КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

кібербезпеки та комп`ютерної інженерії

(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

на тему: «Система захищеного доступу на основі Open VPN»

ЧУБ РОДІОН АНДРІЙОВИЧ
(прізвище, ім’я та по батькові студента повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

(факультет)

кібербезпеки та комп`ютерної інженерії

(кафедра)

ЗАТВЕРДЖУЮ
Завідувач кафедри КБКІ
к.т.н., доцент Делембовський М.М.

_____
„___” _____2025 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

на тему: "Система захищеного доступу на основі Open VPN"

Виконав: Студент спеціальності

125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)

Чуб Р.А.
(прізвище та ініціали)

Керівник д.т.н., проф. Терентьєв О.О.
(прізвище та ініціали)

Рецензент к.т.н., доц. Баліна О.І.
(прізвище та ініціали)

Київ, 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій
Кафедра: кібербезпеки та комп`ютерної інженерії
Освітній рівень: «магістр» за ОПП
Спеціальність: 125 «Кібербезпека та захист інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри КБКІ
к.т.н., доцент Делембовський М.М.

_____

„_____” _____2025 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

Чуб Родіон Андрійович

Тема роботи: Система зхищеного доступу на основі Open VPN
затверджена наказом ректора КНУБА № ____ від « » 2025 р.
2. Керівник роботи: Терентьєв О.О., д.т.н, професор кафедри ІТППМ
3. Строк подання студентом роботи до захисту: грудень 2025 р.
4. Зміст пояснювальної записки за розділами:
Р.1. Аналіз предметної області та постановка задачі
Р.2. Аналіз протоколів VPN мереж
Р.3. Розробка захищеного доступу на основі Open VPN
5. Інформаційні слайди:
С.1. Дерево функцій, дерево цілей системи
С.2. Топологія мережі типової організації
С.3. Концептуальна модель системи
С.4. Діаграма класів, прецендентів, послідовностей, потоків даних системи
С.5. Програмне забезпечення системи
С.6. Тестовий приклад програми

6. Календарний план виконання кваліфікаційної роботи

Види робіт та їх зміст	Дата виконання
Р. 1. Аналіз предметної області та постановка задачі	Вересень 2025 р.
Р. 2. Аналіз протоколів VPN мереж	Жовтень 2025 р.
Р. 3. Розробка захищеного доступу на основі Open VPN	Грудень 2025 р.
Остаточне оформлення роботи	Грудень 2025 р.
Направлення роботи на рецензування, плагіат	Грудень 2025 р.
Попередній захист роботи на кафедрі	Грудень 2025 р.

7. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Прийом програмного продукту	к.т.н. доц. Баліна О.І.		

8. Дата видачі завдання: 22 вересня 2025 року

Керівник _____ Терентьєв О.О.
(підпис) (прізвище та ініціали)

Бакалавр _____ Чуб Р.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

«Система захищеного доступу на основі Open VPN».

Кваліфікаційна робота бакалавра за спеціальністю: 125. «Кібербезпека та захист інформації» – Київський національний університет будівництва та архітектури. – Київ, 2025.

Актуальність даної теми обумовлена тим, що в даний час оперативний обмін інформацією - один з основних інструментів успішної роботи, але питання захищеності такого обміну при збереженні зручності між підрозділами, відкритий. Одним з варіантів забезпечення такої передачі є побудова VPN мережі. В основі концепції побудови віртуальних мереж VPN лежить досить проста ідея: якщо в глобальній мережі є два вузла, яким потрібно обмінятися інформацією, тоді між цими двома вузлами необхідно побудувати віртуальний захищений тунель для забезпечення конфіденційності і цілісності інформації, що передається через відкриті мережі; доступ до цього віртуального тунелю повинен бути надзвичайно утруднений всіх можливих активним і пасивним зовнішнім спостерігачам.

SUMMARY

"Open VPN-protected access system".

Certification master's thesis in the specialty: 125. "Cybersecurity" - Kyiv National University of Construction and Architecture. - Kyiv, 2025.

The urgency of this topic is due to the fact that currently operational information exchange - one of the main tools for successful work, but the issue of the security of such exchanges while maintaining the convenience between the divisions, is open. One of the options for providing such a transfer is to build a VPN network. The concept of constructing VPN virtual networks is based on a rather simple idea: if there are two nodes in the global network that need to exchange information, then a virtual secure tunnel must be built between these two nodes to ensure the confidentiality and integrity of the information transmitted through open networks; access to this virtual tunnel should be extremely difficult for all possible active and passive external observers.

ЗМІСТ

ВСТУП

Останнім часом в світі телекомунікацій спостерігається підвищений інтерес до віртуальних приватних мереж. Це обумовлено необхідністю зниження витрат на утримання корпоративних мереж за рахунок більш дешевого підключення віддалених офісів і віддалених користувачів через мережу Internet. Дійсно, при порівнянні вартості послуг по з'єднанню декількох мереж через Internet, наприклад, з мережами Frame Relay можна помітити суттєву різницю у вартості. Однак необхідно відзначити, що при об'єднанні мереж через Internet, відразу ж виникає питання про безпеку передачі даних, тому виникла необхідність створення механізмів які дозволяють забезпечити конфіденційність і цілісність інформації, що передається. Мережі, побудовані на базі таких механізмів, і отримали назву VPN.

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. Недолік технології Open VPN в тому, що кошти побудови VPN не є повноцінними засобами виявлення і блокування атак. Вони можуть запобігти ряду несанкціонованих дій, але далеко не всі можливості можуть використовуватися для проникнення в корпоративну мережу. Переваги технології Open VPN в тому, що реалізація віддаленого доступу робиться не через телефонну лінію, а через Internet, що набагато дешевше і краще. Але, незважаючи на все це, технологія Open VPN має перспективи на подальший розвиток. Слід зазначити, що для реалізації VPN існують цілі апаратні комплекси, однак вони не знайшли широкого поширення в силу своєї спрямованості на обслуговування великих підприємств і, як наслідок дорожнечі. Обчислювальна потужність апаратних рішень зазвичай дуже висока але не завжди затребувана, тому програмні рішення, а тим більше стандартні, які не потребують додаткових витрат на пошук і придбання

додаткового програмного забезпечення, придбали таку величезну популярність. Побудована в результаті цього, технологія Open VPN дуже проста, але вона вказує на основні моменти побудови VPN. За допомогою Open VPN - реалізується безпека не тільки інформації, яка передається, але і самого підключення. Технологія OpenVPN повністю виправдовує себе. З мінусів виділяється деяка складність налаштування і створення Open VPN мережі. З плюсів - кроссплатформенність. На мою думку, технологія Open VPN має перспективу на широке поширення по всьому світу.

1 ДОСЛІДЖЕННЯ ПОБУДОВИ ТА ВИКОРИСТАННЯ OPEN VPN

1.1 Основні поняття і функції мережі VPN

VPN – технологія що дозволяє забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Незважаючи на те, що комунікації здійснюються по мережах з меншим невідомим рівнем довіри (наприклад, публічні мережі), рівень довіри до побудованої логічної мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікації, інфроструктури відкритих ключів, засобів для захисту від повторів і змін переданих по логічної мережі повідомлень).

Мета VPN-технологій полягає в максимальному ступені відокремлення потоків даних одного підприємства від потоків даних всіх інших користувачів мережі. Відособленість повинна бути забезпечена відносно параметрів пропускної здатності потоків які гарантують конфіденційність. Таким чином, завданнями технології VPN є забезпечення в мережах загального користування гарантованої якості обслуговування для потоків даних, а також захист їх від можливого несанкціонованого доступу.

Оскільки основним завданням VPN є захист трафіку, тому віртуальна мережа повинна задовільняти велику кількість вимог і впершу чергу, мати надійну криптографію, що гарантує захист від прослуховування, зміни навантаження трафіку. Крім того, VPN повинна мати надійну систему управління ключами і кріптоінтерфейсом, що дозволяє здійснювати кріптоопераціі: захищена пошта, програми шифрування дисків і файлів і ін. В даний час інтерес до використання засобів для побудови VPN постійно зростає, що обумовлено цілим рядом причин:

- низькою вартістю експлуатації за рахунок використання мереж загального користування замість власних або орендованих ліній зв'язку;
- масштабованістю рішень;
- простотою зміни конфігурації;

- "прозорістю" для користувачів і додатків.

При використанні VPN-технологій можна забезпечити:

- захист (конфіденційність, аутентичність і цілісність) переданої інформації;

- захист внутрішніх сегментів мережі від несанкціонованого доступу з боку мереж загального користування;

- приховування внутрішньої структури захищених сегментів мережі;

- ідентифікацію та аутентифікацію користувачів мережевих об'єктів;

- централізоване управління політикою корпоративної мережевої безпеки і VPN-мережі.

1.2 Способи створення захищених віртуальних каналів

Будь-який з двох вузлів віртуальної мережі, між якими формується захищений тунель, може належати кінцевій або проміжній точці захисту потоку повідомлень. Відповідно можливі різні способи захищеного віртуального каналу, приклад якого зображений на рисунку 1.1.

Варіант, коли кінцеві точки захищеного тунелю збігаються з кінцевими точками захищеного потоку повідомлень, є з точки зору безпеки кращим. У цьому випадку забезпечується повна захищеність каналу вздовж усього шляху проходження пакетів повідомлень. Однак такий варіант веде до децентралізації управління і надмірності ресурсних витрат. Потрібна установка засобів, створення захищених тунелів на кожний клієнтський комп'ютер локальної мережі, що ускладнює централізоване управління доступом до комп'ютерних ресурсів і економічно не завжди виправданий. У великій мережі окреме адміністрування кожного клієнтського комп'ютера з метою конфігурації в ньому засобів захисту є досить трудомістською процедурою.

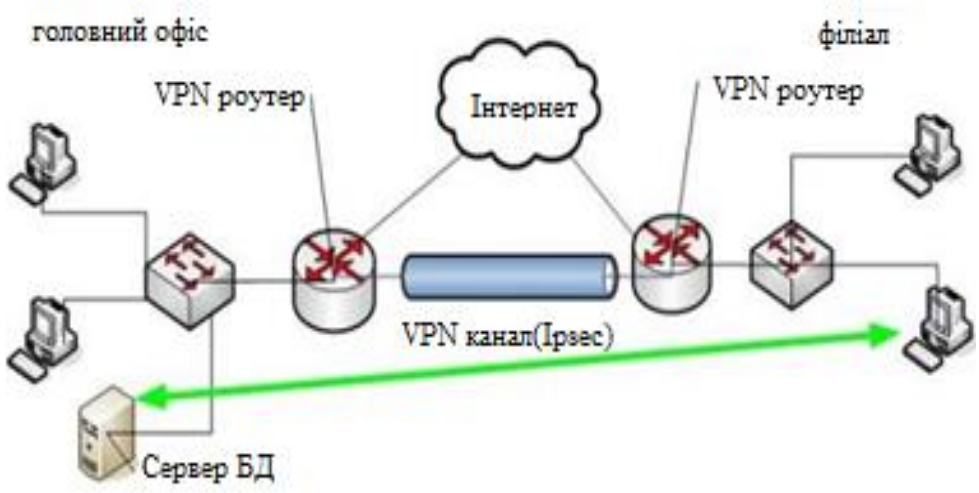

Рисунок 1.1 - Захищений віртуальний канал

Тому, якщо відсутня необхідність захисту трафіку всередині локальної мережі, що входить в віртуальну мережу, то в якості кінцевої точки захищеного тунелю доцільно вибрати брандмауер або прикордонний маршрутизатор цієї локальної мережі. У разі ж, коли всередині локальної мережі потік повідомлень також повинен бути захищений, то в якості кінцевої точки тунелю в цій мережі повинен виступати комп'ютер, який представляє одну із сторін захищеної взаємодії. При доступі до локальної мережі віддаленого користувача комп'ютер цього користувача також повинен бути кінцевою точкою захищеного віртуального каналу.

Поширений також варіант, що характеризується більш низькою безпекою, але більш високою зручністю застосування. Відповідно до даного варіанту робочі станції і сервери локальної мережі, а також вилучені комп'ютери не беруть участі у створенні захищеного тунелю, який прокладається тільки всередині публічної мережі з комутацією пакетів, наприклад, всередині Internet. В якості кінцевих точок такого тунелю найчастіше виступають провайдери Internet або прикордонні маршрутизатори (брандмауери) локальної мережі. При віддаленому доступі до локальної мережі тунель створюється між сервером віддаленого доступу провайдера Internet, а також прикордонним провайдером Internet або маршрутизатором (брандмауером) локальної мережі. При об'єднанні локальних мереж тунель

може формуватися тільки між прикордонними провайдерами Internet або маршрутизаторами (брандмауерами) локальної мережі.

Аргументацією на користь описаного варіанта створення віртуальних мереж виступає той факт, що уразливими для зловмисників більшою мірою є мережі з комутацією пакетів, такі, як Internet, а не канали телефонної мережі або виділені канали зв'язку. Віртуальні мережі, побудовані за цим варіантом, мають гарну масштабованість і керованість. Для клієнтських комп'ютерів і серверів локальної мережі, що входять в віртуальну мережу, захищені тунелі повністю прозорі і програмне забезпечення цих вузлів залишається без змін. Однак через те, що частина захищеного трафіку проходить в незахищеному вигляді в публічних каналах зв'язку, даний варіант істотно знижує безпеку інформаційної взаємодії. Крім того, велика частина роботи по створенню захищених тунелів лягає на провайдерів,

Створення захищеного тунелю виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором і термінатором тунелю. Ініціатор тунелю інкапсулює (вбудовує) пакети в новий пакет, що містить поряд з вихідними даними новий заголовок з інформацією про відправника та одержувача. Хоча всі передані по тунелю пакети є пакетами IP, інкапсулюємі пакети можуть належати до протоколу будь-якого типу, включаючи пакети не маршрутизуємих протоколів, таких, як NetBEUI. Маршрут між ініціатором і термінатором тунелю визначає звичайна маршрутизація мережі IP, яка може бути і мережею, відмінною від Internet. Термінатор тунелю виконує процес, зворотний інкапсуляції - він видаляє нові заголовки і направляє кожен вихідний пакет в локальний стек протоколів або адресату в локальній мережі. Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, переданих по тунелю VPN. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту інкапсулюємих пакетів. Конфіденційність інкапсулюємих пакетів забезпечується шляхом їх криптографічного закриття, тобто зашифровують, а цілісність і автентичність відбитку - шляхом

формування цифрового підпису. Оскільки існує велика кількість методів криптозахисту даних, дуже важливо, щоб ініціатор і термінатор тунелю використовували одні й ті ж методи і могли погоджувати один з одним цю інформацію, передану по тунелю VPN. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту інкапсулюємих пакетів. Конфіденційність інкапсулюємих пакетів забезпечується шляхом їх криптографічного закриття, а цілісність і аутентичність відбитку - шляхом формування цифрового підпису.

1.3 Класифікація VPN мереж

Класифікувати VPN рішення можна за кількома основними параметрами, які представлені на рисунку 1.2.

За типом використовуваного середовища:

Захищені VPN мережі. Найбільш поширений варіант приватних мереж. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, як правило, Інтернету.

Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

Довірчі VPN мережі. Використовуються у випадках, коли передавальну середу можна вважати надійною і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN є: MPLS і L2TP. Ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec.

За способом реалізації:

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.

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

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

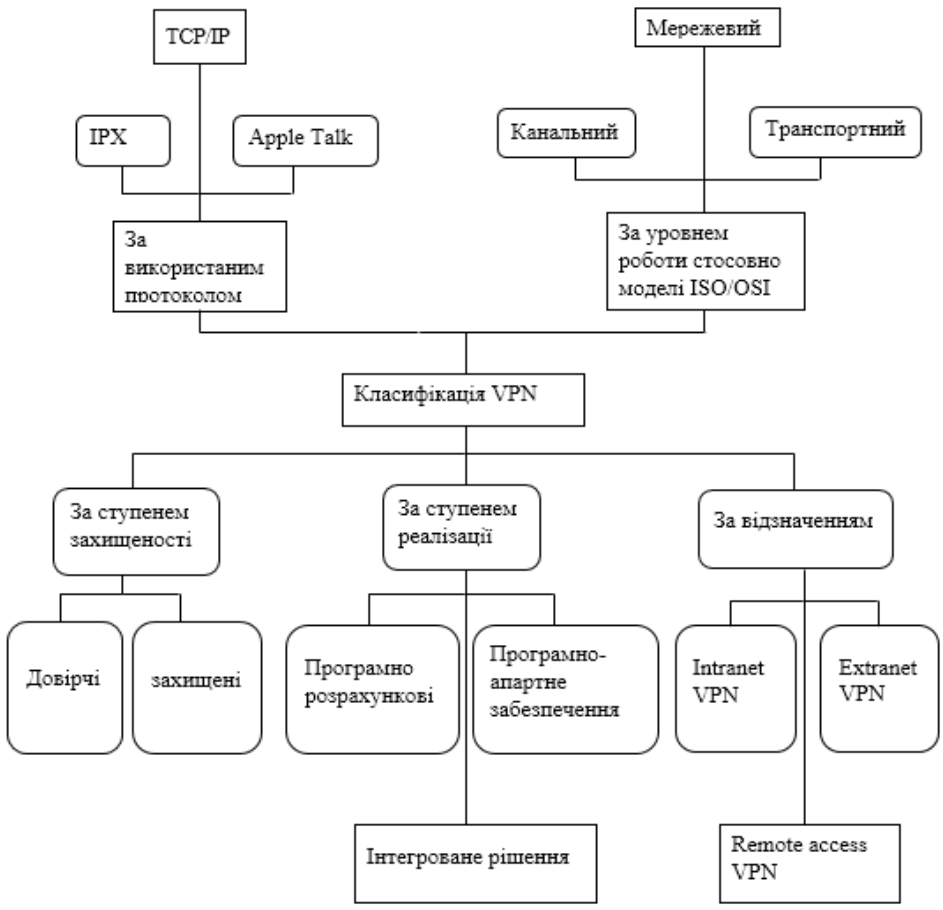

Рисунок 1.2 - Класифікація VPN

1.3.1 По архітектурі

За архітектурою технічного рішення прийнято виділяти три основних види віртуальних приватних мереж:

- внутрішньокорпоративні VPN (Intranet VPN);
- VPN з віддаленим доступом (Remote Access VPN)
- міжкорпоративні VPN (Extranet VPN).

