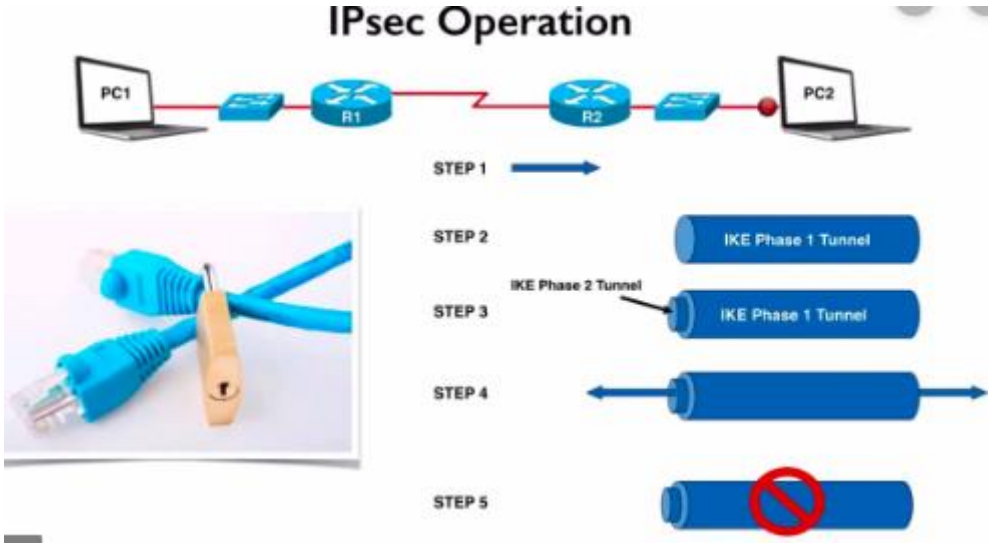

Рисунок 2.11.Перша фаза IKE.

Перша фаза:

IKE створює безпечний канал між двома вузлами, званий IKE security association (IKE SA).Перша фаза IKE може проходити в одному з двох режимів:

Основний режим

Складається з трьох двосторонніх обмінів між відправником і отримувачем:

Під час першого обміну узгоджуються алгоритми і хеш-функції, які будуть використовуватися для захисту IKE з'єднання, за допомогою зіставлення IKE SA кожного вузла.. Також вузли перевіряють ідентифікацію

один одного шляхом передачі та підтвердження послідовності псевдовипадкових чисел.

По зашифрованому IP-адресою перевіряється ідентичність протилежного боку. В результаті виконання основного режиму створюється безпечний канал для подальшого ISAKMP - обміну (цей протокол визначає порядок дій для аутентифікації з'єднання вузлів, створення і управління SA, генерації ключів, а також зменшення загроз, таких як DoS-атака або атака повторного відтворення).

Агресивний режим

Цей режим обходиться меншим числом обмінів і, відповідно, числом пакетів. У першому повідомленні міститься практично вся потрібна для встановлення IKE SA інформація: відкритий ключ Діффі-Хеллмана, для синхронізації пакетів, що підтверджується іншим учасником, ідентифікатор пакета. Одержувач посилає у відповідь все, що треба для завершення обміну. Першому вузлу потрібно тільки підтвердити з'єднання.

З точки зору безпеки агресивний режим слабкіше, так як учасники починають обмінюватися інформацією до встановлення безпечного каналу, тому можливий несанкціонований перехоплення даних. Однак, цей режим швидше, ніж основний. За стандартом IKE будь-яка реалізація повинна підтримувати основний режим, а агресивний режим підтримувати вкрай бажано.

Друга фаза

У фазі два IKE існує тільки один, швидкий, режим. Швидкий режим виконується тільки після створення безпечного каналу в ході першої фази. Він погоджує загальну політику IPsec, отримує загальні секретні ключі для алгоритмів протоколів IPsec (AH або ESP), встановлює IPsec SA. Використання послідовних номерів забезпечує захист від атак повторної передачі. Також швидкий режим використовується для перегляду поточної IPsec SA і вибору нової, коли час життя SA закінчується. Стандартно швидкий

режим проводить оновлення загальних секретних ключів, використовуючи алгоритм Діффі-Хеллмана з першої фази.

Що стосується псеводслучайних функцій, то в даний час замість спеціальних PRF використовується хеш функція в конструкції HMAC (HMAC - механізм аутентифікації повідомлень з використанням хеш функцій). Для визначення HMAC нам знадобиться криптографічний хеш функція (позначимо її як H) і секретний ключ K. Ми припускаємо, що H є хеш функцією, де дані хешіруются за допомогою процедури стиснення, послідовно застосовується до послідовності блоків даних. Ми позначимо за B довжину таких блоків в байтах, а довжину блоків, отриманих в результаті хешування - як L (L <B). Ключ K може мати довжину, меншу або рівну B. Якщо додаток використовує ключі більшої довжини, спочатку ми повинні хешірованного сам ключ з використанням H, і тільки після цього використовувати отриману рядок довжиною L байт, як ключ в HMAC. B обох випадках рекомендована мінімальна довжина для K становить L байт.

SPD є дуже гнучким механізмом управління, який допускає дуже хороше управління обробкою кожного пакету. Пакети класифікуються за великим числом полів, і SPD може перевіряти деякі або всі поля для того, щоб визначити відповідну дію. Це може привести до того, що весь трафік між двома машинами передаватиметься за допомогою одного SA, або окремі SA будуть використовуватися для кожного додатка, або навіть для кожного TCP з'єднання.

Протокол ISAKMP визначає загальну структуру протоколів, які використовуються для встановлення SA і для виконання інших функцій управління ключами. ISAKMP підтримує кілька Областей Інтерпретації (DOI), однією з яких є IPSec-DOI. ISAKMP не визначає закінчений протокол, а надає "будівельні блоки" для різних DOI і протоколів обміну ключами.

Протокол Oakley - це протокол визначення ключа, який використовує алгоритм заміни ключа Діффі-Хеллмана. Протокол Oakley підтримує ідеальну

пряму безпеку (Perfect Forward Secrecy - PFS). Наявність PFS означає неможливість розшифровки всього трафіку при компрометації будь-якого ключа в системі.

Для того, щоб почати обмінюватися даними між двома сторонами, необхідно встановити з'єднання, що носить назву SA (Асоціація безпеки). Концепція SA фундаментальна для IPsec, власне, є його сутью. Она описує, як сторони будуть використовувати сервіси для забезпечення захищеного загального користування. Соединение SA є симплексним (однонаправленим), тому для взаємодії сторона необхідно встановити два з'єднання. Крім того, використовуються стандартні протоколи IPsec, що дозволяють виконувати наступні точки захисту захищеного каналу як SA для передачі трафіку всіх взаємодіючих через цей канал хостів, так і створити для цього цілий цілий виробник численних безпечних асоціацій, наприклад, за кожним на кожному TCP-з'єднанні. Це дає можливість вибирати нужну ступінь деталізації захисту. Встановлення з'єднання починається з взаємної аутентифікації сторона. Далі відбувається вибірка параметрів (буде здійснена аутентифікація, шифрування, перевірка цільових даних) та необхідність передачі даних (AH або ESP). Після цього вибираються конкретні алгоритми (наприклад, шифрування, хеш-функція) з декількох можливих схем, деякі з яких визначені стандарти (для шифрування - DES, для їх функціонування - MD5 або SHA-1), а інші постачаються виробниками продуктів, використовуючи IPsec

Обрабка вихідних IPSec пакетів. Якщо передавальний IPsec-модуль визначає, що пакет пов'язаний з SA, яке передбачає ESP-обробку, то він починає обробку. Залежно від режиму (транспортний або режим тунелювання) вихідний IP-пакет обробляється по-різному. У транспортному режимі передає IPsec-модуль здійснює процедуру обрамлення протоколу верхнього рівня (наприклад, TCP або UDP), використовуючи для цього ESP-заголовок (поля Security Parameters Index і Sequence Number заголовка) і ESP-кінцевик (інші поля заголовка, наступні за полем даних - Payload data), не зачіпаючи при цьому заголовок вихідного IP-пакета. У режимі тунелювання IP-пакет

обрамляється ESP-заголовком і ESP-кінцевиком (інкапсуляція), після чого обрамляється зовнішнім IP-заголовком (який може не збігатися з вихідним - наприклад, якщо IPsec модуль встановлений на шлюзі). [8] Далі проводиться шіфрованіе- в транспортному режимі шифрується тільки повідомлення протоколу вище лежачого рівня (тобто все, що знаходилося після IP-заголовка у вихідному пакеті), в режимі туннелірованія- весь вихідний IP-пакет. Передавальний IPsec-модуль із запису про SA визначає алгоритм шифрування і секретний ключ. Стандарти IPsec дозволяють використання алгоритмів шифрування Triple DES, AES і Blowfish, якщо їх підтримують обидві сторони. Інакше використовується DES, прописаний в RFC 2405. Так як розмір відкритого тексту повинен бути кратний певному числу байт, наприклад, розміром блоку для блокових алгоритмів, перед шифруванням проводиться ще й необхідне доповнення шифруемого повідомлення. Зашифроване повідомлення поміщається в поле Payload Data. В поле Pad Length поміщається довжина доповнення. Потім, як і в AH, обчислюється Sequence Number. Після чого вважається контрольна сума (ICV). Контрольна сума, на відміну від протоколу AH, де при її обчисленні враховуються також і деякі поля IP-заголовка, в ESP обчислюється тільки по полях ESP-пакета за вирахуванням поля ICV. Перед обчисленням контрольної суми воно заповнюється нулями. Алгоритм обчислення ICV, як і в протоколі AH, передає IPsec-модуль дізнається із запису про SA, з яким пов'язаний опрацьований пакет.

