ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

На тему: **«Розроблення критеріїв вибору та методів реалізації віртуальної приватної мережі організації»**

На здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерна інженерія

освітньо-професійної програми Комп'ютерна інженерія

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Дмитро ГОРДІЄНКО*

Виконав	*Дмитро ГОРДІЄНКО*
Керівник	*Наталія ЛАЩЕВСЬКА*
Рецензент	

Київ 2024

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 74 стор._20, рис., 4 табл., 9 джерел.

У роботі вирішено завдання розроблення рекомендацій щодо віртуальних приватних мереж на основні порівняльного аналізу за вибраними критеріями.

Проведено дослідження особливостей побудови віртуальних приватних мереж як об'єктів створення захищеної інформаційно-комунікаційної системи організації: варіантів побудови віртуальних захищених каналів, засобів забезпечення безпеки VPN, у тому числі на канальному рівні та на мережному рівні.

Проведено обґрунтування основних критеріїв вибору конфігурації та методів побудови віртуальної приватної мережі організації на основі політики безпеки та виявлено дві групи критеріїв: До першої групи критеріїв пропонується віднести: критерії сертифікації, критерій стандартизації/сумісності, критерій продуктивності/надійності, критерій наявності системи діагностики, критерій пріоритету трафіку, критерій можливості роботи з частиною інформаційних потоків без шифрування, критерій масштабованості VPN. До другої групи критеріїв може бути віднесена робота з криптографічними ключами та підтримки роботи центру сертифікації ключів. До додаткових критеріїв вибору можна віднести остаточну вартість VPN, наявність технічної підтримки та гарантійного обслуговування, а також адаптованого до умов використання програмного забезпечення та технічної документації.

Наведені рекомендації щодо реалізації віртуальної приватної мережі організації із заданими характеристиками за допомогою протоколів IPSec та Open VPN.

Результати виконаної роботи можуть бути використані при виборі та впровадженні VPN в інформаційно-комунікаційні системи підприємств (організацій).

КЛЮЧОВІ СЛОВА: автентифікація, авторизація, алгоритм шифрування, віртуальна приватна мережа, гешування, домен, мережа, міжмережний екран, політика безпеки, обмін ключами, сертифікат, тунелювання.

ЗМІСТ

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

БД – база даних

ЗОТ – засоби обчислювальної техніки

ІБ – інформаційна система

КІС – корпоратива інформаційна система

ЛОМ – локальна обчислювальна мережа

МЕ – міжмережий екран

НСД – несанкціонований доступ

ОС – операційна система

ПБ – політика безпеки

ПЗ – програмне забезпечення

DMZ – Demilitarized Zone

IDS – Intrusion Detection System

IETF – Internet Engineering Task Force

LAN – local area network

NAT – Network Address Translation

SPI – Security Parameters Index

TTL – Time to live

ВСТУП

Ефективне управління великою компанією з наявністю віддалених структурних підрозділів здійснюване тільки в разі узгодженості дій між центральним офісом та її віддаленими підрозділами. На сьогодні це можливо тільки при використанні можливостей глобальної мережі Інтернет. Інтернет сьогодні є одночасно - інформаційним полем спілкування, сферою управління, як загально-громадськими питаннями так і військовими, а також є активним споживчим ринком, товарною і валютною біржею. Так як сучасна адміністративна інфраструктура компаній є дуже розгалуженої та розосередженою географічно, створення достатньо захищеної корпоративної мережі обміну інформаційними ресурсами стало складнішим завданням.

Розвиток технологій глобальної інформаційної інфраструктури і, зокрема, мережі Інтернет, потребує необхідності безпеки інформаційних ресурсів, які передаються за допомогою розподіленої корпоративної мережі відкритого доступу. Інтернет є незахищеною мережею, тому є необхідність застосовувати способи захисту конфіденційних даних, які передаються по відкритих каналах незахищеної мережі.

Для ефективної протидії атакам на інформаційні потоки в мережах і забезпечення можливості безпечного використання відкритих мереж, активно розвивається концепція створення віртуальних приватних мереж - VPN (Virtual Private Network).

У основі концепції побудови віртуальних мереж VPN лежить необхідність побудови віртуального захищеного тунелю для забезпечення захисту інформаційних потоків, конфіденційності і цілісності інформації, яка передається відкритими каналами. Доступ до цього віртуального тунелю має бути максимально ускладнений для всіх можливих небажаних користувачів.

VPN – це технологія, яка об'єднує довірені мережі, вузли і користувачів через відкриті мережі, яким «немає довіри». На мій погляд, це найбільш яскравий образ технології, яка набуває все більшого поширення не тільки серед

технічних фахівців, але і серед користувачів, яким також потрібно захищати свою інформацію. Зважаючи на це, можна зробити висновок, що тема дипломної роботи, присвячена аналізу технологій побудови віртуальних приватних мереж, є актуальною.

РОЗДІЛ 1. Віртуальні приватні мережі, як засоби захищеної інформаційно-комунікаційної системи організації.

1.1. Основні поняття і функції мережі VPN

Абревіатура VPN розшифровується як Virtual Private Network - віртуальна приватна мережа. У цій розшифровці частково закладено принцип роботи технології. Мережа "віртуальна", тому що створена на основі вже існуючих мереж, а "приватна" тому, що доступ до неї отримує обмежена кількість користувачів. Дані всередині мережі шифруються, і ключ до цього шифру отримують тільки її учасники. Спочатку ця технологія розроблялася для потреб великих компаній, щоб об'єднувати розрізнені локальні мережі в єдиний, безпечний для зламування ззовні, мережний простір.

Принцип роботи VPN заснований на двох "китах":

- використання сервера-посередника для анонімізації;
- тунелювання даних, що передаються і приймаються.

Звучить досить складно, але, на практиці, це має такий вигляд: між користувачем та умовним "інтернетом" знаходиться сервер-посередник, щоб приховати вашу IP-адресу (у цій частині технологія працює аналогічно проксі-серверу, про який ми розповімо наприкінці статті). Цей сервер-посередник бере ваш запит, підміняє вашу мережну адресу і передає запит на цільовий інтернет-ресурс, а потім приймає від нього отримані дані. Пакет даних, якими обмінюється сервер-прокладка з інтернетом від вашого імені, надсилається не у вихідному вигляді, а зашифрованим. Ключ до цього шифру, при цьому, доступний тільки власнику VPN. Тобто шифрування створює своєрідний "тунель" або виділений канал для ваших даних, захищаючи їх від витоку.

Отже, суть технології доволі проста, проте сама вона доволі складна в реалізації, бо потребує певних ресурсів для організації тунелювання даних за таким алгоритмом:

- шифрування запиту;

- його відправлення на сервер-прокладку;
- дешифрування запиту на сервері;
- надсилання дешифрованого запиту на цільовий інтернет-ресурс;
- отримання відповіді від інтернет-ресурсу і повторення всіх цих дій у зворотному порядку.

Забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті мережі, зокрема через мережу Інтернет, можливо шляхом ефективного вирішення наступних завдань:

- Забезпечення анонімності та конфіденційності в мережі. VPN приховує точку входу в мережу і шифрує вихідний трафік. У підсумку до нього не можуть отримати доступ ні зловмисники, ні навіть провайдер Інтернету. Водночас користувач може визначити кому надати доступ до зашифрованої інформації - надаючи ключ до неї;
- Обхід цензури та фаєрволів. VPN дає змогу обійти встановлені адміністратором мережі обмеження;
- Обхід контентних обмежень. За допомогою VPN можна отримати доступ до контенту, обмеженого за географічною або іншими ознаками;
- Безпечне підключення до громадських мереж. Заходячи в громадські Wi-Fi-мережі через VPN забезпечується безпека даних;
- Захист від онлайн-загроз. Шифрування переданих даних захищає їх від прямого злому хакерами, фішингу даних або від DDoS атак;
- Захист від стеження. Якщо захищений канал передавання даних не можна зламати, то й відстежувати будь-які дії онлайн неможливо;
- Забезпечення безпечного доступу до віддалених ресурсів. Сьогодні він дає змогу співробітникам великих компаній працювати в захищених мережах із будь-якої точки світу;
- Забезпечення захищеного зв'язку. Забезпечує повну конфіденційність обміну даними між організаціями та фізичними особами.

Локальні мереж та окремі комп'ютери захищені від несанкціонованих дій із зовнішнього середовища міжмережними екранами (МЕ). МЕ, які розташовані

між локальною і відкритою мережею, шляхом фільтрації двостороннього потоку повідомлень підтримують безпеку інформаційного обміну, фільтруючи двосторонній потік повідомлень та виконують функції посередництва під час обміну інформацією. На окремому віддаленому комп'ютері, який з'єднаний з відкритою мережею можливе встановлення програмного забезпечення (ПЗ) міжмережного екрану і тоді такий міжмережний екран називається персональним.

Передача інформації з використанням відкритих каналів Інтернет потребує захисту. Для цього використовуються захищені віртуальні приватні мережі (VPN), що є об'єднанням локальних мереж і окремих комп'ютерів, через відкрите зовнішнє середовище передачі інформації, в єдину віртуальну корпоративну мережу, яка забезпечує безпеку циркулюючих в ній інформаційних потоків.

Формування віртуальної захищеної мережі VPN здійснюється шляхом побудови віртуальних захищених каналів, на базі відкритих каналів зв'язку загальнодоступної мережі Інтернет.

Ці захищені канали називаються тунелями VPN за допомогою яких, відповідно, в мережі VPN відбувається з'єднання головного офісу компанії з офісами філій, офісами бізнес-партнеров і віддалених користувачів з можливістю безпечного передаванням інформаційних потоків через відкриту мережу Інтернет (рисунок 1.1).

Тунель VPN - це віртуальне зашифроване стійким алгоритмом з'єднання, по якому з використанням відкритої мережі Інтернет передаються криптографічно захищені пакети повідомлень віртуальної мережі. Наочно, його можна представити у вигляді непрозорої труби, а ще краще тунелю, один кінець якого впирається в комп'ютер рядового користувача, а другий в спеціалізований сервер, що знаходиться, як правило, в іншій країні.

Тунель VPN, який сформований пристроями VPN, володіє властивостями захищеної виділеної лінії, в рамках загальнодоступної мережі.

Захист інформаційних потоків при передачі їх по тунелю VPN заснований:

- на автентифікації абонентських сторін;
- криптографічному закритті даних;
- контролі достовірності і цілісності інформації, що доставляється.

При реалізації цих функцій використовуються криптографічні методи захисту інформації. Ефективність захисту досягається за рахунок сумісного використання симетричних і асиметричних криптографічних систем. Залежно від застосовуваних протоколів і призначення, VPN може забезпечувати з'єднання трьох видів: вузол-вузол, вузол-мережа та мережа-мережа. Засоби VPN можуть відігравати у віртуальних мережах роль VPN-клієнта, VPN-сервера або шлюзу безпеки VPN.

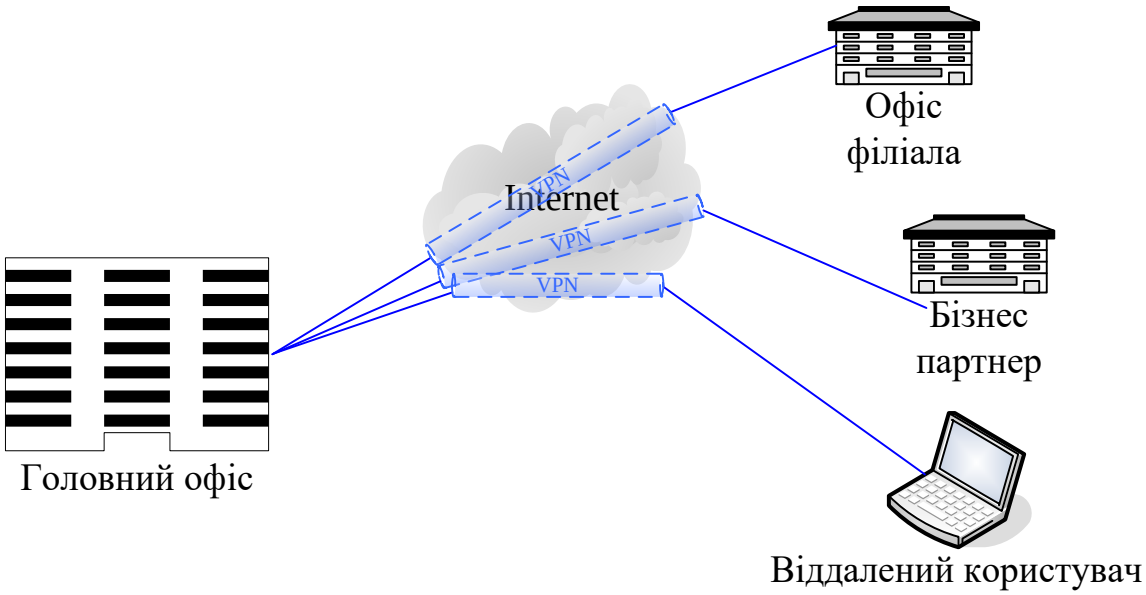

Рис. 1.1. Захищена віртуальна приватна мережа VPN

VPN-клієнт це програмно-апаратний чи програмний комплекс на базі персонального комп'ютера, мережне ПЗ якого модифікується для виконання шифрування і автентифікації трафіку, за яким цей пристрій працює з іншими VPN-клієнтами, шлюзами безпеки VPN або VPN-серверами. Як правило, реалізація VPN-клієнта є програмним рішенням, доповнюючим стандартну операційну систему (ОС), - Windows XP/7 або Unix подібну.

VPN-сервер є програмним або програмно-апаратним комплексом на базі

комп'ютера, який виконує функції сервера.

VPN-сервер виконує функцію захисту серверів від несанкціонованого доступу із зовнішніх мереж та забезпечує захищені з'єднання з комп'ютерами сегментів локальних мереж, окремими комп'ютерами. VPN-сервер також може підтримувати захищені з'єднання з користувачами мобільних абонентських систем.

Шлюз безпеки VPN (security gateway) - це мережний пристрій, що виконує функції шифрування і автентифікації для хостів, розташованих за ним. Шлюз безпеки VPN призначений для внутрішньої корпоративної мережі та розміщається так, щоб через нього проходив весь трафік цієї мережі. Шлюз безпеки VPN може бути реалізований програмним рішенням, окремим апаратним пристроєм, маршрутизатором або МЕ, доповнених функціями VPN.

Зовнішні мережі передачі інформації включають, як канали швидкісної передачі даних (мережа Інтернет) так і повільніші загальнодоступні канали зв'язку (канали телефонної мережі). Ступінь захищеності інформації у відкритих каналах зв'язку визначає ефективність віртуальної приватної мережі VPN.

Між відправником і одержувачем даних встановлюється своєрідний тунель - логічне з'єднання, яке дозволяє інкапсулювати дані одного протоколу в пакети іншого.

1.2. Варіанти побудови віртуальних захищених каналів

Безпека процесу інформаційного обміну забезпечується як при об'єднанні локальних мереж, так при доступу до них віддалених або мобільних користувачів. Основними схемами при проектуванні VPN є:

1. віртуальний захищений канал між локальними мережами;
2. віртуальний захищений канал між вузлом (користувачем) і локальною мережею (рис. 1.2).

За схемою 1 з'єднання створюються постійно доступні захищені канали між локальними мережами, де шлюз безпеки служить інтерфейсом між

тунелем і ЛОМ для спілкування користувачів один з одним..

За схемою 2 захищені канали VPN використовуються для з'єднань з віддаленими або мобільними користувачами. Ініціатором тунелю є клієнт (віддалений користувач), який для зв'язку зі шлюзом, що захищає віддалену мережу запускає на своєму комп'ютері спеціальне клієнтське ПЗ.

Цей вид VPN може використовуватися разом з традиційними методами віддаленого доступу та замінювати собою комутовані з'єднання.

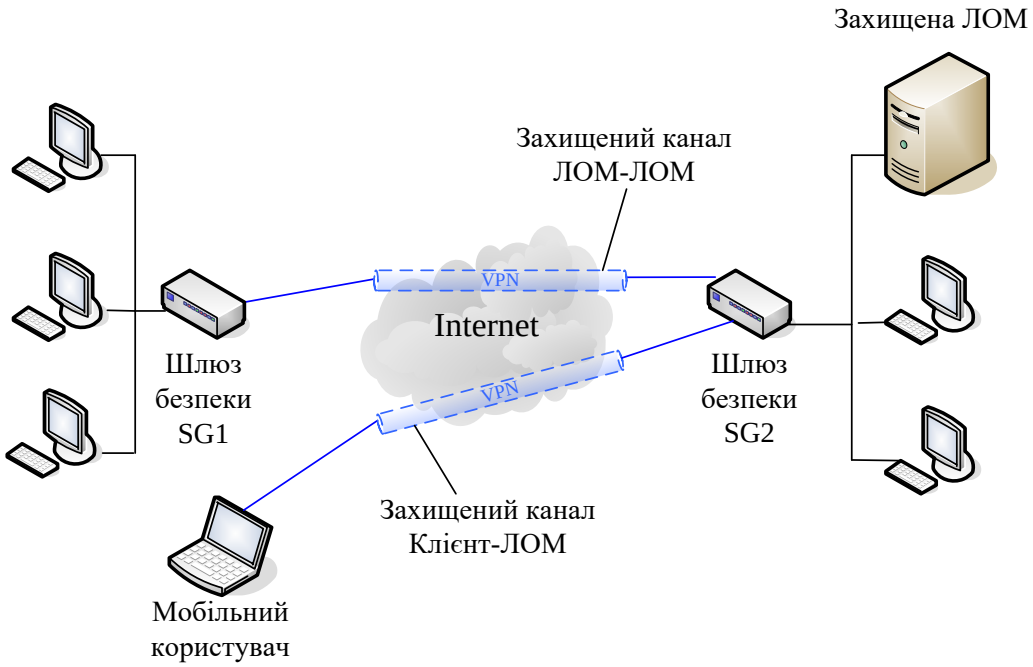

Рисунок 1.2. Віртуальні захищені канали типу ЛОМ-ЛОМ і КЛІЄНТ-ЛОМ

Якщо трафік для локальної мережі в складі віртуальної мережі не потребує захисту, то в цьому випадку кінцевим пунктом захищеного тунелю вибирається МЕ або прикордонний маршрутизатор цієї локальної мережі.