Intranet VPN використовується для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку. При організації такої схеми підключення потрібна наявність VPN серверів яка дорівнює кількості офісів.

Даний спосіб доцільно використовувати як для звичайних філій, так і для мобільних офісів, які матимуть доступ до ресурсів «материнської» компанії, а також без проблем обмінюються даними між собою.

Інтранет побудований на базі тих же понять і технологій, які використовуються для Інтернету, такі як архітектура клієнт-сервер і стек протоколів Інтернет (TCP/IP). У Інтранет зустрічається всі відомі інтернет-протоколи, наприклад, протоколи HTTP (веб-служби), SMTP (електронна пошта), і FTP (передача файлів). Інтернет-технології часто використовуються для забезпечення сучасних інтерфейсів функціями інформаційних систем, які розміщують корпоративні дані.

Інтранет можна уявити як приватну версію Інтернету, або як приватне розширення Інтернету, обмеженого організацією за допомогою брандмауера. Перші інтранет-веб-сайти і домашні сторінки почали з'являтися в організаціях в 1990-1991. Проте за неофіційними даними, термін Інтранет вперше став використовуватися в 1992 році в таких установах, як університети і корпорації, що працюють в технічній сфері.

Інтранет також протиставляють екстранеті; доступ до Інтранету надано тільки службовцям організації, в той час як в екстранеті можуть отримати доступ клієнти, постачальники, або інші затверджені керівництвом особи. У Екстранет-технології крім приватної мережі, користувачі мають доступ до Інтернет ресурсів, але при цьому здійснюються спеціальні заходи для безпечного доступу, авторизації, і аутентифікації.

Інтранет компанії не обов'язково повинні забезпечувати доступ до Інтернету. Коли такий доступ все ж забезпечується, зазвичай це відбувається через мережевий шлюз з брандмауером, захищаючи Інтранет від несанкціонованого зовнішнього доступу. Мережевий шлюз часто також

здійснює призначену для користувача аутентифікацію, шифрування даних, і часто - можливість з'єднання по віртуальній приватній мережі (VPN) та знаходяться за межами підприємства співробітників, щоб вони могли отримати доступ до інформації про компанії, обчислювальних ресурсів і внутрішнім контактам.

Переваги Intranet VPN:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;

- надійність функціонування при виконанні таких критичних додатків, як системи автоматизованого продажу і системи управління базами даних;

- гнучкість управління ефективним розміщенням швидко зростаючого числа нових користувачів, нових офісів і нових програмних додатків.

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 або смартфона.

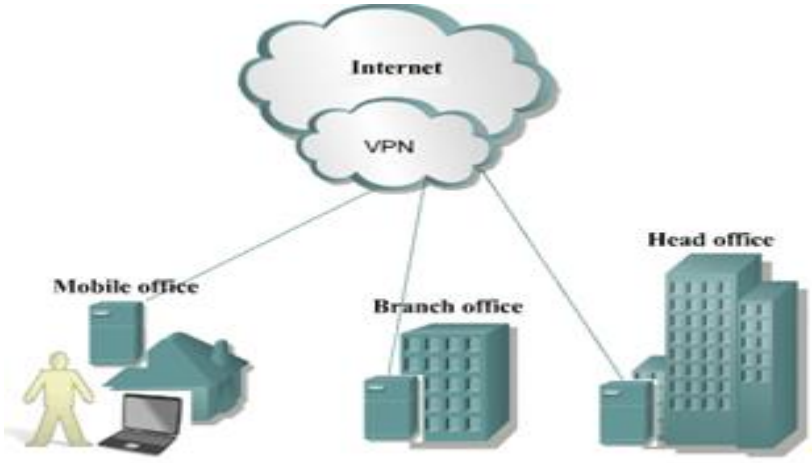

Рисунок 1.3 - Схема підключення Intranet VPN

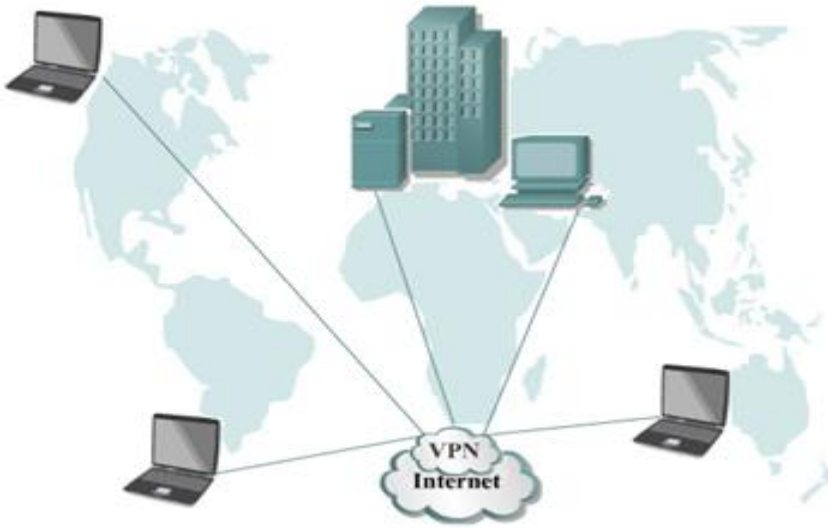

Рисунок 1.4 - Схема віддаленого доступу VPN

Переваги переходу від персонально керованих dial networks до Remote Access VPN:

- можливість використання місцевих dial-in numbers замість міжміських дозволяє значно знизити витрати на міжміські телекомунікації;

- ефективна система встановлення аутентичності віддалених і мобільних користувачів забезпечує надійне проведення процедури аутентифікації;

- висока масштабованість і простота розгортання для нових користувачів, що додаються до неї;

- зосередження уваги компанії на основних корпоративних бізнес-цілях замість відволікання на проблеми забезпечення роботи мережі.

Істотна економія при використанні Remote Access VPN є потужним стимулом, однак застосування відкритого Інтернет в якості об'єднуючої магістралі для транспорту чутливого корпоративного трафіку стає все більш масштабним, що робить механізми захисту інформації життєво важливими елементами даної технології.

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.

Мережі Extranet VPN в цілому схожі на внутрішньо-корпоративні віртуальні приватні мережі з тією різницею, що проблема захисту інформації є для них більш гострою. Для Extranet VPN характерно використання стандартизованих VPN-продуктів, які гарантують здатність до взаємодії з різними VPN-рішеннями, які ділові партнери могли б застосовувати в своїх мережах.

Коли кілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні подбати про те, щоб їх нові партнери мали доступ тільки до певної інформації. При цьому конфіденційна інформація повинна бути надійно захищена від несанкціонованого використання. Саме тому в міжкорпоративних мережах велике значення надається контролю доступу з відкритої мережі за допомогою МЕ. Важлива і аутентифікація користувачів, яка може гарантувати, що доступ до інформації отримують тільки ті, кому він дійсно дозволений. Разом з тим, розгорнута система захисту від несанкціонованого доступу не повинна привертати до себе уваги.

З'єднання Extranet VPN розгортаються, використовуючи ту ж архітектуру і протоколи, які застосовуються при реалізації Intranet VPN і Remote AccessVPN. Основна відмінність полягає в тому, що дозвіл доступу, який дається користувачам Extranet VPN, пов'язаний з мережею їх партнера.

1.3.2 За типом технічної реалізації

Існують різні варіанти побудови VPN. 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 простим трафіком, не кажучи вже про VPN. Досвід показує, що для побудови VPN найкраще використовувати спеціалізоване обладнання,

однак якщо є обмеження в засобах, то можна звернути увагу на чисто програмне рішення. Розглянемо деякі варіанти побудови VPN.

VPN на базі брандмауерів. Брандмауери більшості виробників підтримують туннелювання і шифрування даних. Всі подібні продукти засновані на тому, що трафік, який проходить через брандмауер шифрується. До програмного забезпечення брандмауера додається модуль шифрування. Недоліком цього методу можна назвати залежність продуктивності від апаратного забезпечення, на якому працює брандмауер. При використанні брандмауерів на базі ПК треба пам'ятати, що подібне рішення можна застосовувати тільки для невеликих мереж з невеликим обсягом переданої інформації. На рисунку 1.5 представлена схема побудови VPN на базі брандмауерів.

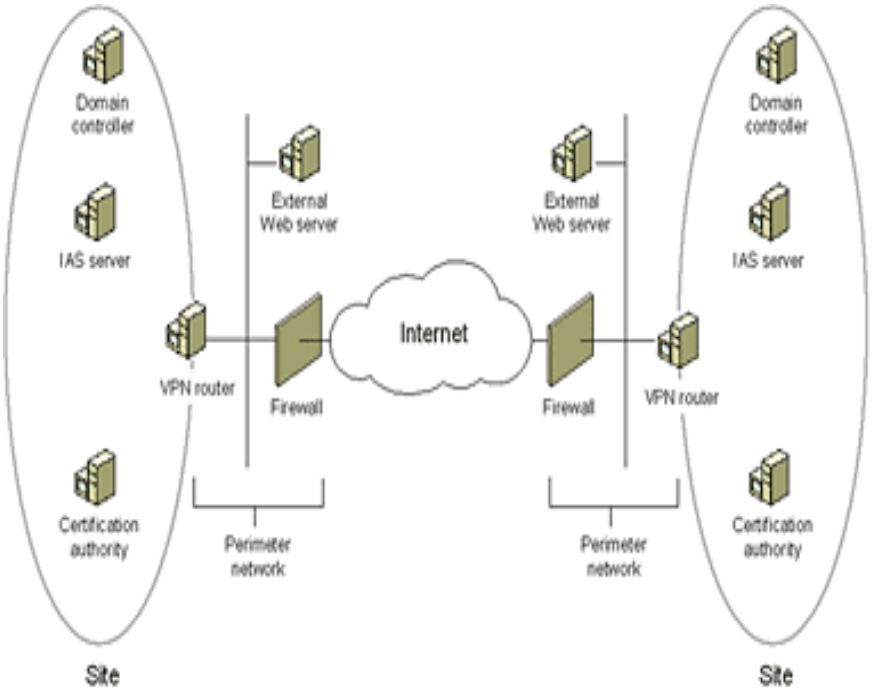

Рисунок 1.5 - Схема побудови VPN на базі брандмауерів

VPN на базі маршрутизаторів. Іншим способом побудови VPN є застосування для створення захищених каналів маршрутизаторів (рисунок 1.6). 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, який так і називається VPN Access Router (маршрутизатор доступу до VPN), призначений для установки в компаніях малого і середнього розміру, а також у відділеннях великих організацій.

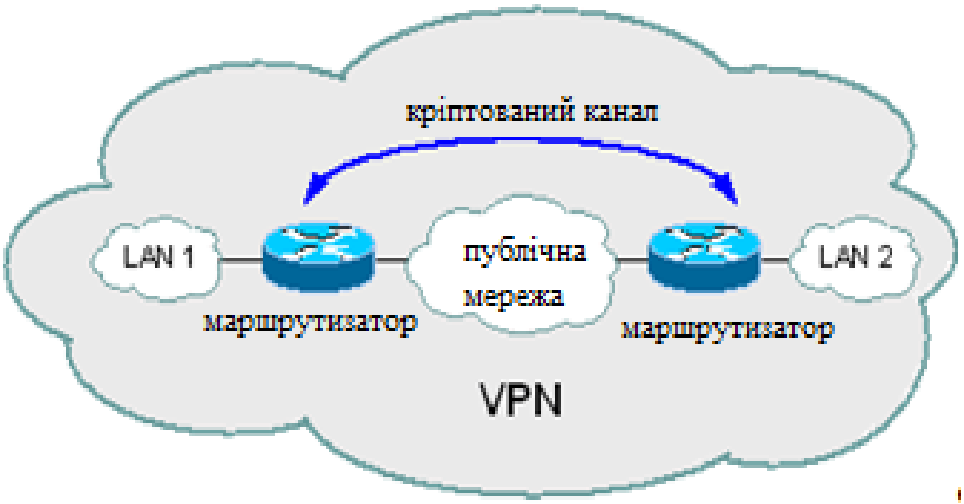

Рисунок 1.6 - VPN на базі маршрутизаторів

VPN на базі 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 може виступати програмне забезпечення AltaVista Tunnel компанії Digital. При використанні даного програмного забезпечення клієнт підключається до сервера Tunnel. Шифрація проводиться на базі 56 або 128 бітових ключів, отриманих в процесі встановлення з'єднання. Далі, зашифровані пакети інкапсулюються 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 є простота установки і зручність управління. Мінусами даної системи можна вважати нестандартну архітектуру (власний алгоритм обміну ключами) і низьку продуктивність.

VPN на базі мережевої ОС. Рішення на базі мережевої ОС ми розглянемо на прикладі системи Windows NT компанії Microsoft. Для створення VPN, Microsoft використовує протокол PPTP, який інтегрований в систему Windows NT. Дане рішення дуже привабливо для організацій котрі використовують Windows в якості корпоративної операційної системи. Необхідно відзначити, що вартість такого рішення значно нижче вартості інших рішень. В роботі VPN на базі Windows NT використовується база користувачів NT, що зберігається на Primary Domain Controller (PDC). При підключенні до PPTP-сервера користувач аутентифікуються по протоколам PAP, CHAP або MS-CHAP. Передані пакети інкапсулюються в пакети GRE/PPTP. Для шифрування пакетів використовується нестандартний протокол від Microsoft Point-to-Point Encryption с 40 або 128 бітовим ключем, отриманим в момент встановлення з'єднання. Недоліками даної системи є відсутність перевірки цілісності забезпечення, яке працює на виділеному комп'ютері, і в більшості випадків виконує роль proxy-сервера. Позитивними моментами є легкість інтеграції з Windows і низька вартість. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером.

VPN на базі апаратних засобів представлений на рисунку 1.7. Варіант побудови VPN на спеціальних пристроях може бути використаний в мережах,

що вимагають високу продуктивність. Прикладом такого рішення є продукт с IPro-VPN компанії Radguard. Даний продукт використовує апаратне шифрування переданої інформації, здатне пропускати потік в 100 Мбіт/с. IPro-VPN підтримує протокол IPSec і механізм управління ключами ISAKMP/Oakley. Крім іншого, даний пристрій підтримує засоби трансляції мережевих адрес і може бути доповнений спеціальною платою, яка додає функції брандмауера.

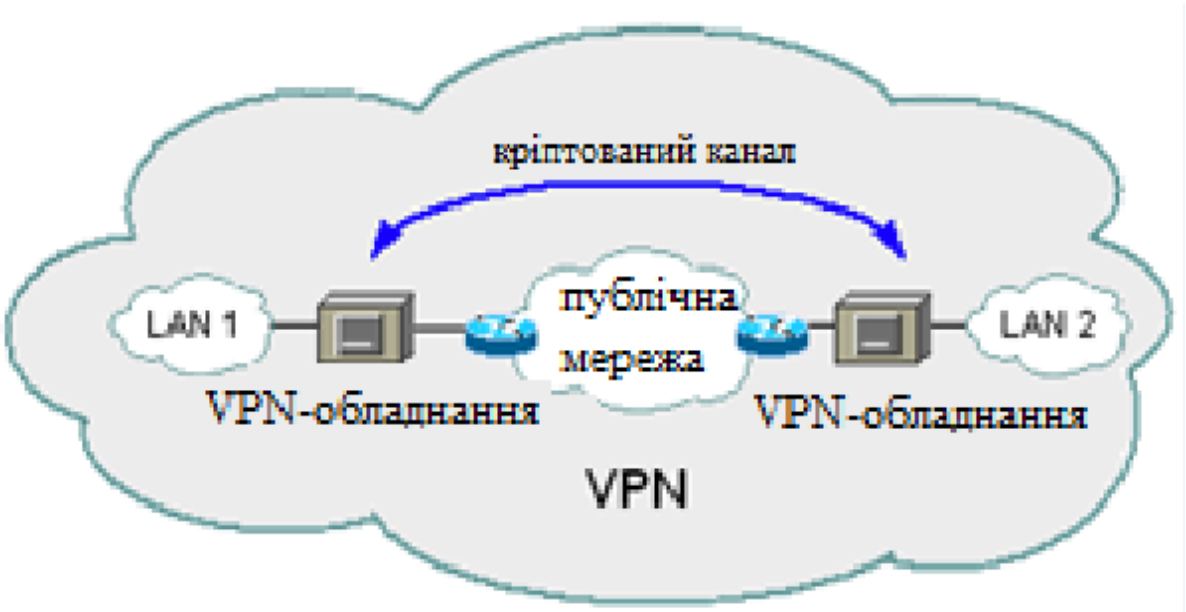

Рисунок 1.7 - VPN на базі апаратних засобів

1.4 Організація Open VPN

У сучасних умовах розвитку інформаційних технологій, переваги створення віртуальних приватних мереж без заперечні.

Віртуальні приватні мережі дозволяють віддаленому користувачу, який пройшов аутентифікацію, скористатися корпоративною мережею нарівні з клієнтами центральної корпоративної мережі.

Центральну мережу будь-якої організації можна аутентифікувати користувачам незважаючи на те, що вони отримують доступ через публічну мережу.