Обробка вхідних пакетів. Після отримання пакета, що містить повідомлення ESP-протоколу, приймальний IPsec-модуль шукає відповідне захищене віртуальне з'єднання (SA) в SAD, використовуючи IP-адреса одержувача, протокол безпеки (ESP) і індекс SPI [8]. Якщо відповідне SA, не знайдено, пакет знищується. Знайдене захищене віртуальне з'єднання (SA) вказує на те, чи використовується послуга щодо запобігання повторної передачі пакетів, тобто на необхідність перевірки поля Sequence Number. Якщо послуга використовується, то поле перевіряється. Для цього, так само як і в AH, використовується метод ковзного вікна. Прийомний IPsec-модуль

формує вікно з шириною W. Лівий край вікна відповідає мінімальному послідовному номеру (Sequence Number) N правильно прийнятого пакета. Пакет з полем Sequence Number, в якому міститься значення, починаючи від N + 1 і закінчуючи N + W, приймається коректно. Якщо отриманий пакет виявляється по ліву межу вікна-він знищується. Потім, якщо Ви маєте послугу аутентифікації, приймальний IPsec-модуль обчислює ICV за відповідними полями прийнятого пакета, використовуючи алгоритм аутентифікації, який він дізнається із запису про SA, і порівнює отриманий результат зі значенням ICV, розташованим в поле «Integrity Check Value». Якщо обчислене значення ICV збіглося з прийнятим, то прийшов пакет вважається дійсним. Якщо перевірка дала негативний результат, то прийомний пакет знищується. Далі проводиться розшифрування пакету. Прийомний IPsec-модуль дізнається із запису про SA, який алгоритм шифрування використовується і секретний ключ. Треба зауважити, що перевірка контрольної суми і процедура розшифрування можуть проводитися не тільки послідовно, але й паралельно. В останньому випадку процедура перевірки контрольної суми повинна закінчитися раніше процедури розшифрування, і якщо перевірка ICV провалилася, процедура розшифрування також повинна припинитися. Це дозволяє швидше виявляти зіпсовані пакети, що, в свою чергу, підвищує рівень захисту від атак типу «відмова в обслуговуванні» (DOS-атаки). Далі розшифроване повідомлення відповідно до полем Next Header передається для подальшої обробки.

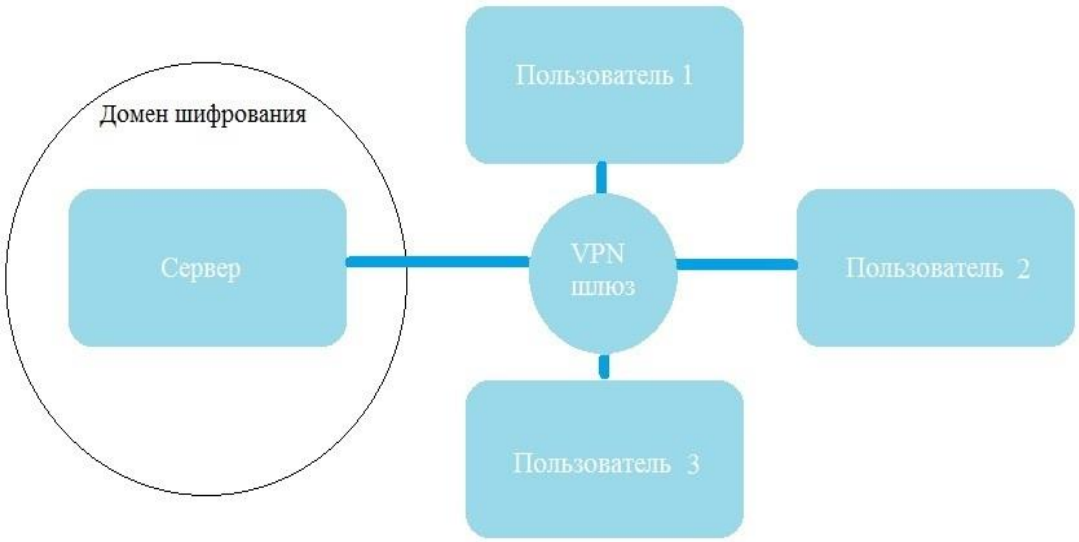

Рисунок 2.12.Рознесення абонентів за допомогою шлюза.

Протокол IPsec використовується, в основному, для організації VPN-тунелів. У цьому випадку протоколи ESP і AH працюють в режимі тунелювання. Крім того, налаштовуючи політики безпеки певним чином, протокол можна використовувати для створення мережевого доступу. Сенс брандмауера полягає в тому, що він контролює і фільтрує проходять через нього пакети відповідно до заданих правил. Встановлюється набір правил, і екран переглядає всі, хто проходить через нього пакети. Якщо передані пакети потрапляють під дію цих правил, міжмережевий екран обробляє їх відповідним чином [14]. Наприклад, він може відхиляти певні пакети, тим самим перериваючи небезпечні сполуки. Налаштувавши політику безпеки відповідним чином, можна, наприклад, заборонити веб-трафік. Для цього достатньо заборонити відсилання пакетів, в які вкладаються повідомлення протоколів HTTP і HTTPS. IPsec можна застосовувати і для захисту серверів - для цього відкидаються всі пакети, окрім пакетів, необхідних для коректного виконання функцій сервера. Наприклад, для Web-сервера можна блокувати весь трафік, за винятком з'єднань через 80-й порт протоколу TCP, або через порт TCP 443 в випадках, коли застосовується HTTPS.

За допомогою IPsec тут забезпечується безпечний доступ користувачів до сервера. При використанні протоколу ESP всі звернення до сервера і його

відповіді шифруються. Однак за VPN-шлюзом (в домені шифрування) передаються відкриті повідомлення. Інші приклади використання IPsec шифрування трафіку між файловим сервером і комп'ютерами в локальній мережі, використовуючи IPsec в транспортному режимі або з'єднання двох офісів з використанням IPsec в тунельному режимі.

Наразі існує ряд різних пропозицій щодо інкапсуляції одного протоколу над іншим протоколом. Інші типи інкапсуляцій запропоновані для транспортування IP через IP для цілей політики. GRE протокол який дуже схожий з вищезазначеними пропозиціями, але є загальнішим.

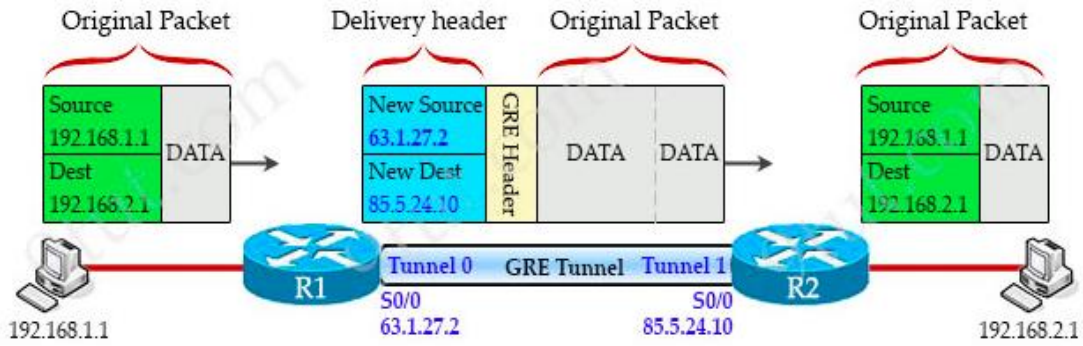

Рисунок 2.12.Реалізація VPN за допомогою GRE.

Намагаючись бути більш загальним, існує багато нюансів , характерних для протоколу. Результат полягає в тому, що ця пропозиція може бути менш придатною для ситуації, коли описана конкретна інкапсуляція "X над Y". Це спроба цього протоколу створити простий механізм загального призначення, який зменшує проблему інкапсуляції до більш керованого розміру. У найбільш загальному випадку система має пакет, який потрібно інкапсулювати та доставити до якогось пункту призначення. Ми будемо називати це пакетом корисного навантаження. Склад корисного навантаження спочатку інкапсулюється в пакет GRE. Отриманий пакет GRE потім може бути інкапсульований у якомусь іншому протоколі і потім пересланий. Цей зовнішній протокол називається протоколом доставки.

Капсульований пакет GRE має вигляд:

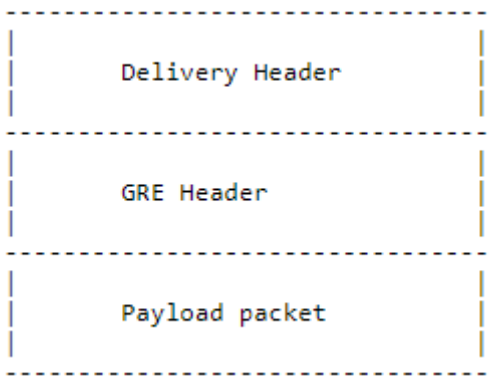

Рисунок 2.13.Вигляд GRE пакета.

Заголовок пакету GRE має вигляд:

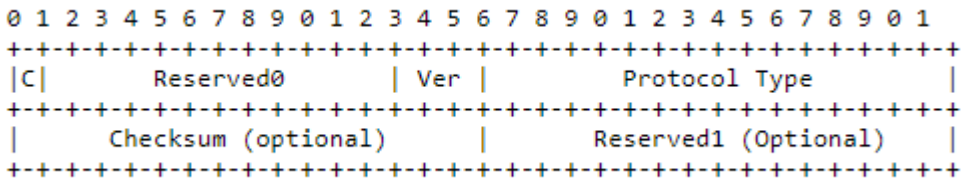

Рисунок 2.14.Заголовок GRE пакета.

2.2. Принципи структурної побудови мереж VPN

Існують різні варіанти реалізації VPN мереж. При виборі рішення потрібно враховувати фактори продуктивності засобів побудови VPN. Наприклад, якщо маршрутизатор і так працює на межі потужності свого процесора, то додавання тунелів VPN і застосування шифрування / дешифрування інформації можуть зупинити роботу всієї мережі через те, що цей маршрутизатор не справлятиметься з навантаженням простим трафіком, не кажучи вже про трафік VPN. Для побудови VPN найкраще використовувати спеціалізоване обладнання, однак якщо є обмеження в засобах, то можна звернути увагу на чисто програмне рішення.

