МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Захищена мережа на базі інструментальних засобів технології VPN»

Виконавець: _____ Анастасія ЮРЧЕНКО
(підпис)

Керівник: _____ Віталій КУРУШКІН
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Юрченко Анастасії Андріївни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Захищена мережа на базі інструментальних засобів технології VPN»
затверджена наказом ректора від « 29 » березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи:протоколи VPN, структура мережі, тунелювання, шифрування, архітектура мереж VPN, комутована мережа
4. Зміст пояснювальної записки: поняття та класифікація VPN мереж; особливості побудови vpn мереж; захищена мережа на базі інструментальних засобів технології VPN
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: як працює vpn?, класифікація vpn, протоколи vpn мережі, модель osi, як працює шифрування, віртуальні захищені канали типу мережа – мережа, клієнт – мережа, захищена мережа засобом програмно-апаратного захисту інформації шифр-vpn

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-23.05.2023	Виконано
2	Аналіз науково-технічної літератури	24.05.2023-25.05.2023	Виконано
3	Поняття та класифікація vpn мереж	26.05.2022-31.05.2022	Виконано
4	Особливості побудови vpn мереж	01.06.2022-07.06.2022	Виконано
5	Захищена мережа на базі інструментальних засобів технології vpn	08.06.2022-14.06.2022	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Анастасія ЮРЧЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота складається із вступу, трьох розділів, загальних висновків, переліку використаних джерел, і має 69 сторінок, 21 рисунок, 25 використаних джерел.

Ключові слова: VPN, КОРПОРАТИВНА МЕРЕЖА, ПРОТОКОЛИ VPN, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, КОНФІДЕНЦІЙНІСТЬ, МЕРЕЖІ VPN, КОНФІГУРАЦІЯ VPN, PROXY.

Метою кваліфікаційної роботи є захист мережі від несанкціонованого доступу з використанням технології VPN. У кваліфікаційній роботі були проаналізовані основні підходи що до створення захищеної мережі з використанням VPN технології та було досліджено побудову захищеної мережі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

КМ — корпоративна мережа

ЛОМ — локальна обчислювальна мережа

МЕ — міжмережний екран

ОС — операційна система

ПЗ — програмне забезпечення

IP — Internet Protocol (IP-адреса)

AES — Advanced Encryption Standard (алгоритм блочного шифрування)

LAN — Local Area Network (Локальна комп'ютерна мережа)

TCP — Transmission Control Protocol (Протокол керування передаванням)

IT — Information Technologies (Інформаційні технології)

RAM — Random Access Memory (пам'ять з довільним доступом)

HTTP — Hyper Text Transfer Protocol (протокол передачі гіпертексту)

NAT — Network Address Translation (перетворення мережевих адрес)

IPSec — IP Security (протокол безпеки)

IETF — Internet Engineering Task Force (міжнародне співтовариство Інтернету)

ISP — Internet Service Provider (постачальник послуг інтернету)

DNS — Domain Name System (доменна система імен)

PKI — Public Key Infrastructure (Інфраструктура відкритих ключів)

SSL — Secure Sockets Layer (рівень захищених сокетів)

HMAC — Hash Message Authentication Code (хеш-код аутентифікації повідомлень)

VPN — Virtual Private Network (віртуальна приватна мережа)

PPTP — Point-to-Point Tunneling Protocol (тунельний протокол типу точка-точка)

L2TP — Layer 2 Tunneling Protocol (протокол тунелювання другого рівня)

ВСТУП

В основі захисту інформації в корпоративних мережах лежить запобігання викрадення інформації. Переважна більшість людей має доступ до мережі Internet, а хакерів на сьогоднішній день більше як ніколи. Постає питання захисту мережі, яке не варто відкладувати на потім, з рештою, це може обернутись збитками для компанії.

Сьогодні Інтернет став невід'ємною частиною побуту, він постійно розвивється, удосконалюється, і це змінило вид діяльності багатьох людей і організацій. Деякі організацій були атаковані зловмисниками, і це привело до великих втрат. Мережі організацій, які не знають або ігнорують проблеми захисту інформації від витоку, піддають себе великому ризику бути атакованими злочинцями.

Існує також багато інших причин, як, приклад вразливість сервісів TCP/IP. Деякі із сервісів TCP/IP можуть бути атакованими злочинцями, особливо вразливі сервіси які використовуються для покращення управління мережею.

Мета та завдання. Метою роботи є дослідження захищеної мережі з використанням інструментальних засобів технології VPN. Для побудови захищених корпоративних мереж. Завданнями дослідження є:

1. Поняття та класифікація VPN мереж. Дослідити протоколи VPN.
2. Особливості побудови VPN мереж. Поняття "тунелю" під час передачі даних у мережі. Види архітектури VPN мереж.
3. Побудова захищеної мережі засобами технології VPN.

Об'єктом дослідження є безпека захищеної мережі.

Предметом дослідження є побудова в корпоративних мережах систем захисту інформації.

РОЗДІЛ 1
ПОНЯТТЯ ТА КЛАСИФІКАЦІЯ VPN МЕРЕЖ

1.1. Основні поняття і функції мережі VPN

VPN – це технологія, яка може забезпечити одне або кілька мережних з'єднань (логічні мережі) поверх іншої мережі (наприклад, Інтернет). Незважаючи на те, що всі комунікації, які здійснюються через мережі з меншим невідомим рівнем довіри (наприклад, по публічним мережам), рівень довіри до побудованої логічної мережі не повинен залежати від рівня довіри до базових мереж, завдяки задіянню методів криптографії (шифрування, аутентифікації, використанняінфраструктури для відкритих ключів, засобів для захисту від колізій і зміни повідомлень переданих по логічної мережі).

У VPN-технологій мета полягає в максимальному рівні відокремлення потоків даних одного користувача від потоків даних всіх інших користувачів в мережі загального користування. Відокремленість повинна бути забезпечена відносно параметрів пропускної здатності каналів і в яких буде гарантуватися конфіденційність. Отже, завданнями технологій VPN є максимальне забезпечення в мережах загального користування їхній захист від можливого несанкціонованого доступу, та гарантованої якості обслуговування для потоків даних.

З рештою, основним завданням VPN є захист трафіку, саме тому віртуальна мережа повинна бути задовольняти великій кількості вимог і, в першу чергу, мати надійну криптографію, яка буде гарантувати захист від прослуховування, зміни, завадостійкості. Крім того, VPN мати повинна надійну систему управління ключами та кріптоінтерфейс, це дозволить здійснити криптоопераціі: програми шифрування дисків і файлів, захищена пошта і ін. На сьогодні інтерес до використання засобів щоб побудувати VPN постійно зростає, це обумовлено нізкою причин:

- низька вартість експлуатації за рахунок використання мереж загального користування замість орендованих ліній зв'язку або власних;

- масштабованість використанних рішень;

- простотою щоб змінити конфігурацію;

- "прозорістю" для користувачів і додатків.

При використанні VPN-технологій ще можно забезпечити:

- захист (автентичність, цілісність та конфіденційність) переданої мережами загального користування інформації;

- захист сегментів в середені мережі від несанкціонованого доступу з боку мережі загального користування;

- приховування структури, ще всередені захищених сегментів мережі;

- аутентифікацію та ідентифікацію користувачів мережевих об'єктів;

- централізоване управління безпекою в корпоративній мережі і VPN - мережі.

1.2. Способи створення захищених віртуальних каналів

З будь-якого з двох вузлів віртуальної мережі, між якими буде формуватися захищений тунель, може належати проміжній або кінцевій точці захищеного потоку повідомлень. Відповідно можуть бути різні способи утворення захищеного віртуального каналу, приклад захищеного віртуального каналу зображений на рисунку 1.1.