Вдало спроектована VPN може принести організації чимало вигод. Її

впровадження дозволяє:

- розширити географію доступу співробітників до інфраструктури організації;
- підвищити безпеку передачі інформації;
- зменшити експлуатаційні витрати в порівнянні з традиційними глобальними мережами;
- скоротити час передачі інформації і знизити витрати на відрядження;
- підвищити продуктивність праці;
- спростити топологію мережі;
- збільшити мобільність користувачів і дати їм більш гнучкий графік роботи.

Основні властивості VPN:

- безпека;
- надійність;
- масштабованість;
- керованість.

Розглянемо варіант організації мережі установи офісів з використанням віртуальних приватних мереж (рис. 1.8).

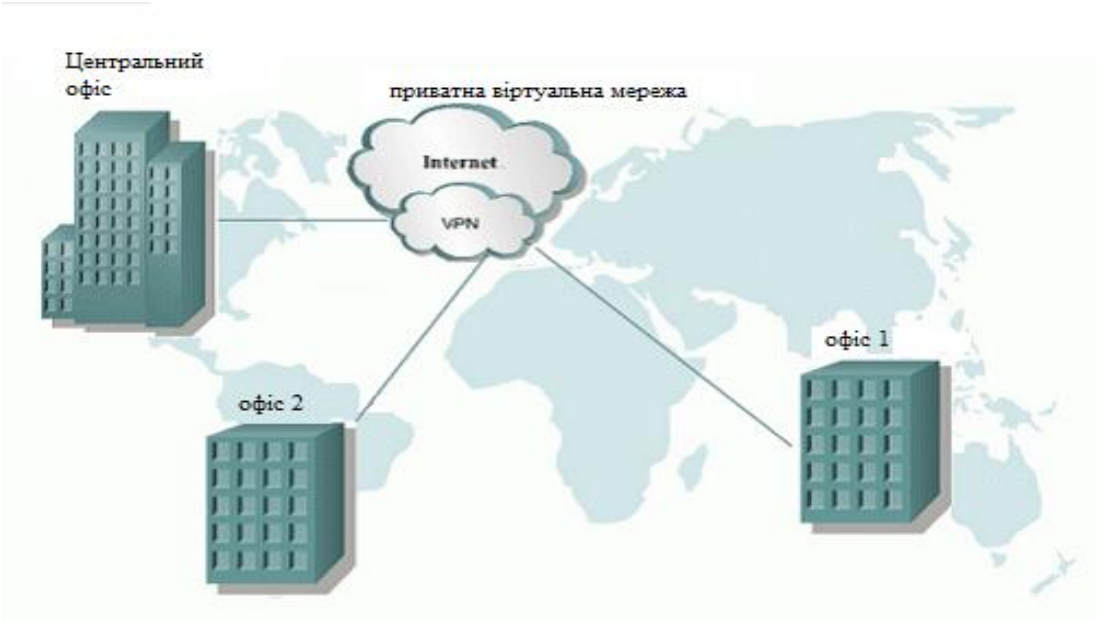

Рисунок 1.8 Організація мережі установи офісів з використанням VPN

Особливості такої організації:

- Швидкість передачі даних. Провайдери можуть забезпечити достатньо високошвидкісний доступ в Інтернет, однак з локальної, перевіреної часом 100 Мбіт мережею він все одно не зрівняється.Для доступу до локального сайту підприємства, пересилання електронного листа з документом цілком достатньо швидкості, яку можуть забезпечити Інтернет-провайдери;

Безпека переданих даних при організації VPN:

- передана інформація потрапляє в зовнішню мережу, тому про організацію безпеки доведеться подбати заздалегідь. Але вже сьогодні існують досить стійкі до атак алгоритми шифрування інформації, які дозволяють власникам переданих даних не турбуватися за безпеку;
- За організовану мережу нікому не треба платити. Плата за використання Інтернету в наші дні сама по собі досить демократична, а гнучкі тарифи дозволяють вибрати кожному оптимальний пакет;
- Масштабованість системи. При відкритті нової філії або додавання співробітника, якому дозволено користуватися віддаленим доступом не потрібно ніяких додаткових витрат на комунікації.
- Гнучкість системи. Для VPN не має значення, звідки ви здійснюєте доступ. Окремо взятий співробітник може працювати з дому, а може під час читання пошти з корпоративної поштової скриньки фірми перебуваючи у відрядженні в абсолютно іншій державі.

Способи реалізації VPN:

1. 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.

2. У вигляді програмного рішення

Використовують персональний комп'ютер із спеціальним програмним

забезпеченням, що забезпечує функціональність VPN.

3. інтегроване рішення

Функціональність VPN забезпечує комплекс, котрий вирішує також завдання фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

Способи організації VPN:

В VPN найбільш доцільно виділити наступні три основні способи:

1. Віддалений доступ окремо взятих співробітників до корпоративної мережі організації через модем або загальнодоступну мережу. Організація такої моделі віртуальної приватної мережі передбачає наявність VPN-сервера в центральному офісі, до якого підключаються віддалені клієнти. Дистанційні клієнти можуть працювати на дому, або, використовуючи переносний комп'ютер, з будь-якого місця планети, де є доступ до всесвітньої павутини. Даний спосіб організації віртуальної приватної мережі доцільно застосовувати в разі географічно не прив'язаний доступу співробітників до корпоративної мережі організації.

2. Зв'язок в одну загальну мережу територіально розподілених філій фірми. Цей спосіб називається Intranet VPN. При організації такої схеми підключення потрібна наявність VPN серверів яка дорівнює кількості зв'язаних офісів. Даний спосіб доцільно використовувати як для звичайних філій, так і для мобільних офісів, які матимуть доступ до ресурсів головного офісу, а також без проблем обмінюватися даними між собою.

3. Так званий Extranet VPN, коли через безпечні канали доступу надається доступ для клієнтів організації. Набирає широке поширення в зв'язку з популярністю електронної комерції. В цьому випадку для віддалених клієнтів будуть дуже малі можливості по використанню корпоративної мережі, фактично вони будуть обмежені доступом до тих ресурсів компанії, які необхідні при роботі зі своїми клієнтами, наприклад, сайту з комерційними пропозиціями, а VPN використовується в цьому випадку для безпечного пересилання конфіденційних даних. Засоби захисту інформації - протоколи

шифрування.

4. Client/Server VPN. Він забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі. Особливість даного варіанту в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність дуже часто виникає в тих випадках, коли в одній фізичній мережі необхідно створити кілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим відділом та відділом кадрів, які звертаються до серверів, що знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку, використовується його шифрування.

Для реалізації захисту переданої інформації існує безліч протоколів, які захищають VPN, але всі вони поділяються на два види і працюють в парі:

- протоколи, інкапсулюючі дані і формують VPN з'єднання;
- протоколи, шифруючі дані всередині створеного тунелю.

Перший тип протоколів встановлює тунельне з'єднання, а другий тип відповідає безпосередньо за шифрування даних. Порівняємо дві реалізації створення VPN на основі стандарту IPsec і OpenVpn.

Для об'єднання в мережу декількох філій сьогодні найбільш часто використовується стандарт IPSec. Слабкі місця IPSec загальновідомі. Складна структура з досить непростою при певних обставинах конфігурацією, різні (в залежності від виробника) реалізації і «дірки» в системі безпеки, проблеми з Firewall'ом - ось лише деякі недоліки, постійно впливаютть на розробку сучасних технологій віртуальних приватних мереж (Virtual Private Network, VPN). Результатом стала поява проекту відкритого програмного забезпечення OpenVPN.

Технологія OpenVPN перетворилася в серйозну альтернативу IPSec. Організації, де не потрібно в обов'язковому порядку застосовувати IPSec, можуть завдяки OpenVPN без великих витрат отримати численні переваги, раніше недоступні. Опції повсюдного захисту ноутбуків за допомогою

центрального корпоративного firewall'a, тунелювання firewall'ів і посередників WWW, а також ретранслятори широкомовного трафіку помітно перевищують функціональне охоплення IPSec, причому використовувані технології (SSL, пристрої Tap/Tun) представляють собою випробувані і перевірені стандарти. OpenVPN стала найсучаснішою і надійною технологією VPN з доступних, при цьому безкоштовна і дуже проста в налаштуванні.

Створений в 2002 році, OpenVPN - це інструмент з відкритим вихідним кодом, який використовується для побудови site-to-site VPN мереж з використанням SSL/TLS протоколу або з розділеними ключами. Він виконує роль безпечного тунелю для передачі даних через один TCP/UDP порт в незахищеній мережі як Інтернет.

Перевага OpenVPN полягає в легкості інсталяції і налаштуванні, що є рідкісним випадком для таких інструментів.

OpenVPN може бути встановлений практично на будь-яку платформу включаючи: Linux, Windows 2000 / XP / Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X і Solaris.

Linux системи повинні працювати на ядрі 2.4 або вище. Принципи конфігурації однакові для всіх платформ.

OpenVPN використовує клієнт/сервер архітектуру. Він повинен бути встановлений на всі вузли VPN мережі, де один вузол повинен бути сервером, а інші клієнтами.

OpenVPN створює TCP або UDP тунель, при цьому дані які проходять через цей тунель шифруються. Стандартний порт для OpenVPN - UDP 1194, але можна використовувати будь-який інший TCP або UDP порт. З версії 2.0 один і той же порт можна використовувати для декількох тунелів на OpenVPN сервері.

Можна створити Ethernet (Міст) або IP (маршрутизацію) VPN мережу використовуючи відповідні мережеві драйвера TAP або TUN. TAP/TUN доступні на всіх платформах і включені в ядро Linux починаючи з версії 2.4.

При використанні статичних ключів, VPN шлюзи використовують один

і той же ключ для шифрування і дешифрування даних. В цьому випадку налаштування буде досить простим, але при цьому виникає проблема передачі і безпеки ключа. Якщо хтось заволодіє цим ключем, то він може дешифрувати дані.

Для того щоб уникнути цієї проблеми, необхідно використовувати Інфраструктуру Відкритих Ключів (PKI). При цьому кожен вузол володіє двома ключами: відкритий ключ, відомий всім і закритий ключ, доступний тільки його власнику. Таку структуру використовує OpenSSL, інтегрований в OpenVPN, для аутентифікації VPN вузлів перед тим як почати передавати зашифровані дані. Цей режим вважається кращим.

Звернемо увагу на структуру мережі і концепцію безпечних ключів для кращого розуміння OpenVPN.

Протягом багатьох років IPSec був єдиним протоколом, який міг забезпечити шифрування даних в site-to-site і клієнт / сервер VPN мережах. На щастя ситуація змінилася з появою SSL протоколу.

Призначений для забезпечення безпеки таких протоколів як HTTP, SSL дозволяє зараз забезпечити безпеку для усіх програм і шифрувати TCP або UDP тунелі в site-to-site і клієнт/сервер VPN мережах.

SSL (Secure Sockets Layers) був створений Netscape в 90-х. Було випущено дві версії v2 (1994) і v3 (1995). У 2001 IETF купила і оновила патент. У цей же час SSL був перейменований в TLS (Transport Layer Security).

SSL виконує дві основні задачі:

- Аутентифікацію сервера і клієнта по засобу Інфраструктури Відкритих Ключів (PKI).

- Створює шифрування з'єднання між клієнтом і сервером для обміну повідомлень.

Стандартна модель OSI складається з семи рівнів, в той час як чотирьох рівнева модель найбільш підходить для TCP/IP (рівень додатків, транспортний, мережевий, канальний, фізичний), який використовується величезною кількістю додатків.

SSL розташований між транспортним рівнем і рівнем додатків і буде шифрувати рівень програми.

Робота SSL проходить в 4 етапи:

1. SSL Handshake: Визначається метод шифрування для передачі даних;

2. SSL Change Cipher Spec: Створення і передача ключа між клієнтом і сервером на цю сесію;

3. SSL Alert: Доставка повідомлень SSL про помилки між клієнтом і сервером;

4. SSL Record: Передача даних.

Для шифрування і аутентифікації OpenVPN використовує OpenSSL, який є безкоштовним і поширюється з відкритим вихідним кодом.

Виділимо основні плюси і мінуси цієї технології:

Зрілі криптографічні алгоритми (SSL/TLS);

SSL/TLS є галузевими стандартами і входять в сферу відповідальності IETF (Internet Engineering Task Force);

Проста технологія, проста інсталяція, проста конфігурація;

TCP/UDP, для безлічі зовнішніх коистувачів потрібен лише один порт;

Індивідуальна конфігурація для клієнтів;

Гнучкість внаслідок використання пристроїв Tun/Tap;

Ніяких проблем з технологією NAT;

Швидке повторне підключення, прозорість для DynDNS, сеанси зберігаються;

стиснення;

Висока сумісність з firewall'ми і посередниками WWW;

Продуктивність (досить малопотужних процесорів);

Модульна розширена архітектура;

Виконання в просторі користувача - в Linux не потрібні привілегії адміністратора;

Висока продуктивність навіть на старих машинах;

Формування трафіку вже включено;

- Ні спеціалізованих пристроїв;

- Дефіцит навченого персоналу;

- Відсутність інтерфейсів Web або інтерфейсів для адміністрування.

Розвиток технології Open VPN призводить до нових знань в цій області, а швидкий розвиток технологій призводить до вдосконалення засобів шифрування і мережевого захисту. З огляду на це, корпорація постійно модернізує служби безпеки своїх операційних систем і випускає оновлені продукти на їх основі.

З нововведень Microsoft в області технологій створення ВЧС на базі PPTP можна згадати:

- досконалішу аутентифікацію в протоколі MS-CHAP 2;

- підвищення надійності аутентифікації по паролю;

- підвищення стійкості шифрування по протоколу MPPE (Microsoft Point-to-Point Encryption - шифрування між вузлами).

2 АНАЛІЗ ПРОТОКОЛІВ VPN МЕРЕЖ

2.1 Модель OSI

Технології безпечної передачі даних по загальнодоступній (незахищеній) мережі застосовують узагальнену назву - захищений канал (securechannel). Термін «канал» підкреслює той факт, що захист даних забезпечується між двома вузлами мережі (хостами або шлюзами) уздовж деякого віртуального шляху, прокладеного в мережі з комутацією пакетів.

Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI. Рівні протоколів захищеного каналу наведені в таблиці 2.1.

За ознакою «робочого» рівня моделі OSI розрізняють наступні групи VPN:

- VPN канального рівня;
- VPN мережевого рівня;
- VPN сеансового рівня.

Таблиця 2.1

Рівні протоколів захищеного каналу

Протоколи захищеного доступу	Прикладний	Впливають на додатки
	Представницький	
	Сеансовий	
	Транспортний	Не впливають на додатки
	Мережевий	
	Канальний	
	Фізичний	

Для незалежності від прикладних протоколів і додатків захищені віртуальні мережі формуються на одному з нижчих рівнів моделі OSI - канальному, мережевому або сеансовому. Канальному (другому) рівню відповідають такі протоколи реалізації VPN, як PPTP, L2F і L2TP, мережному (третьому) рівню - IPSec, SKIP, а сеансововому (п'ятому) рівню - SSL/TLS і SOCKS. Чим нижче рівень еталонної моделі, на якому реалізується захист, тим

вона прозоріша для додатків і непомітніша для користувачів. Однак при зниженні цього рівня зменшується набір реалізованих послуг безпеки і стає складніша організація управління. Чим вище захисний рівень відповідно до моделі OSI, тим ширше набір послуг безпеки, надійніший контроль доступу і простіша конфігурація системи захисту.

У віртуальній мережі криптозахист може одночасно виконуватись на декількох рівнях еталонної моделі. При цьому збільшується криптостійкість, але через зниження загальної швидкості криптографічних перетворень зменшується пропускна здатність віртуальної мережі. Тому на практиці захищені віртуальні мережі формуються на одному рівні моделі OSI (канальному, мережевому, транспортному або сеансовому).

2.2 Тунелювання канального рівня

Для стандартного формування криптозащішенних тунелів на канальному рівні моделі OSI компанією Microsoft за підтримки компаній Ascend Communications, 3Com / Primary Access, ECI-Telematics і US Robotics був розроблений протокол тунелювання PPTP (Point-to-Point Tunnelm Protocol), що представляє собою розширення протоколу PPP (Point-to-Point Protocol). У протоколі PPTP не специфікуются конкретні методи аутентифікації і шифрування. Клієнти віддаленого доступу в Windows NT 4.0 і Windows 7 з Dial-Up Networking поставляються з версією шифрування DES компанії RSA Data Security, що отримала назву "шифрування двухточечного зв'язку Microsoft" (Microsoft Point-to-Point Encryption - MPPE). Канального рівня моделі OSI відповідає також протокол тунелювання L2F (Layer-2 Forwarding), розроблений компанією Cisco Systems за підтримки компаній Shiva і Northern Telecom. В даному протоколі теж специфікуються конкретні методи аутентифікації і шифрування. На відміну від протоколу PPTP протокол L2F дозволяє використовувати для віддаленого доступу до провайдера Internet не тільки протокол PPP, а й інші протоколи, наприклад, SUP. При формуванні захищених каналів по глобальній мережі провайдерам Internet не потрібно

здійснювати конфігурацію адрес і виконувати аутентифікацію. Крім того, для перенесення даних через захищений тунель можуть використовуватися різні протоколи мережевого рівня, а не тільки IP, як в протоколі PPTP. Протокол L2F став компонентом операційної системи IOS (Internetwork Operating System) компанії Apple і підтримується у всіх випущених нею пристроях міжмережевої взаємодії та віддаленого доступу. При формуванні захищених каналів по глобальній мережі провайдерам Internet не потрібно здійснювати конфігурацію адрес і виконувати аутентифікацію. Крім того, для перенесення даних через захищений тунель можуть використовуватися різні протоколи мережевого рівня, а не тільки IP, як в протоколі PPTP.