При необхідності захисту локальної мережі кінцевою точкою тунелю в цій мережі має бути комп'ютер, що бере участь у взаємодії захисту. При доступі до ЛОМ віддаленого користувача його комп'ютер має бути кінцевою точкою віртуального захищеного каналу.

Поширеним є варіант, коли захищений тунель створюється всередині відкритої мережі з комутацією пакетів. Позитив цього варіанту - зручність застосування, а негатив - порівняно низький рівень безпеки. Кінцевими

точками такого тунелю є провайдери Інтернету чи прикордонні маршрутизатори (міжмережні екрани) локальної мережі.

Віддалений доступ до локальної мережі потребує створюється тунелю між сервером провайдера віддаленого доступу та прикордонним провайдером чи маршрутизатором (МЕ) локальної мережі.

Створені за таким варіантом VPN мають добру масштабованість і керованість. Сформовані при цьому захищені тунелі повністю прозорі для комп'ютерів клієнтів і серверів локальної мережі в складі віртуальної мережі. ПЗ цих вузлів залишається без змін.

Однак цей варіант характеризується низьким рівнем безпеки інформаційної взаємодії, так як трафік частково проходить відкритими каналами зв'язку не захищеним.

В процесі створення захищеного тунелю беруть участь компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти називають *ініціатором* тунелю і *термінатором* тунелю.

Функції *ініціатора тунелю* полягають в процесі інкапсуляції початкового пакету в новий пакет з новим заголовком, в якому міститься інформація про відправника і одержувача. Інкапсульовані пакати можуть належати до протоколів будь-якого типу. Маршрут між ініціатором і термінатором визначає звичайна мережа IP, що підлягає маршрутизації.

Ініціювати і розривати захищений тунель можливо різними мережними пристроями і ПЗ, а саме: ноутбуком мобільного користувача, обладнаним модемом і відповідним ПЗ; маршрутизатором локальної мережі з наділеними відповідними функціями. Тунель закінчується шлюзом провайдера послуг або комутатором мережі.

Функції *термінатора тунелю* полягають в зворотньому процесі інкапсуляції, коли видаляються нові заголовки і кожен початковий пакет направляється адресатові в локальній мережі.

Шляхом шифрування пакетів, що інкапсулюються забезпечується їх конфіденційність, а цілісність і достовірність - формуванням електронного

цифрового підпису. Зважаючи на безліч методів і алгоритмів криптозахисту даних, необхідне своєчасне, погодження та використання ініціатором і термінатором тунелю, одних і тих же методів і алгоритмів захисту та підтримка функції безпечного обміну ключами.

Спектр різновидів віртуальних приватних мереж варіює від провайдерських мереж, до корпоративних мереж VPN, які розгортаються і керуються самими компаніями. Виділяються три основні види віртуальних приватних мереж:

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

VPN з віддаленим доступом (рис.1.3) за принципом їх роботи не складні. Після встановлення з'єднання з територіальною точкою доступу до глобальної мережі виклики користувачів тунелюються через інтернет, *потім всі виклики концентруються на відповідних* вузлах і спрямовуються в корпоративні мережі.

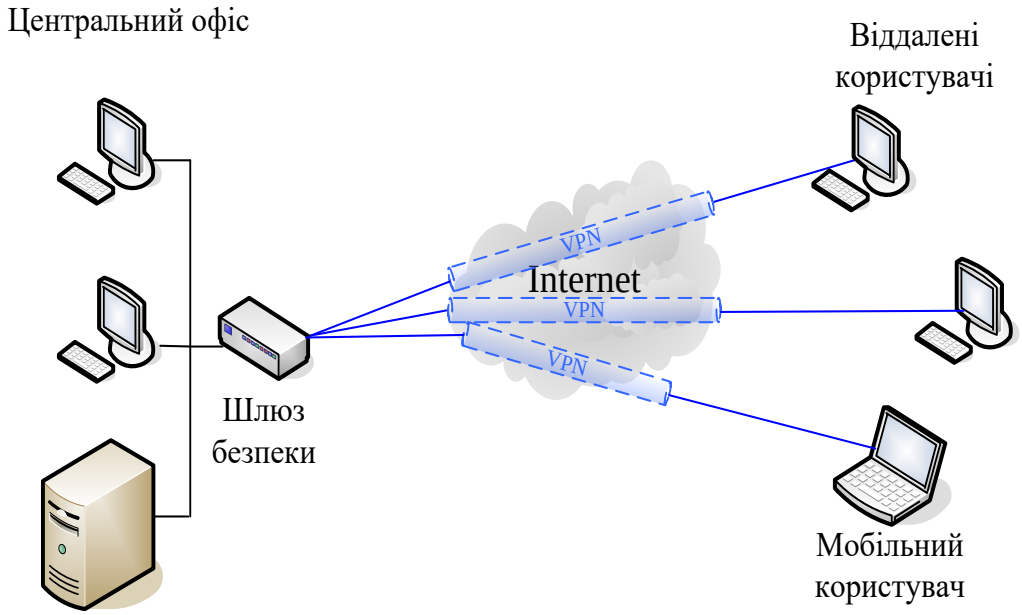

Рис.1.3. Віртуальна приватна мережа з віддаленим доступом

Внутрішньокорпоративні мережі (Intranet VPN) (рис.1.4) створюються з використанням Internet або розділеними сервіс-провайдерами мережними інфраструктурами. Компанії відмовляються від дорогих виділених ліній, заміняючи їх дешевшим зв'язком через Internet. Це значно скорочує витрати на використання смуги пропускання, так як в Internet відстань не впливає на вартість з'єднання.

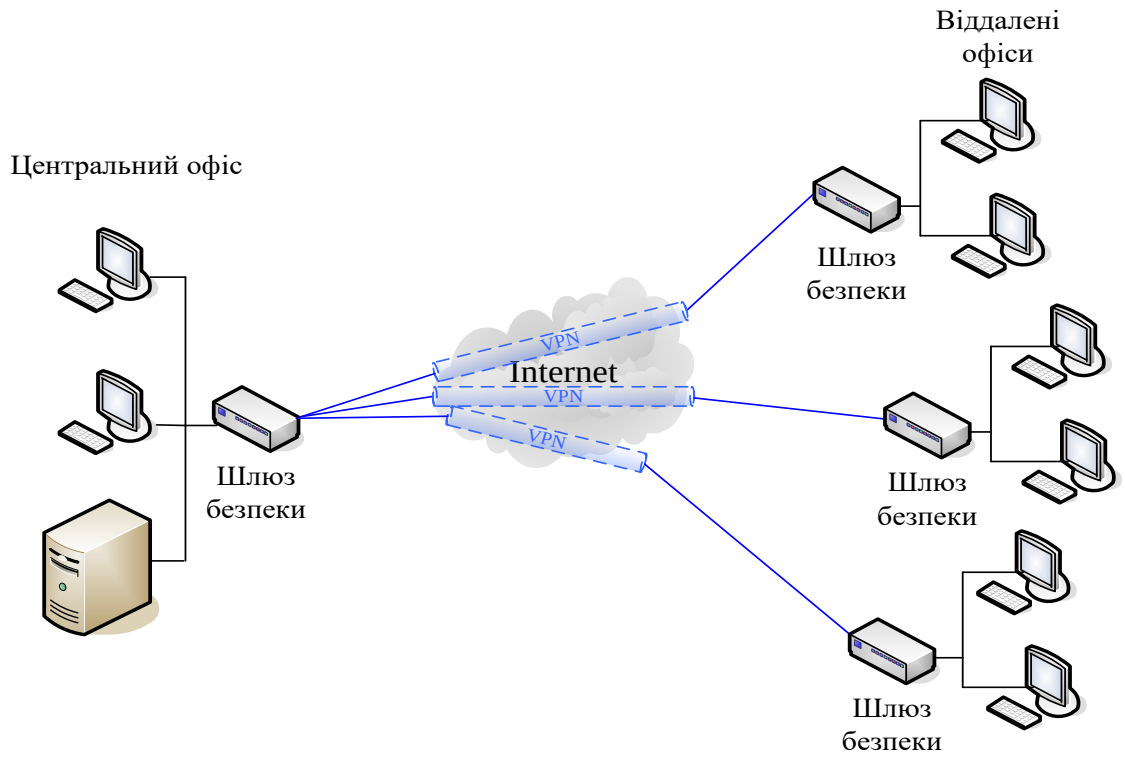

Рис. 1.4. З'єднання вузлів мережі за допомогою технології Intranet VPN

Створення Intranet VPN, з використанням Internet, це найбільш рентабельний спосіб реалізації VPN-технології. Однак в Internet рівні сервісу не завжди гарантуються. Для гарантії рівня сервісу, необхідно розглядати можливість розгортання своїх VPN з використанням мережних інфраструктур розділених сервіс-провайдерами.

Міжкорпоративна мережа VPN (Extranet VPN) (рис. 1.5) - є мережною технологією із забезпеченням прямого доступу між мережами двох компаній, що таким чином, підвищує надійність зв'язку в ході ділової співпраці.

Мережі Extranet VPN схожі на внутрішньокорпоративні VPN з різницею в тому, що проблема захисту інформації для мережі Extranet VPN є гострішою.

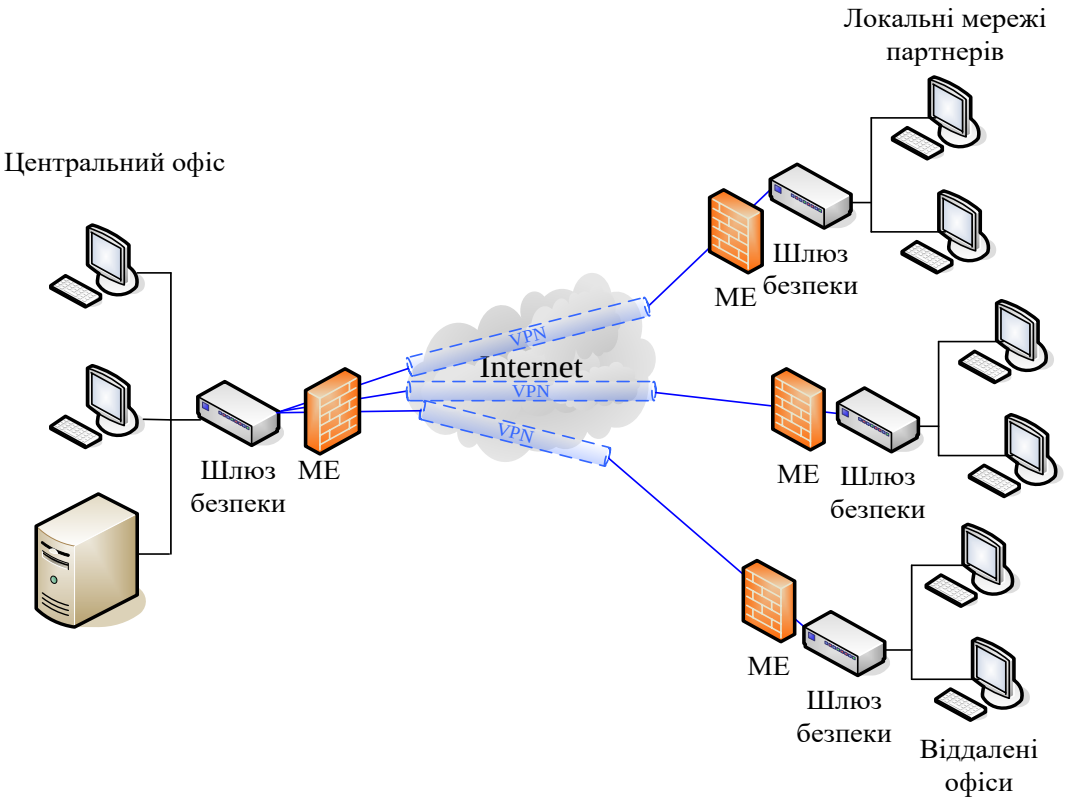

Рисунок 1.5. Міжкорпоративна мережа Extranet VPN

Для з'єднання Extranet VPN використовуються ті ж архітектура і протоколи, які застосовуються при реалізації Remote Access VPN і Intranet VPN. Основною відмінністю є дозвіл доступу, який надається користувачам Extranet VPN пов'язаний з мережею їх партнера.

В даний час спостерігається тенденція до конвергенції різних способів реалізацій VPN.

1.3. Обгрунтування основних критеріїв вибору конфігурації та методів побудови VPN організації.

1.3.1. Формування політики безпеки віртуальних приватних мереж

Важливою складовою частиною політики безпеки є мережна політика безпеки або політика мережного підключення. Політикою мережного підключення повинні бути визначені типи пристроїв, дозволені для підключення до мережі. У ній повинні бути детально визначені настройки систем, які дозволено підключати до мережі. Ця політика може включати наступні розділи:

- опис процесу установки і налагодження операційної системи (ОС) і додатків, а також їх функціональних можливостей, які дозволено використовувати;
- місцеположення в мережі (фізичній підмережі) систем визначеного типу і процедура вирішення питань адресації в мережі;
- вимога про установку і регулярне оновлення антивірусного ПЗ;
- опис налаштування прав користувачів і захисту ресурсів, забезпечуваних ОС;
- процедури, яким необхідно слідувати для створення нового облікового запису користувача, і аналогічні процедури для його видалення;
- заборона на установку додаткових апаратних або програмних компонентів без схвалення мережного адміністратора (або іншої відповідальної особи).

При створенні мережної ПБ необхідно визначити процедури захисту власної мережі, її вмісту і користувачів від збитку і втрат. З цієї точки зору мережна ПБ грає роль проведення в життя загальної ПБ, визначеної в організації. Мережна ПБ концентрується на контролі мережного трафіку і його використанні. Вона визначає мережні ресурси і загрози, використання і можливості мережі, а також детальні плани дій при порушенні ПБ.

При застосуванні мережної ПБ необхідно стратегічно реалізувати захисні межі всередині власної мережі. Ці стратегічні межі називаються мережними периметрами. Встановлюючи рівні безпеки мережних периметрів, можна здійснювати множинний контроль безпеки мережного трафіку.

Для встановлення мережних периметрів необхідно визначити комп'ютери, що захищаються і мережі, а також визначити захисні механізми для них. Одним з основних таких елементів є міжмережний екран. Щоб встановити правильний периметр безпеки, міжмережний екран (МЕ) повинен бути шлюзом для всіх з'єднань між довіреними мережами, не довіреними і невідомими.

Довіреними мережами є мережі всередині мережного периметру безпеки. Під довіреними мережами розуміються мережі, над якими фахівці організації мають повний адміністративний контроль. При установці МЕ необхідно точно ідентифікувати типи мереж, які приєднуються до МЕ за допомогою мережних адаптерів. Після початкової конфігурації довірені мережі включають МЕ і всі мережі позаду нього.

Недовіреними мережами є мережі, які знаходяться поза встановленим мережним периметром. При установці МЕ необхідно також точно визначити недовірені мережі, від яких МЕ може допускати запити.

Невідомими мережами є мережі, які не є ні довіреними, ні недовіреними. Невідомі мережі існують поза периметром безпеки (за замовчуванням всі недовірені мережі розглядаються як невідомі).

Кожна мережа може містити безліч внутрішніх периметрів. Щоб зрозуміти, як мережні периметри розташовуються щодо один одного, розглянемо два типи мережних периметрів: зовнішній і внутрішній.

У простому випадку мережний периметр організації включає зовнішній і внутрішній периметри (рисунок 1.6).

Зовнішній мережний периметр ідентифікує точку розділення між пристроями, які контролюються, і тими, які не контролюються. Зазвичай цією точкою є маршрутизатор, який використовується для розділення власної мережі від мережі провайдера Інтернету.

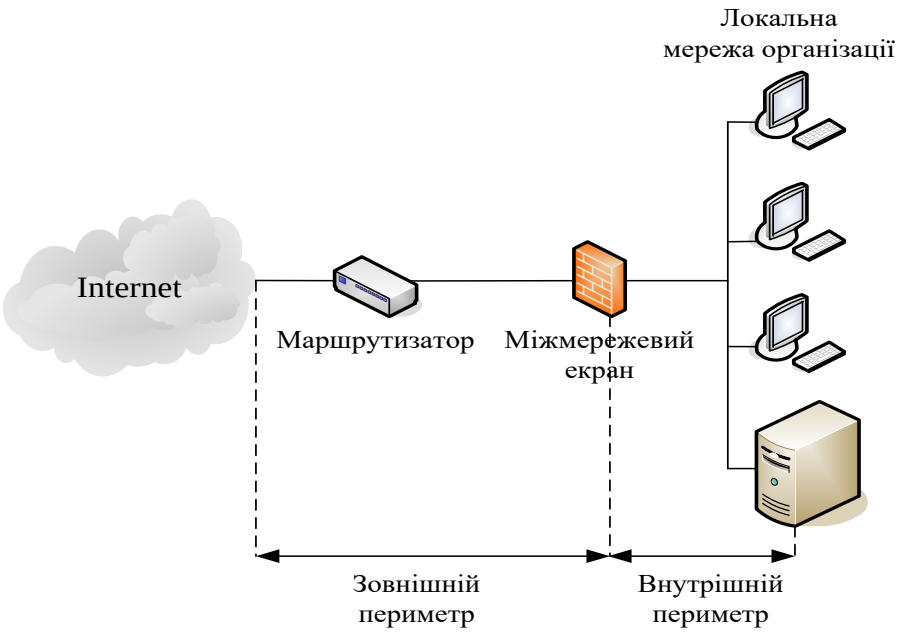

Рисунок 1.6. Мережний периметр організації.