Основні варіанти побудови VPN:

- Remote access VPN

- Site-to-site VPN

2.2.1. Remote access VPN

Remote access VPN - означає, що тунель організовується між установленим на комп'ютері клієнта додатком(наприклад Cisci Any Connect) і будь-яким пристроєм, який виступає в якості сервера і організовує підключення від різних клієнтів (наприклад, VPN-концентратор, маршрутизатор, Cisco ASA і будь-які інші в залежності від вибору організації)

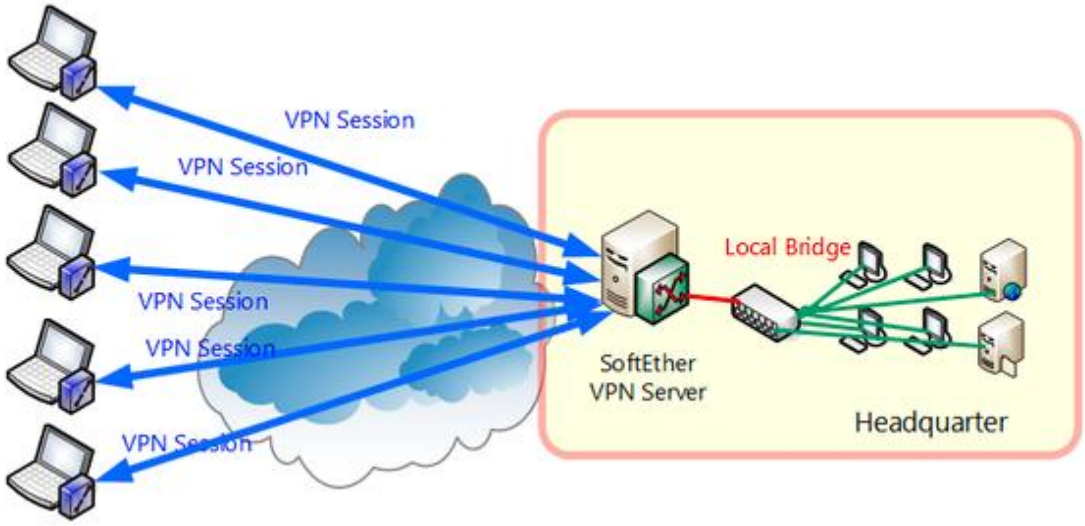

Рисунок 2.15.Структура Remote access VPN

VPN з віддаленим доступом більш тісно пов'язаний зі додатками VPN, які використовуються для захисту особистої ідентичності та даних користувача. VPN з віддаленим доступом спочатку були запроваджені для працівників, які працюють в будь-якій точці світу, надійно з'єднуватися з віддаленою локальною мережею своєї компанії. Віддалені працівники можуть отримати доступ до захищених ресурсів у локальній мережі своєї компанії, з будь-якої точки світу. Як і у всіх VPN, віддалені VPN-мережі мають на меті забезпечити безпеку ваших даних. За допомогою VPN з віддаленим доступом пристрій віддаленого користувача відповідає за шифрування та розшифрування даних, що надсилаються або отримуються.

Для VPN віддаленого доступу потрібен NAS (сервер мережевого доступу) або шлюз VPN для аутентифікації облікових даних будь-якого пристрою, який намагається увійти в VPN. Це насправді NAS, віддалений користувач, з'єднуєтесь, коли хочете використовувати VPN з віддаленим доступом.

Як правило, віддалений доступ до VPN також вимагає, щоб пристрій був забезпечений клієнтським програмним забезпеченням. Це програмне забезпечення клієнта VPN спілкується з шлюзом VPN, який автентифікує користувача як віддаленого користувача та створює захищений "віртуальний" тунель між локальною мережею та шлюзом.

Після створення тунелю будь-які дані, які ви надсилаєте з цього пристрою, інкапсулюються та шифруються VPN вашого віддаленого доступу, а потім надсилаються до шлюзу VPN, який знаходиться безпосередньо за межами віддаленої локальної мережі. Потім шлюз VPN розшифровує ваш трафік і ретранслює дані в локальну мережу.

Не тільки весь трафік, що надсилається через віртуальний тунель, забезпечений, але будь-який трафік, який користувач отримує від локальної мережі (або його серверів), також проходить через цей тунель у зворотному напрямку і захищений. Шлюз VPN шифрує вхідний трафік (докористувача), який потім отримує клієнт VPN.

2.2.2. Site-to-site VPN

Site-to-site VPN – означає, що схема має в наявність два пристрої (наприклад, маршрутизаторів), між якими є тунель, в цьому випадку, користувачі знаходяться за пристроями, в локальний мережах і на їх комп'ютерах не потрібно установки будь-якого спеціального програмного забезпечення.

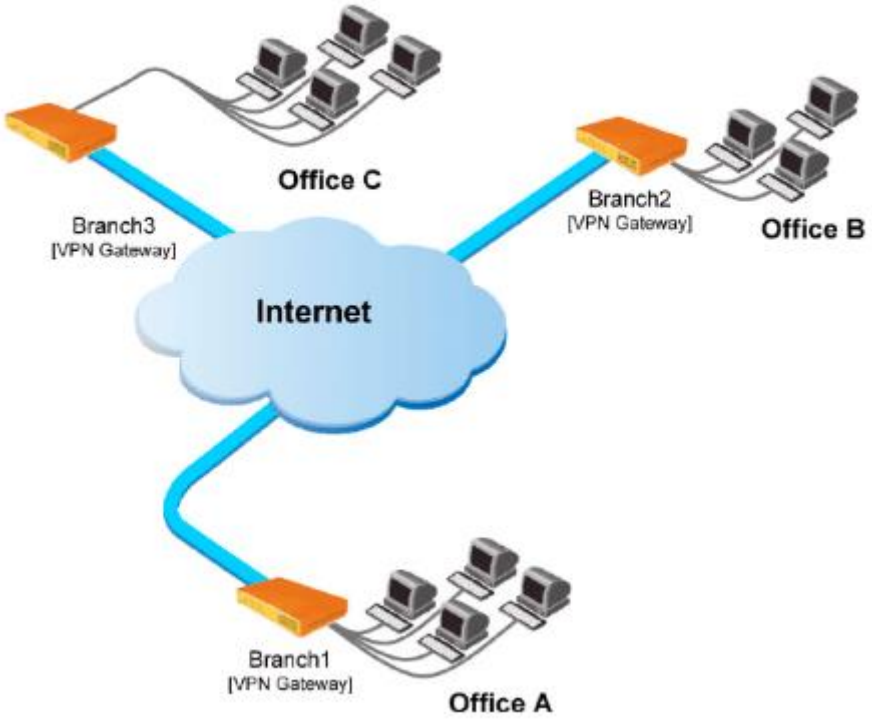

Рисунок 2.16.Структура Site-to-site VPN

Тоді як VPN з віддаленим доступом надійно з'єднують окремі пристрої з віддаленою локальною мережею, VPN site-to-site надійно з'єднують дві або більше локальних мереж у різних фізичних місцях. VPN від сайту до сайту використовують загально доступний Інтернет для розширення мережі вашої компанії на кілька офісних місць.

Існує два поширені типи VPN від сайту до сайту: інтранет та екстранет. Внутрішні мережеві VPN на базі внутрішньої мережі використовуються для об'єднання локальних мереж декількох офісних локацій в одну приватну мережу, яка б тоді була відома як WAN (Wide Area Network).

З іншого боку, VPN, що базуються на екстранеті, дозволяють компанії використовувати загальнодоступний Інтернет для підключення своєї локальної мережі до мереж інших компаній, клієнтів чи громад. Це дозволяє компанії обмінюватися інформацією зі своїми партнерами, зберігаючи свою локальну мережу (intranet).

За допомогою VPN site-to-site, шлюз VPN однієї віддаленої локальної мережі зв’язується зі шлюзом іншої локальної мережі (або мережі HQ) для

створення захищеного тунелю. На відміну від VPN з віддаленим доступом, віддаленим пристроям не потрібен клієнт VPN, а надсилають звичайний трафік через шлюзи VPN.

За відсутності клієнтів VPN, шлюзи VPN відповідають за автентифікацію користувача та мережі, шифрування та цілісність даних. Шлюз приймає зашифровані дані, розшифровує їх, а потім передає дані цільовому пристрою в мережі. Тунель, створений VPN від сайту до сайту, дозволяє компанії ділитися мережею та ресурсами між своїми основними та віддаленими відділеннями - незалежно від відстані. Пристрої в одній локальній мережі можуть спілкуватися з пристроями іншої локальної мережі так, ніби вони є частиною однієї мережі.

Існує два основні методи створення VPN від сайту до сайту: VPN на базі Інтернету та MPLS (Multiprotocol Label Switching) VPN.

2.3. Методи реалізації VPN мереж

2.3.1. VPN на основі брандмауерів

Брандмауери більшості виробників підтримують тунелювання і шифрування даних. Всі подібні продукти засновані на тому, що трафік, що проходить через брандмауер шифрується. До програмного забезпечення власне брандмауера додається модуль шифрування. Недоліком цього методу можна назвати залежність продуктивності від апаратного забезпечення, на якому працює брандмауер.

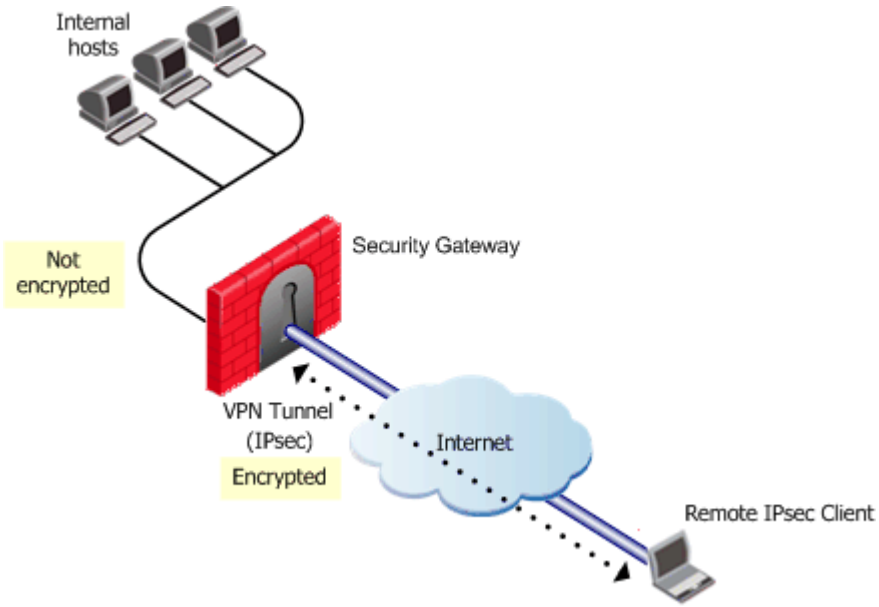

Рисунок 2.17.VPN на основі брандмауерів

При використанні брандмауерів на базі ПК треба пам'ятати, що подібне рішення можна застосовувати тільки для невеликих мереж з невеликим обсягом переданої інформації.