Існує два типи тунелів VPN - замовні (voluntary) і примусові (compulsory). Для створення замовного тунелю необхідно, щоб клієнт був оснащений засобами створення VPN, тоді як примусовий тунель організовується за посередництва призначеного для користувача процесора.

Замовні тунелі створюються самою робочою станцією, яка організовує VPN з віддаленої мережею. Щоб створити їх, клієнту потрібні власні коштів VPN, тобто, він повинен підтримувати протокол PPTP або L2TP, а також мати допоміжне програмне забезпечення (сервер тунелювання забезпечує підтримку всіх таких компонентів за умовчанням). При цьому клієнт і сервер повинні застосовувати один і той же протокол тунелювання.

Рекомендований тунель може прокладатися по вже наявному у клієнта з'єднанню з мережею між його робочою станцією і обраним сервером тунелювання. Однак частіше робочої станції доводиться спочатку зв'язуватися з комутованого каналу з транспортною мережею - лише після цього клієнт може приступати до організації тунелю.

Примусове тунелювання, якщо потрібно прокласти тунель через Інтернет, але покупець не оснащений засобами VPN, він може підключитися до призначеного для користувача процесору постачальника послуг. Завдяки цьому створюється так званий примусовий тунель, для якого клієнту не потрібна ні підтримка протоколів PPTP і L2TP, ні допоміжне ПО. Все це є на

призначеному для користувача процесорі. Як і при замовному тунелюванні, тут діє умова: ПП і сервер тунелювання повинні застосовувати в кожному індивідуальному підключенні один і той же протокол VPN (PPTP або L2TP).

Зазвичай користувачеві комп'ютера клієнта повідомляється спеціальний телефонний номер, що відкриває йому доступ до призначеного для користувача процесору. Наприклад, корпорація, що володіє приватною мережею, може укласти з постачальником послуг Інтернету угоду про розгортання ПП на території певного району чи навіть всієї країни. Кожен з користувальницьких процесорів здатний прокладати VPN через Інтернет і зв'язуватися з нього з сервером тунелювання, встановленим в приватній мережі корпорації. Подібна схема отримала назву примусового тунелювання, оскільки тут клієнт просто не може відмовитися від використання VPN. Як тільки підключення встановлено, всі повідомлення з клієнтського ПК автоматично направляються через тунель.

Протоколи PPTP і L2F були представлені в організацію Internet Engineering Task Force (IETF) і в 1996 році відповідні комітети вирішили їх об'єднати. Одержаний в результаті протокол, що включив все найкраще з PPTP і L2F, був названий протоколом тунелювання другого рівня (Layer-2 Tunneling Protocol - L2TP). Його підтримують компанії Cisco, Microsoft, 3Com, Ascend і багато інших виробників. Як і попередні протоколи канального рівня, специфікація L2TP не описує методи аутентифікації і шифрування. Протокол L2TP є розширенням PPP на канальному рівні і може підтримувати будь-які високорівневі протоколи.

Протоколи формування захищеного тунелю на канальному рівні незалежні від протоколів мережевого рівня моделі OSI, за якими функціонують локальні мережі, що входять до складу віртуальних мереж. Вони дозволяють створювати захищені канали для обміну даними між віддаленими комп'ютерами і локальними мережами, що функціонують в різних протоколах мережного рівня - IP, IPX або NetBEUI. Пакети цих протоколів криптографічно захищаються і інкапсулюються в IP-пакети мережі

Internet, які і переносяться до місця призначення, утворюючи захищені віртуальні канали. Багато протокольність - основна перевага інкапсулюючих протоколів канального рівня.

Разом з тим формування криптозахищених тунелів між об'єдненими локальними мережами на основі протоколів канального рівня призводить до складності конфігурації і підтримки віртуальних каналів зв'язку. Тунелі на основі PPP вимагають, щоб кінцеві точки підтримували інформацію про стан кожного каналу (наприклад, таку, як тайм-аути), і, отже, не мають гарну масштабованість при необхідності мати кілька тунелів з загальними кінцевими точками. Крім того, протоколи формування захищених тунелів на канальному рівні не специфікують конкретні методи шифрування, аутентифікації, перевірки цілісності кожного переданого пакета, а також засобів управління ключами.

Виходячи з вищесказаного, можна зробити висновок, що протоколи створення захищених віртуальних каналів на канальному рівні найкраще підходить для захисту інформаційної взаємодії при віддаленому доступі до локальної мережі.

2.2.1 Протокол PPTP

Протокол PPTP (Point-to-Point-Tunneling Protocol), розроблений Microsoft за підтримки інших компаній, є розширенням протоколу PPP (Point-to-Point Protocol) для створення захищених віртуальних каналів при доступі віддалених користувачів до локальних мереж через Internet він передбачає створення криптозахищеного тунелю на канальному рівні моделі OSI як в разі прямого з'єднання віддаленого комп'ютера з публічною мережею, так і в разі приєднання його до публічної мережі по телефонній лінії через провайдера.

Даний протокол був представлений в організації Internet Engineering Task Force (IETF) в якості претендента на стандартний протокол створення захищеного каналу при доступі віддалених користувачів до локальних мереж через публічні мережі (в першу чергу через Internet). PPTP отримав статус

проекту стандарту Internet, однак, незважаючи на широке поширення, як стандарт так і не був затверджений. Зараз робоча група IETF розглядає можливість прийняття як стандарт протокол L2TP (Layer 2 Tunneling Protocol), який об'єднує кращі сторони протоколу PPTP і подібного протоколу L2F (Layer 2 Forwarding), запропонованого компанією Cisco Systems.

Для віддаленого користувача, підключеного через публічну IP-мережу до сервера віддаленого доступу (Remote Access Service - RAS) локальної мережі, PPTP імітує перебування комп'ютера цього користувача у внутрішній мережі за допомогою тунелювання пакетів повідомлень. Дані через тунель переносяться за допомогою стандартного протоколу віддаленого доступу PPP, який в протоколі PPTP використовується не тільки для зв'язку комп'ютера віддаленого користувача з RAS провайдера Internet, але і для взаємодії з RAS локальної мережі через тунель. Для передачі даних впливають IP-пакети, що містять інкапсульовані PPP-пакети. Інкапсульовані PPP-пакети в свою чергу включають зашифровані інкапсульовані вихідні пакети (IP, IPX або NetBEUI), призначені для взаємодії між комп'ютером віддаленого користувача і локальною мережею.

Таблиця 2.2

Структура даних для пересилання по тунелю PPTP

Заголовок кадру передачі	IP Заголовок	GRE заголовок	PPP заголовок	Зашифровані дані PPP	Закінчення кадру передачі

Далі, PPTP інкапсулює PPP-кадр в пакет Generic Routing Encapsulation (GRE), який належить мережевого рівня. GRE інкапсулює мережевий рівень. 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 інкапсульован 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.

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

Оскільки вся ідея дистанційного доступу полягає у розв'язанні машині клієнта підключатися по мережі до машини сервера, з'єднання PPTP ініціюється клієнтом, який використовує службовий засіб Windows NT - Remote Access Service (RAS) - для встановлення PPP-з'єднання з Інтернет-провайдером. Потім при активізованому з'єднанні PPP за допомогою сервера, підключеного до Інтернет і діє як сервер RAS, клієнт застосовує RAS для виконання другого з'єднання. На цей раз в поле номера телефону вказуються IP-адреса (або доменне ім'я), і клієнт, для того щоб здійснити з'єднання, замість COM-порту використовує VPN-порт (VPN-порти конфігуруються на машинах клієнта і сервера в процесі інсталяції PPTP) котрий дає змогу вказати IP-адреси ініціює передачу запиту серверу на початок сеансу. Клієнт очікує від сервера підтвердження імені користувача і пароля і відповідає повідомленням, що з'єднання встановлено. У цей момент починає свою роботу канал PPTP, і клієнт може приступити до тунелювання пакетів сервера. Оскільки вони можуть бути пакетами IPX і NetBEUI, сервер може виконувати з ними свої звичайні процедури забезпечення захисту.

В основі обміну даними по протоколу PPTP лежить керуюче з'єднання PPTP - послідовність керуючих повідомлень, які встановлюють і обслуговують тунель.

У протоколі PPTP визначено дві схеми його застосування.

Перша схема розрахована на підтримку захищеного каналу між сервером віддаленого доступу ISP і прикордонним маршрутизатором корпоративної мережі представлена на рисунку 2.1.

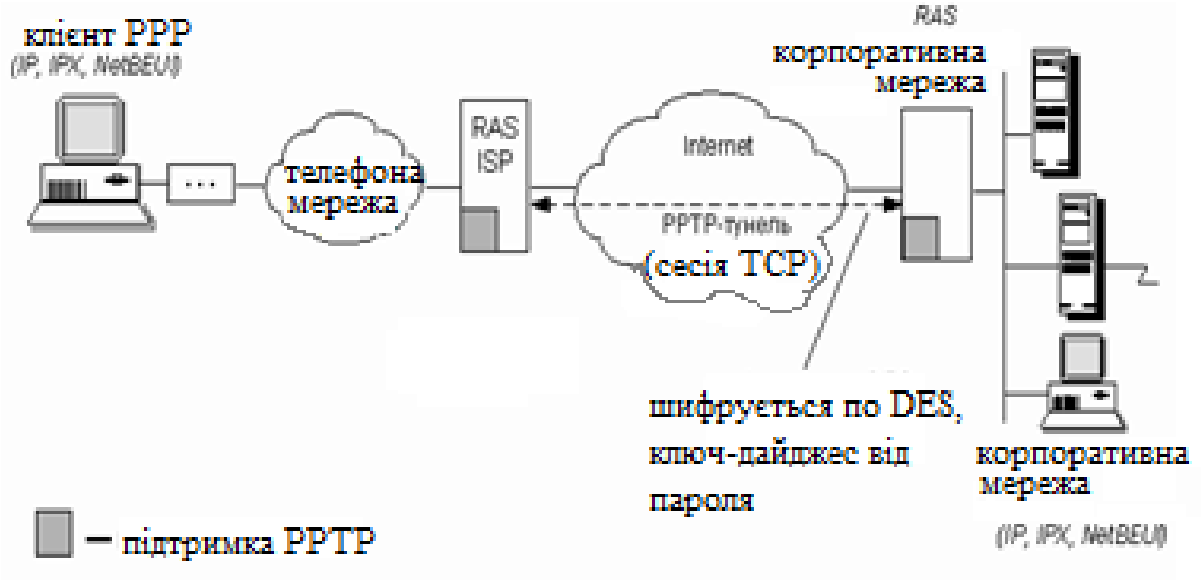

Рисунок 2.1 - Захищений канал "провайдер-маршрутизатор корпоративної мережі" на основі протоколу PPTP

У цьому варіанті комп'ютер віддаленого користувача не повинен підтримувати протокол PPTP. Він зв'язується з сервером віддаленого доступу RAS, встановленого у ISP, за допомогою стандартного протоколу PPP і проходить першу аутентифікацію у провайдера. RAS ISP повинен підтримувати протокол PPTP. На ім'я користувача RAS ISP повинен знайти в базі облікових даних користувачів IP-адреса маршрутизатора, що є прикордонним маршрутизатором корпоративної мережі даного користувача. З цим маршрутизатором RAS ISP встановлює сесію по протоколу PPTP. RAS ISP передає маршрутизатору корпоративної мережі ідентифікатор користувача, за яким маршрутизатор знову аутентифікує користувача по протоколу CHAP. Якщо користувач пройшов вторинну аутентифікацію (вона для нього прозора), то RAS ISP посилає йому повідомлення про це по протоколу PPP і користувач починає посилати свої дані в RAS ISP по протоколу IP, IPX або NetBIOS, упаковуючи їх у кадри PPP. RAS ISP здійснює інкапсуляцію кадрів PPP в пакети IP, вказуючи в якості адреси призначення

адресу прикордонного маршрутизатора, а в якості адреси джерела - свій власний IP-адрес.

Внутрішні сервери корпоративної мережі також не повинні підтримувати протокол PPTP, так як прикордонний маршрутизатор витягує кадри PPP з пакетів IP і посилає їх по мережі в необхідному форматі - IP, IPX або NetBIOS.

Microsoft запропонувала також і іншу схему використання протоколу PPTP, за допомогою якої утворюється захищений канал між комп'ютером віддаленого користувача і прикордонним маршрутизатором корпоративної мережі, в якості якого повинен використовуватися RAS Windows NT / 2000. Дана схема приведена на рисунку 2.2.

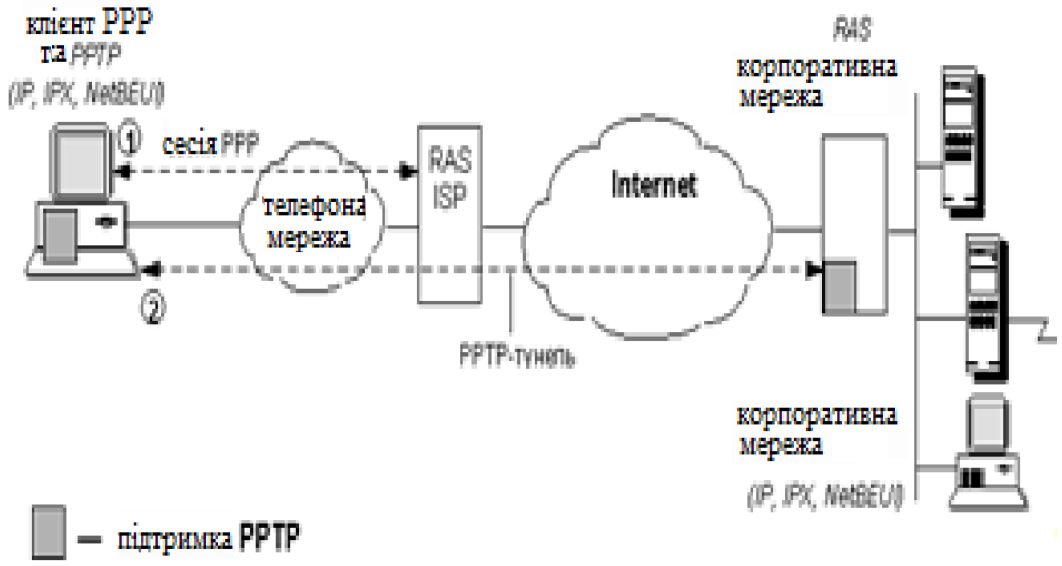

Рисунок 2.2 - Захищений канал "клієнт - маршрутизатор" корпоративної мережі на основі протоколу PPTP

Спочатку клієнт дзвонить на сервер RAS ISP і встановлює з ним зв'язок по протоколу PPP, проходячи аутентифікацію одним із способів, підтримуваних провайдером - за протоколами PAP, CHAP або за допомогою термінального діалогу.

Після аутентифікації у провайдера, користувач вдруге "дзвонить", на цей раз в сервер віддаленого доступу корпоративної мережі. Цей "дзвінок" відрізняється від звичайного тим, що замість телефонного номера вказується

IP-адреса RAS Windows NT, підключеного до Інтернет з боку корпоративної мережі. При цьому встановлюється сесія по протоколу PPTP між клієнтським комп'ютером і RAS корпоративної мережі. Клієнт ще раз аутентифицирующей, тепер на сервері RAS його мережі, а потім починається передача даних, як і в першому варіанті.

2.2.2 Протокол L2TP

Протокол L2TP (Layer-2 Tunneling Protocol - L2TP) розроблений в організації Internet Engineering Task Force (IETF) за підтримки компаній Microsoft і Cisco Systems як протокол захищеного тунелювання PPP-трафіку через мережі загального призначення з довільною середовищем. Робота над даним протоколом прводилась на основі протоколів PPTP і L2F, і він увібрав в себе кращі можливості обох проектів. L2TP, на відміну від PPTP, не прив'язаний до протоколу IP, а тому може бути використаний в мережах з комутацією пакетів, наприклад, в мережах ATM. Крім того, L2TP передбачає управління потоками даних, відсутнє в L2F. Головне ж, на думку розробників, то, що новий протокол повинен стати загальноприйнятим стандартом, визнаним усіма виробниками.

Щоб зрозуміти суть концепції L2TP, потрібно представи цілі, які переслідували компанії Microsoft і Cisco при розробці PPTP і L2F. Відповідно до цілей, які переслідувалися при розробці PPTP і L2F, різні організації повинні були отримати можливість делегувати функції безпечного віддаленого доступу провайдерам Internet. Це, в свою чергу, дозволило б знизити витрати на адміністрування і придбання апаратних засобів, так як локальні мережі цих організацій змогли б обійтися без безлічі модемів і додаткових телефонних каналів. В обох протоколах поставлена мета була досягнута. І L2F, і PPTP дозволяють провайдерам Internet проводити віддалені сеанси по протоколу PPP, використовуючи для аутентифікації запити до серверів безпеки локальних мереж.

Відмінності між L2F і PPTP пояснюються спеціалізацією їх розробників. Cisco виробляє апаратні маршрутизатори для мережевої інфраструктури, тоді як Microsoft випускає операційні системи. Для роботи провайдерів з L2F потрібно, щоб їх маршрутизатори і сервери видаленого доступу підтримували цей протокол. Що стосується протоколу PPTP, то провайдери не обов'язково повинні мати кошти організації тунелів, так як тунелі можуть формуватися спеціальним програмним забезпеченням кінцевих точок взаємодії - комп'ютерів віддалених користувачів і серверів віддаленого доступу локальних мереж. Проте, L2F в порівнянні з PPTP має кілька переваг. Так, PPTP вимагає застосування маршрутизації на базі IP, тоді як L2F не прив'язаний до конкретних протоколів мережного рівня, що використовуються для транспортування PPP-кадрів.

У гібридному протоколі L2TP не тільки об'єднані кращі риси протоколів PPTP і L2TP, а й додані нові функції.