Варіант, при якому кінцеві точки захищеного тунелю збігаються з кінцевими точками захищеного потоку повідомлень, є більш кращим з точки зору безпеки. У цьому випадку забезпечена повна захищеність каналу на всьому шляху де прямують пакети повідомлень. Однак такий варіант веде до децентралізації управління і надмірності витрат за ресурсами. Потрібна установка засобів для створення захищених тунелів на кожен клієнтський комп'ютер локальної мережі, це створює перешкоду централізованому управлінню

доступом до ресурсів комп'ютерів і економічно не завжди виправдано. У великій мережі окреме адміністрування кожного клієнтського комп'ютера з метою конфігурації в ньому засобів захисту є досить важкою процедурою [3].

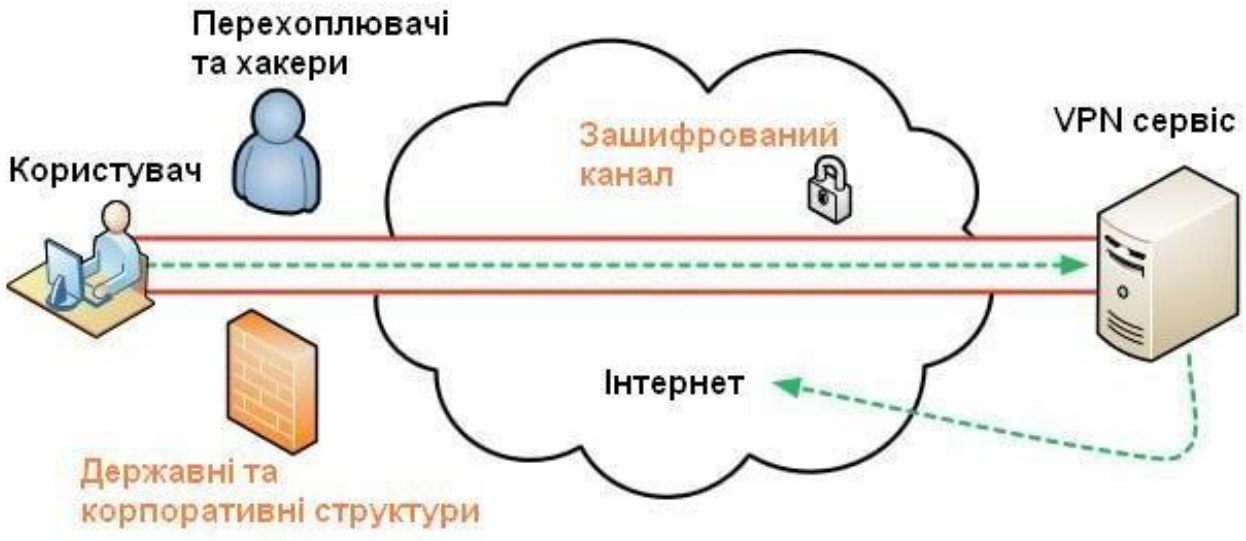

Рис. 1.1. Створення захищеного віртуального каналу

Тому у випадку, якщо немає необхідності у захисті трафіку всередині локальної мережі, яка входить в віртуальну мережу, то в якості кінцевої точки захищеного тунелю є сенс вибрати фаєрвол або прикордонний маршрутизатор цієї локальної мережі. У разі ж, коли потрібно всередині локальної мережі потік повідомлень також захистити, то в якості кінцевої точки створеного тунелю в цій мережі повинен виступати комп'ютер, який представляє одну зі сторін захищеної лінії. При доступі до локальної мережі віддаленого користувача, його комп'ютер також повинен бути кінцевою точкою в захищеному віртуальному каналі.

Розповсюджений також варіант, що характеризується ще більш низькою безпекою, але в одночас більш високою зручністю застосування. Відповідно до цього варіанту робочі станції і сервери в локальній мережі, а також інші комп'ютери не беруть участь у створенні захищеного тунелю, який створюється тільки всередині загальної мережі з комутацією пакетів, напри-

клад, всередині Internet. В якості кінцевих точок такого тунелю найчастіше виступають провайдери мережі Internet або прикордонні маршрутизатори (брандмауери) локальної мережі. При віддаленому доступі до локальної мережі тунель буде створюватись між сервером віддаленого доступу провайдера Internet, а також прикордонним провайдером Internet, або маршрутизатором (брандмауером) локальної мережі. При об'єднанні локальних мереж тунель буде формуватись тільки між прикордонними провайдерами Internet або маршрутизаторами (брандмауерами) локальної мережі.

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

Компоненти віртуальної мережі виконують створення захищеного тунелю, що функціонують на вузлах, між якими формується тунель. Ці компоненти мають назву ініціатора і термінатора тунелю. Ініціатор тунелю інкапсулює (вбудовує) існуючі пакети в новий пакет, що створює поряд з вихідними даними новий заголовок з інформацією про одержувача та відправника. Хоча всі пакети передані по тунелю є пакетами IP, інкапсульовані пакети можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, які не маршрутизуються (наприклад NetBEUI). Звичайна маршрутизація мережі IP визначає маршрут між ініціатором і термінатором тунелю, яка може бути і мережею, відмінною від Internet. Термінатор тунелю буде виконувати процес, зворотний інкапсуляції – він видаляє нові заголовки і направляє

будь який вихідний пакет в локальний стек протоколів або адресату в локальній мережі. Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, переданих по тунелю VPN. Але завдяки використанню інкапсуляції з'являється можливість повного криптографічного захисту пакетів, які інкапсулюються. Секретність цих пакетів забезпечується шляхом їх криптографічного закриття, тобто шифрування, а автентичність відбитку і цілісність – шляхом формування цифрового підпису [4]. Оскільки існує безліч методів захисту даних з криптографією, дуже важливо, щоб ініціатор і термінатор тунелю використовували однакові методи і могли погоджувати один з одним цю інформацію.

1.3. Класифікація VPN мереж

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

За типом середовища, що використовується:

Захищені VPN мережі. Це найбільш поширений варіант створення приватних мереж. При їх використанні можливо створити надійну і захищену підмережу на основі ненадійної мережі, як правило, Інтернету.

Прикладом створення захищених VPN мереж: OpenVPN, IPSec і PPTP.

Довірені VPN мережі. Використовуються у випадках, коли середовище, яке передає можна вважати надійним і необхідно вирішити тольки завдання створення віртуальної підмережі в межах більшої мережі. Є неактуальними питання забезпечення безпеки. Прикладами подібних VPN мерекж: MPLS і L2TP. Точніше буде зазначити, що ці протоколи передають завдання забезпечення безпеки на іншіпротоколи, наприклад, L2TP, який, як правило, використовується в парі з IPSec.