Як приклад VPN на базі брандмауерів можна назвати FireWall-1 компанії Check Point Software Technologies. FairWall-1 використовує для побудови VPN стандартний підхід на базі IPSec. Трафік, що приходить в брандмауер, дешифрується, після чого до нього застосовуються стандартні правила управління доступом.

2.3.2. VPN на базі маршрутизаторів

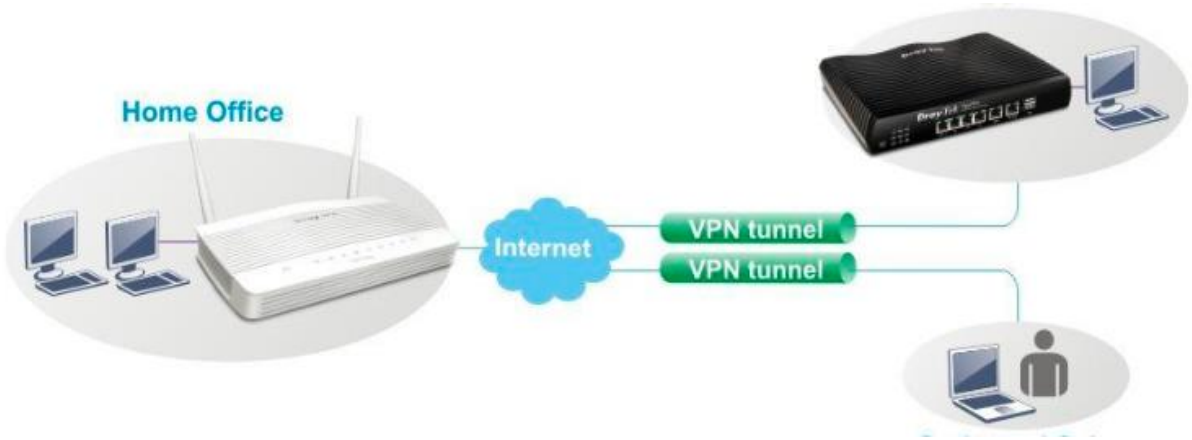

Рисунок 2.18.VPN на основі маршрутизаторів

Іншим способом побудови VPN є застосування для створення захищених каналів маршрутизаторів. Так як вся інформація, яка виходить із локальної мережі, проходить через маршрутизатор, то доцільно покласти на цей маршрутизатор і завдання шифрування.

Прикладом обладнання для побудови VPN на маршрутизаторах є обладнання компанії Cisco Systems. Починаючи з версії програмного забезпечення IOS 11.3, маршрутизатори Cisco підтримують протоколи L2TP і IPSec. Крім простого шифрування інформації, що проходить Cisco підтримує і інші функції VPN, такі як ідентифікація при встановленні тунельного з'єднання і обмін ключами.

Для підвищення продуктивності маршрутизатора може бути використаний додатковий модуль шифрування ESA. Крім того, компанія Cisco System випустила спеціалізований пристрій для VPN, яке так і називається Cisco 1720 VPN Access Router (маршрутизатор доступу до VPN), призначене для установки в компаніях малого і середнього розміру, а також у відділеннях великих організацій.

2.3.3. VPN на базі програмного забезпечення

Рисунок 2.19.VPN на основі програмного забезпечення

Наступним підходом до побудови VPN є чисто програмні рішення. При реалізації такого рішення використовується спеціалізоване програмне забезпечення, яке працює на виділеному комп'ютері, і в більшості випадків виконує роль proxy-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером.

Як приклад такого рішення можна виступає програмне забезпечення AltaVista Tunnel 97 компанії Digital. При використанні даного програмного забезпечення клієнт підключається до сервера Tunnel 97, аутентифицирующей на ньому і обмінюється ключами. Шифрація проводиться на базі 56 або 128 бітових ключів, отриманих в процесі встановлення з'єднання. Далі, зашифровані пакети инкапсулируются в інші IP-пакети, які в свою чергу відправляються на сервер. Крім того, дане програмне забезпечення кожні 30 хвилин генерує нові ключі, що значно підвищує захищеність з'єднання.

Позитивними якостями AltaVista Tunnel 97 є простота установки і зручність управління. Мінусами даної системи можна вважати нестандартну архітектуру (власний алгоритм обміну ключами) і низьку продуктивність.

2.4. Топології мереж VPN і їх характеристика

Зазвичай, при створенні VPN, використовують підключення типу точка-точка до певного сервера, або установку ethernet-тунелю з певним сервером, при якій тунелю призначають певну підмережу. Сервер VPN при цьому виконує функції маршрутизації та фільтрування трафіку для доступу до локальної мережі через VPN.

При використанні такого підходу ми все ще маємо можливість фільтрувати трафік на підставі способу підключення (наприклад, використовувати для локальної мережі та для віддалених користувачів різні фільтри), але виключається необхідність налаштування маршрутизації, а віддалені машини включаються прямо в локальну мережу, бачать ресурси, навіть здатні використовувати широкосмугові посилки взагалі без додаткового налаштування. Через такий VPN у них відображаються всі

комп'ютери локальної мережі Windows, всі доступні XDMCP-сервери при XDMCP broadcast.

VPN з'єднання завжди складається з каналу типу точка-точка, також відомого під назвою тунель. Тунель створюється в незахищеній мережі, в якості якої найчастіше виступає Інтернет. З'єднання точка-точка має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються вузлами або peers. Кожен peer відповідає за шифрування даних до того, як вони потраплять в тунель і розшифровку цих даних після того, як вони тунель покинуть.

Хоча VPN-тунель завжди встановлюється між двома точками, кожен peer може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьом віддаленим станцій необхідно зв'язатися з одним і тим же офісом, буде створено три окремих VPN-тунелю до цього офісу. Для всіх тунелів peer на стороні офісу може бути одним і тим же. Це можливо завдяки тому, що вузол може шифрувати і розшифровувати дані від імені всієї мережі, як це показано на рисунку 1.20:

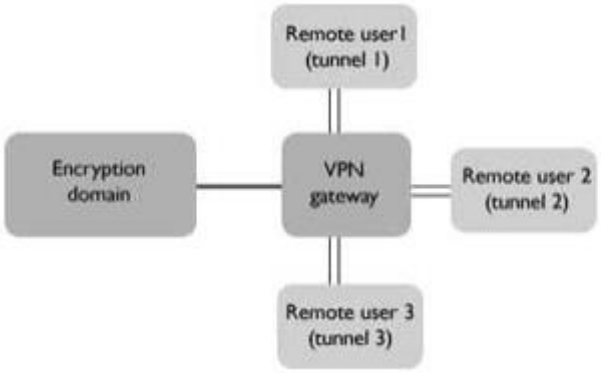

Рисунок 2.20.Рознесення користувачів за допомогою шлюза

В цьому випадку VPN-вузол називається VPN-шлюзом, а мережа за ним - доменом шифрування (encryption domain). Використання шлюзів зручно з кількох причин. По-перше, всі користувачі повинні пройти через один пристрій, який полегшує завдання управління політикою безпеки і контролю вхідного і вихідного трафіку мережі. По-друге, персональні тунелі до кожної робочої станції, до якої користувачеві треба отримати доступ, дуже швидко

стануть некерованими (так як тунель - це канал типу точка-точка). При наявності шлюзу, користувач встановлює з'єднання з ним, після чого користувачеві відкривається доступ до мережі (домену шифрування).

Цікаво відзначити, що всередині домену шифрування самого шифрування не відбувається. Причина в тому, що ця частина мережі вважається безпечною і знаходиться під безпосереднім контролем на противагу Інтернет. Це справедливо і при з'єднанні офісів за допомогою VPN-шлюзів. Таким чином гарантується шифрування тільки тієї інформації, яка передається по небезпечному каналу між офісами. Рисунок 2 показує VPN, що сполучає два офіси.

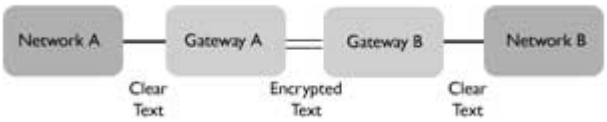

Рисунок 2.21 VPN на основі незахищеної мережі.

Мережа А вважається доменом шифрування VPN-шлюзу А, а мережа В - доменом шифрування VPN-шлюзу В, відповідно. Коли користувач мережі А виявляє бажання відправити дані в мережу В, VPN шлюз А зашифрує їх і відішле через VPN-тунель. VPN шлюз В розшифрує інформацію і передасть одержувачу в мережі В.

Всякий раз, коли з'єднання мереж обслуговують два VPN-шлюзу, вони використовують режим тунелю. Це означає, що шифрується весь пакет IP, після чого до нього додається новий IP-заголовок. Новий заголовок містить IP-адреси двох VPN-шлюзів, які і побачить пакетний сниффер при перехопленні. Неможливо визначити комп'ютер-джерело в першому домені шифрування і комп'ютер-одержувач у другому домені.

За допомогою тунелювання пакети даних транслюються через загальнодоступну мережу як по звичайному з'єднанню. Між кожною парою “відправник – отримувач” даних встановлюється своєрідний тунель - безпечне

логічне з'єднання, що дозволяє приховувати дані одного протоколу в пакети іншого. Основними компонентами тунелює:

• ініціатор;

• маршрутизатор мережі;

• тунельний комутатор;

• один або кілька тунельних термінаторів.

Сам по собі принцип роботи VPN який суперечить основним мережним технологіям і протоколам. Наприклад, при встановленні з'єднання віддаленого доступу клієнт посилає серверу потік пакетів стандартного протоколу PPP. У разі організації віртуальних виділених ліній між локальними мережами їх маршрутизатори також обмінюються пакетами PPP. Проте, принципово новим моментом є пересилання пакетів через безпечний тунель, організований в межах загальнодоступної мережі. Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічне середовище, що використовує інший протокол. В результаті з'являється можливість вирішити проблеми взаємодії кількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності даних і закінчуючи подоланням невідповідностей зовнішніх

протоколів або схем адресації.