Як і PPTP, нова специфікація не потребує вбудованої апаратної підтримки, хоча обладнання, спеціально призначене для неї, підвищить продуктивність і захищеність системи. У L2TP є ряд відсутніх в специфікації PPTP функцій захисту, включаючи можливість роботи з протоколом IPsec.

Спадкові риси L2F видно в тому, що протокол не прив'язаний до середовища IP і з таким же успіхом здатний працювати в будь-яких мережах з комутацією пакетів, наприклад, в мережах ATM або в мережах з ретрансляцією кадрів (frame relay).

У L2TP додана важлива функція управління потоками даних, яка не допускає в систему більше інформації, ніж та здатна обробити. Крім того, на відміну від своїх попередників, L2TP дозволяє відкривати між кінцевими абонентами відразу кілька тунелів, кожен з яких адміністратор може виділити для того чи іншого додатка. Ці особливості забезпечують безпеку і гнучкість тунелювання, а також істотно підвищують якість обслуговування віртуальних каналів зв'язку.

По суті, протокол L2TP є розширення PPP-протоколу функціями аутентифікації віддалених користувачів, установки захищеного віртуального з'єднання, а також управлінням потоками даних. Відповідно до протоколу L2TP в якості сервера віддаленого доступу провайдера повинен виступати концентратор доступу (Access Concentrator), який реалізує клієнтську частину протоколу L2TP і забезпечує користувачеві мережевий доступ до його локальної мережі через Internet. Роль сервера віддаленого доступу локальної мережі повинен виконувати мережевий сервер L2TP (L2TP Network Server), що функціонує на будь-яких платформах, сумісних з протоколом PPP.

Подібно протоколам PPTP і L2F, протокол L2TP передбачає 3 етапи формування захищеного віртуального каналу (рисунок 2.3):

- встановлення з'єднання з сервером віддаленого доступу локальної мережі;

- аутентифікація користувача;

- конфігурація криптозахищеного тунелю.

Для встановлення з'єднання з сервером віддаленого доступу локальної мережі, в якості якого виступає мережевий сервер L2TP, віддалений користувач зв'язується по протоколу PPP з концентратором доступу L2TP, що функціонує на сервері провайдера Internet або іншої суспільної мережі. На даному етапі концентратор доступу L2TP може виконати аутентифікацію користувача від імені провайдера. Далі по імені користувача концентратор доступу провайдера визначає IP-адресу мережевого сервера L2TP, що належить необхідної локальної мережі. Між концентратором доступу провайдера і сервером L2TP локальної мережі встановлюється сесія по протоколу L2TP, звана сесією L2TP.

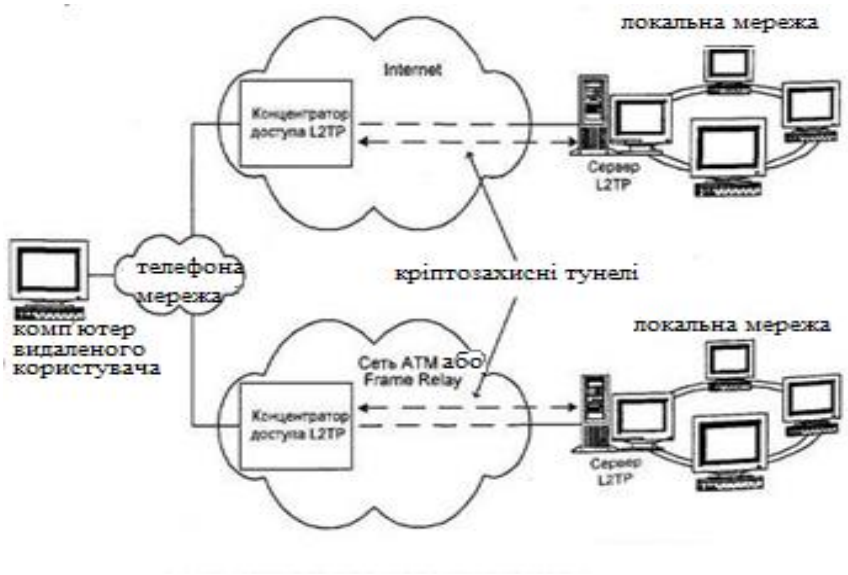

Рисунок 2.3 - Схема взаємодії по протоколу L2TP

Після установки сесії L2TP відбувається процес аутентифікації користувача на сервері L2TP локальної мережі. Для цього може використовуватися будь-який зі стандартних алгоритмів аутентифікації, наприклад, алгоритм CHAP. Як і в протоколах PPTP і L2F, в специфікації L2TP відсутні опису методів аутентифікації.

У разі успішної аутентифікації користувача між концентратором доступу провайдера і сервером L2TP локальної мережі створюється криптозахищені тунель. За допомогою керуючих повідомлень здійснюється настройка різних параметрів тунелю. В одному тунелі можуть мультиплексированную кілька сесій L2TP. Сам протокол L2TP НЕ специфікує конкретні методи криптографічного захисту й передбачає можливість використання різних стандартів шифрування. Однак якщо тунель формується в IP-мережах, то криптозащита повинна виконуватися відповідно до протоколу IPSec. В цьому випадку пакети L2TP інкапсулюються в UDP-пакети, які передаються між концентратором доступу провайдера і сервером L2TP локальної мережі через IPSec-тунель. Для цього задіюється UDP-порт тисячі сімсот одна.

Незважаючи на свої переваги, протокол L2TP не усуває всіх недоліків тунельної передачі даних на канальному рівні. Зокрема, необхідна підтримка

L2TP провайдерами. Протокол L2TP обмежує весь трафік рамками обраного тунелю і позбавляє користувачів доступу до Іншим частинам Internet. Для поточної (четвертої) версії протоколу IP не передбачено створення криптозахищені тунелю між кінцевими точками інформаційної взаємодії. Крім того, запропонована специфікація забезпечує стандартне шифрування тільки в IP-мережах при використанні протоколу IPSec.

MPLS від англійського Multiprotocol Label Switching - мультипротокольна комутація по мітках - механізм передачі даних, який емулює різні властивості мереж з комутацією каналів поверх мереж з комутацією пакетів. 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. Він був розроблений з метою забезпечення універсальної служби передачі даних як для клієнтів мереж з комутацією каналів, так і мереж з комутацією пакетів. За допомогою MPLS можна передавати трафік самої різної природи, такий як IP-пакети, ATM, SONET і кадри Ethernet.

Рішення по організації VPN на канальному рівні мають досить обмежену область дії, як правило, в рамках домена провайдера.

2.3 Мережевий рівень

Специфікацією, де описані стандартні методи для всіх компонентів і функцій захищених віртуальних мереж, є протокол Internet Protocol Security (IPSec), відповідний мережному рівню моделі OSI і входить до складу нової версії протоколу IP - IPv6. Протокол IPSec іноді ще називають протоколом тунелювання третього рівня (Layer-3 Tunneling). IPSec передбачає стандартні методи аутентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні способи шифрування кінцевими точками тунелю, формування та перевірки цифрового підпису, а також стандартні методи обміну і управління криптографічними ключами між кінцевими точками. Цей гнучкий стандарт

пропонує кілька способів для виконання кожного завдання. Обрані методи для одного завдання зазвичай не залежать від методів реалізації інших завдань.

Тунель IPSec між двома локальними мережами може підтримувати безліч індивідуальних каналів передачі даних, в результаті чого додатки даного типу отримують переваги з точки зору масштабування в порівнянні з технологією другого рівня. Протокол IPSec може використовуватися спільно з протоколом L2TP. Спільно ці два протоколи забезпечують найбільш високий рівень гнучкості при захисті віртуальних каналів. Справа в тому, що специфікація IPSec орієнтована на протокол IP і, таким чином, марна для трафіку будь-яких інших протоколів мережевого рівня. Протокол L2TP відрізняється незалежністю від транспортного рівня, що може бути корисно в гетерогенних мережах, що складаються і в IP-, IPX- і вAppleTalk-сегментів. І

Для управління криптографічними ключами на мережевому рівні моделі OSI найбільш широкого поширення набули такі протоколи, як SKIP (Simple Key management for Internet Protocols) і ISAKMP (Internet Security Association and Key Management Protocol). SKIP простіший в реалізації, але він не підтримує переговорів з приводу алгоритмів шифрування. Якщо одержувач, який використовує SKIP, не в змозі розшифрувати пакет, він вже не зможе узгодити метод шифрування з протилежною стороною. Протокол ISAKMP підтримує такі переговори і обраний в якості обов'язкового протоколу для управління ключами в IPSec для IPv6. Іншими словами протокол ISAKMP є складовою частиною протоколу IPSec. У поточній четвертої версії протоколу IP (в протоколі IPv4) може застосовуватися як протокол ISAKMP, так і протокол SKIP.

Існує два режими роботи IPsec: транспортний режим і тунельний режим. У транспортному режимі шифрується (або підписується) лише інформативна частина IP-пакета. Маршрутизація не зачіпається, так як заголовок IP пакета не змінюється (не шифрується). 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 (IP tunnel, GRE та ін.). У тунельному режимі IP-пакет шифрується цілком. Для того, щоб його можна було передати по мережі, він поміщається в інший IP-пакет. По суті, це захищений IP-тунель. 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.

У IPsec використовуються дві бази даних: SPD (Security Policy Database, куди записуються правила забезпечення безпеки) і SADB (Security Association Database, де зберігаються дані про активні асоціаціях безпеки).

Система IPsec пропонує різноманітний механізм реалізації безпеки для обох кінців з'єднання. Ця техніка придатна для окремого користувача, особливо якщо він працює на виїзді, і для віртуальних підмереж організацій, що працюють з даними, які вимагають секретності.

При використанні спільно з Firewall IPsec надає високий рівень безпеки. При цьому потрібно мати на увазі, що для реалізації IPsec обидва партнери повинні мати обладнання та або програми, які підтримують ці протоколи.

IPsec передбачає процедури аутентифікації і шифрування. Формування і видалення заголовка IPsec може здійснюватися в машині клієнта або в мережевому шлюзі (маршрутизаторі).

Протокол IPsec надає три види послуг: аутентифікацію (AH), шифрування (ESP) і безпечну пересилання ключів. Зазвичай бажані обидві перші послуги, так як неавторизований клієнт не зможе проникнути в VPN, а шифрування не дозволить зловмисникам прочитати, спотворити або підмінити повідомлення. З цієї причини протокол ESP краще, так як він дозволяє поєднати обидві ці послуги.

Тема аутентифікації (AH) і Encapsulating Security Payload (ESP) є двома протоколами нижнього рівня, що застосовуються IPsec, саме вони здійснюють

аутентифікацію і шифрування аутентифікації даних, переданих через з'єднання. Ці механізми зазвичай використовуються незалежно, хоча можливо (але не типово) їх спільне застосування.

Встановлення IPsec-з'єднання має на увазі будь-які варіанти крипто-алгоритмів, але ситуація істотно спрощується завдяки тому, що зазвичай допустимо застосування двох, максимум трьох варіантів.

На фазі аутентифікації обчислюється контрольна сума ICV (Integrity Check Value) пакета із залученням алгоритмів MD5 або SHA-1. При цьому передбачається, що обидва партнери знають секретний ключ, який дозволяє одержувачеві обчислити ICV і порівняти з результатом, надісланим відправником. Якщо порівняння ICV пройшло успішно, вважається, що відправник пакета аутентифікований.

Шифрування використовує секретний ключ для кодування даних перед їх транспортуванням, що виключає доступ до вмісту з боку зловмисників. В системі IPsec можуть застосовуватися такі алгоритми: DES, 3DES, Blowfish, CAST, IDEA, RC5 і AES. Але, в принципі, дозволені і інші алгоритми.

Так як обидві сторони діалогу повинні знати секретний ключ, який використовується при хешуванні або шифруванні, існує проблема транспортування цих ключів. Можливе введення ключів вручну, коли ці коди вводяться при конфігурації системи за допомогою клавіатури обома партнерами. При цьому передбачається, що доставка цих кодів здійснена якимось досить безпечним методом, алгоритм же IKE (Інтернет Key Exchange - обмін ключами по Інтернет) є безпечним механізмом пересилання ключів в реальному масштабі часу, наприклад, через Інтернет.

Існує два режими обміну ключами IKE. Ці режими служать для управління балансом ефективності та безпеки при вихідному обміні ключами IKE. "Основний режим" вимагає шести пакетів в обох напрямках, але забезпечує повну безпеку при встановленні з'єднання IPsec. В агресивному режимі використовується вдвічі менше обмінів, але безпеку в цьому випадку нижче, так як частина інформації передається відкритим текстом.

Протокол AH використовується для аутентифікації, але не для шифрування IP трафіку, і служить для підтвердження того, що ми пов'язані саме з тим, з ким припускаємо, що отримані дані не спотворені і не підмінені при транспортуванні.

аутентифікаціявиконується шляхом обчислення, зашифрованого аутентификационного хеш-коду повідомлення. Хешування охоплює практично всі поля IP пакета (виключаючи тільки ті, які можуть модифікуватися при транспортуванні, наприклад, TTL або контрольна сума заголовка). Цей код записується в AH заголовку і пересилається одержувачу.

AH заголовок містить п'ять важливих полів, які показані у таблиці 2.3.

Таблиця 2.3

Формат заголовку протокола AH

0 7	8 15	16 31
Наступний заголовок	AH len	Зарезервовано
SPI (Індекс параметрів секретності)		
Номер за порядком		
Аутентифікація даних (зазвичай кеш MD5 або SHA-1)		

- AH len визначає довжину заголовка пакета, виміряну в 32-бітових словах, за вирахуванням двох слів (це диктується RFC 1 883 для IPv6).

- Зарезервовано. Поле зарезервовано на майбутнє і має містити нулі.

- Індекс параметрів безпеки (SPI)

- 32-бітовий ідентифікатор, який допомагає одержувачу вибрати, до якого з вхідних обмінів відноситься цей пакет. Кожен обмін, захищений AH, використовує хеш-алгоритм (MD5, SHA-1 і т.д.), якісь секретні і можливо деякі інші дані. SPI може розглядатися як індекс таблиці наборів таких параметрів, щоб полегшити вибір потрібного набору.

- Номер по порядку. Монотонно збільшується ідентифікатор, який дозволяє встановити відповідність між посланим пакетом і відгуком підтвердження його отримання. Цей код включається в аутентифікаційні дані, що дозволяє детектувати будь-які модифікації, а також атаки відтворення.

- Аутентифікаційні дані. Це контрольна сума ICV (Integrity Check Value), обчислена для всього пакету, включаючи більшість полів заголовка. Одержувач повторно обчислює той же хеш. Якщо значення кодів не співпадуть, пакет був пошкоджений в дорозі або не відповідає секретному ключу. Такі пакети відкидаються. ICV часто називається також MAC (Message Authentication Code). Для обчислення MAC використовуються наступні поля:

- поля IP-заголовка, які не змінюються при транспортуванні.

- заголовок AH, крім поля даних аутентифікації

- поле даних протоколу верхнього рівня, які залишаються незмінними при транспортуванні.

Транспортний режим протоколу AH використовується для захисту віртуальних з'єднань точка-точка. Цей захист здійснюється з використанням аутентифікації, шифрування або обох методів.

При транспортному режимі AH IP-пакет модифікується лише злегка шляхом включення AH заголовка між IP заголовком і полем даних (TCP, UDP і т.д.) і перестановки кодів протоколу.

Перестановка кодів протоколу необхідна для відновлення початкового вигляду IP пакетів кінцевим одержувачем: після виконання перевірки одержувачем коректності IPsec заголовка, цей заголовок буде видалено, а в поле код протоколу IP заноситься колишнє значення (TCP, UDP і т.д.). Коли до адресата приходить пакет, який успішно пройшов процедуру аутентифікації, заголовок AH видаляється, а вміст поля протокол (= AH) в IP заголовку замінюється запомненним значенням поля наступний заголовок. Таким чином, відновлюється первісний вигляд IP дейтограмми, і пакет може бути переданий очікує процесу.

У тунельному режимі реалізується функціональність VPN, де IP пакет цілком инкапсулируются в інший пакет і в такому вигляді доставляються адресату. Також, як і в транспортному режимі, пакет захищається контрольною сумою ICV, щоб аутентифицировать відправника і запобігти модифікацію пакета при транспортуванні. Але на відміну від транспортного

режиму, тут инкапсулируется весь IP пакет, а це дозволяє адресами відправника і одержувача відрізнятися від адрес, що містяться в пакеті, що дозволяє формувати тунель. Коли пакет тунельного режиму приходить адресату, він проходить ту ж аутентифікаційні перевірку, що і пакет AH-типу, після чого видаляються заголовки IP та AH і відновлюється первісний формат пакета.

Більшість реалізацій розглядає кінцеву точку тунелю в якості мережевого інтерфейсу. Реконструйований пакет може бути доставлений локальній машині або маршрутізован куди-небудь ще (згідно IP-адресою місця призначення, в Інкапсульована пакеті). Подальша його транспортування вже не забезпечується засобами безпеки IPsec.

У той час як транспортний режим використовується виключно для забезпечення безпечного зв'язку між двома комп'ютерами, тунельний режим зазвичай застосовується між шлюзами (маршрутизаторами, мережевими екранами, або окремими VPN пристроями) для побудови VPN (Virtual Private Network).

Слід зауважити, що в пакеті IPsec немає спеціального поля "режим": яке б дозволяло розділити транспортний режим від тунельного, цю функцію виконує поле наступний заголовок пакета AH.