Внутрішній мережний периметр є додатковими межами, в яких розміщуються інші механізми безпеки, такі як МЕ і фільтруючі маршрутизатори. У цьому випадку зовнішній і внутрішній периметри визначені розміщенням зовнішнього і внутрішнього маршрутизаторів і МЕ. Розташування МЕ між внутрішнім і зовнішнім маршрутизаторами дає найбільший додатковий захист від атак з обох боків, але значно зменшує трафік, який повинен досліджувати МЕ, оскільки йому не потрібно проглядати пакети, циркулюючі у внутрішній мережі.

З погляду користувачів зовнішніх мереж МЕ представлений всіма комп'ютерами довіреної мережі. Він визначає центральну точку, через яку повинні проходити всі з’єднання між двома мережами.

Зовнішній мережний периметр є найбільш небезпечною областю мережної інфраструктури організації. Зазвичай ця область призначається для маршрутизаторів, МЕ і загальнодоступних інтернет-серверів, таких як HTTP, FTP або e-mail. Оскільки до цієї області легко дістати доступ, вона часто атакується (зазвичай для того, щоб через неї дістати доступ до внутрішньої

мережі). Тому критичні дані, призначені тільки для внутрішнього використання, не повинні знаходитись в зовнішньому мережному периметрі.

Можна використовувати безліч внутрішніх МЕ для побудови безлічі внутрішніх мережних периметрів (рисунок 1.7).

Використання внутрішніх міжмережних екранів дозволяє обмежити доступ до спільно використовуваних внутрішніх ресурсів мережі.

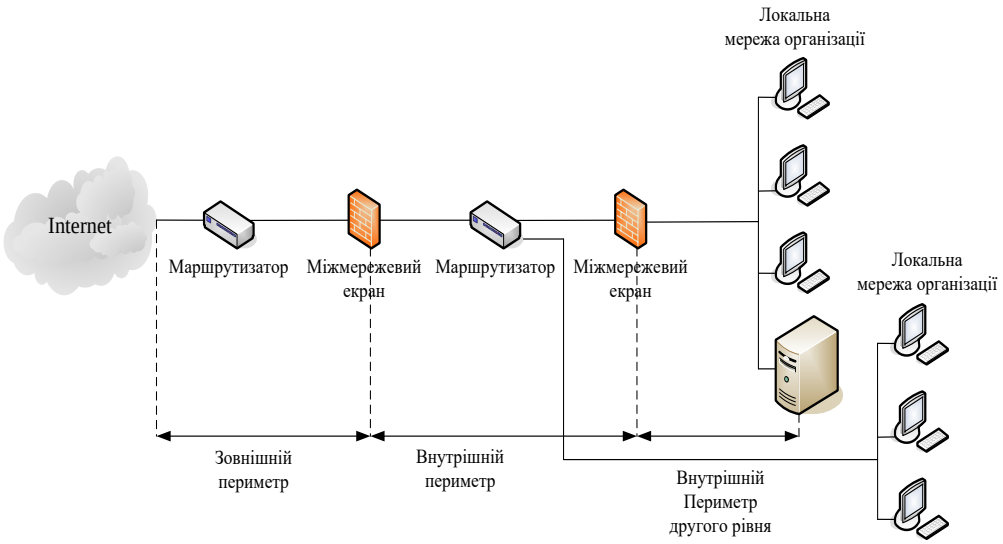

Рисунок 1.7 Декілька внутрішніх мережних периметрів.

Область зовнішнього мережного периметра називають демілітаризованою зоною (Demilitarized Zone, DMZ). Демілітаризована зона — по міжнародному праву територія, на якій ліквідовані військові зміцнення і споруди, заборонене утримання збройних сил.

Оскільки абревіатура DMZ прижилася в Інтернеті і комп'ютерних публікаціях, будемо використовувати її.

Основним недоліком використання Інтернету для з’єднання ЛОМ є відсутність конфіденційності даних, передаваних по Інтернету між ЛОМ, а також існує можливість підміни пакетів та інших атак.

Питання безпеки не є єдиним при взаємодії ЛОМ з Інтернетом. Інтернет не забезпечує належної пропускної спроможності та надійності каналу і це

залежить від окремих маршрутизаторів та загального стану мереж з яких складається Інтернет.

Для забезпечення безпеки *VPN* використовують шифрування. В залежності від загального рівня безпеки системи до VPN висуваються наступні вимоги:

Середній рівень безпеки. Віртуально приватними мережами між ЛОМ не мають передаватися критично важливі інформаційні ресурси при недостатньому рівні безпеки. Для такої передачі використовуються інші способи.

Високий рівень безпеки. Для організації віртуальних приватних мереж при використанні Інтернету між ЛОМ необхідно забезпечити можливість швидкого створення резервного каналу для передачі інформаційних ресурсів у разі тимчасової неможливості передачі через Інтернет.

За допомогою VPN наразі створюється одна мережа з декількох незалежних мереж. Загальна безпека VPN буде відповідати безпеці найменш захищеної ЛОМ.

1.3.2. Основні критерії вибору VPN.

Велика кількість рішень, що забезпечують побудову віртуальних приватних мереж, призводить до підвищення актуальності проблеми розробки критеріїв їх вибору та реалізації [8].

В даній дипломній роботі будемо керуватися ключовими факторами для вибору і реалізації VPN якими є: реалізований протокол захищеного інформаційного обміну та організація роботи з ключовою інформацією.

До першої групи критеріїв пропонується віднести.

Критерії сертифікації, що передбачає насамперед: наявність сертифікату на криптоядро; легітимність ввезення обладнання, що містить функції шифрування на територію держави; сертифікацію засобу захисту (виробу цілком, а не його окремих компонент).

Критерій стандартизації/сумісності. Стандартизовані VPN значно спрощують проблему сумісності з інформаційно-комунікаційною

інфраструктурою: комунікаційним обладнанням, програмними застосуваннями, системою управління мережею.

Критерій продуктивності/надійності є дуже значимим при виборі VPN тому, що продуктивності часто завищують в рекламних проспектах. Тому застосування цього критерію потребує порівняльних випробувань, а також передбачення можливості резервування.

Критерій наявності системи діагностики, яка використовується для пошуку і усунення помилок, викликаних, найчастіше, як неправильною конфігурацією системи, так і помилками розробників.

Критерій пріоритету трафіку, який забезпечить не тільки захист передавання даних, але й мультимедійних сервісів, що реалізовані у цій же інфраструктурі.

Критерій можливості роботи з частиною інформаційних потоків без шифрування використовується, якщо частина інформаційних потоків спрямовується у зовнішній інформаційний простір без шифрування. У протилежному випадку прийдеться організовувати доступ до цих ресурсів в обхід засобів захисту, що може створити додаткові загрози інформаційним ресурсам.

Критерій масштабованості VPN може передбачати мінімальну та максимальну кількість встановлених пристроїв та кількість абонентів підключатися до одного сервера доступу.

До другої групи критеріїв може бути віднесена робота з криптографічними ключами та підтримки роботи центру сертифікації ключів.

При цьому важливим показником є зручність і безпечність роботи з криптографічними ключами: система повинна дозволяти управляти ключами в ручному, автоматичному та напівавтоматичному режимах. Якщо інфраструктура відкритих ключів уже існує, то важливо її використати у створюваній VPN.

До додаткових критеріїв вибору можна віднести остаточну вартість VPN, наявність технічної підтримки та гарантійного обслуговування, а також

адаптованого до умов використання програмного забезпечення та технічної документації.

Одержані таким чином критерії вибору та реалізації VPN можуть бути покладені в основу формалізованих методик щодо реалізації VPN різноманітних організацій та установ.

1.4. Класифікація та основні варіанти архітектури мереж VPN

Найчастіше використовуються різні ознаки класифікації VPN:

- «робочий» рівень моделі OSI;
- спосіб технічної реалізації VPN.

Класифікація VPN по «робочому» рівню моделі OSI

Для безпечної передачі даних по загальнодоступній (незахищеній) мережі застосовують узагальнену назву - захищений канал. Його можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI (таб. 1.1).

Таблиця 1.1 Моделі взаємодії відкритих систем OSI

Протоколи захищеного доступу	Прикладний	Впливають на додатки
	Представлення	
	Сеансовий	
	Транспортний	
	Мережний	Прозорі для додатків
	Канальний	
	Фізичний	

За ознакою «робочого» рівня моделі OSI розрізняють наступні групи VPN: VPN канального, мережного та сеансового рівнів.

VPN канального рівня. Засоби віртуальних приватних мереж, які використовуються на канальному рівні моделі OSI надають змогу забезпечувати інкапсуляцію трафіків третього рівня різних видів, та побудову віртуальних

тунелів від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу локальної мережі.

VPN мережного рівня. VPN-продукти мережного рівня виконують інкапсуляцію IP в IP. Самим відомим протоколом цього рівня є протокол IPSec (IP Security), який призначений для тунелювання, автентифікації та шифрування IP-пакетів.

Також з цим протоколом пов'язаний протокол IKE (Internet Key Exchange), який слугує для вирішення завдання безпечного управління і обміну криптографічними ключами між віддаленими пристроями.

VPN сеансового рівня. На цьому рівні може використовуватись дещо інший підхід під назвою «посередники каналів» (circuit proxy). Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо.

Класифікація VPN за способом технічної реалізації

Характеристики і конфігурація віртуальної приватної мережі також визначаються типом пристроїв, які використовуються у VPN.

VPN розрізняють за способом технічної реалізації на основі:

- маршрутизаторів;
- міжмережних екранів;
- програмних рішень;
- спеціалізованих апаратних засобів з вбудованими шифропроцесорами.

VPN на основі маршрутизаторів. При даному способі побудови VPN маршрутизатори застосовуються для створення захищених каналів. Так як вся інформація з локальної мережі проходить через маршрутизатор, то на нього покладається і завдання шифрування. Прикладом устаткування для віртуальних приватних мереж на маршрутизаторах є пристрої компанії Cisco Systems.

VPN на основі міжмережних екранів. Міжмережні екрани підтримують функції тунелювання і шифрування даних. Використання МЕ на базі ПК підходить тільки для невеликих мереж з невеликим обсягом передаваної інформації. Висока вартість рішення в перерахунку на одне робоче місце і

залежність продуктивності від апаратного забезпечення, на якому працює МЕ є недоліками цього методу.

VPN на основі програмного забезпечення. VPN-продукти, які реалізовані програмним способом поступаються спеціалізованим пристроям, однак володіють достатньою потужністю для реалізації VPN-мереж. В разі віддаленого доступу вимоги до необхідної смуги пропускання невеликі. Тому програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Гнучкість і зручність в застосуванні та відносно невисока вартість є перевагою програмних продуктів.

VPN на основі спеціалізованих апаратних засобів. Головною перевагою віртуальних приватних мереж на основі спеціалізованих апаратних засобів є висока продуктивність, так як швидкодія обумовлена тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Недолік – висока вартість.

Основні способи використання архітектури мереж VPN

Використовуючи VPN, організація може допомогти захистити приватний мережний трафік незахищеною мережею, такою як Інтернет. VPN можна використовувати для доступу до веб-сайтів, обмежених по регіону, для захисту вашого браузера від зацікавлених очей на громадському Wi-Fi і т.д.

VPN допомагає забезпечити безпечний механізм шифрування та інкапсуляції приватного мережного трафіку та переміщення його через проміжну мережу. Дані зашифровуються для забезпечення конфіденційності, а пакети, які можуть бути перехоплені у спільній або загальнодоступній мережі, нерозбірливі без правильних ключів шифрування. Дані також інкапсульовані або загорнуті в заголовок IP, що містить інформацію про маршрутизацію.

VPN допомагають користувачам, які працюють вдома, в дорозі або у філії, безпечно підключатися до віддаленого корпоративного серверу за допомогою Інтернету. З точки зору користувачів VPN є двоточковим з'єднанням між комп'ютером користувача і корпоративним сервером. Характер проміжної

мережі, Інтернету, не має відношення до користувача, оскільки він виглядає так, ніби дані відправляються виділеним приватним лінком.

Існує кілька способів використання VPN. Найпоширеніший сценарій – це коли віддалений користувач звертається до приватної мережі через Інтернет за допомогою VPN-з'єднання віддаленого доступу. В іншому випадку віддалений офіс підключається до корпоративної мережі, використовуючи або постійне або site-to-site VPN-з'єднання (також відоме як VPN-з'єднання маршрутизатор-маршрутизатор). Кожен із цих сценаріїв VPN може бути розгорнутий для забезпечення підключення через загальнодоступну мережу, таку як Інтернет, або через приватну інтрамережу.

З'єднання VPN також можуть бути розгорнуті в сценарії екстрамережі для безпечної взаємодії з діловими партнерами. Екстранет функціонує як інтрамережа, яка може бути надійно поділена з призначеним діловим партнером. Завдяки підключенню віддаленого доступу та з'єднання "site-to-site", VPN дозволяє організації замінювати міжміські або лізингові лінії локальним набором або виділеними лініями постачальнику послуг Інтернету (ISP).

Основні компоненти VPN:

Протоколи безпеки. VPN використовують протокол безпеки, який захищає будь-яку інформацію через сервер. Цей протокол створює безпечне з'єднання, а також впливає на тип шифрування, який використовує VPN. Хоча протоколи безпеки не такі добрі, як справжня приватна мережа (або фізичний кабель). Існують різні типи протоколів, що використовуються з різних причин. Загалом, найбезпечнішим протоколом є OpenVPN, і зазвичай це найкращий протокол для використання.

Шифрування. Шифрування йде пліч-о-пліч з протоколом безпеки. Ця функція захищає ваші дані, шифруючи їх. Таким чином, навіть якщо хакер чи хтось інший захопить ваші дані, вони не зможуть їх розшифрувати. Найкращі VPN використовують AES 128-bit та 256-bit. AES означає Advanced Encryption Standard, і це найпоширеніший шифр. Більшість віртуальних приватних мереж

використовують його і він сумісний з усіма основними протоколами VPN. Номери 128 і 256 відповідають довжині ключа і є можливою кількістю комбінацій. Щоб уявити це в перспективі, найшвидший комп'ютер займе понад мільярд років, щоб вигадати всі можливі комбінації для AES 128-біт. Шифрування є вирішальним фактором, коли справа доходить до VPN.

Сервери. Багато разів ви чуєте, як певні VPN-сервери хваляться своєю кількістю серверів. Це пов'язано з тим, що зазвичай краще мати широкий спектр серверів та локацій. Навіщо? Зазвичай, коли ви користуєтесь Інтернетом, ви надсилаєте свої дані на сервер із запитом на певний сайт. Потім сервер відправляє інформацію веб-сайту назад на ваш пристрій. Коли ви використовуєте VPN, ваші дані спочатку відправляються на сервер VPN, а потім VPN відправляє його на передбачуваний сервер. Це важливо, тому що, коли ви пінгували сервер для веб-сайту, ви постійно надсилаєте дані по цьому з'єднанню.

Якщо ви вставляєте VPN посередині, ваш запит на веб-сайт надсилається на сервер, але ваші дані переміщуються лише між вашим пристроєм і сервером VPN (який також проходить через зашифрований тунель). Тому гаданий сервер не отримує жодної інформації. Так, користувачі VPN залишаються анонімними в Інтернеті. Це також те, як VPN можуть змінити ваше місце розташування, щоб розблокувати певні сайти.

РОЗДІЛ 2. Особливості застосування формалізованих методик щодо реалізації віртуальної приватної мережі за основними критеріями вибору

2.1 Застосування методик щодо реалізації захисту VPN

Коли використовується VPN, ваші дії та дані передаються через мережу за допомогою процесу, відомого як тунелювання.

Дані, що передаються через VPN-тунель, розділені на фрагменти, відомі як “пакети”, які поміщаються всередині інших пакетів даних. Цей процес називається “інкапсуляція.” Також всі ці дані шифруються, що не дає стороннім отримати доступ до їхнього вмісту.

2.1.1. Тунельний режим реалізації захисту VPN

Тунелювання - це мережна технологія, яка дозволяє інкапсулювати один тип пакета протоколу в дейтаграму іншого протоколу. Наприклад, з'єднання Windows VPN можуть використовувати пакети протоколу тунелювання (PPTP) від точки до точки, щоб інкапсулювати та відправляти приватний мережний трафік, такий як трафік TCP/IP у загальнодоступній мережі, такій як Інтернет. Для протоколу PPTP та L2TP тунель схожий на сеанс. Обидві кінцеві точки тунелю повинні погоджуватися з тунелем і погоджувати змінні конфігурації, такі як призначення адреси, шифрування або параметри стиснення.

У більшості випадків дані, що передаються тунелем, відправляються з використанням протоколу на основі дейтаграми. Протокол керування тунелем використовується як механізм створення, обслуговування та завершення тунелю. Після встановлення тунелю дані можуть бути відправлені. Клієнт тунелю або сервер використовує протокол передачі даних тунелю для підготовки даних передачі. Наприклад, коли клієнт тунелю надсилає корисне навантаження на тунельний сервер, клієнт тунелю спочатку додає заголовок протоколу передачі даних тунелю в корисне навантаження. Потім клієнт відправляє отримане інкапсульоване корисне навантаження через мережу, яка направляє її на сервер тунелів. Сервер тунелів приймає пакети, видаляє

заголовок протоколу передачі тунелю і пересилає корисне навантаження в цільову мережу.. Інформація, що передається між тунельним сервером та клієнтом тунелю, поводиться аналогічним чином.