Існуюча мережева інфраструктура корпорації може бути підготовлена до

використання VPN як за допомогою програмного, так і за допомогою апаратного забезпечення. Організацію віртуальної приватної мережі можна порівняти з прокладанням кабелю через глобальну мережу.

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

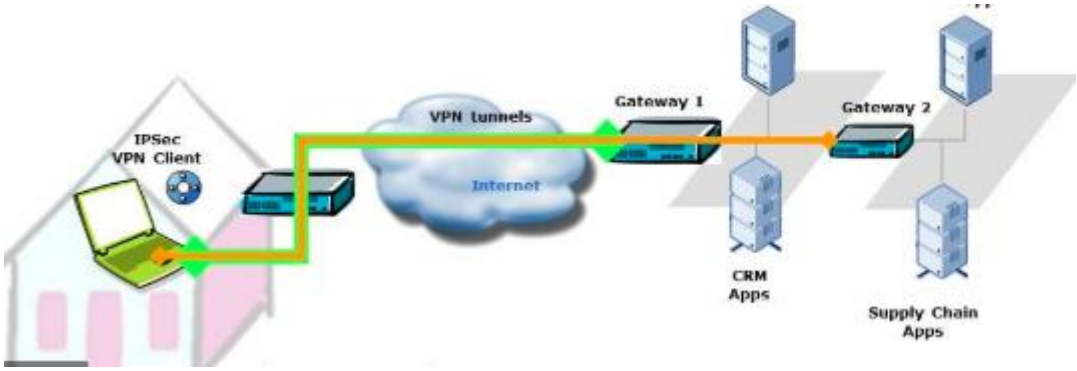

Рисунок 2.22. Типове використання VPN за допогою VPN агента

Рисунок 2.22. ілюструє типове використання VPN, яка дозволяє віддаленим користувачам з перенесення комп'ютера і користувачів, які працюють з дому, мати доступ до офісної мережі. Щоб ця схема запрацювала, користувач повинен мати встановлене ПЗ - VPN- клієнт, який забезпечить створення VPN-тунелю до віддаленого VPN-шлюзу. За сценарієм використовується режим тунелю, так як користувач хоче отримати доступ до ресурсів домена, а не самого шлюзу. Єдиною випадок, коли включається режим транспорту - це якщо одного комп'ютера потрібно отримати доступ до іншого безпосередньо.

Існує багато варіантів VPN-шлюзів і VPN-клієнтів. Це може бути апаратний пристрій або програмне забезпечення, яке встановлюється на маршрутизаторах або на ПК. Скажімо, ОС FreeBSD поставляється разом з ПЗ для створення VPN-шлюзу і для настроїти клієнт VPN. Свої VPN-рішення існують і для ПО компанії Microsoft.

Назалежно від використовуваного ПО, всі VPN працюють за наступними принципами:

1. Кожен з вузлів ідентифікує один одного перед створенням тунелю, щоб упевнитися, що шифровані дані будуть відправлені на потрібний вузол.

2. Обидва вузла вимагають заздалегідь налаштовані політики, що вказує, які протоколи можуть використовуватися для шифрування і забезпечення цілісності даних.

3. Вузли звіряють політики, щоб домовитися про використовувані алгоритмах; якщо це не виходить, то тунель не встановлюється.

4. Як тільки досягнуто згоди по алгоритмам, створюється ключ, який буде використаний в симетричному алгоритмі для шифрування / розшифрування даних.

Висновки до розділу 2

Отже, існують різні реалізації VPN мереж всі можуть забезпечувати надійний захист даних, але мають відмінності в структурі та логіці роботи.

VPN на базі МЕ є єдиним оптимальним варіантом з погляду забезпечення комплексної безпеки корпоративної інформаційної системи від атак з відкритих мереж. Сьогодні практично всі провідні виробники маршрутизаторів і інших мережевих пристроїв заявляють про підтримку в своїх продуктах різних VPN-протоколів. об'єднання функцій МЕ і VPN-шлюзу в одній крапці під контролем єдиної системи управління і аудиту - не тільки технічно грамотне, але і зручне для адміністрування рішення.

Реалізація мережі VPN здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

У вигляді програмного рішення використовують персональний комп’ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN, інтегроване рішення, функціональність VPN забезпечує комплекс, вирішальним завданням фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

3. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ VPN

Важливість захисту інформаційних ресурсів компанії очевидна - від цього безпосередньо залежить безпека даних, які належать підприємству, його ефективності і рентабельності. Та й користувачеві не дуже приємно, коли його дані перехоплюють, засипають спамом або блокують певні сервери.

Існує безліч продуктів і інструментів програмного забезпечення, що дозволяють убезпечити дані в Інтернеті від віртуальних атак зловмисників. У певних випадках зручніше і найефективніше для захисту інформації, приватної чи корпоративної, застосовувати VPN.

З ростом сучасних організацій зростають і її інформаційні потреби в обчислювальних ресурсах по обробці даних. Це має на увазі зростаючу кількість обладнання з'єднаного мережею. Однак розвиток комп'ютерних мереж на підприємствах тягне за собою зростання кількості інформаційних ризиків. Однією з основних загроз в даному випадку є можливість маніпуляцій з трафіком в процесі передачі всередині мережі. Відповідно виникає необхідність в розробці методів протидії даній загрозі.

Залежно від застосовуваних протоколів і призначення, VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережу та мережу-мережу.

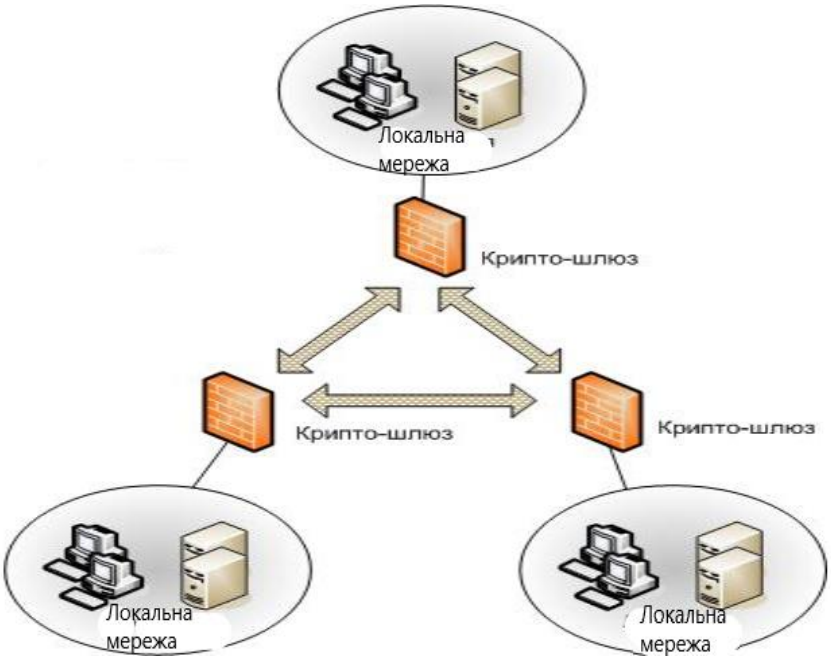

Рисунок 3.1. Структура мережі організації

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути кілька, і «зовнішня» мережу, через яку проходить інкапсульоване з'єднання (зазвичай використовується Інтернет). Можливо також підключення до віртуальної мережі окремого комп'ютера. Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або під час активного з'єднання з іншого захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Програмні засоби захисту інформації.

Засоби захисту інформації

- Антивірусна програма (антивірус) - програма для виявлення комп'ютерних вірусів і лікування інфікованих файлів, а також для

профілактики - запобігання зараженню файлів або операційної системи шкідливим кодом.

- Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби. Крім програм шифрування і криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації.
- Міжмережеві екрани (також звані брандмауерами або файрвол - від нього. Brandmauer, англ. Firewall - «протипожежна стіна»). Між локальної та глобальної мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь проходить через них трафік мережевого / транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищена різновид методу - це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.
- Proxy-servers (proxy - довіреність, довірена особа). Весь трафік мережевого / транспортного рівнів між локальної та глобальної мережами забороняється повністю - маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях - наприклад, на рівні додатку (віруси, код Java і JavaScript).
- VPN (віртуальна приватна мережа) дозволяє передавати секретну інформацію через мережі, в яких можливе прослуховування трафіку сторонніми людьми. Використовувані технології: PPTP, PPPoE, IPSec.

3.1. Незахищеність мереж передачі даних

Велика група загроз пов'язана з недосконалістю протоколів, зокрема протоколів стека протоколів TCP / IP. Відомо, що ці протоколи розроблялися в час, коли проблема забезпечення безпеки даних ще не стояла на порядку денному. Користувачі Інтернету представляли собою обмежене коло зацікавлених в ефективній роботі мережі фахівців, і ніхто не робив спроб порушити її працездатність. Створювані в таких умовах протоколи не містили механізмів, що дозволяють протистояти можливим (тоді тільки теоретично) атакам зловмисників. Наприклад, хоча в протоколах FTP і telnet передбачена аутентифікація, клієнт передає пароль сервера по мережі в незашифрованому вигляді, а значить, зловмисник може перехопити його і отримати доступ до даних користувача.

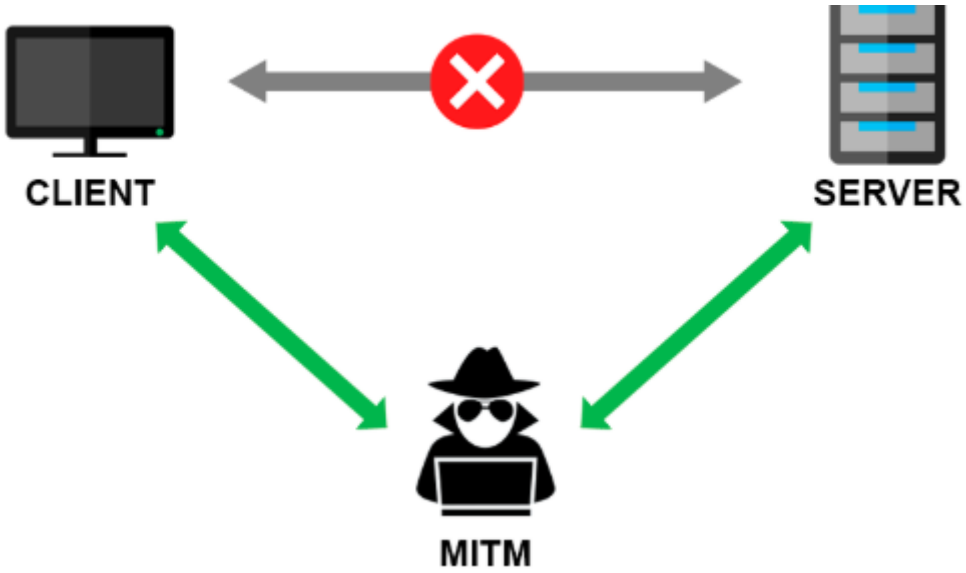

Рисунок 3.2. Загроза MITM атаки

Під підключенням до мережі слід розуміти будь-яке підключення комп'ютера до зовнішнього середовища для спілкування з іншими ресурсами, коли вже не можна бути повністю впевненим, що до цього комп'ютера та інформації в ньому мають доступ тільки користувач комп'ютера або тільки санкціоновані користувачі з мережі.