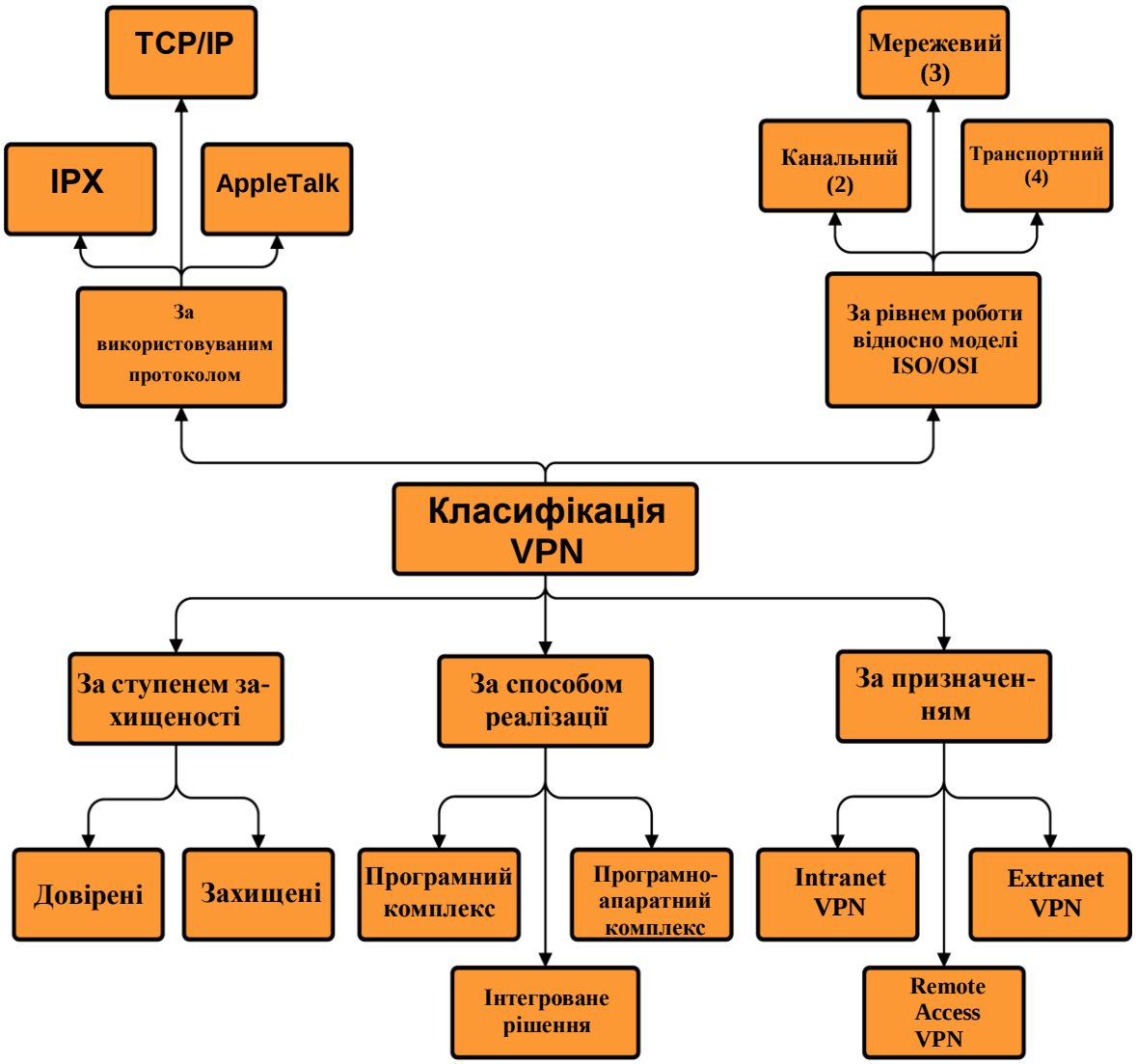

Рис. 1.2. Класифікація VPN

За способом реалізації:

VPN мережі у вигляді програмного рішення. Вони використовують персональний комп'ютер зі спеціальним програмним забезпеченням, яке забезпечує функціональність VPN.

VPN мережі у вигляді спеціального програмно-апаратного забезпечення. Створення цієї VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація може забезпечити високу продуктивність, а слідом, високий ступінь захищеності.

.

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

1.3.1. Класифікація VPN по робочому рівню моделі OSI

Для створення безпечної передачі даних по загальнодоступній (незахищеній) мережі, застосовують узагальнену назву – захищений канал. Саме термін «канал» підкреслює той факт, що захист даних буде забезпечуватись між двома вузлами мережі (шлюзами або хостами) впродовж деякого віртуального шляху якій прокладений в мережі з комутацією пакетів.

Створити захищений канал можна за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI (Рис. 1.3).

Класифікувати VPN за робочими рівнями моделі OSI має значний інтерес, оскільки від вибраного рівня моделі OSI багато в чому буде залежати функціональність VPN мережі, та її сумісність з додатками інформаційної системи, а також з іншими засобами захисту.

Розрізняють наступні класи VPN, за ознакою робочого рівня моделі OSI:

- VPN 2-го (канального) рівня;
- VPN 3-го (мережевого) рівня;
- VPN 5-го (сеансового) рівня.

Розглянемо більш детально класи VPN, які працюють на рівнях моделі OSI: канальному, мережевому і сеансовому [2].

- VPN канального рівня

Засоби VPN, використовувані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку 3-го рівня і вище, та побудову віртуальних тунелів типу «точка-точка». До цього класу відносяться VPN-рішення, які використовують протоколи L2F і PPTP, а також недавно затверджений стандарт L2TP, якій розробили фірми Cisco Systems і Microsoft.

Дані	7 рівень прикладний - application	Доступ до мережевих служб
	6 рівень представницький - presentation	Представлення і кодування даних
	5 рівень сеансовий - session	Управління сеансом зв'язку
Сегменти	4 рівень транспортний - transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 рівень мережевий - network	Визначення маршруту і логічна адресація
Кадри	2 рівень канальний - data link	Фізична адресація
Біти	1 рівень фізічний - phisical	Робота з середовищем передачі, сигналами і двійковими даними

Рис. 1.3. Рівні протоколів захищеного каналу

Протокол L2TP, має домінуюче рішення при організації видаленого доступу до мережі. Тим самим, ймовірно, рішення 2-го рівня не набуде такого ж значення для взаємодії з мережею, при необхідності мати декілька тунелів із загальними кінцевими точками, як наслідок її недостатньої масштабованості.

Протокол PPTP забезпечує прозорість засобів захисту для додатків і служб прикладного рівня і не залежить від задіяного протоколу мережевого рівня. Протокол PPTP захищеного каналу базується на PPP протоколі, який широко використовується в з'єднаннях «точка-точка», наприклад при роботі по виділених лініях. Зокрема, протокол PPTP може транспортувати пакети як в IP мережах, та в мережах, що працюють на основі протоколів IPX або NetBEUI. PPTP не можна вважати універсальним засобом, оскільки цей протокол задіяний не у всіх мережах. Саме, використання різних канальних протоколів в різних частинах великої складової мережі, заважає, за допомогою єдиного протоколу канального рівня, прокласти через це гетерогенне середовище захищений канал.

- VPN мережевого рівня

VPN-продукти мережевого рівня виконують інкапсуляцію IP пакетів в IP. Зараз протокол IPSec, призначений для автентифікації, тунелювання і шифрування IP-пакетів, витісняє широко відомий протокол SKIP. Протокол IPSec реалізував в собі всі кращі рішення по шифруванню пакетів і застосовується як обов'язковий компонент в протоколі IPv6.

Протокол IPSec передбачає стандартні методи ідентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні методи обміну і управління ключами шифрування між кінцевими точками, а також стандартні способи використовування шифрування кінцевими точками тунелю.

IPSec стрімко завоював популярність та став домінуючим протоколом VPN для взаємодії між мережами. Як відомо, специфікація IPSec орієнтована на IP а, отже, не підходить для трафіку будь-яких інших протоколів мережевого рівня [14]. Цей протокол може працювати спільно з L2TP; в поєднанні ці два протоколи забезпечують стандартизоване шифрування, надійнішу ідентифікацію, та цілісність даних. Тунель IPSec створений між двома мережами може підтримувати безліч індивідуальних каналів передачі даних [12], внаслідок цього додатки даного типу одержують переваги в масштабуванні в разі порівняння з технологією другого рівня.

- VPN сеансового рівня

Деякі VPN мережі використовують дещо інший підхід під назвою «посередники каналів». Цей метод є працючим над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо (орієнтовані на сокети операції часто називають операціями сеансового рівня).