Існує два типи тунелювання:

● *Добровільне тунелювання*

● *Обов'язкове тунелювання*

Добровільне тунелювання. Користувацький або клієнтський комп'ютер може надати запит VPN для налаштування та створення добровільного тунелю. У цьому випадку комп'ютер користувача є кінцевою точкою тунелю та діє як клієнт тунелю. Добровільне тунелювання відбувається, коли клієнтський комп'ютер або сервер маршрутизації створює віртуальне з'єднання з цільовим сервером тунелів. Для цього на клієнтському комп'ютері необхідно встановити тунельне клієнтське програмне забезпечення та відповідний протокол тунелювання. Для протоколів, які обговорюються в цій технічній довідковій інформації, для добровільних тунелів потрібне IP-з'єднання.

У ситуації комутованого доступу клієнт повинен встановити з'єднання з мережею, що комутується, до того, як клієнт зможе налаштувати тунель. Це найпоширеніший випадок. Найкращим прикладом цього є користувач віддаленого доступу до Інтернету, який повинен набирати ISP та отримувати інтернет-з'єднання до того, як тунель через Інтернет може бути створений. Для клієнтського комп'ютера, підключеного до локальної мережі, є з'єднання з мережею, яка може забезпечити маршрутизацію інкапсульованих корисних навантажень на вибраний сервер тунелю LAN. Це буде місце для клієнта, який використовує постійне широкосмугове підключення до Інтернету.

Це поширена помилка, що для VPN-з'єднань потрібне підключення комутованого з'єднання. Вони потребують лише IP-з'єднання між VPN-клієнтом та VPN-сервером. Деякі клієнти (наприклад, домашні комп'ютери) використовують комутовані підключення до Інтернету для встановлення IP-транспорту. Це попередній крок у підготовці до створення тунелю і є частиною самого тунельного протоколу.

Обов'язкове тунелювання. У разі примусового тунелювання сервер віддаленого доступу з підтримкою VPN налаштовує та створює примусовий тунель. У разі використання обов'язкового тунелю комп'ютер користувача не є кінцевою точкою тунелю. Іншим пристроєм, сервером віддаленого доступу між комп'ютером користувача і тунельним сервером є кінцева точка тунелю і діє як клієнт тунелю. Ряд постачальників, які продають сервери віддаленого доступу, реалізували можливість створення тунелю від імені віддаленого клієнта.

Комп'ютер або мережний пристрій, що надає тунель для клієнтського комп'ютера, по-різному відомий як процесор переднього кінця (FEP) для PPTP або L2TP концентратор доступу (LAC) для L2TP. Для цього посилання термін FEP використовується для опису цієї функціональності незалежно від протоколу тунелювання. Для виконання своєї функції FEP повинен мати відповідний протокол тунелювання та повинен бути здатним встановити тунель під час підключення клієнтського комп'ютера. При примусовому тунелюванні клієнтський комп'ютер розміщує виклик віддаленого доступу до NAS з підтримкою тунелювання в ISP.

Наприклад, корпорація могла б укласти контракт із інтернет-провайдером для розгортання загальнонаціонального набору FEP. Ці FEP можуть встановлювати тунелі через Інтернет на тунельний сервер, підключений до приватної мережі організації, об'єднуючи виклики з географічно різних місць в одне підключення до Інтернету в організації. Ця конфігурація відома як примусове тунелювання, тому що клієнт повинен використовувати тунель, створений FEP. Після початкового підключення весь мережний трафік із клієнтом і від нього автоматично відправляється через тунель.

У разі примусового тунелювання клієнтський комп'ютер робить одне PPP-з'єднання. Коли клієнт набирає номер у NAS, створюється тунель і весь трафік автоматично маршрутизується через тунель. FEP можна налаштувати для тунелювання всіх клієнтів віддаленого доступу певний тунельний сервер. FEP також може тунелювати окремих клієнтів на основі імені користувача чи адресата. На відміну від окремих тунелів, створених для кожного

добровільного клієнта, кілька клієнтів віддаленого доступу можуть спільно використовувати тунель між FEP та сервером тунелів. Коли другий клієнт набирає сервер доступу (FEP) для досягнення адресата, для якого вже існує тунель, немає необхідності створювати новий екземпляр тунелю між сервером FEP та тунелем. Натомість трафік даних для нового клієнта переноситься поверх існуючого тунелю. Оскільки в одному тунелі може бути кілька клієнтів, тунель не переривається доти, доки останній користувач тунелю не відключиться.

Весь ваш трафік проходить через VPN-тунель, що забезпечує повний захист від сторонніх очей, у тому числі від вашого власного інтернет-провайдера. Завдяки VPN ваша початкова IP-адреса буде замінена IP-адресою VPN-сервера, до якої одночасно підключені сотні користувачів. Як наслідок, ніхто не зможе сказати напевно, яка саме дія була зроблена саме вами. Це захищає всі ваші онлайн-дії, листування та будь-який інший трафік від зацікавлених інтернет-провайдерів, уряду або хакерів, які відстежують дії користувачів, що підключилися до публічних точок доступу Wi-Fi. VPN-тунель не тільки захищає ваші дані від перехоплення, але й приховує вашу IP-адресу, за допомогою якої сторонні зможуть ідентифікувати вас під час роботи в Інтернеті. Але коли ви підключитеся до VPN, сайти будуть бачити вже не вашу вихідну IP-адресу та місцезнаходження, а, власне, обраного вами VPN-сервера.

Таким чином, VPN-тунелі допомагають обійти цензурні блокування як локальних мереж, так і сервісів, до яких ви хотіли б отримати доступ.

Що таке VPN-тунель?

Виходячи в мережу через VPN, ви встановлюєте безпечний канал зв'язку для передачі інформації між вашим пристроєм та Інтернетом. Цей канал і називається VPN-тунелем — він зашифровує та інкапсулює всі ваші дані, роблячи їх нечитаними для тих, хто не має спеціального ключа для їх розшифровки.

Це схоже на пересилання листа особистим кур'єром замість звичайної поштової служби, але до того ж цей кур'єр перекладає кожен ваш лист

(вихідний та вхідний) на мову, зрозумілу тільки вам. Навіть якщо хтось вкраде і спробує прочитати вашу пошту — вам нема про що турбуватися! Точніше, майже нема про що. Ступінь захисту інформації залежить від протоколу шифрування, який використовує VPN-сервіс, тобто від мови, якою ваш кур'єр перекладає ваші листи. Нижче ми розповімо про різні VPN-протоколи з різними варіантами використання та рівнями безпеки, але спочатку давайте докладніше розглянемо процес створення та роботи VPN-тунелю.

Як працює VPN-тунель?

Коли ви натискаєте на посилання та завантажуєте файли на веб-сайтах, ви надсилаєте інформаційні запити, щоб отримати інформацію у відповідь. Без VPN-захисту ці запити даних з вашого пристрою йдуть до вашого інтернет-провайдера (ІП), а потім передаються до Інтернету, щоб ви могли отримати те, що запросили. При цьому ваш ІП, веб-сайт та будь-яка особа, здатна відстежити ваше з'єднання, може бачити та ідентифікувати різні частини вашого інформаційного потоку, а потім використовувати чи продавати ці дані у своїх інтересах. Щоб уникнути цього VPN, встановлює безпечне з'єднання через VPN-тунель з одним із своїх серверів:

• Крок 1: Ви надсилаєте запит на створення VPN-тунелю через свого VPN-клієнта на один із його серверів;

• Крок 2: фаза 1 – це етап узгодження взаємодії вашого пристрою та VPN-сервера: вони ідентифікують один одного та перевіряють, які заходи безпеки їм необхідні;

• Крок 3: фаза 2 — створення VPN-тунелю, через який передаватимуться ваші дані;

• Крок 4: зашифровані дані через встановлений тунель передаються до Інтернету та з Інтернету так, що навіть ваш інтернет-провайдер їх не бачить;

• Крок 5: після закінчення заданого часу або вичерпання обсягу даних термін дії тунелю спливає, і він автоматично закривається. Якщо ви хочете продовжити користуватися з'єднанням VPN, VPN створить новий тунель з кроку 1.

Цей процес може бути складним, але на практиці безпека інтернет-з'єднання забезпечується дуже швидко. Головне питання полягає в тому, наскільки безпечним фактично є VPN-тунель. Відповідь на нього залежить від того, який протокол тунелювання ви використовуєте.

2.1.2. VPN-протоколи

Безпека передачі даних між різними мережами — головна мета всіх протоколів VPN, але оскільки вони відрізняються між собою, ступінь безпеки інтернет-протоколу залежить від надійності використовуваного протоколу VPN. Протоколи VPN – це правила, що забезпечують безперебійну, безпечну та надійну роботу VPN-сервісу. Протокол VPN — це набір правил для створення віртуальної приватної мережі або участі в ній. Він виступає в ролі набору інструкцій з напряму даних та трафіку між комп'ютером та VPN-сервером.

За допомогою протоколів VPN-сервіси створюють та налаштовують свої мережі на основі наявних цифрових принципів. Теоретично кожен VPN-провайдер може розробити та використовувати власні протоколи, але це буде нераціональним витрачанням часу та ресурсів. Тому більшість з них використовують надійні та перевірені протоколи з відкритим вихідним кодом та підтримкою кількох операційних систем. Багато користувачів просто підключаються до VPN-сервера, не замислюючись про те, який саме VPN-протокол при цьому використовується - достатньо того, що з'єднання встановлено та працює. Однак параметри за замовчуванням – не завжди найкращий варіант.

Базовий протокол, який використовує VPN, впливає на затримку, продуктивність та надійність зашифрованого тунелю. Аналіз підключень у різних куточках світу показує, що протоколи працюють по-різному, тому користувачам варто дізнатися більше про різні варіанти.

Насправді сьогодні користувачам пропонується зовсім небагато хороших VPN-протоколів - нижче наведені деякі з них, з якими можна зіткнутися на практиці.

1. OpenVPN - багатофункціональна VPN-система з відкритим вихідним кодом для з'єднань «точка-точка» або «сайт-сайт» як клієнтських, так серверних додатків. OpenVPN дозволяє одноранговим вузлам-учасникам аутентифікувати один одного за допомогою загальних секретних ключів, облікових даних та сертифікатів, що забезпечує високу безпеку та швидкість двостороннього підтвердження.

OpenVPN — одна з найбезпечніших і найдоступніших технологій VPN, так як може бути реалізована у вигляді протоколу. OpenVPN використовує 256-бітний алгоритм шифрування AES і може легко застосовуватись на різних платформах, включаючи Windows, Mac, Android та iOS.

Завдяки відкритості вихідний код OpenVPN ретельно вивчений експертами з кібербезпеки. Єдиними недоліками OpenVPN можна назвати його середню швидкість та складність налаштування вручну без стороннього програмного забезпечення.

OpenVPN TCP vs. UDP: що таке?

OpenVPN TCP та OpenVPN UDP – це не два окремі VPN-протоколи. TCP і UDP — це різні протоколи транспортного рівня, які OpenVPN може використовувати для встановлення VPN-підключення.

TCP гарантує стабільність з'єднання, стежачи за порядком надходження пакетів даних.

UDP передає дані швидше, упорядковуючи пакети даних після прибуття.

Для користувачів рекомендується спробувати обидва ці протоколи та використовувати той, який дає більш якісне підключення на вашому пристрої.

Плюси:	***Мінуси:***
Надійна безпека	Середня швидкість
Хороші методи аутентифікації та верифікації	Важко налаштувати вручну

Високоякісне шифрування	
Відкритий вихідний код	

Рекомендація: *Рекомендується для більшості завдань.*

2. IKEv2/IPSec Internet Key Exchange version 2 (IKEv2) "версія 2 протоколу обміну ключами" - це протокол автентифікації, що використовується разом з VPN-протоколом IPSec ("безпека інтернет-протоколу"). Оскільки IPSec працює у фоновому режимі у ядрі системи, він дозволяє IKEv2 бути дуже швидким.

IKEv2 реалізований у більшості операційних систем, тому може легко використовуватися замість повільнішого OpenVPN. IKEv2 використовує ті ж ефективні інструменти безпеки, що і OpenVPN, при цьому його набагато простіше масштабувати та підтримувати на рівні сервера.

Протокол Internet Key Exchange версії 2 (IKEv2) популярний серед мобільних користувачів завдяки своїй швидкості та безпеці. Він використовується разом із пакетом IPsec для встановлення зіставлень безпеки між одноранговими вузлами, аналогічно з певними сертифікатами OpenVPN.

IKEv2 сумісний з більшістю висококласних шифрів, включаючи 256-бітний AES, і підключення з його використанням налаштовується відносно просто. Головна перевага IKEv2 — його виняткова швидкість при підключенні до серверів, що розташовані неподалік.

Плюси:	**Мінуси:**
Надійна безпека	Швидкість залежить від відстані між пристроєм та сервером
Високі швидкості	
Високоякісне шифрування	
Добре працює у мобільних мережах	

Хороші методи аутентифікації та верифікації	

Рекомендації: *Рекомендується для більшості завдань, особливо для мобільних пристроїв.*

3. WireGuard - найновіший пункт у списку VPN-протоколів. Не маючи багаторічної практики використання та тестування, як OpenVPN, WireGuard завдяки своїй простоті пропонує безпеку та шифрування найвищого рівня на неперевершеній швидкості, а його реалізація на Linux та Android означає, що він продовжуватиме успішно використовуватись.

WireGuard перевершує IPsec і OpenVPN за показниками енергоспоживання та продуктивності, забезпечуючи той самий рівень безпеки. Він забезпечує більш високу швидкість з'єднання, ніж IKEv2 та OpenVPN, використовуючи при цьому всього 4000 рядків коду (для порівняння – OpenVPN та IPsec використовують 400 000 та 600 000 рядків відповідно). Короткість коду спрощує його перевірку і теоретично підвищує стабільність. Це спрощує незалежну перевірку його безпеки, знижує ймовірність переривання з'єднання та прискорює повторне підключення. Ці відмінності важливі для всіх, хто використовує VPN-тунелі переважно з метою безпеки.

WireGuard — безкоштовна і проста в установці програма (зокрема, в порівнянні з OpenVPN) з відкритим вихідним кодом. WireGuard також доступний у вигляді протоколу, що дозволяє VPN-провайдерам застосовувати його у своїх службах.

Плюси:	***Мінуси:***
Безпека	Відносно новий - потрібен час на тестування
Всього 4000 рядків коду	
Відкритий вихідний код	

Виняткова швидкість	
Не вимагає встановлення з'єднання	
Простота налаштування	

Рекомендація: *Наполегливо рекомендується для більшості завдань.*

4. SoftEther – це багатопротокольний VPN-клієнт та серверне програмне забезпечення з відкритим вихідним кодом. Він додає розширені функціональні можливості — управління GUI (графічний інтерфейс користувача) і RPC (віддалений виклик процедур) — через HTTPS (hypertext transfer protocol — «протокол передачі гіпертексту»).

За швидкістю він перевершує OpenVPN і може використовувати ті самі засоби безпеки. При цьому він протестований менше, ніж OpenVPN (через відносну новизну) і не такий швидкий і простий у використанні, як WireGuard.

Плюси:	**Мінуси:**
Швидкий, стабільний, надійний	Відносно новий - потрібен час на тестування
Пропонує додаткові функції для таких протоколів, як OpenVPN	
Відкритий вихідний код	

Вердикт: *Гарна альтернатива OpenVPN.*

5. PPTP. Point-to-Point Tunneling Protocol (PPTP) "протокол тунелювання для двоточкового зв'язку" - дуже застарілий протокол тунелювання, який взагалі не повинен використовуватися VPN-сервісами. Він підтримує лише шифрування до 128 біт і має кілька відомих уразливостей, розкритих урядом США та АНБ (Агентством національної безпеки). З позиції прихильників

онлайн-безпеки та конфіденційності не рекомендуємо PPTP для жодних завдань.

Але завдяки своїй простоті PPTP хоч і рідко, але й досі використовується. На сьогоднішній день PPTP не має собі рівних за швидкістю з'єднання та простотою налаштування. Цей протокол тунелювання підходить для потокової передачі аудіо або відео, або для пристроїв із повільними та застарілими процесорами.

Однак, загалом використовувати PPTP не рекомендується, за винятком випадків, коли безпека з'єднання не критична.

Плюси:	***Мінуси:***
Дійсно швидкий	Несумісність із гарним шифруванням
Простота налаштування	Простота експлуатації
	Застарілий та забутий

Рекомендація: *Не рекомендується ні для яких завдань.*

6. SSTP. Протокол тунелювання захищених сокетів (SSTP) — VPN-тунель, створений для передачі безпосередньо між двома маршрутизаторами без участі іншого хоста чи іншої мережі. SSTP використовує канал SSL "рівень захищених сокетів", який забезпечує ефективне узгодження, шифрування та перевірку трафіку. Цей протокол з високим рівнем безпеки не використовує фіксовані порти, що дозволяє SSTP легко оминати брандмауери.

Недоліком SSTP є те, що його було створено для Windows, хоча його можна налаштувати для роботи на пристроях з Linux, BSD та Mac OS. З іншого боку, він коли не коли проходив незалежні аудиторські перевірки, т.к. розробники не мають доступу до його коду, що ускладнює його використання VPN-провайдерами. З точки зору швидкості, SSTP теж не найкращий варіант: його продуктивність може сильно знижуватися через брак додаткової пропускної спроможності.