Якщо комп'ютер підключений до локальної мережі, то, потенційно, до цього комп'ютера та інформації в ньому можна отримати несанкціонований доступ з локальної мережі.

Якщо локальну мережу з'єднали з іншими локальними мережами, то до можливих несанкціонованим користувачам додаються і користувачі з цих віддалених мереж.

Якщо комп'ютер підключили безпосередньо через провайдера до зовнішньої мережі, наприклад через модем до Інтернет, для віддаленого взаємодії зі своєю локальною мережею, то комп'ютер і інформація в ньому потенційно доступні хакерам з Інтернет. А найнеприємніше, що через цей комп'ютер можливий доступ зломщиків і до ресурсів локальної мережі.

Природно при всіх таких підключених застосовуються або штатні засоби розмежування доступу операційної системи, або спеціалізовані засоби захисту від несанкціонованого доступу, або криптографічні системи на рівні конкретних програм, або і те й інше разом.

Однак всі ці заходи, на жаль, не можуть гарантувати бажаної безпеки при проведенні мережевих атак, і пояснюється це наступними основними причинами:

- Операційні системи (ОС), особливо WINDOWS відносяться до програмних продуктів високої складності, створенням яких займається великі колективи розробників. Детальний аналіз цих систем провести надзвичайно важко. У зв'язку з чим, достовірно обґрунтувати для них відсутність штатних можливостей, помилок або недокументованих можливостей, випадково або навмисно залишених в ОС, і якими можна було б скористатися через мережеві атаки, не представляється можливим.

- В багатозадачій ОС, зокрема WINDOWS, одночасно може працювати багато різних додатків, для яких також важко обгрунтувати відсутність штатних можливостей, помилок або недокументованих можливостей, що дозволяють скористатися інформаційними ресурсами через мережеві атаки.

- У сучасних системах присутня маса різноманітних механізмів віддаленого завантаження і запуску виконуваних програм, проконтролювати роботу яких дуже складно.

3.2. Захищені канали передачі

Більш масштабним засобом захисту трафіку в порівнянні з захищеними каналами є віртуальні приватні мережі (VPN). Подібна мережа являє собою свого роду «мережу в мережі», тобто сервіс, який створює у користувачів ілюзію існування їх приватної мережі всередині публічної мережі. Одним з найважливіших властивостей такої «приватної мережі» є захищеність трафіку від атак користувачів публічної мережі. Мереж VPN доступна не тільки здатність імітації приватної мережі; вони дають користувачеві можливість мати власний адресний простір (наприклад, приватні IP-адреси, такі як адреси мережі 10.0.0.0) і забезпечувати якість обслуговування, близьке до якості виділеного каналу.

Віртуальна приватна мережа на основі шифрування може бути визначена як сукупність захищених каналів, створених підприємством в відкритої публічної мережі для об'єднання своїх філій.

Тобто в VPN техніка захищених каналів застосовується вже в інших масштабах, пов'язуючи не двох користувачів, а будь-яку кількість клієнтських мереж.

Технології VPN на основі шифрування включають шифрування, аутентифікацію і тунелювання.

Шифрування гарантує конфіденційність корпоративних даних при передачі через відкриту мережу. Аутентифікація відповідає за те, щоб взаємодіючі системи (користувачі) на обох кінцях VPN були впевнені в ідентичності один одного. Туннелирование надає можливість передавати зашифровані пакети по відкритої публічної мережі.

Для підвищення рівня захищеності віртуальних приватних мереж технології VPN на основі шифрування можна застосовувати спільно з технологіями VPN на основі розмежування трафіку.

При виборі засобів побудови захищених віртуальних мереж необхідно враховувати такі характеристики цих коштів, як функціональна повнота, надійність, гнучкість, продуктивність, керованість і сумісність. Існує кілька способів організації VPN володіють різними перевагами та недоліками:

1) VPN на базі маршрутизаторів

Переваги:

- Функції підтримки мереж VPN можуть бути вбудовані в маршрутизирующие пристрої, що не потребує додаткових витрат на придбання засобів, що реалізують ці функції;

- Спрощується адміністрування VPN.

Недоліки:

- Функціонування VPN може негативно вплинути на інший трафік.

- Канал між одержувачем інформації всередині локальної мережі і маршрутизатором може стати вразливою ланкою в системі захисту.

2) Програмне забезпечення VPN для брандмауерів

Переваги:

- Можливий контроль туннеліруемого трафіку;

- Досягається висока ефективність адміністрування захищених віртуальних мереж;

- Забезпечується комплексний захист інформаційного обміну;

- Відсутня надмірність апаратних платформ для засобів мережевого захисту.

Недоліки:

- Операції, пов'язані з шифруванням даних, можуть надмірно завантажувати процесор і знижувати продуктивність брандмауера;

- Якщо захищений тунель завершується робота брандмауера, то канал між одержувачем інформації всередині локальної мережі і брандмауером може стати вразливою ланкою в системі захисту;

- При підвищенні продуктивності серверних продуктів апаратне забезпечення буде потрібно модернізувати.

3) VPN на базі спеціалізованого програмного забезпечення

Переваги:

- Можливість модернізації і оновлення версій;

- Оперативність усунення помилок;

- Не потрібно спеціальних апаратних засобів.

Недоліки:

- Адміністрування VPN може зажадати окремого додатка, можливо, навіть виділеного каталогу;

- При підвищенні продуктивності серверних продуктів апаратне забезпечення може знадобитися модернізувати.

4) VPN на базі апаратних засобів

Переваги:

- Забезпечується більш висока продуктивність;

- Багатофункціональні апаратні пристрої полегшують конфігурацію і обслуговування;

- Однофункціональні апаратні пристрої допускають тонке налаштування для досягнення найвищої продуктивності.

Недоліки:

- У багатофункціональних блоках продуктивність однієї програми підвищується часто на шкоду іншому;

- Однофункціональні пристрої можуть зажадати окремих інструментів адміністрування і каталогів;

- Модернізація для підвищення продуктивності нерідко виявляється занадто дорогої або неможливою;

- Канал між одержувачем інформації всередині локальної мережі і апаратним пристроєм шифрування трафіку може стати вразливою ланкою в системі захисту

IPSec може застосовуватися в транспортному або тунельному режимі. У першому режимі застосовується для захисту з'єднання «точка - точка», наприклад, між двома комп'ютерами, що належать одній локальній мережі. У тунельному режимі IPSec застосовується для об'єднання двох віддалених офісів і для надання доступу комп'ютера до віддаленого офісу.

При роботі в транспортному режимі IPSec залишає IP-заголовок незмінним (за винятком номера протоколу) і інкапсулює дані після нього. При роботі в тунельному режимі IPSec додає новий IP-заголовок до пакету і інкапсулює колишній IP-заголовок і дані після нього.

IPSec отримав визнання в якості стандарту для надійної комунікації по IP. Він повсюдно вживається як розширення IPv4 і є невід'ємною складовою частиною IPv6. Пакет протоколів забезпечує конфіденційність, цілісність і аутентифікацію джерела даних. Аутентифікація досягається за допомогою заздалегідь наданих загальних секретних ключів або цифрових підписів; надійний обмін ключами здійснюється по протоколу обміну ключами Internet (Internet Key Exchange, IKE).

Крім типових конфігурацій VPN існують ще дві області застосування стандарту IPSec. Цими областями є динамічні з'єднання між хостами через Internet і захист внутрішнього трафіку в локальній мережі.

IPSec можна використовувати для організації надійного каналу зв'язку безпосередньо між взаємодіючими хостами без залучення додаткового обладнання. Це здійснюється шляхом створення з'єднання між хостами по протоколу IPSec із застосуванням транспортного режиму. В цьому режимі кадр IPSec вставляється в вихідний пакет IP слідом за заголовком IP. На противагу тунельному режиму ніякі додаткові заголовки IP не повинні додаватися. Таке рішення вимагає реалізації підтримки IPSec в стеках IP на обох хостах.

Щоб захищений трафік IP міг пройти через міжмережеві екрани мереж партнерів, адміністратори повинні відкрити UDP-порт 500 для протоколів IKE і NAT Traversal. Останнє гарантує, що інформаційний обмін по протоколу IPSec не перериватиме при проходженні через обладнання NAT.

Протокол NAT Traversal (NAT-T) інкапсулює трафік IPSec і одночасно створює пакети UDP, які NAT коректно пересилає. Для цього NAT-T поміщає додатковий заголовок UDP перед пакетом IPSec, щоб він у всій мережі оброблявся як звичайний пакет UDP і хост одержувача не проводив ніяких перевірок цілісності. Після надходження пакету за місцем призначення заголовок UDP видаляється, і пакет даних продовжує свій подальший шлях як інкапсульований пакет IPSec.

Протокол IPSec дозволяє встановлювати захищені комунікаційні канали в локальній мережі. Його прозорість полегшує реалізацію, і при цьому в додатку не потрібно вносити значні виправлення.

IPSec можна поетапно вводити в існуючі мережеві середовища. На перехідному етапі адміністратор має можливість дозволити незахищені з'єднання з хостами, які ще не можуть підтримувати IPSec.