Шифрування інформації, що передається між ініціатором і термінатором тунелю, часто здійснюється за допомогою захисту транспортного рівня TLS. Для проходу через брандмауер, визначили протокол під назвою SOCKS, якій застосовується для стандартизованої реалізації посередників каналів.

Клієнтський комп'ютер встановлює автентифікований сокет (сеанс) з сервером, що виконує роль проксі. Цей посередник – єдиний спосіб зв'язку че-

рез брандмауер. У свою чергу, посередник проводить будь-які операції, які запитав клієнт. Посереднику відомо про трафік на рівні сокета, і він може провадити ретельний контроль, таким чином, якщо вони не мають необхідних повноважень, блокувати конкретні додатки користувачів. Для порівняння, віртуальні приватні мережі рівнів 2 і 3 зазвичай просто відкривають або закривають канал для всього трафіку по автентифікованому тунелю. Це може являти проблему, якщо користувач, на іншому кінці тунелю, не до кінця довіряє мережі.

Мережі VPN з посередником каналу типа IPSec орієнтовані на протокол IP [2]. Якщо IPSec, поширює мережу IP в захищений тунель, то рішення на основі протоколу SOCKS розширюють його на всі додатки і на кожен сокет окремо. На відміну від рівня 2 і 3, де створені тунелі працюють однаково в обох напрямах, мережі VPN рівня 5 допускають незалежне управління передачею в кожному напрямку. Мережі VPN рівня 5 можна використовувати з іншими типами віртуальних приватних мереж, аналогічно протоколу IPSec і протоколам другого рівня, оскільки дані технології не є взаємовиключними.

1.3.2. Класифікація по архітектурі технічного рішення

Протоколи VPN виділяють по архітектурі технічного рішення на три основні види віртуальних приватних мереж:

- VPN з віддаленим доступом;
- внутрішньокорпоративні VPN;
- міжкорпоративні VPN.

Мережі VPN з віддаленим доступом призначені для забезпечення захищеного віддаленого доступу до інформаційних ресурсів корпорації мобільним чи віддаленим співробітникам компанії. Принцип їх роботи полягає в наступному: користувачі встановлюють з'єднання через місцеву точкою доступу до глобальної мережі, після цього їх виклики тунелюються через Internet. Потім всі виклики з’єднуються на відповідних вузлах і передаються до корпоративної мережі.

VPN з віддаленим доступом має низку переваг, зокрема:

• ефективну систему встановлення справжності віддалених та мобільних користувачів, які забезпечується надійною процедурою автентифікації:

• зосередження уваги компанії на основних бізнес-цілях замість відволікання на проблеми забезпечення роботи мережі;

• високу масштабованість та простоту розгортання для нових користувачів, що додаються до мережі.

Внутрішньокорпоративні мережі VPN призначені для забезпечення захищеної взаємодії між підрозділами на підприємстві, або між групою підприємств, об'єднаних корпоративними мережами зв'язку.

Інтранет VPN ще називають "точка - точка", або LAN-LAN VPN. Інтранет технології використовують для організації захищеного з'єднання між підрозділами одного або різних підприємств, об'єднаних корпоративними мережами зв'язку. При організації віддаленого доступу між центральними офісами та філіями компанії змушені використовувати виділені лінії. Однак це велика стаття витрат. Для вирішення цієї проблеми можна використати віртуальну приватну мережу. Внутрішньокорпоративні мережі VPN будуються з використанням мережі Інтернет або мережевих інфраструктур, що поділяються, які надаються сервіс-провайдерами.

Міжкорпоративні мережі VPN забезпечують співробітникам підприємства захищений обмін інформацією із партнерами по бізнесу, постачальниками, гуртовими замовниками, клієнтами, користувачами та ін.

Міжкорпоративна мережа забезпечує прямий доступ від мережі однієї компанії до мережі іншої, таким чином сприяючи підвищенню надійності зв'язку, який підтримується в діловій співпраці. У міжкорпоративних мережах велика увага надається автентифікації користувачів та контролю доступу за допомогою мережевого екрану.

Звернемо увагу, що останнім часом спостерігається тенденція до конвергенції різних конфігурацій і способів реалізацій VPN.

1.3.3. Класифікація за способом технічної реалізації

Для побудови VPN мереж існують різні варіанти. При виборі оптимального рішення потрібно враховувати чинники продуктивності засобів, з яких побудована VPN мережа. Якщо процесор маршрутизатора і так працює на межі потужності, то створення тунелів VPN і створення шифрування/дешифрування інформації можуть взагалі зупинити роботу всієї мережі через те, що цей маршрутизатор не зможе виконувати роботу з простим трафіком, не кажучи вже про забезпечення VPN. Час та досвід показує, що для створення VPN найкраще використовувати спеціалізоване обладнання, але якщо є обмеження в засобах, то є можливість звернути увагу на саме програмне рішення. Далі розглянемо деякі варіанти побудови VPN мереж.

За способом технічної реалізації розрізняють наступні групи VPN:

- VPN на основі маршрутизаторів;
- VPN на основі мережевого екрану;
- VPN на основі програмних рішень;
- VPN на основі мережевої операційної системи;
- VPN на основі спеціалізованих апаратних засобів з вбудованими кріптопроцесорами.

➢ VPN на основі мережевої ОС

Для реалізації VPN на основі мережевої ОС можна розглянути на прикладі операційної системи Windows. Для створення VPN існує протокол PPTP, інтегрований в операційну систему. Таке рішення більш привабливе для організацій, що використовують Windows як корпоративну ОС. У мережах VPN, заснованих на Windows, використовується база даних клієнтів, яка зберігається в первісному контролері домену. При підключенні до PPTP-серверу користувач авторизується по протоколах PAP, CHAP або MS CHAP. Для шифрування застосовується нестандартний протокол Point-to-Point Encryption та одержаним при встановленні з'єднання з 40-бітовим ключем.

Недолік такої системи – недостатня захищеність протоколу PPTP.

Як перевагу наведеної схеми, слід зазначити, що вартість рішення на основі мережевої системи значно нижче за вартість інших рішень.

- VPN на основі маршрутизаторів

Даний спосіб побудови VPN припускає застосування маршрутизаторів для створення захищених каналів [1]. Оскільки вся інформація, що виходить з локальної мережі, проходить крізь маршрутизатор, то цілком природньо покласти на нього ще задачі шифрування.

Використання устаткування для VPN на маршрутизаторах – пристрої компанії Cisco Systems. Маршрутизатори Cisco обслуговують протоколи L2TP і IPSec. Окрім звичайного шифрування інформації, компанія Cisco реалізує і інші функції VPN, а саме, обмін ключами і ідентифікація при встановленні тунельного з'єднання. Використання додаткового модулю шифрування ESA, підвищує продуктивності роботи маршрутизатора.

- VPN на основі міжмережевих екранів

Міжмережеві екрани, або брандмауери, у більшості виробників містять функції шифрування даних і тунелювання. У основі такого рішення лежить просте міркування [1]: оскільки інформація проходить через міжмережевий екран, чом би її заразом не зашифрувати? До програмного забезпечення може бути доданий модуль шифрування.

До недоліків такого методу відноситься дуже висока вартість рішення для одного робочого місця і залежність від апаратного забезпечення, продуктивності. При використанні екранів на базі комп’ютера треба пам’ятати, що подібний варіант підходить тільки для невеликих мереж з обмеженим об'ємом інформації, що передається (рис. 1.4).

Як рішення на основі мережевого екрану можна назвати продукт Firewall-1 компанії Check Point Software Technologies.

.