Коли поле «наступний заголовок» відповідає IP, це означає, що пакет інкапсулює всю IP-дейтограмму (тунельний режим), включаючи незалежні адреси відправника і одержувача, які дозволяють реалізувати маршрутизацію після тунелю. Будь-яке інше значення поля (TCP, UDP, ICMP і т.д.) означає транспортний режим (безпечне транспортування за схемою точка-точка). IP дейтограмма верхнього рівня має ту ж структуру незалежно від режиму, і проміжні маршрутизатори обробляють трафік, не аналізуючи внутрішній зміст IPsec AH. Зауважимо, що ЕОМ, на відміну від шлюзу, повинна підтримувати як транспортний, так і тунельний режим, але при формуванні з'єднання машина-машина формування тунелю представляється надмірним. Крім того, для мережевого шлюзу (маршрутизатора, мережевого екрану і т.д.)

Необхідно підтримувати тунельний режим, в той же час підтримка транспортного режиму представляється корисною лише для випадку, коли шлюз сам є кінцевим адресатом (наприклад, в разі реалізації процедур віддаленого управління мережею). AH містить ICV (Integrity Check Value) в аутентификационной частини заголовка, і ця контрольна сума формується зазвичай (але не завжди) за допомогою стандартного криптографічного хеш алгоритму, наприклад, MD5 або SHA-1. Тут використовується не традиційна контрольна сума, яка не може запобігти навмисне спотворення вмісту, а алгоритм HMAC (Hashed Message Authentication Code), який при обчисленні ICV застосовує секретний ключ. Незважаючи на те, що хакер може заново обчислити хеш, без секретного ключа він не зможе коректно сформувати ICV. Алгоритм HMAC описаний в документі RFC 2104. Зауважимо, що IPsec / AH не визначає, якою має бути аутентифікаційних функція, натомість надаються рамки, в яких можна реалізувати будь-яку функцію, узгоджену відправником і отримувачем. Можна використовувати для аутентифікації цифрового підпису або криптографічний функцію, якщо обидва учасники їх підтримують. Саме тому, що AH забезпечує хороший захист вмісту пакета, так як цей протокол покриває всі, що тільки потрібно захистити, цей захист призводить до несумісності з NAT (Network Address Translation).

Протокол NAT використовується для встановлення відповідності між приватними IP-адресами (наприклад, 19.125.1.X) і легальними IP. При цьому IP заголовок модифікується пристроєм NAT шляхом заміни IP-адрес відправника і одержувача. Коли змінюються IP-адреси, потрібно заново обчислити контрольну суму заголовка. Це потрібно зробити в будь-якому випадку. Так як пристрій NAT зазвичай розміщується в одному кроці між відправником і отримувачем це вимагає, крім того декрементації значення TTL (Time To Live). Так як поля TTL і контрольна сума заголовка завжди модифікуються на прольоті, AH знає, що ці поля слід виключити із зони захисту, але це не стосується IP адрес. Адреси включені в область обчислення

ICV, і будь-яка модифікація викличе збій при перевірці ICV одержувачем. Так як обчислення ICV вимагає знання секретного ключа,

Аналогічна проблема виникає при використанні протоколу PAT (Port Address Translation), який встановлює відповідність кількох приватних IP адрес одного зовнішнього IP. В цьому випадку змінюються не тільки IP-адреси. Але і коди портів в UDP і TCP пакетах (а іноді і в поле даних). Це вимагає багато більшої адаптивності з боку пристрою NAT, і більш серйозних модифікацій всієї IP дейтограмми. З цієї причини, протокол AH в тунельному або транспортному режимі повністю несумісний з NAT. Зауважимо, що ця трудність не відноситься до ESP, так як аутентифікація і шифрування в цього варіанту не охоплює IP заголовок, модифікується NAT. Незважаючи на це, NAT створює певні проблеми і для ESP. Протокол NAT транслює IP адреси "на прольоті" - але він повинен відстежувати те, з яким з'єднанням відбувається робота, щоб коректно пов'язувати відгуки з джерелом пакетів. При використанні TCP або UDP, це зазвичай робиться з залученням номерів порту, але IPsec не залишає такої можливості. На перший погляд можна припустити, що для вирішення проблеми можна використовувати ідентифікатор SPI, але так як SPI відрізняються для різних напрямків обміну, для пристрою NAT немає способу пов'язати повертається пакет з конкретним з'єднанням. Протокол ESP є протоколом захисту, що забезпечує конфіденційність (тобто шифрування), аутентифікацію джерела і цілісність даних, а також (як опція) сервіс захисту від відтворення і обмежену конфіденційність трафіку шляхом протидії спробам аналізу потоку даних. На перший погляд можна припустити, що для вирішення проблеми можна використовувати ідентифікатор SPI, але так як SPI відрізняються для різних напрямків обміну, для пристрою NAT немає способу пов'язати повертається пакет з конкретним з'єднанням.

Протокол ESP забезпечує конфіденційність за допомогою шифрування на рівні пакетів IP. При цьому підтримується безліч алгоритмів симетричною схеми шифрування, наприклад, DES, triple-DES, AES і Blowfish для

шифрування поля даних. Алгоритм, який використовується для конкретного з'єднання, специфицируется асоціацією безпеки SA, SA включає в себе не тільки алгоритм, але і використовується ключ.

На відміну від протоколу AH, який вводить невеликий заголовок перед полем даних, ESP "оточує" захищається поле даних. Поля індекс параметрів безпеки (Security Parameters Index) і номер по порядку служать для тих же цілей, що і в разі AH, але в ESP є також поля заповнювача, наступного заголовка, і опционно аутентифікаційних даних в кінці ESP. Формат ESP-пакета розглянуто на рисунку 2.4.

Можливе використання ESP без будь-якого шифрування (щоб застосувати NULL алгоритм). Цей режим не забезпечує конфіденційності, і його має сенс використовувати в поєднанні з аутентифікацією ESP. Неефективно використовувати ESP без шифрування або аутентифікації (якщо тільки це не робиться для тестування протоколу).

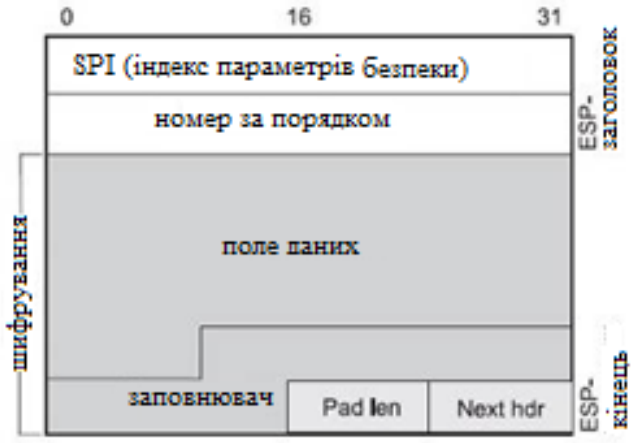

Рисунок 2.4 - Формат ESP-пакета без аутентифікації

Крім шифрування, ESP може опціонально надавати можливість аутентифікації, з залучення алгоритму HMAC. На відміну від AH, однак, ця аутентифікація проводиться тільки для ESP заголовка і зашифрованого поля даних. При цьому не перекривається весь IP пакет. Це не суттєво послаблює безпеку аутентифікації, але дає деякі важливі переваги.

Коли сторонній розглядає IP пакет, що містить дані ESP, принципово неможливо визначити IP адреси відправника і одержувача, порушник, звичайно, дізнається, що це ESP дані (це видно з заголовка пакета), але тип поля даних і самі дані зашифровані.

Дивлячись на сам пакет, неможливо навіть визначити, присутні чи ні аутентифіковані дані (це можна зробити лише, використовуючи індекс параметрів безпеки).

Як і в випадку AH, транспортний режим передбачає инкапсуляцию поля даних дейтограмм, і протокол орієнтований на обмін машина-машина. Вихідний IP заголовок залишений на місці (за винятком заміненого поля протокол), і це означає, що адреси відправника і одержувача також залишаються незмінними.

ESP в тунельному режимі проводить инкапсуляцию всієї IP-дейтограмми всередину зашифрованою оболонки.

Реалізація шифрованого з'єднання в тунельному режимі дуже близька до традиційних VPN.

На відміну від AH, де спостерігач може легко сказати, відбувався обмін в тунельному або транспортному режимі, тут ця інформація недоступна. Це відбувається через те, що вказівка на те, що наступний заголовок є IP, знаходиться в зашифрованому поле даних і, тому не видно для учасника, нездатного дешифрувати пакет.

IPSec спирається на ряд технологічних рішень і методів шифрування яке можна представити у вигляді наступних основних етапів:

Крок 1. Початок процесу IPSec. Трафік, якому потрібно шифрування відповідно до політики захисту IPSec, узгодженої сторонами IPSec, починає IKE-процес.

Крок 2. Перша фаза IKE. IKE-процес виконує аутентифікацію сторін IPSec і веде переговори про параметри асоціацій захисту IKE, в результаті чого створюється захищений канал для ведення переговорів про параметри асоціацій захисту IPSec в ході другої фази IKE.

Крок 3. Друга фаза IKE. IKE-процес веде переговори про параметри асоціації захисту IPSec і встановлює відповідні асоціації захисту IPSec для пристроїв сполучених сторін.

Крок 4. Передача даних. Відбувається обмін даними між сполученими сторонами IPSec, який ґрунтується на параметрах IPSec і ключах, що зберігаються в базі даних асоціацій захисту.

Крок 5. Завершення роботи тунелю IPSec. Асоціації захисту IPSec завершують свою роботу або в результаті їх видалення, або через перевищення граничного часу їх існування.

Протокол MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol - протокол взаємної аутентифікації Microsoft) містить механізм аутентифікації, необхідний для перевірки реєстраційних даних користувача в доменах Windows NT. Створені з його допомогою сеансу ключі застосовуються для шифрування даних користувача.

Шифруванням називається процес кодування даних з метою запобігання несанкціонованому доступу до них, особливо в процесі пересилання по відкритих каналах зв'язку. Шифрування проводиться із застосуванням спеціалізованих алгоритмів на основі так званих секретних ключів, що перетворюють дані (наприклад, пароль) в псевдовипадковий набір знаків. Прочитати закриту таким способом інформацію здатний тільки той, кому відомий відповідний ключ. Хешировать пароль, скажімо, може бути дешифрований лише на тому комп'ютері, де є такий же ключ (згадаємо дитяче шифрування за допомогою двох однакових паперових матриць). Застосовувані при шифруванні алгоритми, особливо з ключами довжиною понад 128 біт, практично повністю виключають можливість дешифрування інформації сторонніми.

3 РОЗРОБКА ЗАХИЩЕНОГО ДОСТУПУ НА ОСНОВІ OPEN VPN

3.1 Аналіз загроз інформаційної безпеки

Під загрозою розуміють потенційно можливу подію, яка може привести до нанесення збитку чиїмось інтересам. Надалі під загрозою безпеки АС обробки інформації будемо розуміти можливість впливу на АС, яке прямо або побічно може завдати шкоди її безпеки.

В даний час відомий великий перелік загроз інформаційній безпеці АС, що містить сотні позицій.

Розгляд можливих загроз інформаційної безпеки проводиться з метою визначення повного набору вимог до розроблюваної системі захисту.

Перелік загроз, оцінки ймовірностей їх реалізації, а також модель порушника служать основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту АС. Крім виявлення можливих загроз, доцільно проведення аналізу цих загроз на основі їх класифікації за рядом ознак. Кожен з ознак класифікації відображає одне з узагальнених вимог до системи захисту. Загрози, що відповідають кожному ознакою класифікації, дозволяють деталізувати отражаемое цим ознакою вимога.

Необхідність класифікації загроз інформаційній безпеці АС обумовлена тим, що зберігається і обробляється інформація в сучасних АС піддається впливу надзвичайно великого числа факторів, в силу чого стає неможливим формалізувати задачу опису повної множини загроз. Тому для захищається системи зазвичай визначають не повний перелік загроз, а перелік класів загроз.

Класифікація можливих загроз інформаційної безпеки АС може бути проведена за наступними базовим ознаками:

1. За природою виникнення:

- природні загрози, викликані впливами на АС об'єктивних фізичних процесів або стихійних природних явищ;

- штучні загрози безпеки АС, викликані діяльністю людини.

2. За ступенем навмисності прояви:

- загрози, викликані помилками або халатністю персоналу, наприклад, некомпетентне використання засобів захисту, введення помилкових даних;

- загрози навмисного дії, наприклад, дії зловмисників.

3. За безпосереднього джерела загроз:

- природне середовище, наприклад, стихійні лиха, магнітні бурі та ін .;

- людина, наприклад, вербування шляхом підкупу персоналу, розголошення конфіденційних даних і т.д;

- санкціоновані програмно-апаратні засоби, наприклад, видалення даних, відмова в роботі ОС;

- несанкціоновані програмно-апаратні засоби, наприклад, зараження комп'ютера вірусами з деструктивними функціями.

4. Відповідно до положення джерела загроз:

- позаконтрольованої зони АС, наприклад, перехоплення даних, переданих по каналах зв'язку, перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв;

- в межах контрольованої зони АС, наприклад, застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації і т.д;

- безпосередньо в АС, наприклад, некоректне використання ресурсів АС.

5. За ступенем залежності від активності АС:

- незалежно від активності АС, наприклад, розтин шифрів

криптозахисту інформації;

- тільки в процесі обробки даних, наприклад, загрози виконання і розповсюдження програмних вірусів.

6. За ступенем впливу на АС:

- пасивні загрози, які при реалізації нічого не змінюють у структурі та змісті АС, наприклад, загроза копіювання секретних даних;

- активні загрози, які при впливі вносять зміни в структуру і зміст АС, наприклад, впровадження троянських коней і вірусів.

7. По етапах доступу користувачів або програм до ресурсів АС:

- загрози, які проявляються на етапі доступу до ресурсів АС, наприклад, загрози несанкціонованого доступу в АС;

- загрози, які проявляються після дозволу доступу до ресурсів АС, наприклад, загрози несанкціонованого або некоректного використання ресурсів АС.

8. За способом доступу до ресурсів АС:

- загрози, що здійснюються з використанням стандартного шляху доступу до ресурсів АС, наприклад, незаконне отримання паролів і інших реквізитів розмежування доступу з подальшою маскуванням під зареєстрованого користувача;

- загрози, що здійснюються з використанням прихованого нестандартного шляху доступу до ресурсів АС, наприклад, несанкціонований доступ до ресурсів АС шляхом використання недокументованих можливостей ОС.

9. За поточним місцем розташування інформації, що зберігається і оброблюваної в АС:

- загрози доступу до інформації, що знаходиться на зовнішніх запам'ятовуючих пристроях, наприклад, несанкціоноване копіювання секретної інформації з жорсткого диска;

- загрози доступу до інформації, що знаходиться в оперативній пам'яті,

наприклад, читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті з боку прикладних програм;

- загрози доступу до інформації, що циркулює в лініях зв'язку, наприклад, незаконне підключення до ліній зв'язку з подальшим введенням помилкових повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим введенням дезінформації та нав'язуванням неправдивих повідомлень;

- загрози доступу до інформації, яка відображається на терміналі або друкується на принтері, наприклад, запис інформації, що відображається на

приховану відеокамеру.

Як уже зазначалося, небезпечні впливу на АС поділяють на випадкові і навмисні. Аналіз досвіду проектування, виготовлення і експлуатації АС показує, що інформація піддається різним випадковим впливам на всіх етапах життєвого циклу і функціонування АС.

Причинами випадкових впливів при експлуатації АС можуть бути:

- аварійні ситуації через стихійних лих і відключень електроживлення;
- відмови і збої апаратури;
- помилки в програмному забезпеченні;
- помилки в роботі обслуговуючого персоналу і користувачів;
- перешкоди в лініях зв'язку через впливів зовнішнього середовища.

Помилки в ПО є поширеним видом комп'ютерних порушень. ПО серверів, робочих станцій, маршрутизаторів і т. Д. Написано людьми, тому воно практично завжди містить помилки. Чим вище складність подібного ПО, тим більша ймовірність виявлення в ньому помилок і вразливостей. Більшість з них не представляють ніякої небезпеки, деякі ж можуть привести до серйозних наслідків, таких як отримання зловмисником контролю над сервером, непрацездатність сервера, несанкціоноване використання ресурсів (використання комп'ютера як плацдарм для атаки і т. п.). Зазвичай подібні помилки усуваються за допомогою пакетів оновлень, регулярно випускаються виробником ПО. Своєчасна установка таких пакетів є необхідною умовою безпеки інформації.

Навмисні загрози пов'язані з цілеспрямованими діями порушника. Як порушника може бути службовець, відвідувач, конкурент, найманець і т. Д. Дії порушника можуть бути обумовлені різними мотивами: невдоволенням службовця своєю кар'єрою, суто матеріальним інтересом (хабар), цікавістю, конкурентною боротьбою, прагненням самоствердитися будь-якою ціною.

Несанкціонований доступ - найбільш поширений і різноманітний вид комп'ютерних порушень. Суть НСД полягає в отриманні користувачем

(порушником) доступу до об'єкта в порушення правил розмежування доступу, встановлених відповідно до прийнятої в організації політикою безпеки. НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректної встановлення та налаштування. НСД може бути здійснений як штатними засобами АС, так і спеціально створеними апаратними та програмними засобами.

Основні канали НСД, через які порушник може отримати доступ до компонентів АС і здійснити розкрадання, модифікацію і / або руйнування інформації:

- штатні канали доступу до інформації (термінали користувачів, оператора, адміністратора системи; засоби відображення і документування інформації; канали зв'язку) при їх використанні порушниками, а також законними користувачами поза межами їх повноважень;

- технологічні пульти управління;

- лінії зв'язку між апаратними засобами АС;

- побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення і заземлення та ін.

З усього розмаїття способів і прийомів НСД зупинимося на наступних поширених і пов'язаних між собою порушення:

- перехоплення паролів - «маскарад»;

- незаконне використання привілеїв.

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача увійти в систему програма-перехоплювач імітує на екрані дисплея логуватись користувача, які відразу пересилаються власнику програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається ОС.