Плюси:	**Мінуси:**
Легко обходить брандмауери	Код ніколи не розкривався/не перевірявся
Може використовувати стандартне шифрування	Складність сумісності з усіма операційними системами, крім Windows
Добре справляється з узгодженням та перевіркою інтернет-трафіку	Код недоступний для розробників VPN
Простота налаштування у Windows	

Рекомендація: *Теоретично непоганий, але загалом не рекомендується.*

7. L2TP/IPsec. Layer 2 Tunneling Protocol (L2TP) "протокол тунелювання рівня 2" - це протокол тунелювання, який сам по собі не забезпечує безпеку і використовує IPSec для шифрування. L2TP двічі інкапсулює дані, що знижує швидкість з'єднання.

Як наступник PPTP, протокол L2TP («протокол тунелювання рівня 2») створювався як вдосконалений варіант свого попередника. L2TP використовується з пакетом безпеки інтернет-протоколу (IPsec), що створює два рівні інкапсуляції та шифрування. Інтернет-провайдери (ІП) часто використовують його для надання деяких своїх послуг.

L2TP сумісний з 256-бітним шифром AES - найкращим алгоритмом безпеки для шифрування даних. Багаторівневий підхід до безпеки забезпечує відносну надійність L2TP, але в частині автентифікації та верифікації цей протокол поступається IKEv2, OpenVPN та WireGuard.

L2TP більш безпечний у порівнянні зі своїм попередником, але йому не вистачає швидкості та гнучкості. При цьому його подвійне шифрування сповільнює передачу даних. L2TP використовує фіксовані порти і зазвичай не

справляється з обходом брандмауерів, а це означає, що веб-сайти з кращою інфраструктурою можуть легко блокувати користувачів цього протоколу.

Плюси:	***Мінуси:***
Рівень безпеки вищий, ніж у PPTP, але недостатній	Застарілий
Відносно швидкий	Не шифрує сам
	Не справляється із брандмауерами
	Слабка автентифікація та цілісність

Рекомендація: *Не рекомендується.*

Порівняння VPN-протоколів

Таблиця 2.1

Таблиця порівняння VPN протоколів

VPN-протокол	**Безпека**	**Потенціал швидкості**	**Стабільність**	**Шифрування**	**Налаштування**	**Підходить для**
OpenVPN/ TCP	Дуже надійний (немає відомих уразливостей)	Дуже швидкий	Залежить від конфігурації сервера	AES-256-GCM	Легко з VPN, складно самостійно	Сумісність із роутером, повсякденне використання для будь-яких завдань
OpenVPN UDP	Дуже надійний (немає відомих уразливостей)	Дуже швидкий	Залежить від конфігурації сервера	AES-256-GCM	Легко з VPN, складно самостійно	Сумісність із роутером, повсякденне використання для будь-яких завдань
IKEv2/IPSec	Дуже надійний (немає відомих уразливостей)	Дуже швидкий	Залежить від конфігурації сервера	AES-256-GCM	Легко з VPN, складно самостійно	З'єднання на короткі відстані, мобільні мережі, повсякденне використання
WireGuard	Дуже надійний (немає	Дуже швидкий	Залежить від конфігурації сервера	AES-256-GCM	Просто	Повсякденне використання

	відомих уразливостей)					
SoftEther	Дуже надійний (немає відомих уразливостей)	Дуже швидкий	Залежить від конфігурації сервера	AES-256-GCM	Налаштування клієнта	Повсякденне використання
PPTP	Небезпечний	Дуже швидкий	Залежить від конфігурації сервера	128-бітне	Дуже просто	Тільки застаріле обладнання та старі пристрої
SSTP	Середній	Середній	Залежить від конфігурації сервера	AES-256-GCM	Легко у Windows	Підключення пристроїв до Windows
L2TP/IPsec	Безпека	Швидкий	Залежить від конфігурації сервера	AES-256-GCM	Легко у Windows	Нічого, що не може запропонувати IKEv2/IPSec

Який VPN-протокол вибрати?

WireGuard та IKEv2/IPSec на сьогодні вважаються найкращими VPN-протоколами. OpenVPN займає третє місце - за ефективністю він не поступається першим двом, але з ним складніше працювати. Багато маршрутизаторів сумісні з OpenVPN, що дозволяє використовувати його для VPN-захисту всієї домашньої мережі.

Правду кажучи, «найкращий» — не зовсім коректне слово при виборі VPN-протоколу, оскільки вибрати один ідеальний протокол для всіх ситуацій неможливо. Ваш вибір повинен залежати від того, навіщо VPN-сервіс потрібен особисто вам.

Який VPN-протокол найбезпечніший?

Як і у випадку зі словом "кращий", щодо VPN-протоколу не існує поняття "найбезпечніший". WireGuard, IKEv2 та OpenVPN забезпечують однаковий рівень безпеки – і вони дійсно безпечні. Усі три користуються довірою багатьох галузевих експертів.

Але навіть при використанні безпечних протоколів визначальну роль відіграє те, як провайдер створює та налаштовує свою мережу VPN.

Рекомендуємо не довіряти безкоштовним VPN, навіть якщо вони використовують WireGuard!

Який протокол для VPN найшвидший?

Попри поширену думку, VPN-протоколи не сильно впливають на швидкість з'єднання. По-справжньому важливе значення має таке:

• швидкість інтернет-з'єднання (значний вплив);

• сумісність та якість пристрою (значний вплив);

• навантаження та пропускна здатність VPN-сервера (вплив від помірного до значного);

• відстань між користувачем та VPN-сервером (помірний вплив).

Що стосується швидкості з'єднання, тут найкращим вибором буде WireGuard або IKEv2.

Який VPN-протокол найстабільніший?

OpenVPN TCP (протокол управління передачею) вважається найбільш стабільним протоколом, особливо під час використання у ненадійних мережах. Однак за стабільність доводиться платити швидкістю. Для передачі кожного біта інформації TCP потрібно трохи більше часу, ніж UDP (протокол користувальницьких дейтаграм).

Який VPN найкраще підходить для потокової передачі?

Нікому не подобається, коли при перегляді улюбленого шоу зображення гальмує та «зависає». На жаль, це відбувається. Ви можете уникнути цього, використовуючи швидкі та надійні VPN-протоколи типу WireGuard та IKEv2/IPsec – обидва відмінно підходять для потокової передачі контенту.

Який VPN найкраще підходить для ігор?

Коли ви граєте в онлайн-ігри, ваші успіхи залежать не тільки від ваших навичок, але і швидкості вашого з'єднання. Щоб отримати найнижчий час відповіді, вибирайте WireGuard як основний протокол VPN. На сьогоднішній день це найшвидший варіант та найкращий протокол VPN для онлайн-ігор.

Чому WireGuard, OpenVPN та IKEv2 — найкращі протоколи VPN

Більшість старих протоколів, окрім WireGuard, OpenVPN та IKEv2, вже застаріли та сповнені вразливостей. Важливих причин використовувати інші VPN-протоколи, окрім цих трьох, на сьогодні немає.

Чесно кажучи, для хорошого VPN-сервісу достатньо одного протоколу, але через відмінності у сумісності з маршрутизаторами та різними операційними системами необхідно пропонуємо всі три.

Випробуйте VPN-протоколи в дії

Тепер ми знаємо про VPN-протоколи все, що може бути потрібно користувачеві VPN. Найголовніше - вибрати той протокол, який найкраще підходить для користувацьких потреб. На сьогодні рекомендованими для застосування можуть бути WireGuard або IKEv2 для звичайного використання на пристроях та OpenVPN, якщо вам потрібно налаштувати VPN на маршрутизаторі.

2.1.3. Роздільне VPN-тунелювання

Як видно, одні протоколи VPN-тунелювання створені для конкретних цілей, інші застаріли і відрізняються простотою використання. Вибір потрібно проводити розумно! Говорячи про вибір, слід зазначити ще один вибір, який називають - роздільне VPN-тунелювання.

Роздільне VPN-тунелювання (Bypasser в Surfshark) - це функція, яка дозволяє вибирати, до чого слід підключатися через VPN-тунель. Вона є незамінною, якщо вам потрібно захистити підключення до одного конкретного додатку — або, навпаки, до всіх, крім одного. Наприклад, ви можете налаштувати її так, щоб підключатися через VPN до всього, крім вашої банківської програми. В результаті ви захистите всю решту свого трафіку, а ваш банк не блокуватиме транзакції з іншої країни.

Плюси та мінуси роздільного VPN-тунелювання

Таблиця 2.2

Плюси:	***Мінуси:***
Безпека особистих даних	***Вибірковий захист***

Кожен користувач має дані, які потрібно захищати шифруванням. Якщо ви хочете з будь-якої причини відключити VPN, роздільне тунелювання дозволить вам зробити це без ризику порушення безпеки найконфіденційніших даних.	Єдиним недоліком роздільного тунелювання можна назвати те, навіщо воно було створено. Знімаючи захист із конкретних програм, ви робите їх більш уразливими, оскільки їхні дані перестають бути зашифрованими.
Використання різних IP-адрес	
Іноді зміна IP-адреси неприпустима. Для виконання операцій інтернет-банкінгу або потокової передачі буває необхідно використовувати свою справжню IP-адресу, щоб не порушувати умов обслуговування. У таких випадках ідеальне рішення – це роздільне тунелювання.	
Доступ до домашніх пристроїв	
Більшість домашніх бездротових пристроїв підключаються до тієї ж мережі, що й основний пристрій. Іноді виникають труднощі, оскільки VPN створює видимість, ніби пристрій використовує іншу мережу. Завдяки роздільному тунелюванню ви можете користуватися бездротовими пристроями без увімкнення/вимкнення VPN.	
Виключення «важких» додатків	
Шифрування може уповільнювати роботу пристрою. Зазвичай швидкість знижується несуттєво, але при користуванні програмами з великими обсягами даних уповільнення стає помітним і дратівливим. За допомогою роздільного тунелювання можна виключити їх із VPN-підключення для збереження швидкості, залишивши під захистом все інше.	

Як працює роздільне тунелювання?

Роздільне VPN-тунелювання дозволяє одночасно підтримувати два підключення. VPN-додаток розділяє інтернет-трафік на дві категорії - одна частина шифрується і перенаправляється через захищені VPN-сервери, а інша залишається недоторканою і може безпосередньо взаємодіяти з Інтернетом. У налаштуваннях VPN-програми можна вибрати, які програми є перевіреними і не потребують VPN-захисту.

Різні види роздільного VPN-тунелювання

Зворотне тунелювання Зворотне роздільне тунелювання за умовчанням шифрує підключення повністю, і лише перевірені програми можуть безпосередньо підключатися до Інтернету. Це найбезпечніша форма роздільного тунелювання.

Роздільна тунелювання на основі додатків. За допомогою цього виду тунелювання лише вибрані програми будуть захищені VPN. Решта вашого інтернет-трафіку не буде шифруватися.

Роздільне тунелювання на основі URL-адреси. Якщо потрібно отримати доступ до деяких сайтів за допомогою реальної IP-адреси? Роздільне тунелювання на основі URL-адрес дозволяє вказати, які з них потрібно виключити з VPN-з'єднання. Ця функція доступна у розширеннях для браузерів від NordVPN.

Оскільки з'єднання з VPN-сервером може заблокувати доступ до сайтів та сервісів вашої країни, то може виникнути бажання відключити NordVPN для перегляду місцевого контенту. Пам'ятайте про безпеку: скористайтеся роздільним тунелюванням VPN для захисту важливих даних під час роботи в мережі.

Незалежно від способу застосування роздільне VPN-тунелювання - це дуже зручний інструмент, який, як і будь-який інший, повинен використовуватися в потрібний час та у потрібному місці. Пам'ятайте, що сторонні (включно з вашим інтернет-провайдером) можуть переглядати

незашифрований інтернет-трафік, тому завжди використовуйте захист віртуальної приватної мережі при роботі з конфіденційними даними.

Коли потрібно використовувати роздільне VPN-тунелювання?

• Якщо ви хочете уникнути зниження швидкості Інтернету

NordVPN — найшвидший VPN на ринку, але шифрування та розшифрування даних потребують часу. Хоча в більшості випадків зниження швидкості непомітно, деякі дії в мережі (наприклад, FPS-ігри) вимагають ідеального інтернет-підключення - саме тут роздільне тунелювання буде дуже доречним. Захистіть програми, які обробляють конфіденційні дані, дозволяючи іншим працювати на повній швидкості.

• Якщо необхідно отримати доступ до локального та домашнього контенту одночасно, перебуваючи за кордоном.

• Якщо потрібно підключитися до LAN-пристроїв під час використання VPN.

2.2. Реалізація захисту VPN з використанням засобів безпеки IPSec

Протокол IPsec переважно використовується для організації VPN-тунелів. В даному випадку протоколи ESP і AH функціонують в режимі тунелювання. При налаштуванні політики безпеки певним чином, IPsec можна використовувати для створення міжмережного екрану. Встановлюється відповідний набір правил, і екран відслідковує всі пакети, які проходять через нього. В разі, якщо передані пакети потрапляють під дію відповідного набору цих правил, міжмережевий екран обробляє їх відповідним чином. Наприклад, він може відхиляючи певні пакети, припиняти небезпечні з'єднання. Таким налаштуванням політики безпеки можна, наприклад, заборонити інтернет-трафік.

IPsec застосовується і для захисту серверів — при цьому відкидаються всі пакети, кроме пакетів, необхідних для виконання функцій сервера.

Стек протоколів IPSec також використовується для автентифікації учасників інформаційного обміну, шифрування IP-пакетов і тунелювання

трафіку.

2.2.1. Архітектура засобів безпеки IPSec

Головним призначення протоколів IPSec є убезпечення передачі даних по мережах IP. Застосування IPSec гарантує:

- цілісність даних, які передаються;

- автентичність відправника;

- конфіденційність передаваних даних.

Також слід зазначити, що в поняття безпеки даних включають ще вимогу доступності даних, що можна інтерпретувати як гарантію їх доставки. Протоколи IPSec не забезпечують дану задачу, а залишають її протоколу транспортного рівня TCP. Стек протоколів IPSec здійснює захист інформації на мережному рівні і тим самим робить цей захист невидимим для працюючих застосувань.

Головною одиницею комунікації в IP-мережах є IP-пакет. IP-пакет містить S-адресу джерела і D-адресу одержувача повідомлення, транспортний заголовок, інформацію про тип даних, які переносяться в цьому пакеті, і самі дані (таблиця. 2.3).

Користувач сприймає мережу як надійно захищене середовище тільки в тому випадку, якщо він упевнений, що його партнер по обміну - саме той, за кого він себе видає (автентифікація сторін), що передавані пакети не є видимими сторонніми особами (конфіденційність зв'язку) і що отримувані дані не піддалися зміні в процесі передачі (цілісність даних).

Таблиця 2.3 Структура IP-пакета

IP-заголовок		Транспортний TCP- або UDP-заголовок	Дані
S-адреса	D-адреса		

Для того, щоб забезпечити автентифікацію, конфіденційність і цілісність

передаваних даних стек протоколів IPSec побудований на базі стандартизованних криптографічних технологій:

- обміну ключами згідно алгоритму Діффі-Хеллмана для розподілу секретних ключів між користувачами у відкритій мережі;
- криптографії відкритих ключів для підписки обмінів Діффі - Хеллмана, щоб гарантувати достовірність двох сторін і уникнути атак типу «man-in-the-middle»;
- цифрових сертифікатів для підтвердження достовірності відкритих ключів;
- блокових симетричних алгоритмів шифрування даних;
- алгоритмів автентифікації повідомлень на базі функцій гешування.

Протоколом IPSec визначаються стандартні способи захисту інформаційних потоків на мережному рівні моделі OSI для IP-мережі, що є основним видом відкритих мереж. Даний протокол входить до складу версії протоколу IP (IPv6) і застосовний також до його поточної версії (IPv4). Для протоколу IPv4 підтримка IPSec є бажаною, а для IPv6 - обов'язковою.

Протокол IPSec - це система відкритих стандартів з чітко обкресленим ядром і в той же час дозволяє доповнювати її новими протоколами, алгоритмами і функціями. Стандартизованими функціями IPSec-захисту можуть користуватися протоколи вищих рівнів: протоколи, що управляють, конфігурації, та протоколи маршрутизації.

Основними завданнями встановлення і підтримки захищеного каналу є наступні:

- автентифікація користувачів або комп'ютерів при ініціації захищеного каналу;
- шифрування і автентифікація передаваних даних між кінцевими точками захищеного каналу;
- забезпечення кінцевих точок каналу секретними ключами, необхідними для роботи протоколів автентифікації і шифрування даних.

Для вирішення перерахованих завдань система IPSec використовує комплекс засобів безпеки інформаційного обміну.

Більшість реалізацій протоколу IPSec мають наступні компоненти.

Основний протокол IPSec. Цей компонент реалізує протоколи ESP і AH. Він обробляє заголовки, взаємодіє з БД SPD і SAD для визначення політики безпеки, вживаної до пакету.

Протокол управління обміном ключової інформації IKE (Internet Key Exchange). IKE зазвичай представляється як процес призначеного для користувача рівня, за винятком реалізацій, вбудованих до ОС.

База даних політик безпеки SPD (Security Policy Database). Це один з найважливіших компонентів, оскільки він визначає політику безпеки, вживану до пакету. SPD використовується основним протоколом IPSec при обробці вхідних і витікаючих пакетів.

База даних безпечних асоціацій SAD (Security Association Database). БД SAD зберігає список безпечних асоціацій SA (Security Association) для обробки вхідної і вихідної інформації. Вихідні SA використовуються для захисту вихідних пакетів, а вхідні SA використовуються для обробки пакетів із заголовками IPSec. БД SAD заповнюється SA вручну або за допомогою протоколу управління ключами IKE.