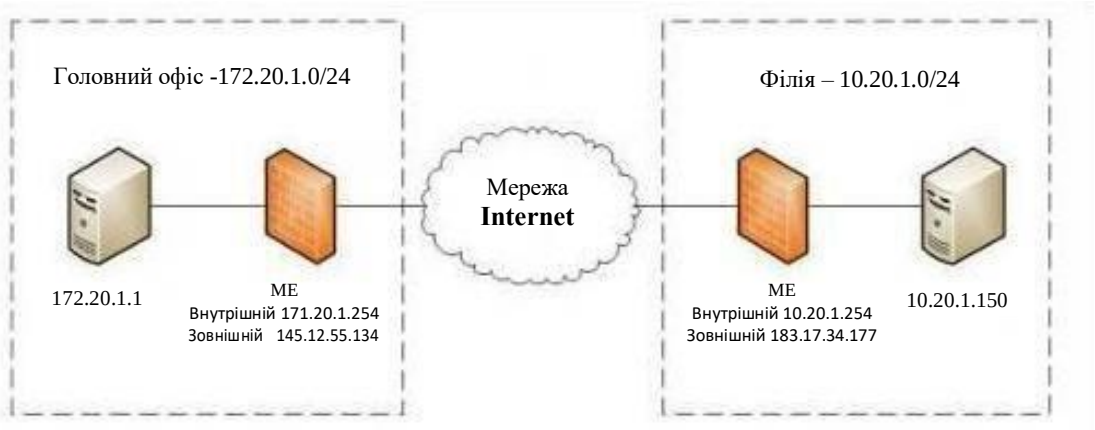

Рис. 1.4. Схема побудови VPN із застосуванням брандмауерів

- VPN на основі програмного забезпечення

Застосування програмних рішень може бути використано для побудови мереж VPN. Для реалізації подібних схем використовується спеціалізоване програмне забезпечення, воно працює на виділеному комп'ютері і в більшості випадків виконує функції проксі-серверу. Комп'ютер з таким програмним забезпеченням може бути розташований за межами ME.

На прикладі програмного рішення, можна вказати ПЗ AltaVista Tunnel. У випадку використання цього ПЗ клієнт підключається до серверу, реєструється на ньому і вони обмінюються ключами. Шифрування каналу здійснюється на базі 56- або 128-бітових ключів. Перед відправкою на сервер пакети зашифровуються та інкапсулюються в інші IP-пакети. Під час роботи, сервер перевіряє цілісність даних по алгоритму MD5 [5]. Система, щопівгодини генерує нові ключі, які значно підвищують захищеність з'єднання.

До переваг AltaVista Tunnel можно віднести – простоту інсталяції і зручність керування. До недоліків цієї програми можна віднести нестандартну архітектуру і низьку продуктивність.

- VPN на основі спеціалізованих апаратних засобів з вбудованими кріптопроцесорами. Такий варіант побудови VPN на спеціалізованих апаратних засобах може бути використаний в мережах, які вимагають високої продуктивності. Прикладом такого рішення служить продукт cIPro-VPN.

1.4 . Протоколи VPN мережі

1.4.1. Використання для захисту протоколів PPTP та L2TP

Віртуальний захищений канал можна побудувати за допомогою системних засобів, які реалізовані на різних рівнях моделі OSI взаємодії відкритих систем. В залежності від обраного робочого рівня OSI буде реалізуватись функціональність VPN і її сумісність з додатками інформаційних систем, а також з іншими засобами захисту. Застосування на канальному рівні моделі OSI, засобів VPN, дозволяє забезпечити інкапсуляцію різних видів трафіку вище 3-го рівня і побудову віртуальних тунелів типу «точка-точка». При створені на сеансовому рівні, захищеної віртуальної мережі з'являється можливість криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а також реалізацію деякіх функцій посередництва між кінцевими точками. Протоколи формування захищених каналів на канальному рівні Протоколи L2F, L2TP і PPTP - це протоколи тунелювання канального рівня моделі OSI. Ці три протоколи, зазвичай відносять до протоколів формування захищеного каналу, однак, цьому визначенню більш точно відповідає тільки протокол PPTP, він забезпечує шифрування і туннелювання переданих даних. Протоколи L2F і L2TP підтримують тільки функції тунелювання. Загальною властивістю всіх цих протоколів є те, що вони використовуються для організації захищеного мільтипротокольного віддаленого доступу до ресурсів корпоративної системи через відкриту мережу. Для захисту даних в тунелі в цих протоколах необхідно використовувати певний додатковий протокол, зокрема IPSec. Для віддаленого доступу клієнтське ПЗ зазвичай використовує стандартний протокол канального рівня PPP. Протоколи PPTP, L2F і L2TP базуються на протоколі PPP та є його розширеннями. Спочатку протокол PPP, був розроблений для інкапсуляції даних і їх доставки по з'єднаннях типу «точка-точка». Цей протокол також використовується для організації комутованих з'єднань. Для передачі конфіденційних даних між точками мережі загального користування, спочатку проводиться інкапсуляція

даних за протоколом PPP, потім протоколи PPTP і L2TP виконують шифрування даних і власну інкапсуляцію. Тунельний протокол доставив пакети з початкової точки тунелю в кінцеву, після цього виконується деінкапсуляція. На 1-му та 2-му рівнях протоколи PPTP і L2TP ідентичні, але на цьому їх схожість закінчується і починаються відмінності.

- Протокол PPTP

Цей протокол PPTP (Point-to-Point Tunneling Protocol) призначений для створення захищених віртуальних каналів під час доступу віддалених користувачів до локальних мереж через мережу Інтернет. Він передбачає створення криптозахищенего тунелю на канальному рівні моделі OSI як для випадку прямого з'єднання віддаленого комп'ютера з відкритою мережею[10], так і для випадку приєднання його до відкритої мережі через провайдера.

Структура пакетів, переданих по протоколу PPTP, має:

- заголовок IP, що містить адреси відправника і одержувача пакету;
- заголовок загального методу інкапсуляції для маршрутизації;
- заголовки канального рівня, які використовується всередині Інтернету, наприклад заголовок кадру Ethernet.

На прийомному вузолі мережі витягуються з пакетів IP кадри PPP, а потім витягується з кадру PPP вихідний пакет IP та він відправляється по локальній мережі конкретного адресата. Інкапсулюючі протоколи типу PPTP канального рівня, мають перевагою перед протоколами захищеного каналу. Застосування протоколів IPSec неможливо при використанні IPX, просто вони орієнтовані на 1 протокол мережевого рівня IP.

За протоколу PPTP створення захищеного віртуального каналу відбувається аутентифікація вилученого користувача і шифрування переданих даних (рис. 1.5).

Використання при шифруванні PPTP гарантує, що ніхто не зможе виявити дані при пересиланні через мережу Internet. При узгодженні параметрів між клієнтом і сервером, протоколи MPPE вміє автоматично вибирати довжину ключа шифрування [11]. Він підтримує використання ключів довжи-

ною 40, 56 або 128 біт, та змінює значення ключа шифрування після кожного прийнятого пакета.

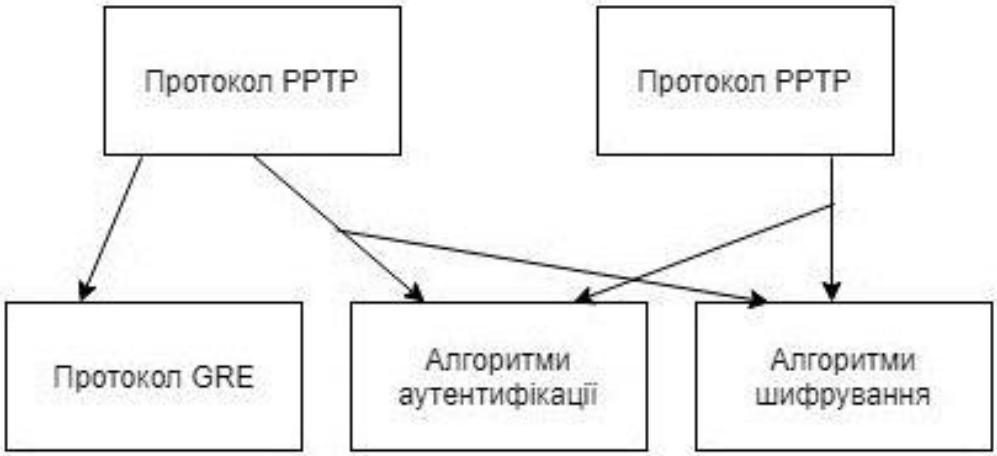

Рис. 1.5. Архітектура протоколу PPTP

Протокол PPTP визначеає дві основні схеми застосування:

1) схема тунелювання при підключенні віддаленого комп'ютера до Інтернету по кабелю через провайдера;

2) схема тунелювання при прямому з'єднанні віддаленого комп'ютера з Інтернетом.