3.2 Побудова захищених мереж на сеансовому рівні

Сеансовий рівень є максимально високим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів. При побудові

захищених віртуальних мереж на даному рівні досягаються найкращі показники по функціональної повноті захисту інформаційного обміну, надійності контролю доступу, а також простоті конфігурації системи безпеки. Протоколи формування захищених віртуальних каналів на сеансовому рівні прозорі для прикладних протоколів захисту, а також високорівневих протоколів надання різних сервісів (протоколів HTTP, FTP, POP3, SMTP, NNTP і ін.). Однак на сеансовому рівні починається безпосередня залежність від додатків, що реалізують високорівневі протоколи.

Так як сеансовий рівень моделі OSI відповідає за установку логічних з'єднань і управління цими сполуками, то на даному рівні з'являється можливість використання програм-посередників, які перевіряють допустимість запитаних з'єднань і забезпечують виконання інших функцій захисту міжмережевої взаємодії. У загальному випадку програми-посередники, які традиційно використовуються в міжмережевих екранах, можуть виконувати такі функції:

- ідентифікація і аутентифікація користувачів;

- криптозащита переданих даних;

- розмежування доступу до ресурсів внутрішньої мережі; - розмежування доступу до ресурсів зовнішньої мережі;

- фільтрація і перетворення потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;

- трансляція внутрішніх мережевих адрес для вихідних пакетів повідомлень;

- реєстрація подій і реагування на поставлені події;

- кешування даних, запитуваних із зовнішньої мережі.

Таким чином, при побудові захищених віртуальних мереж на сеансовому рівні з'являється можливість не тільки криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а й можливість реалізації ряду функцій посередництва між взаємодіючими сторонами.

Для криптографічного захисту інформаційного обміну на сеансовому

Рівні найбільшу популярність отримав протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security), розроблений компанією Netscape Communications.

Протокол Secure Sockets Layer (SSL), споконвічно орієнтований на захист інформаційного обміну між клієнтом і сервером комп'ютерної мережі, є промисловим протоколом сеансового рівня моделі OSI використовують для забезпечення безпеки інформаційного обміну криптографічні методи захисту інформації. Конфіденційність даних забезпечується за рахунок їх криптографічного закриття, а аутентифікація взаємодіючих сторін, а також справжність і цілісність циркулюючої інформації - за рахунок формування і перевірки цифрового підпису.

Ядром протоколу SSL є технологія комплексного використання асиметричних і симетричних криптосистем. Як алгоритмів асиметричного шифрування використовуються такі алгоритми, як RSA (розробки RSA Data Security Inc.), а також алгоритм Діффі-Хеллмана. Для обчислення хеш-функцій можуть застосовуватися стандарти MD5 і SHA-1. Допустимими алгоритмами симетричного шифрування є RC2, RC4, DES, а також потрійний DES. У протоколі SSL третьої версії набір криптографічних алгоритмів є розширюваним. Для аутентифікації взаємодіючих сторін і криптозахисту ключа симетричного шифрування застосовуються цифрові сертифікати відкритих ключів користувачів (клієнта і сервера), завірені цифровим підписом спеціальних сертифікаційних центрів. Підтримуються цифрові сертифікати, відповідні загальноприйнятим стандартом X.509.

Протокол SSL розроблений корпорацією Netscape, а потім підтриманий низкою провідних виробників програмного забезпечення. Через своїх позитивних якостей SSL практично витіснив конкуруючі високорівневі протоколи щодо захисту інформаційного обміну, наприклад, такі як SHTTP (Secure HTTP), і став загальновизнаним неофіційними стандартом захисту в Internet і Intranet мережах. Специфікації SSL були свого часу запропоновані в якості офіційних стандартів Internet, але не отримали цього статусу за

формальними обставинами. Не виключено, що SSL все ж почне просуватися по щаблях формального прийняття IETF як стандарт, так як він вже став промисловим протоколом, що розвивається і просувається поза ієрархії технічних координуючих інститутів Internet. Останньою версією SSL є версія 3.0, про яку і йтиметься.

Клієнтська частина SSL реалізована у всіх популярних Web-навігаторах, до яких відносяться Netscape Navigator компанії Netscape і Internet Explorer від Microsoft, а серверна - в більшості як комерційних, так і розповсюджуються на некомерційних умовах WWW-серверів, наприклад, в серверних додатках компаній IBM, Netscape, Microsoft, Spyglass, Open Market.

Відповідно до протоколу SSL криптозахищені тунелі створюються між кінцевими точками віртуальної мережі (Рисунок 3.1). Ініціаторами якого захищеного тунелю є клієнт і сервер, що функціонують на комп'ютерах в кінцевих точках тунелю. Протокол SSL передбачає два етапи взаємодії клієнта і сервера при формуванні та підтримці захищається з'єднання:

- встановлення SSL-сесії;

- захищене взаємодія.

Процедура встановлення SSL-сесії, яка називається також процедурою "рукостискання", відпрацьовується перед безпосереднім захистом інформаційного обміну і виконується за протоколом початкового привітання (Handshake Protocol), що входить до складу протоколу SSL. У процесі становлення SSL-сесії вирішуються наступні завдання:

- аутентифікація сторін;

- узгодження криптографічних алгоритмів і алгоритмів стиснення, які будуть використовуватися при захищеному інформаційному обміні;

- формування загального секретного майстер-ключа;

- генерація на основі сформованого майстер-ключа загальних секретних сеансових ключів для криптозахисту інформаційного обміну.

У реалізаціях протоколу SSL для аутентифікації взаємодіючих сторін і формування загальних секретних ключів найчастіше використовують

алгоритм RSA розробки RSA Data Security Inc.

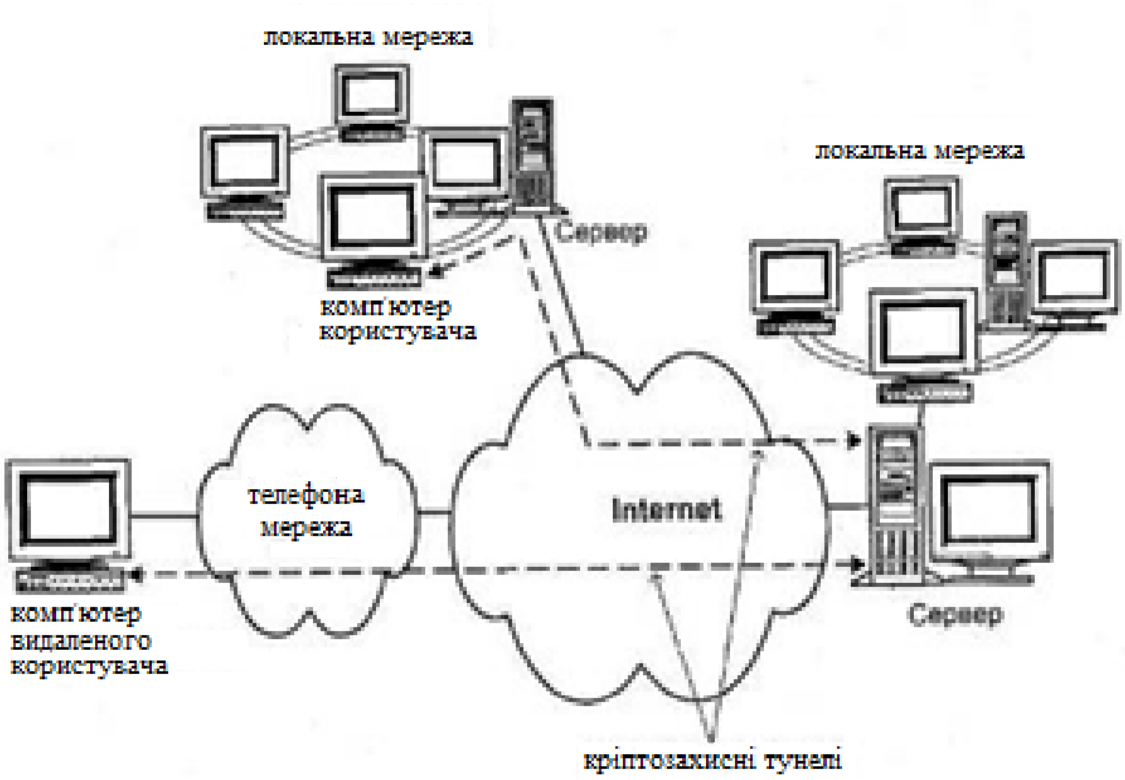

Рисунок 3.1 Криптозахищені тунель на базі протоколу SSL

Однозначне і достовірне відповідність між відкритими ключами і їх власниками встановлюється за допомогою цифрових сертифікатів, які видаються спеціальними Центрами Сертифікації. Сертифікат являє собою блок даних, що містить наступну інформацію:

- ім'я центру сертифікації;
- ім'я власника сертифіката;
- відкритий ключ власника сертифіката;
- період дії сертифіката;
- ідентифікатор і параметри криптоалгоритма, який повинен використовуватися при обробці сертифіката;
- цифровий підпис центру сертифікації, запевняє всі дані в складі сертифіката.

Цифровий підпис центру сертифікації в складі сертифіката забезпечує достовірність і однозначність відповідності відкритого ключа та його

власника. Центр сертифікації виконує роль нотаріуса, який запевняє справжність відкритих ключів, що дозволяє їх власникам користуватися послугами захищеного взаємодії без попередньої особистої зустрічі. Необхідність безумовного довіри до центру сертифікації з боку всіх учасників захищеного обміну пред'являє до нього досить високі вимоги з перевірки автентичності завіряються відкритих ключів. Одним з таких центрів в Internet є компанія VeriSign, заснована RSA Data Security Inc., за участю компаній Visa, IBM, Netscape, Microsoft і Oracle.

Третя версія протоколу SSL підтримує три режими аутентифікації:

- взаємна аутентифікація сторін;

- одностороння аутентифікація сервера без аутентифікації клієнта;

- повна анонімність.

При використанні останнього варіанту взаємодіючі сторони незахищені від атак, пов'язаних з підміною учасників взаємодії, даному режимі забезпечується захист інформаційного обміну без будь-яких гарантій щодо справжності взаємодіючих сторін.

У режимі односторонньої аутентифікації сервера без аутентифікації клієнта процедура встановлення SSL-сесії між клієнтом і сервером включає наступні кроки.

1. Клієнт посилає серверу запит на встановлення захищеного з'єднання, в якому передає деякі формальні параметри цього з'єднання:

- поточний час і дату;

- випадкову послідовність (RAND_CL);

- набір підтримуваних клієнтом алгоритмів симетричного шифрування і алгоритмів обчислення хеш-функції;

- набір підтримуваних алгоритмів стиснення і ін.

2. Сервер обробляє запит від клієнта і передає йому узгоджений набір параметрів:

- ідентифікатор SSL-сесії;

- конкретні криптографічні алгоритми з числа запропонованих клієнтом

(якщо з якої-небудь причини запропоновані алгоритми або їх параметри не задовольняють вимогам сервера, сесія закривається);

- сертифікат сервера, завірений цифровим підписом центру сертифікації;

- випадкову послідовність (RAND_SERV).

3. Клієнт перевіряє отриманий сертифікат сервера за допомогою відкритого ключа центру сертифікації, який йому відомий. При негативному результаті перевірки сесія закривається, а при позитивному - клієнт виконує наступні дії:

- генерує випадкову 48-байтную послідовність Pre_MasterSecret, призначену для генерації загального секретного майстер-ключа; шифрує Pre_MasterSecret по відкритому ключу сервера, отриманого в сертифікаті сервера, і посилає серверу;

- за допомогою узгоджених хеш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів послідовність Pre_MasterSecret, послану сервера випадкову послідовність RAND_CL і отриману від нього випадкову послідовність RAND_SERV;

- використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує загальні з сервером сеансу секретні ключі для симетричного шифрування і обчислення хеш-функцій;

- переходить в режим захищеної взаємодії.

4. Сервер розшифровує отриману послідовність Pre_MasterSecret за своїм закритому ключу і виконує на її основі ті ж операції, що і клієнт:

- за допомогою узгоджених хеш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів Pre_MasterSecret, а також послану клієнту випадкову послідовність RAND_SERV і отриману від нього випадкову послідовність RAND_CL;

- використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує загальні з клієнтом сеансу секретні ключі для симетричного шифрування і обчислення хеш-функцій;

- переходить в режим захищеної взаємодії.

Так як при формуванні параметрів SSL-сесії і клієнт, і сервер користувалися одними і тими ж вихідними даними (узгодженими алгоритмами, спільної секретної послідовність Pre_MasterSecret і випадковими послідовностями RAND_CL і RAND_SERV), то очевидно що в результаті описаних вище дій вони виробили однакові сеансу секретні ключі . Для перевірки ідентичності параметрів SSL-сесії клієнт і сервер посилають один одному тестові повідомлення, зміст яких відомо кожної зі сторін:

- клієнт формує повідомлення з власних посилок на адресу сервера на кроці 1 і посилок, отриманих від сервера на кроці 2, вносячи елемент випадковості у вигляді послідовності MasterSecret, унікальною для даної сесії; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення за загальним сеансовому секретного ключа і відправляє серверу;

- сервер, в свою чергу, формує повідомлення з власних посилок на адресу клієнта на кроці 2, посилок, отриманих від клієнта на кроці 1, і послідовності MasterSecret; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення на загальному сеансовому секретному ключі і відправляє клієнту;

- в разі успішної розшифровки і перевірки цілісності кожної зі сторін отриманих тестових повідомлень, SSL-сесія вважається встановленої і сторони переходять в штатний режим захищеної взаємодії.

В процесі захищеної взаємодії з встановленими криптографічними параметрами SSL-сесії виконуються наступні дії:

- кожна сторона при передачі повідомлення формує MAC-код для подальшої перевірки цілісності повідомлення і потім зашифровує вихідне повідомлення разом з MAC-кодом;

- кожна сторона при прийомі повідомлення розшифровує його і перевіряє на цілісність (обчислюється поточний MAC-код і звіряється з MAC-кодом перевірки цілісності, отриманим разом з повідомленням); в разі виявлення порушення цілісності повідомлення, SSL-сесія закривається.

Незважаючи на те, що протокол SSL підтримується програмним

забезпеченням серверів і клієнтів, що випускаються провідними західними компаніями, в нашій країні є обставини, що перешкоджають поширенню даного протоколу і прийняття його в якості базового для реалізації програм, що вимагають захищеного інформаційного взаємодії сторін-учасниць.

Практично всі існуючі продукти, що підтримують протокол SSL, реалізовані в США і через експортні обмеження доступні тільки в усіченому варіанті (з довжиною сеансового ключа 40 біт для алгоритмів симетричного шифрування і 512 біт для алгоритму RSA, використовуваного на етапі встановлення SSL-сесії), що на сьогоднішній день явно недостатньо.

3.3 Реалізація захищеного доступу на основі Open VPN

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

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

Дамо для зручності маршрутизаторів імена:

- В офісі: Office;
- На складі: Sklad;
- Колокація (сервера у провайдера): Colo;
- Магазин №1: mag1
- Магазин №2: mag2

Мережеві налаштування маршрутизаторів:

Office:

Мережа	інтерфейс	Ip адреса	маска	Шлюз
Інтернет	eth2	213.182.175.230	255.255.255.252	213.182.175.229
Локальна	eth1	192.168.53.250	255.255.255.0	-

Sklad:

Мережа	інтерфейс	Ip адреса	маска	Шлюз
Інтернет	eth2	79.142.87.206	255.255.255.252	79.142.87.211
локальна	eth1	192.168.0.1	255.255.255.0	-

Colo:

Мережа	інтерфейс	Ip адреса	маска	Шлюз
Інтернет	eth2	195.2.240.68	255.255.255.252	195.2.240.60
локальна	eth1	172.16.100.8	255.255.255.0	-

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

Приступимо до встановлення та налаштування.

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

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

Пакет OpenVPN не доступний в стандартному репозиторі, тому підключаємо додатковий репозитор rpmforge:

colo> rpm -Uhv

0.3.6-1.el5.rf.x86_64.rpm

Ця команда завантажує rpm пакет сховища та встановлює його.

Тепер нам став доступний пакет OpenVPN, встановлюємо його:

colo> yum install openvpn

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

Для цього переходимо в конфігураційний каталог OpenVPN і створюємо

каталог під наші майбутні ключі і каталог під конфігураційні файли клієнтів:

colo> cd / etc / openvpn

colo> mkdir keys

colo> mkdir ccd

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

colo> ./ vars

colo> ./ build-ca

Generating a 1 024 bit RSA private key

..... ++++++

.. ++++++

writing new private key to 'ca.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', The field will be left blank.

Країна

Country Name (2 letter code) [US]: UA

Провінція

State or Province Name (full name) [CA]: SPB

Місто

Locality Name (eg, city) [SanFrancisco]: SPB

Назва фірми

Oganization Name (eg, company) [Fort-Funston]: server

Відділення фірми

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

Ім'я сервера OpenVPN

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

Name []: server

Email Address [me@myhost.mydomain]:

Створюємо сертифікат X.509 для сервера:

colo> ./build-key-server server

Країна

Country Name (2 letter code) [US]: UA

Провінція

State or Province Name (full name) [CA]: SPB

Місто

Locality Name (eg, city) [SanFrancisco]: SPB

Назва компанії

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

Відділення компанії

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

Ім'я сервера OpenVPN

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

Поштова адреса

Email Address [root @ localhost]:

Please enter the following 'extra' attributes

to be sent with your certificate request

Пароль

A challenge password []: 123456789

Назва організації

An optional company name []: server

Далі постане питання про підписуванні сертифіката, погоджуємося.