При захисті трафіку локальної мережі віддалені користувачі навряд майже застосовують IPSec-VPN для зв'язку з локальною мережею. Щоб вони могли скористатися захищеними службами, необхідна итерационная техніка

тунелювання. При ітераційне тунелюванні кожен хост має дві або більше асоціації безпеки, відповідно до яких проводиться обмін даними з іншими хостами. Ітераційне туннелирование може бути невидимим для хоста: наприклад, якщо хости встановлюють з'єднання в транспортному режимі від одного сегмента до іншого через тунель IPSec, який проходить через VPN між двома філіями.

Більшість сучасних підприємств, в разі виникнення потреби в захищеному каналі зв'язку всередині локальної мережі або між віддаленими офісами, як правило, використовують технології організації віртуальних мереж. Однак необхідно пам'ятати, що дані рішення мають свої недоліки і абсолютний захист інформації може бути забезпечена тільки при розробці і впровадженні комплексу програмних, апаратних і організаційних заходів для конкретного об'єкта інформаційної діяльності.

SSL VPN - будується на застосуванні криптографічного протоколу для аутентифікації, перевірки і шифрування переданих пакетів інформації. Такий захист надійніше і безпечніше, до того ж дешевше і не вимагає постійних налаштувань. Хоча спочатку SSL розробляли як альтернативну технологію першим способом, сьогодні це окремий пакет. Перевага в тому, що він сумісний з будь-якими операційними системами, для його використання не потрібно встановлювати додатковий софт.

3.3. Порівняння п'яти загальних протоколів VPN

Програми VPN (Virtual Private Network) мають головну роль у приховуванні даних веб-перегляду, серед інших даних. Це робиться шляхом зміни IP-адреси, шифрування даних. Все це можливо завдяки протоколам VPN. Однак це може бути дуже заплутаною темою, оскільки є ряд протоколів, і кожен з них підходить для певних видів онлайн-діяльності. Враховуючи це, розглянемо п’ять найпоширеніших протоколів VPN, їх переваги та недоліки.

Коли організація вирішила використовувати протокол VPN, організація доручає своєму VPN-клієнту обробляти конфіденційні дані певним чином. Як можна очікувати, різні протоколи обробляють дані різними способами, дещо визначаючи пріоритетність продуктивності над безпекою, і навпаки.

3.3.1. PPTP (Point-to-Point Tunneling Protocol)

Таблиця 3.1.Характеристики PPTP

Сумісність платформи	Windows, macOS, Android, iOS, Linux та ін
Шифрування VPN	До 128-розрядних.
Шифрування стандарту безпеки VPN	Відомі вразливості.
Швидкість VPN	висока швидкість через нижчий рівень шифрування)

PPTP - це один із найстаріших протоколів VPN. Перша специфікація для PPTP була опублікована ще в кінці 90-х. Цей тип протоколу VPN досить простий у налаштуванні та має майже універсальну підтримку, але має багато застережень, про які слід знати.

Простий PPTP фактично не має визначеної технології автентифікації або шифрування. Однак, коли PPTP згадується в ці дні, він майже напевно стосується версії, розробленої та поставленої Microsoft разом із Windows. Він утворює пакет технологій, відомий як стек Windows PPTP і дає різні варіанти з точки зору сили шифрування.

PPTP дуже швидкий порівняно з сучасними, сильно зашифрованими протоколами. Це добре, коли мова йде про широкополосні використання, наприклад, потокове відео. Проблема PPTP полягає в тому, що її заходи безпеки протягом багатьох років були порушені. Існує багато нових протоколів, оскільки вразливості в PPTP настільки серйозні. У той час, як PPTP може не допускати крадіжки звичайного трафіку, державна організація

або будь-яка інша організація, що володіє достатніми ресурсами, безумовно може втрутитися і взяти те, що вони хочуть.

Отже, для всіх намірів і цілей PPTP застаріла як технологія конфіденційності та безпеки. Якщо це те, що шукає організація, тоді організації слід вибрати інший протокол. Якщо організація хочете розблокувати лише заблоковані веб-сайти, можливо, варто звернути увагу на постачальника VPN, який пропонує PPTP. Однак у такому випадку може бути кращою ідеєю використовувати іншу технологію, таку як Smart DNS або Proxy, яка не претендує на забезпечення конфіденційності та безпеки, але надасть георозблокування.

3.3.2. L2TP/IPsec (Layer 2 Tunneling Protocol)

Таблиця 3.2. Характеристики L2TP/IPsec

Сумісність із платформою	Windows, macOS, Android, iOS, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Сильна цілісність даних.
Швидкість VPN	Відносно повільна завдяки обробці даних процесором.

Найбільш поширене сполучення з L2TP - це набір протоколів безпеки, відомий як IPsec або просто безпека Інтернет-протоколу. Це IPsec, який фактично містить технологію, яка обробляє аутентифікацію між комп'ютером та сервером VPN. IPsec також містить технологію шифрування пакетів даних із сильним рівнем шифрування. Це робить майже неможливим отримати зашифровані дані.

Насправді L2TP приблизно такий же, як і PPTP, але він не став жертвою багатьох вразливостей. Особливо, якщо мова йде про L2TP / IPsec, який об'єднаний у стандарт, який сьогодні широко використовується. Як і PPTP,

L2TP широко підтримується клієнтами та службами. Однак одна з головних проблем з L2TP полягає в тому, що її можна заблокувати досить легко. Це тому, що він використовує лише невелику кількість мережевих "портів", все, що потрібно зробити, це закрити порти, і VPN перестане працювати.

Нарешті, є лише два стандарти шифрування, які можна вибрати між L2TP / IPsec. 3DES - це один, але через відомі вразливості його ніхто більше не використовує. Стандарт для L2TP / IPsec (і VPN, загалом, сьогодні) є стандартом AES. 256-бітний AES, по суті, неможливо примусити зламати будь-яку існуючу комп'ютерну технологію.

Взагалі, L2TP / IPsec - це чудовий вибір для пересічного користувача Інтернету, який просто має великий рівень безпеки.

3.3.3. SSTP (Secure Socket Tunneling Protocol)

Таблиця 3.3.Характеристики SSTP

Сумісність із платформою	Windows, macOS, Android, Linux та ін.
Шифрування VPN	До 256-бітного.
Сильне шифрування VPN Security	Шифрування SSL включено
Шифрування SSL включено	Повільна швидкість (завдяки високому рівню безпеки).

SSTP - це один з протоколів VPN, який невразливий до атак, що блокує VPN, який отримано з L2TP. Однак слід відразу знати, що SSTP пов'язаний в основному з Windows, тому, якщо запустити його на будь-що інше, можливо, не пощастить. Існує новаторська підтримка macOS та Linux, але налаштування можуть відрізнятися. Якщо організація шукає VPN на базі Windows, то варто зупинитись на SSTP.

Вперше побачили SSTP з випуском пакета оновлень 1 для Windows Vista. SSTP - це власницький протокол, що належить повністю та розроблений

Microsoft. Це може бути проблемою для деяких людей, оскільки внутрішня робота стандарту закрита. Це означає, що завжди є ймовірність того, що Microsoft могла б на базі уряду США вбудувати інший план у свій стандарт. Як завжди, фактичних доказів цього немає, але це слід пам’ятати, залежно від того, чому організація хоче захистити мережу.

SSTP використовує стандарт шифрування SSL 3.0, який тепер є новим стандартом, який має кілька відомих проблем безпеки. Насправді, сама Microsoft випустила консультацію щодо безпеки SSL 3.0 ще в 2014 році, вказуючи, що існують відомі проблеми з протоколом.

Однією з головних переваг SSTP є те, що він може перемогти багато форм блокування VPN, оскільки він може використовувати загальний порт (TCP 443), що, звичайно, використовують загальні веб-сайти SSL для порту. Оскільки Windows поширена в більшості частин світу, є хороший шанс отримати доступ до SSTP як спосіб подолати блокування VPN.

Якщо трохи зрозуміліше ставитись до SSTP, є ще один протокол, який пропонує багато тих же переваг, що і SSTP, але без багажу Microsoft: OpenVPN

3.3.4 OpenVPN

Таблиця 3.4.Характеристики SSTP

Сумісність із платформою	Windows, macOS, Android, iOS, Linux, маршрутизатори тощо.
Шифрування VPN	До 256-бітного.
VPN безпека	Найвища безпека; Цифрова сертифікація.
VPN швидкість	швидкий, незважаючи на високий рівень безпеки

OpenVPN - це одна з найбільш поширених VPN, коли мова заходить про конфіденційність в Інтернеті. Це справжній протокол VPN з відкритим кодом, який постійно зростає і йде в ногу з постійно розквітаючим світом кібербезпеки.

OpenVPN використовує OpenSSL та TLS в основному. Однак є ціла низка інших незначних технологій, які в неї вбудовані. На відміну від PPTP, SSTP та більшості інших протоколів VPN, OpenVPN не має вбудованої підтримки для будь-якої операційної системи або апаратної системи. Таким чином, організація може думати, що OpenVPN є системно-агностичним рішенням. Це і профі, і обмеження для OpenVPN, оскільки це означає, що кожен, хто хоче використовувати OpenVPN, повинен користуватися стороннім VPN-клієнтом.

OpenVPN широко використовується преміальними постачальниками VPN, оскільки ці компанії мають ресурси для розвитку власних VPN-клієнтів. Це також означає, що постачальник VPN в основному визначає, які пристрої він підтримує. Якщо він не створює клієнта для, скажімо, Android, ви не можете ним користуватися. Ну, насправді це не зовсім вірно, оскільки існує багато загальних клієнтів OpenVPN практично на всіх платформах. Проблема в тому, що тепер доведеться довіряти як своєму постачальнику VPN, так і тим,

хто створив загальний клієнт. Що означає вдвічі більший ризик для заднього дверей.

У той час як OpenVPN найкраще працює на ряді портів UDP, ним можна керувати через порт TCP 443. Це дозволяє отримувати зворотній зв'язок на трафіку веб-сайту HTTPS та ухилятися від блокування VPN на основі порта. Оскільки OpenVPN використовує бібліотеку OpenSSL, вона має доступ до всіх технологій шифрування, що входять до цієї бібліотеки. Однак рідко застосовується будь-яке, крім шифрування AES, що добре, якщо достатня довжина ключа.

Підсумком є те, що OpenVPN - це самий гнучкий і безпечний протокол, який організація може отримати сьогодні. Поки провайдер VPN розуміє технологію та впроваджує її належним чином, зазвичай це саме те, що потрібно. Як мінімум, якщо OpenVPN доступний, спершу слід спробувати його, перш ніж перейти до іншої опції.