Розглянемо реалізацію 2-ї схеми тунелювання (рис. 1.6). Віддалений користувач встановлює віддалене з'єднання з локальною мережею за допомогою клієнтської частини сервісу віддаленого доступу RAS. Після цього користувач звертається до сервера віддаленого доступу локальної мережі, вказуючи його IP-адресу [11], та по протоколу PPTP встановлює з ним зв'язок.

Прикордонний маршрутизатор локальної мережі може виконувати функцію сервера віддаленого доступу. Клієнтська частина сервісу RAS і райвер PPTP повинні бути встановлені на комп'ютері віддаленого користувача, а сервер RAS і драйвер PPTP - на сервері віддаленого доступу локальної мережі. Протокол PPTP визначає кілька службових повідомлень, якими обмінюються взаємодіючі сторони. По протоколу TCP передаються службові

повідомлення. Процес захищеного інформаційного обміну починається після успішної аутентифікації.

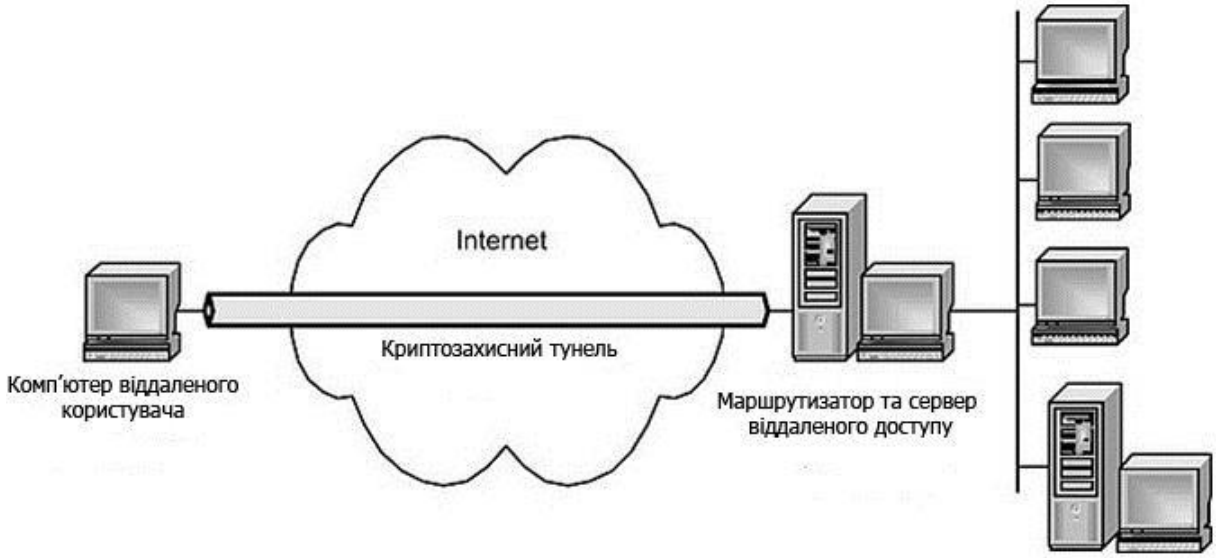

Рис. 1.6. Схема тунелювання при прямому підключенні комп'ютера віддаленого користувача до Internet

Компанією Cisco Systems для створення захищених віртуальних мереж на канальному рівні моделі OSI був розроблений протокол L2F, як альтернатива протоколу PPTP.

На сьогодні він фактично поглинений протоколом L2TP, тому далі будуть розглядатися основні можливості і властивості протоколу L2TP.

- Протокол L2TP

Робота над протоколом велася на основі протоколів PPTP і L2F, і в результаті він увібрав в себе кращі якості вихідних протоколів. Протокол L2TP розроблявся як протокол захищеного тунелювання PPP - трафіку через мережі загального користування з довільним середовищем.

Гібридний протокол L2TP являє собою розширення протоколу PPP функціями аутентифікації віддалених користувачів, створення захищеного віртуального з'єднання і управління потоками даних. Протокол L2TP не прив'язаний протоколу IP, саме тому він може бути використаний в мережах з ко-

мутацією пакетів, або в мережах з ретрансляцією кадрів (рис. 1.7). В протоколі L2TP використовується важлива функція управління потоками даних, а також ряд функцій захисту, тобто, включена можливість роботи з протоколами AH і E5P стека протоколів IPSec.

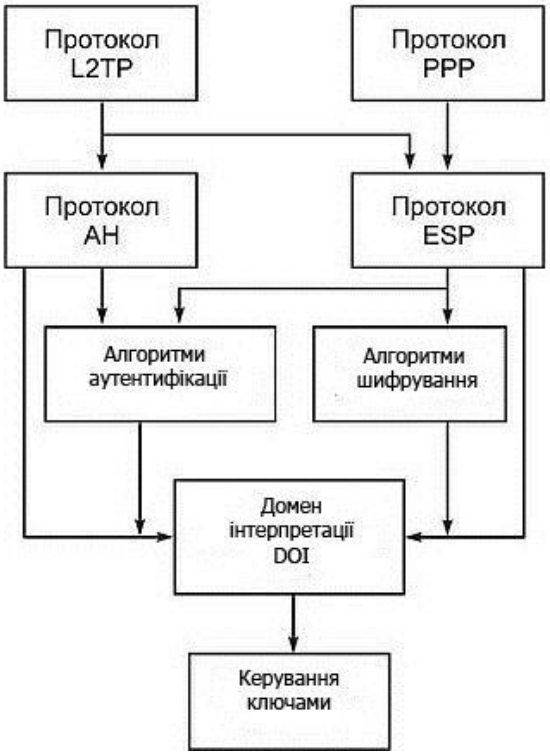

Рис. 1.7. Архітектура протоколу L2TP

Протокол L2TP застосовує в якості транспорту протокол UDP і використовує однаковий формат повідомлень як для пересилання даних, та для управління тунелем.

Протокол L2TP надійніше, хоча протокол PPTP і забезпечує достатній ступінь безпеки. Протокол L2TP забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування даних.

L2TP надає можливість відкривати між кінцевими абонентами відразу кілька тунелів, на відміну від своїх попередників - протоколів PPTP і L2F, кожен з цих тунелів може бути виділений як для окремого додатка. Ці особливості забезпечують гнучкість і безпеку тунелювання.

Після того як L2TP завершує процес аутентифікації комп'ютера, виконується аутентифікація на рівні користувача.

Згідно зі стандартами протоколу L2TP роль сервера віддаленого доступу провайдера повинен виконувати концентратор доступу LAC, який забезпечує доступ його локальної мережі віддаленому користувачеві через мепрежу Інтернет. В якості сервера віддаленого доступу до локальної мережі повинен виступати мережевий сервер LNS [5], якій функціонує на сумісних з протоколом PPP платформах (рис. 1.8).