Створюємо ключ для office:

colo> ./build-key-server office

Generating a 1 024 bit RSA private key

..... ++++++

..... ++++++

writing new private key to 'client.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', The field will be left blank.

Country Name (2 letter code) [US]: UA

State or Province Name (full name) [CA]: SPB

Locality Name (eg, city) [SanFrancisco]: SPB

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

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

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

Email Address [root @ localhost]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: 123456789

An optional company name []: office

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

Створюємо ключ Діффі Хельман для обміну ключами по незахищеному каналу:

colo> ./build-dh

Створюємо ключ для tls-аутентифікації:

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

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

- ca.crt - Головний CA сертифікат, цей файл потрібен і клієнту і серверу;
- dh1024.pem - ключ Діффі Хельман, цей файл потрібен тільки серверу;
- server.crt - Сертифікат сервера, потрібен тільки серверу;
- server.key - Ключ сервера, потрібен тільки сервера (секретний файл);
- office.crt, sklad.crt, mag1.crt, mag2.crt - Сертифікати клієнтів, потрібні тільки відповідним клієнтам;
- office.key, sklad.key, mag1.key, mag2.key - Ключі клієнтів, потрібні тільки відповідним клієнтам (секретні файли);
- ta.key - TLS-ключ, потрібен і клієнтам і сервера.

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

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

```
# Порт на якому працює сервер
port 5000
# Протокол udp
proto udp
# Використовуваний тип пристрою і номер
dev tun0
# Вказуємо файл CA
ca /etc/openvpn/keys/ca.crt
# Вказуємо файл з сертифікатом сервера
cert /etc/openvpn/keys/server.crt
# Вказуємо файл з ключем сервера
key /usr/local/etc/openvpn/keys/server.key
# Вказуємо файл Діффі Хельман
dh /usr/local/etc/openvpn/keys/dh1024.pem
```

```
# Задаємо IP-адреса сервера і маску підмережі віртуальної мережі
server 10.10.200.0 255.255.255.0
# Задаємо маршрути, які передаємо клієнтам, і маску підмережі для того, щоб вони бачили мережу за OpenVPN сервером
# Colo
push "route 172.16.100.0 255.255.255.0"
# Office
push "route 192.168.53.0 255.255.255.0"
# Sklad
push "route 192.168.0.0 255.255.255.0"
# Вказуємо, де зберігаються файли з настройками IP-адрес клієнтів
client-config-dir ccd
# Додаємо маршрути сервер-клієнт
route 10.10.200.0 255.255.255.0
# Office
route 192.168.53.0 255.255.255.0
# Sklad
route 192.168.0.0 255.255.255.0
# Дозволяє бачити клієнтам один одного (по віртуальним IP) по замовчуванням клієнти бачать тільки сервер
client-to-client
# Включаємо TLS аутіфікацію
tls-server
# Вказуємо tls-ключ
tls-auth keys / ta.key 0
# Таймаут до реконекту
tls-timeout 120
# Вибираємо алгоритм хешування
auth MD5
# Включаємо шифрацию пакетів
```

cipher BF-CBC

Перевіряємо активність підключення кожні 10 секунд, якщо в

Протягом 120 сек. немає відповіді, підключення закривається

keepalive 10 120

Стиснення трафіку

comp-lzo

Від якого користувача і групи буде працювати OpenVPN

user nobody

group nobody

Чи не перечитувати ключі після отримання SIGUSR1 або ping-restart

persist-key

Тримати і перевідкривати TUN \ TAP пристрій, після

отримання SIGUSR1 або ping-restart

persist-tun

Логгірування

status /var/log/openvpn/openvpn-status.log

log /var/log/openvpn/openvpn.log

Рівень інформації для налагодження

verb 3

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

office

ifconfig-push 10.10.200.2 10.10.200.1

iroute 192.168.53.0 255.255.255.0

sklad

ifconfig-push 10.10.200.3 10.10.200.1

iroute 192.168.53.0 255.255.255.0

mag1

ifconfig-push 10.10.200.4 10.10.200.1

mag2

ifconfig-push 10.10.200.5 10.10.200.1

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

На цьому налаштування сервера закінчується, запускаємо OpenVPN:

colo>service openvpn start

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

colo>ifconfig tun0

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

inet addr: 10.10.200.1 PtP: 10.10.200.2 Mask: 255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU 1500

Metric: 1

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

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

collisions: 0 txqueuelen: 100

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

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

Створимо конфігураційний файл client.conf:

dev tun

proto udp

remote 195.2.240.68 # (реальний ip сервера)

port 5000

client

resolv-retry infinite

ca keys / ca.crt

cert keys / client.crt

key keys / client.key

tls-client

tls-auth keys / ta.key 1

auth MD5

cipher BF-CBC

ns-cert-type server

comp-lzo

persist-key

persist-tun

Додавання маршруту до мережі за сервером. Цей рядок не потрібна для конфиг. файлів магазинів

up /etc/openvpn_up.sh

status /var/log/openvpn/openvpn-status.log

log /var/log/openvpn/openvpn.log

verb 3

Створимо скрипт openvpn_up.sh для автоматичного додавання маршруту:

#! / Bin / sh

/ Sbin / route add -net 172.16.100.0 netmask 255.255.255.0 gw 10.10.200.1 tun0

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

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

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

Тепер 3 мережі «бачать» один одного. Налаштуємо підключення з

магазинів до серверів. На комп'ютерах в магазинах, варто операційна система Windows XP. Беремо з офіційного сайту дистрибутив OpenVPN і встановлюємо. Потім в установленому каталозі в папку config кладемо наші ключі і конфігураційний файл mag1. Після цього можна запускати.

На цьому етапі налаштування завершені. Маючи захищену корпоративну мережу, можна підключатися безпосередньо до серверів. Перевірити шифрацію можна, прослухавши трафік на одному з роутерів командою TCPDUMP.

Приклад виведення нешифрованих трафіку:

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

Приклад зашифрованого:

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

3.4 Оцінка продуктивності під час використання Open VPN

На рис. 3.2 представлені графіки значень RTT. З них видно, що різниця між каналом без VPN і каналом з використанням VPN, не є суттєвою. Також включення опції стиснення не впливає на час відгуку.

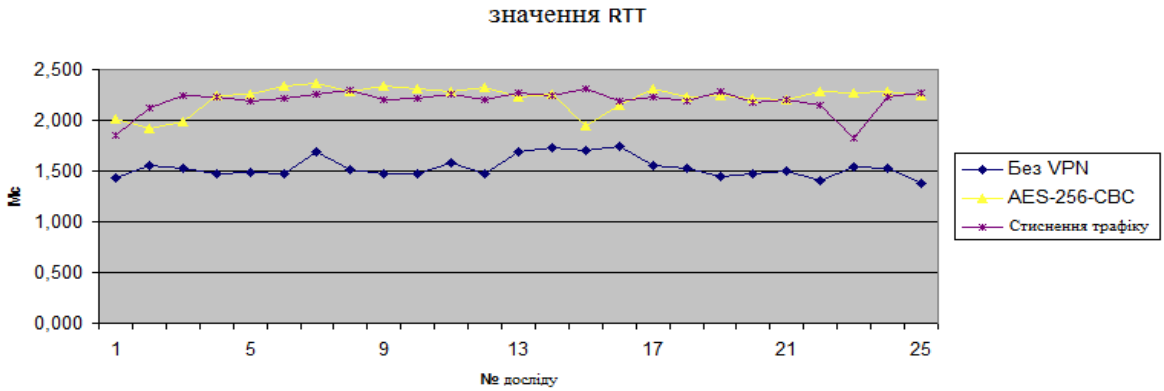

Рисунок 3.2 Графіки значень RTT

На рис. 3.3 представлені графіки пропускної здатності каналу, з яких можна зробити наступні висновки:

- При використанні створеного каналу VPN з штфруванням за допомогою ключа AES-256-CBC втрата в продуктивності 0,5 Мбіт / сек, що склало 5,1% від каналу без використання VPN;
- При включенні стиснення шифрованого трафіку спостерігаємо приріст швидкості в 3 Мбіт / сек, що склало 32.9%.

На рис. 3.4 представлені графіки завантаження ЦП на маршрутизаторах при використанні OpenVPN с шифрацией трафіку, при включеному і вимкненому стисненні.

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

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

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

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

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

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

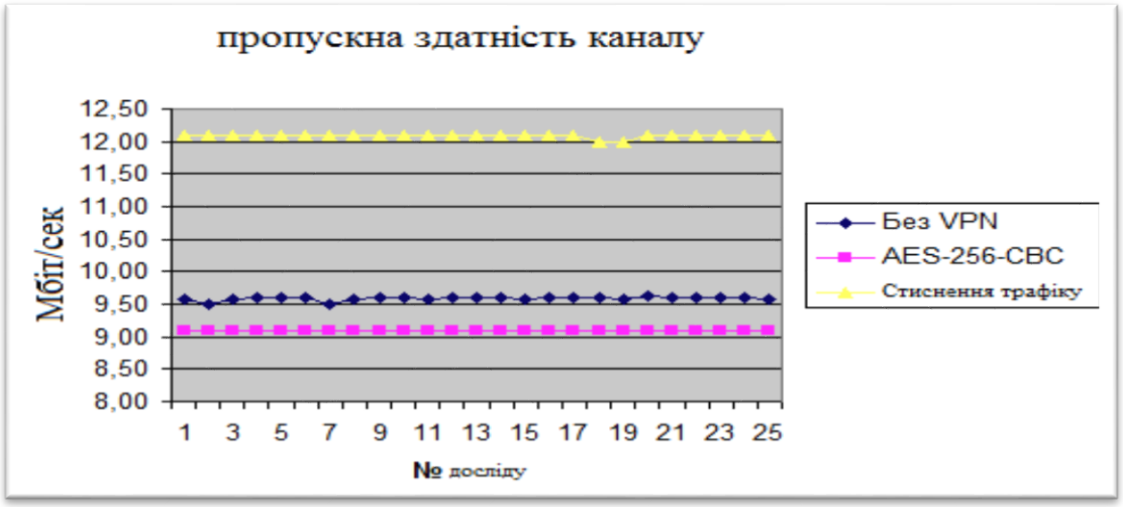

Рисунок 3.3 Графіки пропускної здатності каналу

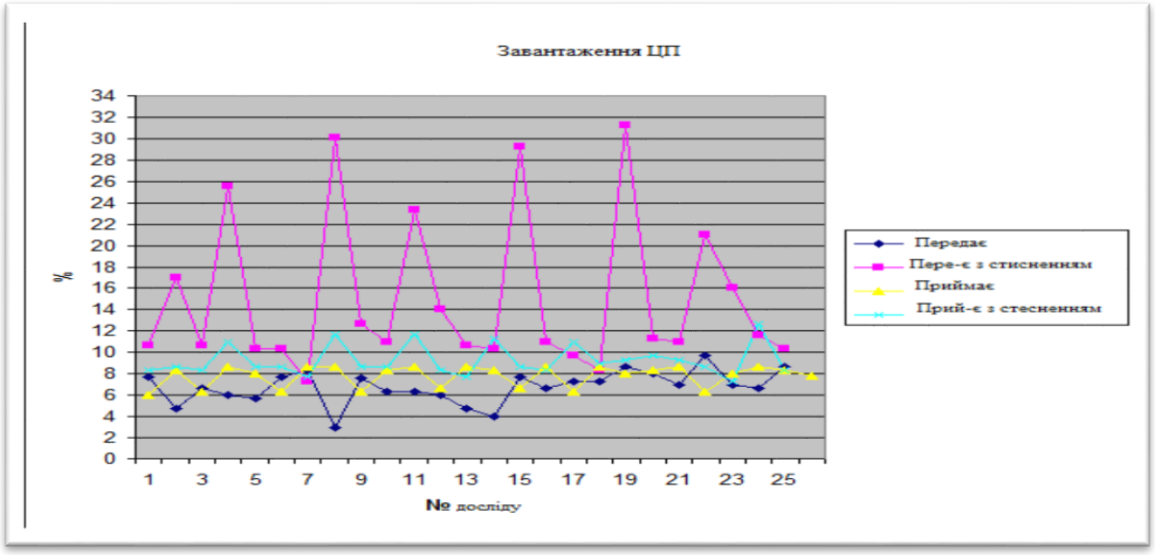

Рисунок 3.4 Графіки завантаження ЦП

Створюючи захищену корпоративну мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифрацііією переданих даних і зростанням швидкості за рахунок стиснення трафіку. Технологія OpenVPN повністю виправдовує себе. З мінусів виділяється деяка складність настройки і створення VPN мережі. З плюсів - кроссплатформенность.

Засоби організації VPN, розроблені Microsoft, дозволяють підключати до серверів на базі Windows NT так звані призначені для користувача процесори (front-end processor, ПП), що управляють доступом клієнтів в мережу даного сервера. Застосування таких посередників дає можливість встановлювати тунельні підключення навіть тим клієнтам, які не оснащені засобами VPN. Користувач може і не знати, підключився він до сервера безпосередньо, або через ПП, який створив для нього тунель. Завдяки цьому в VPN Microsoft забезпечується «прозорий» доступ до клієнтів PPP, що дозволяє їм працювати в середовищах Unix, Win 16, MS-DOS®, а також взаємодіяти з клієнтами Macintosh і іншими.

Призначений для користувача процесор не має доступу до даних, що циркулюють між клієнтом і сервером, тому його цілком можна розмістити на сайті постачальника послуг Інтернету. Тут ПП виконуватиме роль безстороннього регулювальника, якого анітрохи не стосується вміст проходить через нього інформації. З точки зору безпеки це означає, що компанія зберігає повний контроль за доступом в мережу, та й безпеку її даних анітрохи не страждає. Така схема дуже зручна для тих компаній, які готові передати управління віддаленим доступом через комутовані канали в руки сторонніх постачальників послуг, але при цьому хочуть забезпечити повну безпеку своєї інформації.

Для надійного захисту даних необхідно обмежувати доступ до сервера, а не до призначеного для користувача процесору. З цією метою перевірка аутентифікації всіх користувачів, які намагаються підключитися до сервера, проводиться на самому сервері. Функції ПП обмежуються перевіркою

ідентифікатора користувача і створенням тунелю до сервера. Як ми бачимо, цей посередник і тут грає пасивну роль, нітрохи не знижуючи безпеки з'єднання.

ВИСНОВКИ

У бакалаврскій роботі розглянуто протоколи і методи реалізації віртуальних мереж. Дослідження побудови та використання Open VPN вказує на основні поняття і функції мережі VPN. Класифікувати VPN можна трима способами.

При аналізі протоколів VPN мереж робиться акцент на еталонній багаторівневій моделі OSI, а саме на канальному рівні де реалізуються два протоколи це протокол PPTP та протокол L2TP, мережевий рівень на якому робиться реалізація протоколу IPsec. На сеансовому рівні в основному відбувається реалізація побудови захисту мереж сеансового рівня.

Розробка захищеного доступу на основі Open VPN розпочинається з аналізу загороз, які можуть провокувати збій інформаційній безпеці, після чого може відбуватись побудова захищених мереж на сеансовому рівні та розроблюватись реалізація захищеного доступу на основі OpenVPN, після чого може бути оцінка продуктивності під час використання OpenVPN.

Переваги Open VPN в тому, що організація віддаленого доступу робиться через Інтернет, що набагато дешевше і краще, ніж через виділені канали.

Створюючи захищену мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифрацією переданих даних і зростанням швидкості за рахунок стиснення трафіку.

У загальному вигляді технологія OpenVPN повністю виправдовує себе.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a VPN? Virtual private network meaning. (n.d.). NordVPN. https://nordvpn.com/what-is-a-vpn/

2. 14 most interesting uses of a VPN. (n.d.). NordVPN. https://nordvpn.com/blog/interesting-vpn-uses/

3. Global, P. (2022, November 24). Lock it down: Your introduction to securing data with VPN technology. Find the Resources You Need from PivIT Global. https://info.pivitglobal.com/resources/introduction-to-securing-data-with-vpn-technology.

4. What are the different types of VPN protocols? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/types-of-vpn-protocols

5. What is L2TP (layer 2 tunnel protocol)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-l2tp

6. What Is IKEv2 (Internet Key Exchange version 2)? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-ikev2

7. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

8. What Is WireGuard? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-wireguard

9. The ChaCha family of stream ciphers. (n.d.). cr.yp.to. https://cr.yp.to/chacha.html

10. Poly1305-AES: A state-of-the-art message-authentication code. (n.d.). cr.yp.to. https://cr.yp.to/mac.html

11. Blake2. (n.d.). BLAKE2. https://www.blake2.net/

12. Curve25519: High-speed elliptic-curve cryptography. (n.d.). cr.yp.to. https://cr.yp.to/ecdh.html

13. What Is OpenVPN? (n.d.). Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-openvpn

14. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

15. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

16. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

17. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

18. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

19. Oracle VirtualBox - Oracle VirtualBox Documentation. (2019, November 5). Oracle Help Center. https://docs.oracle.com/en/virtualization/virtualbox/

20. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

21. WinBox - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support.

22. Documentation:Setup_and_user_guide [XigmaNAS WIKI]. (n.d.). XigmaNAS – XigmaNAS.

23. OpenVPN - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support.

24. OpenVPN connect user guide. (n.d.). Business VPN For Secure Networking | OpenVPN. https://openvpn.net/connect-docs/user-guide.html

25. Official ubuntu documentation. (n.d.). Official Ubuntu Documentation. https://help.ubuntu.com/

26. Микитишин, А. Г., Митник, М. М., Голотенко, О. С., & Карташов, В. В. (2023). Комплексна безпека інформаційних мережевих систем. Навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка».

27. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

28. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

29. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 499-503). IEEE.

30. Derkach, M., Lysak, V., Skarga-Bandurova, I., & Kotsiuba, I. (2019, September). Parking Guide Service for Large Urban Areas. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 567-571). IEEE.