Управління політикою безпеки і безпечними асоціаціями SA. Це - додатки, які управляють політикою безпеки і SA .

Основний протокол IPSec (реалізовуючий ESP і AH) тісно взаємодіє з транспортним і мережним рівнем стека протоколів TCP/IP. Фактично протокол IPSec є частиною мережного рівня. Основний модуль протоколу IPSec забезпечує два інтерфейси: вхідний і вихідний. Вхідний інтерфейс використовується вхідними пакетами, а вихідний - вихідними. Реалізація IPSec не повинна залежати від інтерфейсу між транспортним і мережним рівнем стека протоколів TCP/IP.

БД SPD і SAD істотно впливають на ефективність роботи IPSec. Вибір структури даних для зберігання SPD і SAD є критичним моментом, від якого

залежить продуктивність IPSec. Особливості реалізації SPD і SAD залежать від вимог продуктивності і сумісності системи.

Всі протоколи, що входять в IPSec, можна розділити на дві групи:

- протоколи, що безпосередньо проводять обробку передаваних даних (для забезпечення їх захисту);
- протоколи, що дозволяють автоматично погоджувати параметри захищених з'єднань, необхідні для протоколів 1-ої групи.

Архітектура засобів безпеки IPSec представлена на рисунку 2.1.

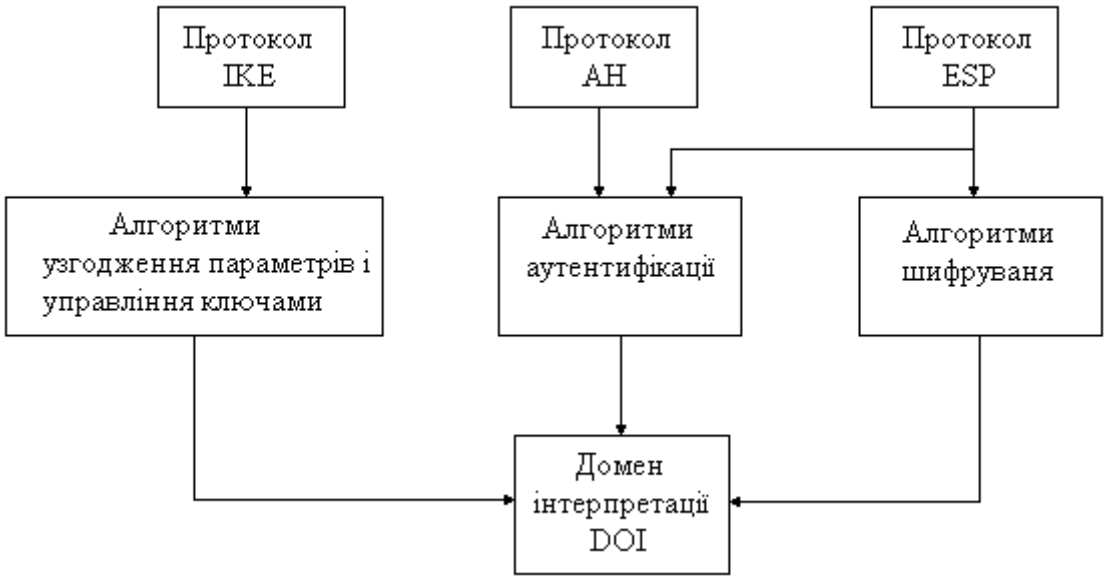

Рисунок 2.1 Архітектура стека протоколів IPSec

На верхньому рівні розташовано 3 протоколи, що складають ядро IPSec:

протокол узгодження параметрів віртуального каналу і управління ключами IKE (Internet Key Exchange), що визначає спосіб ініціалізації захищеного каналу, включаючи узгодження використовуваних алгоритмів криптоза-захисту, а також процедури обміну і управління секретними ключами в рамках захищеного з'єднання;

- протокол автентифікуючого заголовка AH (Authentication header), що забезпечує автентифікацію джерела даних, перевірку їх цілісності і

достовірності після прийому, а також захист від нав'язування повторних повідомлень;

- протокол інкапсулюючого захисту вмісту ESP (Encapsulating Security Payload), що забезпечує криптографічне закриття, автентифікацію і цілісність передаваних даних, а також захист від нав'язування повторних повідомлень.

Розділення функцій захисту між двома протоколами AH і ESP обумовлене вживаною в багатьох країнах практикою обмеження експорту або імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з протоколів AH і ESP може використовуватися як самостійно, так і спільно з іншим. З короткого перерахунку функцій протоколів AH і ESP видно, що можливості цих протоколів частково перекриваються.

Протокол AH відповідає тільки за забезпечення цілісності і автентичності даних, тоді як протокол ESP є могутнішим, оскільки може шифрувати дані, а крім того, виконувати функції протоколу AH (хоча автентифікація і цілісність забезпечуються ним в декілька урізаному вигляді).

Протокол ESP може підтримувати функції шифрування і автентифікації будь-яких комбінаціях, тобто або і ту і іншу групу функцій, або тільки автентифікацію/цілісність, або тільки шифрування.

Середній рівень архітектури IPSec утворюють алгоритми узгодження параметрів і управління ключами, вживані в протоколі IKE, а також алгоритми автентифікації і шифрування, використовувані в протоколах автентифікуючого заголовка AH і інкапсулюючого захисту вмісту ESP.

Слід зазначити, що протоколи захисту віртуального каналу верхнього рівня архітектура IPSec (AH і ESP) не залежить від конкретних криптографічних алгоритмів. За рахунок можливості використання великого числа різноманітних алгоритмів автентифікації і шифрування IPSec забезпечує високий ступінь гнучкості організації захисту мережі. Гнучкість IPSec полягає в тому, що для кожного завдання пропонується декілька способів її рішення. Вибрані методи для одного завдання зазвичай не залежать від методів

реалізації інших завдань. Наприклад, вибір для шифрування алгоритму AES не впливає на вибір функції обчислення дайджеста, використовуваного для автентифікації даних.

Нижній рівень архітектури Ipsec утворює так званий домен інтерпретації DOI (Domain of Interpretation). Необхідність застосування домена інтерпретації DOI обумовлена наступними причинами. Протоколи AH і ESP мають модульну структуру, допускаючи застосування користувачами по їх узгодженому вибору різних криптографічних алгоритмів шифрування і автентифікації. Тому необхідний модуль, який міг би забезпечити спільну роботу всіх вживаних протоколів і алгоритмів, що знов включаються. Саме такі функції покладені на домен інтерпретації DOI. Домен інтерпретації DOI як БД зберігає відомості про протоколи і алгоритми, що використовуються в IPSec , їх параметри, протокольні ідентифікатори і тому подібне. По суті, він виконує роль фундаменту в архітектурі IPSec. Для того, щоб використовувати алгоритми, відповідні національним стандартам як алгоритми автентифікації і шифрування в протоколах AH і ESP, необхідно зареєструвати ці алгоритми в домені інтерпретації DOI.

2.2.2. Особливості реалізації засобів IPSec

Вище було розглянуто, що протоколи AH або ESP можуть захищати передавані дані в двох режимах: тунельному, при якому IP-пакети захищаються цілком, включаючи їх заголовки, і транспортному, що забезпечує захист тільки вмісту IP-пакетів.

Основним режимом є тунельний. У тунельному режимі початковий пакет поміщається в новий IP-пакет і передача даних по мережі виконується на підставі заголовка нового IP-пакета. При роботі в цьому режимі кожен звичайний IP-пакет поміщається цілком в криптозахищеному вигляді в конверт IPSec, а той у свою чергу інкапсулюється в інший захищений IP-пакет. Тунельний режим зазвичай реалізують на спеціально виділених шлюзах безпеки, в ролі яких можуть виступати маршрутизатори або ME. Між такими

шлюзами і формуються захищені тунелі IPSec.

Після прийому на іншій стороні тунеля захищені IP-пакети «розпаковуються» і отримані початкові IP-пакети передаються комп'ютерам приймальної локальної мережі по стандартних правилах. Тунелювання IP-пакетів повністю прозоро для звичайних комп'ютерів в локальних мережах, тунелів, що є утримувачами. На кінцевих системах тунельний режим може використовуватися для підтримки віддалених і мобільних користувачів. В цьому випадку на комп'ютерах цих користувачів повинно бути встановлено ПО, що реалізовує тунельний режим IPSec.

У транспортному режимі передача IP-пакету через мережу виконується за допомогою початкового заголовка цього пакету. У конверт IPSec в криптозахищеному вигляді поміщається тільки вміст початкового IP-пакету і до отриманого конверта додається початковий IP-заголовок. Транспортний режим швидше тунельного і розроблений для застосування на кінцевих системах. Цей режим може використовуватися для підтримки віддалених і мобільних користувачів, а також захисту інформаційних потоків усередині локальних мереж. Слід зазначити, що робота в транспортному режимі відбивається на всіх системах, що входять до групи захищеної взаємодії , і в більшості випадків потрібне перепрограмування мережних додатків.

2.2.3. Основні схеми застосування IPSec

Застосування тунельного або транспортного режиму залежить від вимог, що пред'являються до захисту даних, а також від ролі вузла, в якому працює IPSec. Вузлом, що завершує захищений канал, може бути хост (кінцевий вузол) або шлюз (проміжний вузол). Відповідно розрізняють три основні схеми застосування IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз.

У схемі 1 захищений канал, або, що в даному контексті одне і те ж, SA,

встановлюється між двома кінцевими вузлами мережі, тобто хостамі HI і H2 (рисунок 2.2). Протокол IPSec в цьому випадку працює на кінцевому вузлі і захищає дані що поступають на нього.

Рисунок 2.2 Схема хост-хост

Для хостів, підтримуючих IPSec, дозволяється використовувати як транспортний режим, так і тунельний.

Відповідно до схеми 2 захищений канал встановлюється між двома проміжними вузлами, званими шлюзами безпеки SG1 і SG2 *(Security Gateway)*, на кожному з яких працює протокол IPSec (рисунок 2.3).

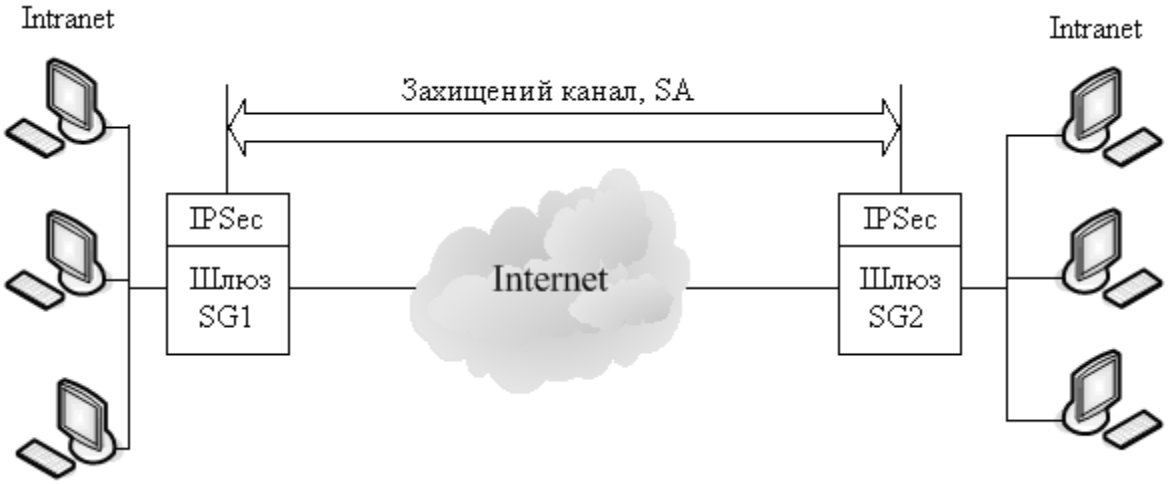

Рисунок 2.3 Схема шлюз-шлюз

Захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібна, вони передають свій трафік в незахищеному вигляді через довірчі мережі Intranet

підприємства. Трафік, що направляється в загальнодоступну мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою IPSec, діючи від свого імені. Шлюзам дозволяється використовувати тільки тунельний режим роботи, хоча вони могли б підтримувати і транспортний режим, але він в цьому випадку малоефективний.

При захищеному віддаленому доступі часто застосовується схема 3 хост-шлюз (рисунок 2.4).

Тут захищений канал організовується між віддаленим хостом H1, на якому працює IPSec, і шлюзом SG, що захищає трафік для всіх хостів, що входять в мережу Intranet підприємства. Віддалений хост може використовувати при відправці пакетів шлюзу як транспортний, так і тунельний режим, шлюз же відправляє пакети хосту тільки в тунельному режимі.

Цю схему можна модифікувати, створивши паралельно ще один захищений канал - між віддаленим хостом H1 і яким-небуть хостом H2 в середині мережі, що захищається шлюзом. Таке комбіноване використання двох SA дозволяє надійно захистити трафік і у внутрішній мережі.

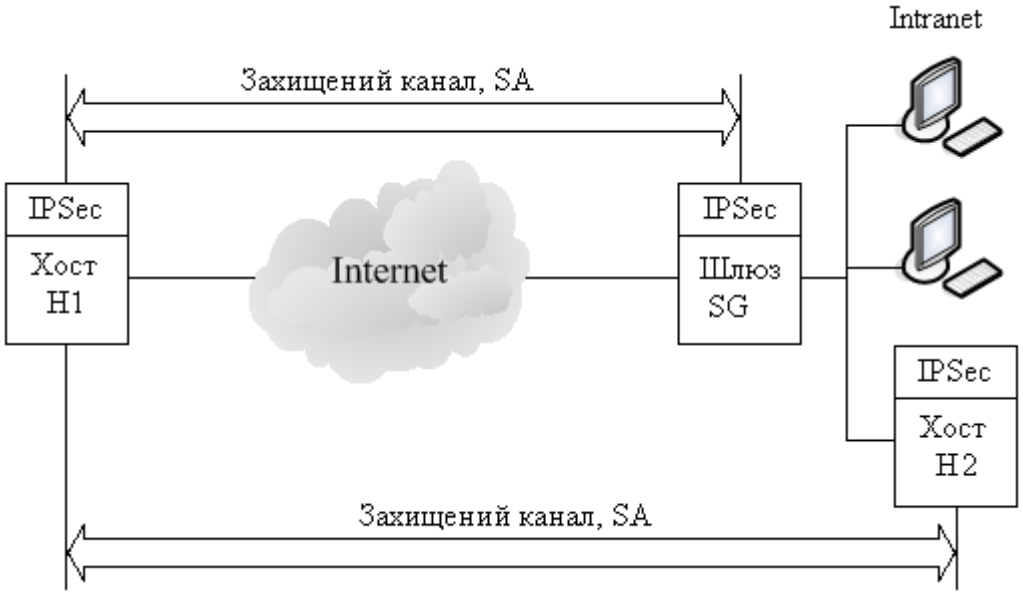

Рисунок 2.4 - Схема хост-шлюз, доповнена каналом хост-хост

Розглянуті схеми побудови захищених каналів на базі IPSec широко застосовуються при створенні різноманітних віртуальних захищених мереж

VPN. Їх спектр варіюється від провайдерських мереж, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних мереж VPN, що розгортаються і керуються самими компаніями. На базі IPSec успішно реалізуються віртуальні захищені мережі будь-якої архітектури, включаючи VPN з віддаленим доступом (Remote Access VPN), внутрішньокорпоративні VPN (Intranet VPN) і міжкорпоративні VPN (Extranet VPN).

2.2.4. Позитивні сторони засобів безпеки IPSec

Система стандартів IPSec увібрала в себе прогресивні методики і досягнення в області мережної безпеки, завоювала визнання фахівців як надійна і легко інтегрована система безпеки для IP-мереж. Система IPSec міцно займає сьогодні лідируючі позиції в наборі стандартів для створення VPN. Цьому сприяє її відкрита побудова, здатна включати все нові досягнення в області криптографії. IPSec дозволяє захистити мережу від більшості мережних атак «скидаючи» чужі пакети ще до того, як вони досягнуть рівня IP на приймаючому комп'ютері. У комп'ютер, що захищається, або мережу можуть увійти тільки пакети від зареєстрованих партнерів по взаємодії. IPSec забезпечує:

- автентифікацію - доказ відправки пакетів вашим партнером по взаємодії, тобто володарем секрету, що розділяється;
- цілісність - неможливість зміни даних в пакеті;
- конфіденційність - неможливість розкриття передаваних даних;
- надійне управління ключами - протокол IKE обчислює секрет, що розділяється, відомий тільки одержувачеві і відправникові пакету;
- тунелювання - повне маскування топології локальної мережі підприємства.

Робота в рамках стандартів IPSec забезпечує повний захист інформаційного потоку даних від відправника до одержувача, закриваючи трафік для спостерігачів на проміжних вузлах мережі. VPN-ріщення на основі

стека протоколів IPSec забезпечують побудову віртуальних захищених мереж, їх безпечну експлуатацію і інтеграцію з відкритими комунікаційними системами.

2.3. Реалізація захисту VPN з використанням протоколу OpenVPN

OpenVPN - вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим вихідним кодом для створення зашифрованих каналів типу точка-точка або сервер-клієнти між комп'ютерами. Вона дозволяє встановлювати з'єднання між комп'ютерами, що знаходяться за Nat-firewall, без необхідності зміни їх налаштувань.

Не будемо зупинятись на технічних подробицях, але найдосконалішим є протокол OpenVPN. Саме на нього варто орієнтуватися під час вибору сервісу, яким будемо користуватися надалі.