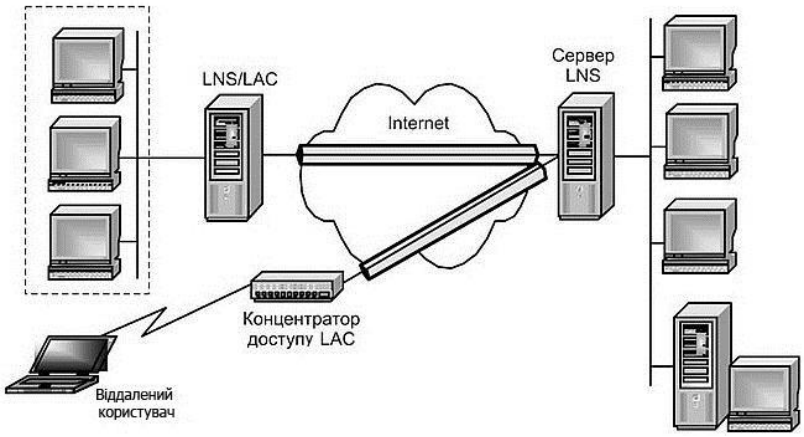

Рис. 1.8. Схеми тунелювання по протоколу L2TP

Створення захищеного віртуального каналу в протоколі L2TP здійснюється в три етапи:

- встановлення з'єднання з сервером віддаленого доступу локальної мережі;
- аутентифікація користувача;
- конфігурація захищеного тунелю.

Якщо захищений тунель планується створити в IP-мережах, то для реалізація криптографічного захисту використовується протокол IPSec. Протокол L2TP не визначає конкретних методів криптографічного захисту й передбачає ймовірність застосування різних стандартів шифрування. Використання алгоритму шифрування 3DES або AES в протоколі L2TP поверх IPSec

забезпечує більш високу ступінь захисту даних, ніж PPTP. Якщо такий високий рівень захисту не потрібен, можна використовувати алгоритм DES з одним 56-розрядним ключем. При використанні алгоритму HMAC, протокол L2TP забезпечує аутентифікацію даних, для чого цей алгоритм створює хеш довжиною 128 біт.

Отже, функціональні можливості протоколів PPTP і L2TP різні. Використання протоколу PPTP може застосовуватися тільки в IP-мережі. L2TP - може використовуватися не тільки в IP-мережах. L2TP поверх IPSec пропонує більше ступенів захисту, ніж PPTP, і може гарантувати майже 100% -ий захист важливих для організації даних.

Протокол L2TP має ряд недоліків тунельної передачі даних на канальному рівні:

- L2TP забезпечує стандартне шифрування тільки в IP-мережах за допомогою протоколу IPSec;
- L2TP обмежує трафік межами обраного тунелю і позбавляє користувачів доступу до інших частин мережі;
- для реалізації протоколу L2TP необхідна підтримка провайдерів ISP.

Для виконання на сеансовому рівні функцій посередництва між взаємодіючими сторонами був прийнятий протокол SOCKS Для захисту інформаційного обміну на сеансовому рівні широке поширення отримав протокол SSL.

1.4.2. Захист за допомогою протоколів SSL/TLS

На сеансовому рівні моделі OSI, застосовується протокол SSL в якості протоколу захищеного каналу. Цей протокол має криптографічні методи захисту інформації для забезпечення безпеки інформаційного обміну. Протокол SSL виконує всі функції по створенню захищеного каналу між двома абонентами мережі, включаючи їх взаємну аутентифікацію, забезпечення конфіденційності, цілісності та автентичності переданих даних. Ядром про-

токолу SSL є технологія комплексного використання асиметричних і симетричних криптосистем.

Використанням симетричних сесійних ключів, забезпечується конфіденційність шифрування переданих повідомлень, якими сторони обмінюються при встановленні з'єднання. Сесійні ключі передаються також в закодованому вигляді, при цьому вони шифруються відкритими ключами, витягнутих з сертифікатів абонентів. Швидкість процесів шифрування і розшифрування на основі симетричного ключа істотно вище [25], ніж при використанні несиметричних ключів. Справжність і цілісністьї інформації забезпечується за рахунок формування та перевірки ЕЦП.

В якості алгоритму асиметричного шифрування використовуються алгоритм RSA, та алгоритм Діффі-Хеллмана. Для обчислення хеш-функцій можуть застосовуватися стандарти MD5 і SHA-1. Допустимими алгоритмами симетричного шифрування є RC2, RC4, DES, 3DES і AES.

Обмін цифровими сертифікатами відкритих ключів користувачів, завіреними підписом спеціальних сертифікаційних центрів виконується взаємна аутентифікація обох сторін в SSL.

За протоколом SSL [13], криптозахищені тунелі створюються між кінцевими точками віртуальної мережі. Клієнт і сервер є ініціаторами кожного захищеного тунелю, що функціонують на комп'ютерах в кінцевих точках тунелю (рис. 1.9).

Формування та підтримка захищеного з'єднання в протоколі SSL передбачає наступні етапи взаємодії між клієнтом та сервером:

- встановлення SSL-сесії; при цому вирішуються наступні завдання:
- аутентифікація сторін;
- узгодження криптографічних алгоритмів і алгоритмів стиснення, які будуть використовуватися при обміні пакетами;
- формування загального секретного майстер-ключа;
- захищене взаємодія.

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

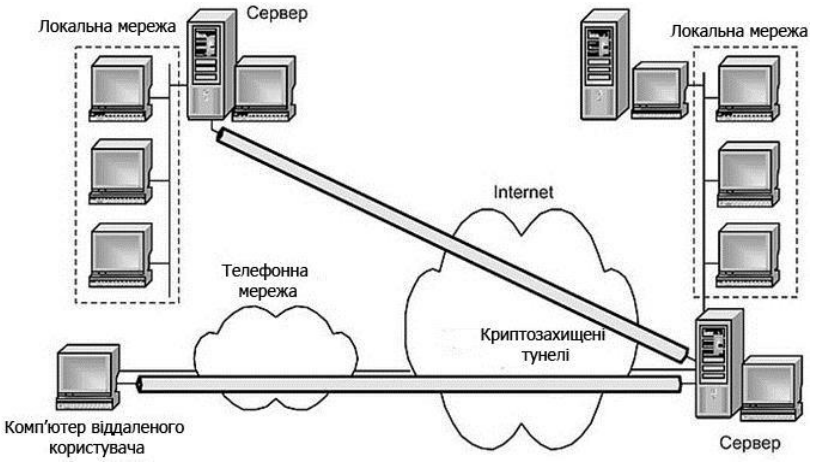

Рис. 1.9. Криптозахищені тунелі, сформовані на основі протоколу SSL

Процедура встановлення SSL-сесії, яка має назву процедурою рукостискання, створюється перед безпосереднім захистом інформаційного обміну і виконується за протоколом початкового привітання, якій входить до складу протоколу SSL.

За повторними з'єднанями між клієнтом і сервером можуть, за взаємною згодою, формуватись нові сеансові ключі на основі «минулого» загального «секрету».

Протокол SSL v. 3.0 підтримує три режими аутентифікації:

- взаємну аутентифікацію сторін [14];
- односторонню аутентифікацію сервера без аутентифікації клієнта;
- повну анонімність.

Використання крайнього варіанту забезпечується захист інформаційного обміну без будь-яких гарантій щодо справжності сторін. При цьому випадку взаємодіючі сторони не захищені від атак, пов'язаних з підміною учасників взаємодії.

Відповідність між відкритими ключами і їх власниками встановлюється за допомогою цифрових сертифікатів, які видаються спеціальними центрами сертифікації.

У протоколу SSL, для аутентифікації взаємодіючих сторін і формування загальних секретних ключів зазвичай використовують алгоритм RSA.