3.3.5 IKEv2/IPsec – Internet Key Exchange

Як і L2TP/IPsec, IKEv2/IPsec - це комбінація різних протоколів тунелювання в поєднанні з набором технологій безпеки IPsec. Це ще один протокол, який не є відкритим за своєю суттю.

IKE - один з найновіших протоколів, випущений в середині 2000-х, і він поки не отримав широкої підтримки або прийняття.

На щастя для всіх, IKE також підтримує інші платформи, менш езотеричні. Наприклад, iOS має підтримку. Фактично, IKEv2 був створений з огляду на безпеку мобільних пристроїв і здатний дозволяти мобільним телефонам переходити з Wi-Fi підключень до мобільного Інтернету, не випадаючи з тунелю VPN. Це пояснюється тим, що протокол підтримує технологію, відому як "мультихомінг", яка дозволяє легко обробляти мережеві зміни.

Визначальною особливістю IKEv2 є те, наскільки це швидко. Залежно від обставин. його часто розглядають як один із найшвидших протоколів VPN,

доступних сьогодні. Тим не менш, VPN-провайдери дуже важко підтримують цю технологію. З одного боку, він має дуже вузьку підтримку платформи. Це також закрита система з корпоративними інтересами.

Отже, хоча цей протокол забезпечує високу стабільність і високу швидкість, він має вузьку підтримку, вразливий до блокування VPN і страждає у безпеці.

Висновки до розділу 3

В даному розділі було було розглянуто п’ять основних протоколів VPN. Дані протоколи мають відмнінності в архітектурі, але найважливішими є відмінності в шифруванні даних, що впливає на захист інформації.

Таблиця 6. Загальне порівняння

	PPTP	L2TP/IPSec	OpenVPN	SSTP
Підтримувані ОС	Windows, Mac OS X, Linux, iOS, Android, Windows Phone, DD-WRT	Windows, Mac OS X, Linux, iOS, Android, Windows Phone, DD-WRT	Windows, Mac OS X, Linux, iOS, Android	Windows
Безпека	Низька	Висока	Дуже висока	Дуже висока
Швидкість	Висока	вимоглива до ресурсів ЦП	Відмінна продуктивність.Працює швидко навіть при з'єднаннях з високими затримками	Відмінна продуктивність. Працює швидко навіть при з'єднаннях з високими затримками

Налаштування	Дуже проста. Протокол вбудований в багато пристроїв. Не потребує додаткового ПЗ.	Проста. Вимагає додаткові налаштування. Протокол вбудований в багато пристроїв. Не потребує додаткового ПЗ.	Вимагає установки додаткового ПЗ. Необхідна установка сертифікатів.	Протокол вбудований в Windows 7 і пізніші. Необхідна установка сертифікатів.
Заключення	Швидкий і дуже легкий в налаштуванні. Хороший вибір, якщо пристрої не підтримують OpenVPN або SSTP.	Хороший вибір, якщо пристрої не підтримують OpenVPN або SSTP і потрібна висока безпека.	Рекомендований протокол для Windows, Linux і Mac OS. Висока продуктивність, безпеку і стабільність.	Працює тільки з Windows. Висока продуктивність, безпеку і стабільність.

Як видно з таблиці 6, протоколи і стандарти мають різні характеристики; деякі пропонують високий рівень захисту, в той час як інші демонструють більшу продуктивність. Тут все залежить виключно від потреб і завдань, так як можна жертвувати продуктивністю заради отримання більшого рівня

захисту і навпаки. Базуючись на результатах дослідження в Розділі 2, можемо зробити висновки, що OpenVPN спрямований на забезпечення швидкої взаємодії між мережами та елементами мережі, а також надійного захисту.

Серед переваг OpenVPN можна відзначити легкий процес налаштування, високий рівень безпеки, підтримку безлічі алгоритмів шифрування, а також хорошу продуктивність проти фаєрволів і доступність за принципом open source. Але для роботи OpenVPN потрібно стороннє ПО, яке може виявитися складним в налаштуванні. Хоча підтримка мобільних пристроїв тут і передбачена, вона поки що не так хороша, як підтримка настільних ПК. Що стосується швидкості в стандартному UDP-режимі, цей алгоритм повинен працювати швидше L2TP, але навряд чи буде швидше PPTP.

ЗАГАЛЬНІ ВИСНОВКИ

Стрімке зростання обсягів трафіку, необхідність підтримки зростаючої кількості користувачів, формування високопродуктивних систем для обробки даних та віртуалізованих середовищ для надання хмарних сервісів - все це серйозно змінило вимоги до телекомунікаційних мереж. Все частіше традиційна мережа стає обмежуючим фактором розвитку обчислювальної інфраструктури.

В якості технології, яка може вирішити проблеми захисту інформації, все частіше використовується VPN. Безліч IT організацій і мережевих провайдерів успішно використовують її, в першу чергу, з метою захисту каналів передачі даних і витрат на її утримання, а також для забезпечення високого рівня безпеки, захищеності, надійності мережі, для зменшення часу і складності розгортання нових сервісів. В процесі виконання роботи було опрацьовано літературні джерела стосовно поставлених задач, досліджено існуючі технології побудови захищених каналів та мереж, описані в перших двох розділах, та вибраний найоптимальніший спосіб реалізації.

З результатів роботи випливає , що для підвищення надійності передачі даних по каналах VPN з використанням OpenVPN слід використовувати найбільшу з можливих довжину ключа шифрування.

Аналізуючи основні проблеми інформаційної безпеки в локальних чи глобальних мережах, якими є віртуальні приватні мережі, можна зробити висновок, що такі системи повинні забезпечувати виявлення внутрішніх і зовнішніх загроз і вторгнень, фільтрацію зовнішнього трафіку, контроль за використанням корпоративних мережевих ресурсів і запобігання витоків конфіденційної інформації. Вхідними даними при цьому є інформація про структуру і характеристиках трафіку (прецедентна інформація), що дозволяє побудувати набір правил, що класифікують нормальні або аномальні компоненти трафіку. У цьому напрямку слід очікувати істотне підвищення безпеки мереж за рахунок оперативного реагування на набір відомих загроз і

на які раніше не зустрічалися аномальні ситуації, а також за рахунок ідентифікації реально функціонуючих мережевих додатків або процесів та управління ними для забезпечення доступності інформаційних сервісів необхідних мережному співтовариству.

Тому стає очевидним необхідність вирішення проблеми зв'язки «тунелювання + аутентифікація + шифрування», яка дозволяє побудувати захищену мережу VPN.

Для звичайної повсякденної роботи в мережі цілком підійдуть OpenVPN, L2TP / IPsec і IKEv2. Якщо на пристрої встановлено ОС Windows, то і SSTP згодиться, однак не варто забувати, що цей протокол може бути уразливий сильніше інших. Це ж справедливо і для L2TP з IKEv2 - в плані безпеки ці протоколи так само сильні. У наш час захистити він не зможе нікого, і вже тим більше він не зможе захистити конфіденційність при роботі в мережі.

Захист забезпечить лише той протокол, який позбавлений вразливостей і слабких місць. На даний момент єдиним таким варіантом є OpenVPN. До того ж, це один з небагатьох протоколів, підтримуваних відразу на декількох платформах.

Переваги OpenVPN:

- Відносно новий протокол з відкритим вихідним кодом, який вважається завдяки своїй надійності «золотим стандартом» в галузі.
- Виключно популярний варіант у сторонніх сервісів, ні на одній з платформ він не підтримується за замовчуванням.
- Підтримує найрізноманітніші алгоритми, що дозволяє надійно захистити користувача.
- Один з найшвидших протоколів. Швидкість залежить від використовуваного шифрування, але звичайні користувачі навряд чи помітять зниження швидкості в більшості випадків.
- Можливо, установка здасться складною, але це лише на перший погляд. Всі VPN-сервіси, що використовують цей протокол, підтримують

автоматичну настройку, що практично не вимагає від користувача брати участь в процесі.

ПЕРЕЛІК ПОСИЛАНЬ

1. VPN протоколы [Електронний ресурс] – Режим доступу до ресурсу: https://www.cactusvpn.com/ru/beginners-guide-to-vpn/vpn-protocol/
2. Virtual private network (VPN) [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Virtual_private_network
3. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. / Учебник. - СПб: Питер, 2002
4. Браун С. Віртуальні приватні мережі. – М.: Радіо та зв'язок, 2001.
5. Деарт В.Ю. Асимметричная цифровая абонентская линия. Описание системы./ Под ред., Д.М. Броннер. Учебное пособие. 2001.
6. A Framework for IP Based Virtual Private Networks [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/rfc/rfc2764.txt
7. Pure hardware VPNs rule high-availability tests [Електронний ресурс] – Режим доступу до ресурсу: https://web.archive.org/web/20070923013848/http://www.networkworld.com/reviews/2000/1211rev.html
8. Райан Норманн Выбираем протокол VPN [Електронний ресурс] – Режим доступу до ресурсу: http://www.osp.ru/win2000/2001/07/175027/
9. 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-difference-choose/
10. IPSec — протокол захисту мережевого трафіку на IP-рівні. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ixbt.com/comm/ipsecure.shtml
11. Базова реалізація бібліотек для роботи з IPsec для Unix-подібних систем [Електронний ресурс] – Режим доступу до ресурсу: http://ipsec-tools.sourceforge.net/

12. Запечников С. В. Основы построения виртуальных частных сетей. - Горячая Линия – Телеком, 2003.
13. Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Н. Г. Медведев, Д.В. Москалик - К: Европ.. ун-та, 2002.
14. Оголюк А., Щеглов А. Технологии построения системы защиты сложных информационных систем, Экономика и производство, №3, 2001.
15. Ситник В.О. Основи інформаційних систем. – К.: КНЕУ, 1997.
16. Файльнер М. Виртуальные частные сети нового поколения LAN, № 11,- 2005.
17. Фортенбери Т. Проектирование виртуальных частных сетей в среде Windows 2000, - Вильямс, 2002.
18. Хетч Б., Колесников О. Создание виртуальных частных сетей (VPN) - КУДИЦ-Образ, 2004.
19. Петров А.А. Компьютерная безопасность: криптографические методы защиты – М.:ДМК, 2000.