Для забезпечення безпеки каналу, і потоку даних, OpenVPN використовує бібліотеку OpenSSL. Завдяки цьому задіюється весь набір шифрів, доступних в даній бібліотеці. Також може використовуватися пакетна авторизація HMAC, для забезпечення більшої безпеки, і апаратне прискорення для поліпшення продуктивності шифрування. Ця бібліотека використовує OpenSSL, а точніше протоколи SSLv3/TLSv1. OpenVPN використовується на Solaris, OpenBSD, FreeBSD, NetBSD, Gnu/Linux, Apple Mac OS X, QNX і Microsoft Windows.

OpenVPN пропонує користувачеві декілька видів автентифікації.

Передвстановлений ключ, - найпростіший метод.

Сертифікатна автентифікація, - найбільш гнучкий в налаштуваннях метод.

За допомогою логіна і пароля, - може користовуватися без створення клієнтського сертифікату (серверний сертифікат все одно потрібний).

OpenVPN проводить всі мережні операції через TCP, або UDP порт. Також можлива робота через велику частину проксі серверів, включаючи HTTP, через NAT і мережні фільтри. Сервер може бути налаштований на призначення мережних налаштувань клієнтові. Наприклад: IP адреса, настройки маршрутизації і параметри з'єднання. OpenVPN пропонує два різні варіанти

мережних інтерфейсів, використовуючи драйвер Tun/Tap. Можливо створити Layer 3-based IP тунель, званий TUN, і Layer 2-based Ethernet - TAP, здатний передавати Ethernet трафік. Також можливе використання бібліотеки компресії LZO, для стиснення потоку даних. Використовуваний порт 1194 виділений Internet Assigned Numbers Authority для роботи даної програми.

Використання в OpenVPN стандартних протоколів TCP і UDP дозволяє йому стати альтернативою IPSec в ситуаціях, коли Інтернет-провайдер блокує деякі VPN протоколи.

2.3.1 Основні можливості OpenVPN

OpenVPN являє собою VPN нового покоління. Хоча інші рішення VPN часто використовують власні або нестандартні механізми, OpenVPN має модульну концепцію, що є основою безпеки створюваних мереж. OpenVPN використовує безпечні, стабільні і добре зарекомендовані SSL / TLS механізми автентифікації і шифрування, а також є простішим в реалізації ніж інші VPN-рішення, як наприклад IPsec. У той же час він надає можливості, які виходить за рамки будь-якої іншого реалізації VPN: Layer 2 і Layer 3 VPN: OpenVPN пропонує два основні режими роботи VPN тунелю.

Таким чином OpenVPN тунелі можуть також транспортувати Ethernet кадри, IPX-пакети та Windows Network Browsing пакети (NetBIOS), що є проблемою для інших рішень VPN.

2.3.2. Мережна взаємодія з OpenVPN

Переваги модульної структури OpenVPN проявляються не тільки при забезпеченні безпеки, а й у гнучкості при побудові мереж. Джеймс Йонан вибрав універсальний TUN / TAP драйвер для мережного адаптера. TUN / TAP драйвер має відкритий вихідний код проекту, який входить до складу всіх сучасних Linux / UNIX систем, а також для Windows і Mac OS X. Система шифрування SSL / TLS використовується в багатьох проектах і постійно вдосконалюється, до неї додаються нові функції. Використання TUN / TAP

пристроїв значно полегшує структуру OpenVPN . Його проста структура дає більш високий рівень безпеки в порівнянні з іншими рішеннями VPN. Складність завжди була і є головним ворогом безпеки. Наприклад, IPsec має складну структуру зі складними змінами в ядрі, тим самим створюючи безліч можливих лазівок безпеки.

Універсальний TUN / TAP драйвер це віртуальний мережний інтерфейс, який є абсолютно прозорим для всіх додатків та користувачів. Кожна програма, що працює з мережним інтерфейсом може працювати через інтерфейс тунелю.

На рисунку 2.5 зображений OpenVPN з використанням стандартних інтерфейсів:

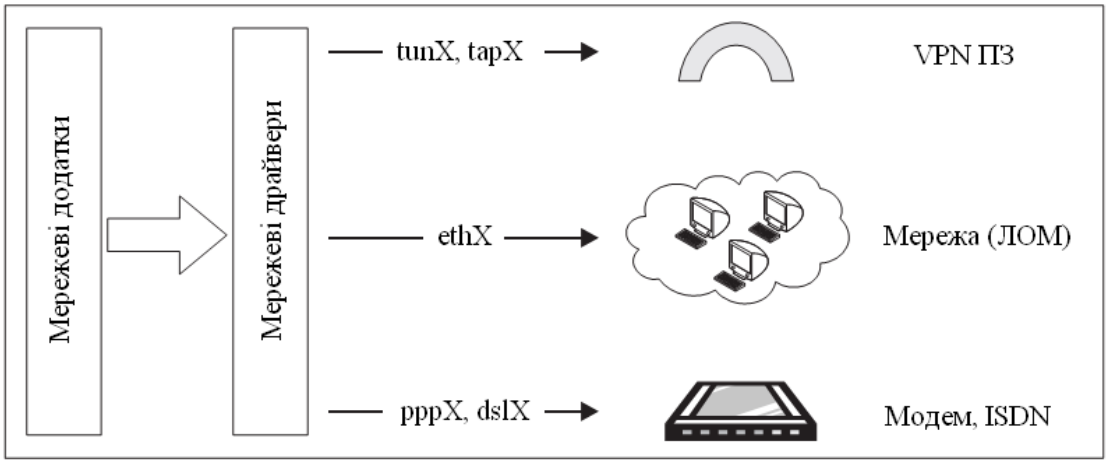

Рисунок 2.5 - Режими OpenVPN

Пристрій TUN може використовуватися як віртуальний точка-точка інтерфейс, як модем або DSL. Це називається маршрутизований режим, тому що для партнера VPN створюються маршрути.

TAP пристрій може бути використаний як віртуальний адаптер Ethernet. Це дозволяє службі прослуховувати інтерфейс для захоплення Ethernet кадрів, чого не можно зробити з пристроями TUN. Цей режим називається режим моста, оскільки мережі з'єднані так як ніби їх з’єднали за допомогою звичайного L2 комутатора.

Додатки можуть посилати інформацію на цей інтерфейс, драйвер тунелю буде приймати всі дані і шифрувати їх за допомогою криптографічних бібліотек SSL / TLS. Шифровані дані можуть передаватися як за допомогою TCP так і UDP протоколу. UDP вибирається за замовчуванням, але якщо є така необхідність то можна вибрати TCP.

2.3.3. Безпека OpenVPN

OpenVPN будується на міцному фундаменті безпеки. Її ядро системи шифрування, SSL / TLS, є найбільш широко поширеними системами в промисловості. Він пройшов ретельні перевірки не виявивши ніяких відомих недоліків. Правильно реалізований, SSL / TLS дає максимальну безпеку в даний час. Творець OpenVPN, Джеймс Yonan, проробив чудову роботу по реалізації SSL / TLS, але на цьому не обмежився. OpenVPN також має додаткові функції, які підвищують здатність справлятися з невідомим уразливості, які можуть виникати в будь-якому OpenVPN або SSL / TLS ядрі.

Генерація ключів

Як тільки SSL / TLS проведе процедуру “рукостискання” завершиться взаємна автентифікація, і будуть згенеровані чотири різних ключі; HMAC відправника, HMAC отримувача, ключ шифрування / дешифрування відправника, і шифрування / дешифрування отримувача. Ніколи не можна використовувати той же ключ декілька разів (асиметричний, симетричний, геш, або цифрового підпису) і OpenVPN дотримується цієї філософії.

Обмін Ключами

З метою захисту даних, здійснюється їх симетричним шифрування. Для роботи симетричного криптоалгоритму один і той самий ключ повинен бути на кожному кінці з'єднання. Це описано в протоколі обміну ключами. IPSec використовує систему під назвою Internet Key Exchange (IKE) для обміну ключами. В ході роботи даної системи пересилається шість повідомлення туди і назад, що в кінцевому підсумку призводить до ідентифікації кожної системи і

генерації або обміну симетричними ключами. OpenVPN використовує стандартне з клієнтом автентифікації для досягнення тієї ж мети.

На рисунку 2.6. наведена схема “рукостискання”.

Пройдемося по кожному з цих повідомлень, і подивимося для чого вони призначені.

Повідомлення 1

Клієнт посилає привітання, починаючи рукостискання. В привітання включений список шифрів, що він підтримує, а також один з параметрів RSA або Diffie-Hellmann генерації ключа.

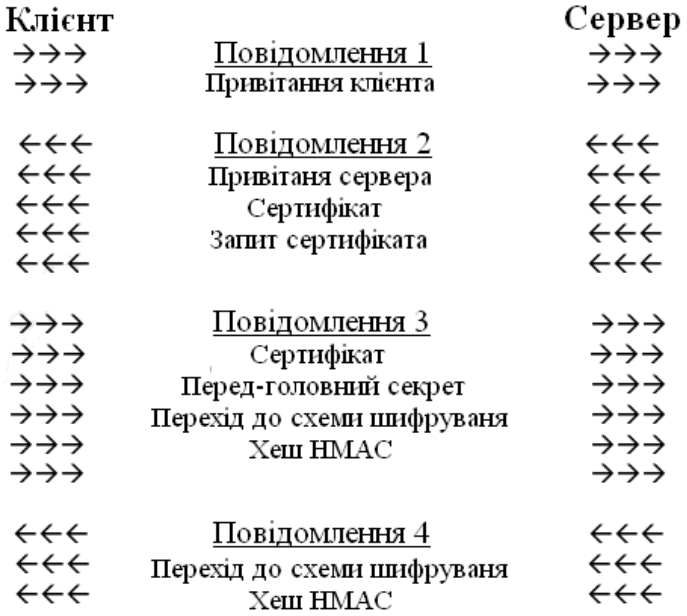

Рисунок 2.6 - RSA / DHE “рукостискання” .

Повідомлення 2

Сервер вибирає шифр зі списку клієнта і відправляє його назад разом із сертифікатом сервера, який включає в себе відкритий ключ сервера підписаний центром сертифікації. Це дуже важлио. Одержаний сертифікат перевіряється на автентичність за допомогою відкритого ключа центра сертифікації. Якщо все вірно клієнт впевнений в достовірності іншої сторони. Якщо не проводити цю процеду система буде вразливою для атак “man in the middle”. Також клієнт

отримає серверну частину RSA або параметр Diffie-Hellmann і запит з сервера на клієнтський сертифікат.

Повідомлення 3

У повідомленні три, клієнт відправляє свій сертифікат, підписаний за допомогою закритого ключа центру сертифікації. Сервер використає відкритий ключ центру сертифікації, щоб перевірити справжність цього сертифіката. Крім того, клієнт формує і посилає те, що називається перед-головний секрет, це називається Exchange Client Key. Це ключовий крок у “рукостисканні”, а основна мета інші кроки. Якщо цей крок піде не так, безпека не буде забезпечена належним чином. Перед-головний секрет останній параметр в ключовому обміні функції (RSA або Diffie-Hellmann) і шифрується за допомогою відкритого ключа сервера. Як тільки сервер отримує цей параметр, обидві сторони матимуть необхідну інформацію для обчислення еквівалентних симетричних ключів. Перед-головний секрет може бути розшифрований тільки за допомогою закритого ключа сервера і, якщо все йде правильно, тільки сторона, що має цей ключ може бути сервером, до якого ми намагаємося підключитися.

В кінці цього повідомлення ми бачимо Change Cipher Spec – це означає, що в даний час переходимо до схеми шифрування про яку домовилися в Повідомлення 2 і всі наступні повідомлення будуть зашифровані. Останній крок HMAC дуже важливий. На цьому етапі клієнт посилає геш-значення всього “рукостискання”. Це гарантує, що обидві сторони отримують одну і ту ж інформацію. В загальнлму випадку на даному етапі атака проводиться з метою підміни шифрів та ключів. Останній крок HMAC виявить такі упущення і закриє з'єднання.

Генерація ключів

У цей момент обидві сторони створюють симетричні ключі необхідні для початку захищеного зв'язку. Перед-головний секрет використовується для генерації головного секрету. Головний секрет по обидві сторони тунелю змінюється за допомогою декількох геш конкатенації створюючи довгий

ключовий блок, який робиться у відповідності до заданого розміру. Всі ключі генеруються з розділів цього ключового блоку.

Повідомлення 4

Сервер робить Change Cipher Spec для початку шифрування за схемою узгодженою в повідомленні 2. Також сервер робить останній крок HMAC, щоб удостовіритись в тому, що всі надіслані та отримані дані правильні. Тепер встановлено шифрований тунель за допомогою симетричного шифрування між нашими двома кінцевими точок.

РОЗДІЛ 3. Рекомендації щодо реалізації віртуальної приватної мережі із заданими характеристиками.

Для більшості компаній малого та середнього бізнесу рано чи пізно постає питання побудови віртуальної приватної мережі. Це може бути зумовлено різнимим потребами як на приклад роботою деяких працівників вдома, або підключенням нового офісу. Перш ніж будувати VPN потрібно визначитись який рівень критичності інформації, що буде передаватися через цю мережу. Потім визначити який рівень OSI повинен бути реалізований даною VPN. Всі інші аспекти не мають такого впливу на вибір технології віртуальної приватної мережі, як два вищезгадані. На базі будь-якої технології можна побудувати VPN віддаленого доступу або ExtranetVPN , Internet VPN, тому призначення не є принциповим питанням при виборі технології VPN.

Розглянемо типову ситуацію для малого та середнього бізнесу (так званий SOHO сегмент). В деякої компанії К був лише один офіс (офіс А головний), але з часом компанія збільшилась і відкрила філіал в іншому місті (офіс В). Звісно ж виникла потреба працівникам філіалу надати доступ до ресурсів головного офісу. Для вирішення даного завдання буде побудована віртуальна приватна мережа наступного вигляду (рисунок 3.1)

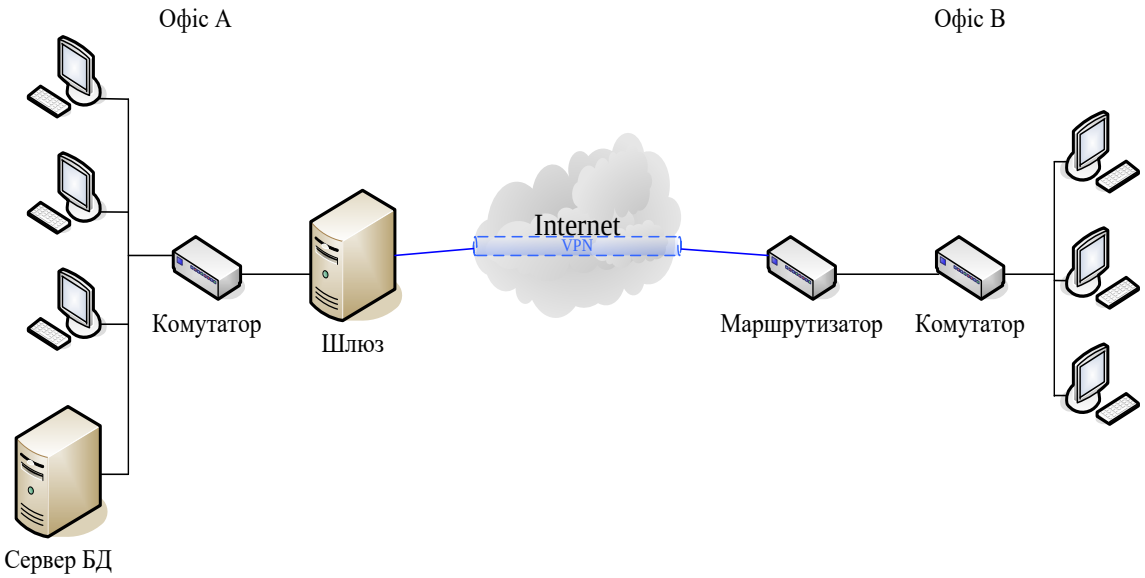

Рисунок 3.1 - Схема VPN компанії К

В якості шлюзу офісу А буде використано програмний маршрутизатор ClearOS 5.2. Даний проект побудований на базі RedHat Linux і має дуже широкий функціонал, більш детально з яким можна ознайомитись на сайті проекту http://www.clearfoundation.com . Нас цікавлять функції стосовно VPN, на базі даного проекту можно організувати сервер VPN: PPTP, IPSec і OpenVPN. Власне на даних технологіях можна і зупинити свій вибір. Три вище згадані технології є основними технологіями побудови захищених VPN.

В якості маршрутизатора офісу В можно використати один з маршрутизаторів MikroTik з рівнем ліцензії ОС не нижче 4. ОС маршрутизаторів MikroTik має дуже широкий функціонал і, що головне для нас підтримує всі розповсюджені технології побудови VPN. В обох маршрутизаторах є системи intrusion detection, intrusion prevention і звісно firewall. І без того не бідний функціонал ClearOS 5.2 можно розширити за домомогою установки додаткового ПО, оскільки він сумісний з RedHat Linux. Функціонал MikroTik розширити не можна, але його більш ніж достатньо для офісу філіала.

Тестовий стенд для моделювання віртуальної приватної мережі буде створено за допомогою системи віртуалізації VirtualBox і роутера D-Link, який

буде грати роль комп’ютера філіала. Отже тестовий стенд буде мати наступний вигляд(рисунок 3.2.)

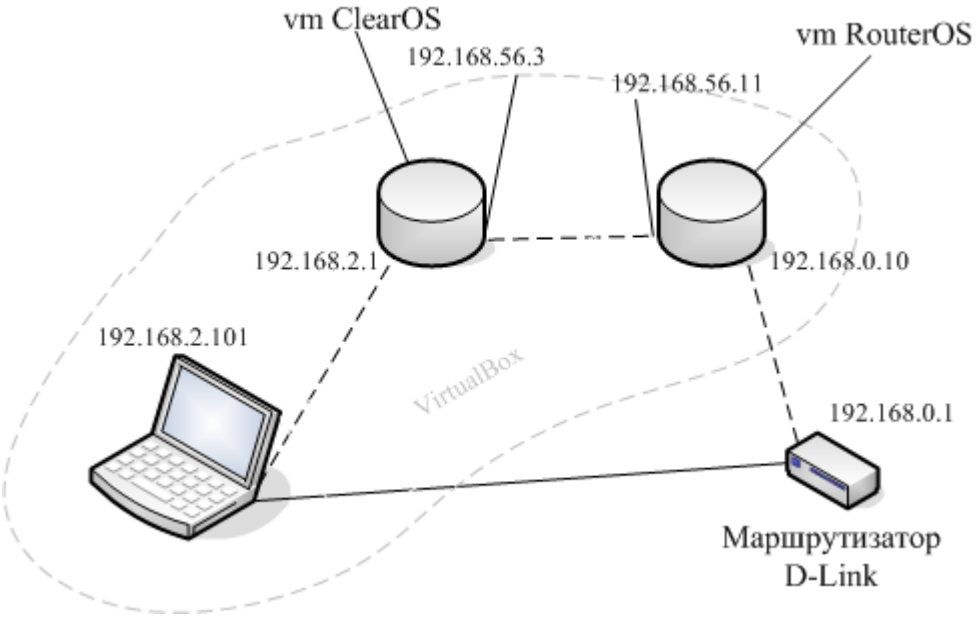

Рис. 3.2 - Тестовий стенд VPN

Не зважаючи на те, що фізично маршрутизатор під’єднаний до комп’ютера, зв’язок між ними може бути тільки при встановленому VPN з’єднанню. Більш детально зупинятись на налаштуваннях тестового стенду немає сенсу - перейдемо одразу до побудови VPN.

3.1 Реалізація VPN за допомогою IPSec

Якщо ж безпеки пропонованої PPTP не достатньо варто звернути увагу на IPSec.

Для налаштування IPSec в ClearOS потрібно ввімкнути IPSec сервіс і додати unmanaged VPN connection. Також ClearOS запропонує відкрити порт ME з чим потрібно погодитись.

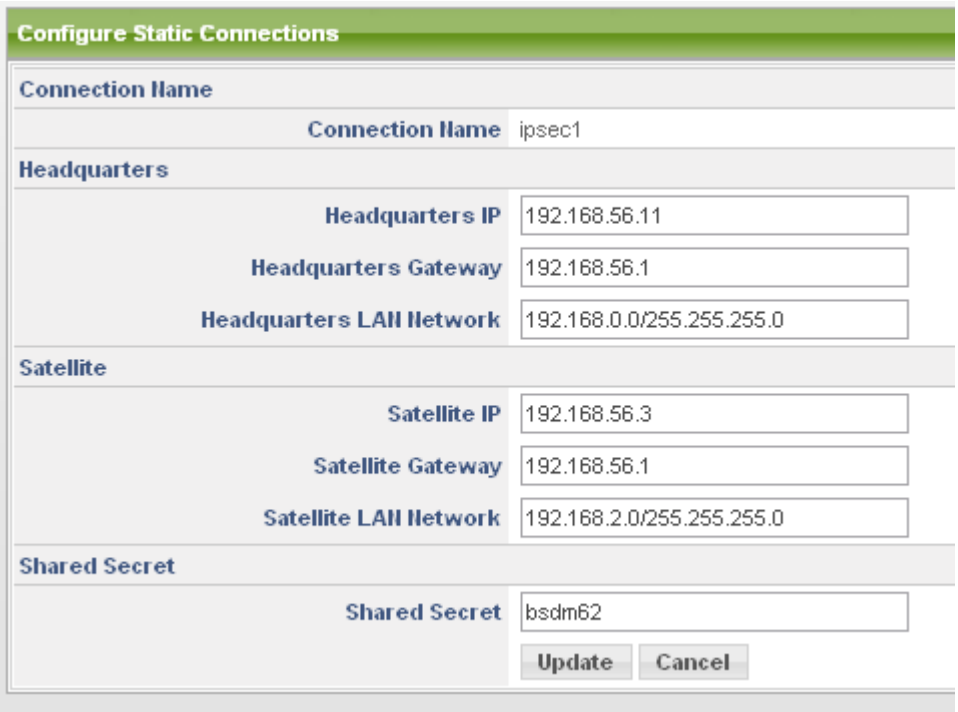

Рис. 3.3 - IPSec налаштування в ClearOS

В даному вікні потрібно вказати назву з'єднання власну адресу, адресу віддаленого клієнта , ключ, а також мережі які потрібно з'єднати. На цьому налаштування ClearOS завершено.

Створимо політику IPSec в RouterOS для цього у вкладці IP виберемо IPSec далі New IPSec Policy

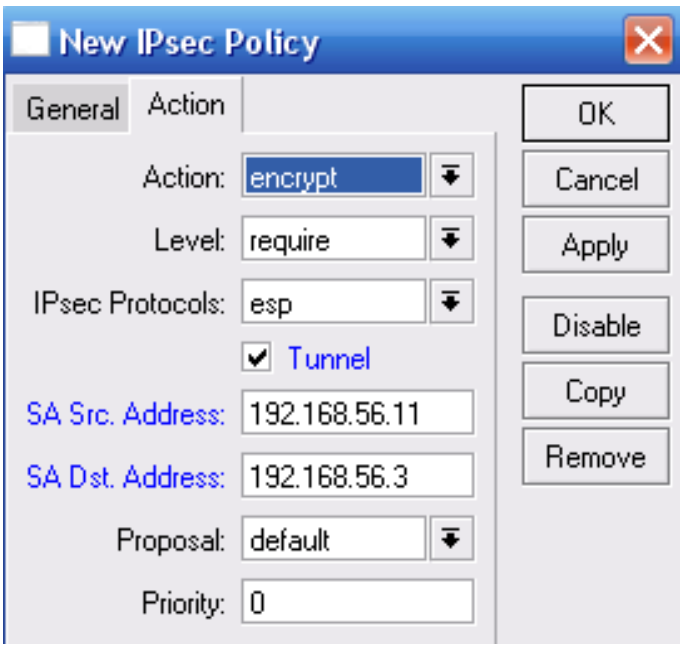

Рис. 3.4 - Створення політики IPSec в RouterOS

На даному етапі слід вказати інкапсулюючий протокол та адреси шлюзів IPSec. Оскільки IPSec не працює через NAT то адреси повинні бути “зовнішні” і постійні. Далі потрібно створити IPSec з’єднання.

На даному етапі потрібно вказати тип автентифікації (статичний ключ, сертифікат), вибрати геш-функцію (sha1, MD5), алгоритм шифрування (DES, 3DES, AES128, AES192, AES256) та групу Діффі-Хелмана. Після того як з’єднання створено потрібно створити правило NAT. В графі IP виберемо Firewall далі NAT і додамо правило. Полю Chain присвоїмо значення srcnat, полю Src. Address 192.168.0.0/24, Dst. Address 192.168.2.0/24, Out. Interface виберемо інтерфейс інтернету в моєму випадку це ether1, полю Action значення masquerade.

На цьому налаштування IPSec завершено. В результаті вищевказаних дій маємо VPN з’єднання з 3DES шифруванням, автентифікацією по статичному ключу та геш функцією MD5.

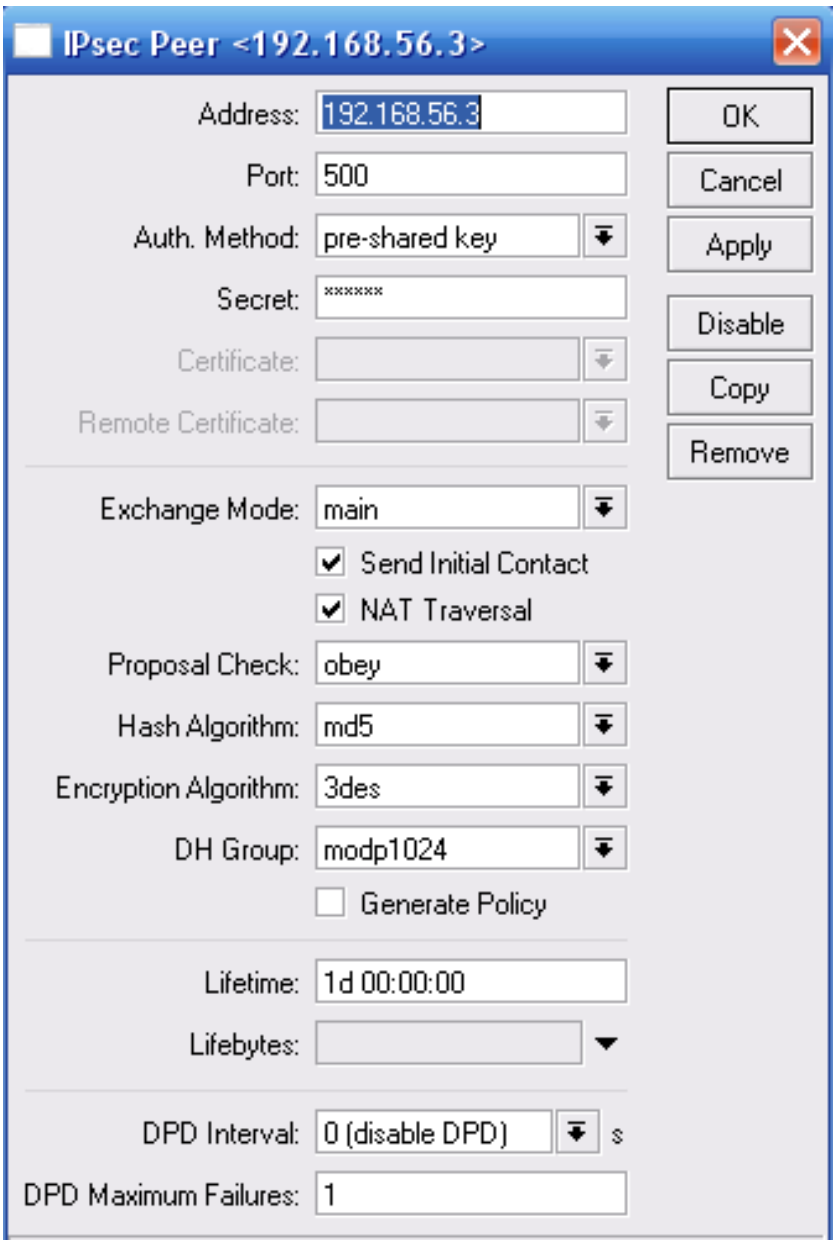

Рис. 3.5 - Створення IPSec з'єднання в RouterOS

3.2 Реалізація VPN за допомогою OpenVPN

Налаштування OpenVPN в ClearOS через веб-інтерфейс не доступні, тому всі налаштування будуть проводитися шляхом редагування конфігураційних файлів.

Для початку потрібно завантажити сертифікат та секретний ключ клієнта та сертифікат центру сертифікації. Як вже було сказано вище сертифікат та ключ створюються при створенні користувача. Для завантаження сертифікату

потрібно ввійти в систему від імені куристувача, сертифікат якого потрібно отримати.

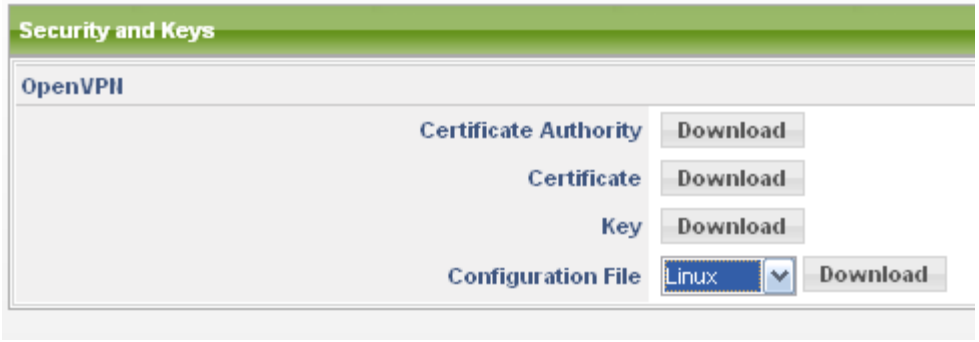

Рис. 3.6 - Завантаження сертифікату та закритого ключа в ClearOS.

Далі потрібно відредагувати файл /etc/openvpn/clients.conf. та вимкнути стиснення трафіку оскільки реалізація VPN в RouterOS його не підтримує

comp-lzo

вибрати тип трафіку tcp

proto tcp

вимкнути додаткову автентифікацію за допомогою логіна і пароля,

прибрати пул адрес ifconfig-pool-persist /var/lib/openvpn/ipp.txt

також можна прибрати параметри DNS, WINS, DOMAIN

Натомість додамо наступне

Вкажемо алгоритм шифрування та автентифікації трафіка

cipher AES-256-CBC

auth sha1,

вкажемо директорію з конфігурацією клієнтів

client-config-dir ccd,

вкажемо маршрут да мережі за маршрутизатором офісу B

route 192.168.0.0 255.255.255.0.

Після того як файл /etc/openvpn/clients.conf відредаговано потрібно створити в client-config-dir файл з іменем клієнта, який має підключатись і наступним змістом:

ifconfig-push 10.8.0.3 10.8.0.1

iroute 192.168.0.0 255.255.255.0

В цьому файлі вказується адреса, що буде видаватись клієнтові та маршрут до мережі за ним.

Запускаємо сервіс OpenVPN кнопкою Start і на цьому налаштування ClearOS можна вважати завершеним.

Сертифікати клієнта, що завантажувалися потрібно імпортувати в RouterOS. Після того як сертифікати імпортовано в меню Interface додамо OVPN Client.

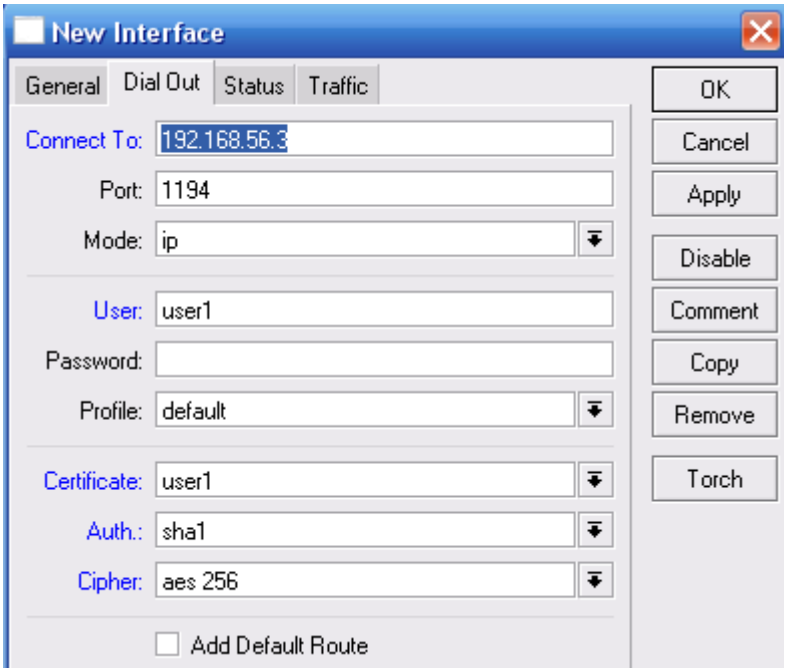

Рис. 3.7- Налаштування клієнта OpenVPN на RouterOS.

На даному етапі потрібно вказати адресу сервера та порт , режим роботи (L2=ethernet,L3=ip), вибрати сертифікат клієнта, алгоритм шифрування та автентифікації.

Після виконання вище вказаних налаштувань отримуємо L3 VPN тунель з шифруваням AES256.

ВИСНОВКИ

Метою даної роботи є вибір до застосування віртуальних приватних мереж на основні порівняльного аналізу за вибраними критеріями.

1. Проведено дослідження особливостей побудови віртуальних приватних мереж як об’єктів створення захищеної інформаційно-комунікаційної системи організації: варіантів побудови віртуальних захищених каналі, засобів забезпечення безпеки VPN, у тому числі на канальному рівні та на мережному рівні.

2. Проведено обґрунтування основних критеріїв вибору конфігурації та методів побудови віртуальної приватної мережі організації на основі політики безпеки та виявлено дві групи критеріїв: До першої групи критеріїв пропонується віднести: критерії сертифікації, критерій стандартизації/сумісності, критерій продуктивності/надійності, критерій наявності системи діагностики, критерій пріоритету трафіку, критерій можливості роботи з частиною інформаційних потоків без шифрування, критерій масштабованості VPN. До другої групи критеріїв може бути віднесена робота з криптографічними ключами та підтримки роботи центру сертифікації ключів. До додаткових критеріїв вибору можна віднести остаточну вартість VPN, наявність технічної підтримки та гарантійного обслуговування, а також адаптованого до умов використання програмного забезпечення та технічної документації.

3. Наведені рекомендації щодо реалізації віртуальної приватної мережі організації із заданими характеристиками за допомогою протоколів IPSec та Open VPN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

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

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

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

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

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

8.Медведев Н. Г. Аспекти інформаційної системи віртуальних приватних мереж / Н. Г. Медведев, Д.В. Москалик - К: Европ.. ун-та, 2002.

9.Ситник В.О. Основи інформаційних систем. – К.: КНЕУ, 1997.