Протокол SSL підтримує ПО серверів і клієнтів, що випускаються провідними західними компаніями. Суттевим недоліком протоколу SSL є те, що практично всі програми, які підтримують SSL, доступні лише в усіченому варіанті (довжина ключа 40 біт для алгоритмів симетричного шифрування і 512 біт для алгоритму RSA).

Використання однакових ключів в SSL, для аутентифікації і шифрування, може за певних умов призвести до потенційної уразливості. Подібне рішення дає можливість зібрати більше статистичного матеріалу, ніж при аутентифікації і шифрування різними ключами.

До недоліків протоколів SSL і TLS можна віднести те, що для транспортування своїх повідомлень вони використовують тільки один протокол - IP, і можуть працювати тільки в IP-мережах.

У загальному випадку програми-посередники, які традиційно використовуються в брандмауері, можуть виконувати такі функції:

- криптозахист переданих даних;
- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- ідентифікацію та аутентифікацію користувачів;
- трансляцію внутрішніх мережевих адрес для вихідних потоків повідомлень;
- фільтрацію і перетворення потоку повідомлень, наприклад пошук вірусів і прозоре шифрування інформації.

Протокол SOCKS може застосовуватися для контролю над напрямами інформаційних потоків і розмежування доступу в залежності від атрибутів користувачів і інформації. Протокол SOCKS не прив'язаний до протоколу IP і

не залежить від ОС. На основі протоколу SOCKS можуть бути створені захищені тунелі для кожної програми і сеансу окремо.

1.4.3. Захист за допомогою протоколу IPSec

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

У схемі захищений канал, встановлюється між двома кінцевими вузлами мережі, тобто хостами H1 і H2 (рис. 1.10). Протокол IPSec в цьому випадку працює на кінцевому вузлі і захищає дані, які надходять на нього.

Рис. 1.10. Схема хост-хост

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

У відповідності зі рисунком 1.11 захищений канал встановлюється між двома проміжними вузлами, званими шлюзами безпеки SG1 і SG2, на кожному з цих шлюзів працює протокол IPSec.

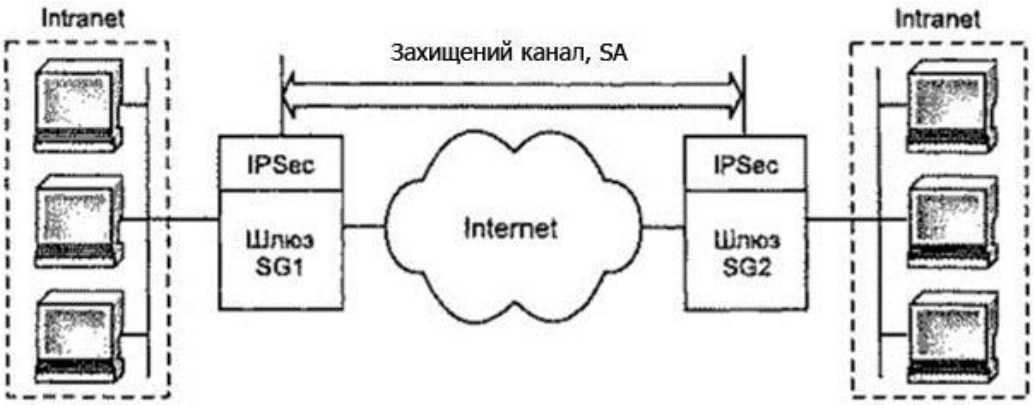

Рис. 1.11. Схема шлюз-шлюз

Створння захищеного обміну даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, та які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібно, вони передають свій трафік в незахищеному вигляді через заслуговують на довіру мережі корпорації. Трафік, який направляється в загальнодоступну мережу, проходить через шлюзи безпеки, та це і забезпечує його захист за допомогою IPSec, діючи від свого імені [17]. 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 застосовується схема хост-шлюз.

- Переваги засобів безпеки IPSec

В наборі стандартів для створення VPN, система IPSec міцно займає сьогодні лідируючі позиції. Стандарти IPSec увібрали в себе прогресивні методики і досягнення в області мережевої безпеки, завоювала визнання фахівців як надійна і легко інтегрована система безпеки для IP-мереж. Цьому сприяє її відкрита побудова [17], здатна включати всі нові досягнення в області криптографії. IPsec дозволяє захистити мережу від більшості мережевих атак. В захищений комп'ютер або мережу можуть увійти тільки пакети від зареєстрованих партнерів по взаємодії.

IPsec забезпечує:

• аутентифікацію - доказ відправки пакетів вашим партнером;

• конфіденційність - неможливість розкриття переданих даних;

• цілісність - неможливість зміни даних в пакеті;

• тунелювання - повне маскування топології локальної мережі підприємства;

• надійне управління ключами - протокол IKE обчислює розділяється секрет, відомий тільки одержувачу і відправнику пакета.

Робота в рамках стандартів IPSec забезпечує повний захист інформаційного потоку даних від відправника до одержувача, закриваючи трафік для спостерігачів на проміжних вузлах мережі. VPN-рішення на основі стека протоколів IPSec забезпечують побудову віртуальних захищених мереж [12], їх безпечну експлуатацію та інтеграцію з відкритими комунікаційними системами.

Між віддаленим хостом H1, на якому працює IPSec, і шлюзом 30 організовується захищений канал, якій захищає трафік для всіх хостів, які входять в мережу підприємства. Шлюз відправляє пакети хосту тільки в тунельному режимі, віддалений хост можно використовувати для відправки пакетів чрез шлюз як транспортний, так і тунельний режим (рис. 1.12).

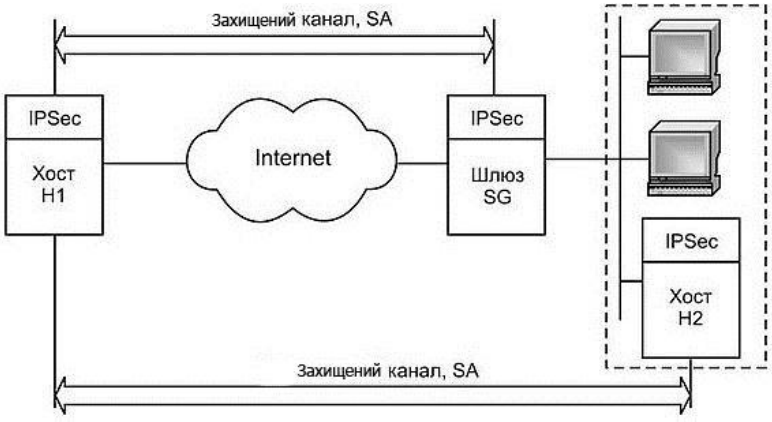

Рис. 1.12. Схема хост-шлюз, доповнена каналом хост-хост

Розглянуті схеми побудови захищених каналів на базі IPSec широко застосовуються при створенні різноманітних віртуальних захищених мереж VPN. Перелік варіюється від провайдерських мереж, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних мереж VPN, що розгортаються і керованих самими компаніями. В основі IPSec успішно реалізуються віртуальні захищені мережі будь-якої архітектури, включаючи VPN з віддаленим доступом, внутрішньокорпоративні та міжкорпоративні VPN.

1.4.4 . Захист за допомогою протоколу Shadowsocks

Shadowsocks (SS) — це приватний протокол без механізму рукостискання, яке використовується як проксі-програмне забезпечення на основі Socks5.

ShadowsocksR (SSR) додає деякі методи обфускації даних на основі shadowsocks, усуває деякі проблеми безпеки та покращує пріоритет QoS. SS і SSR часто використовуються, щоб обійти брандмауер (GFW) для перегляду потрібного контенту. Перевагами Shadowsocks(R) є швидкість, складність виявлення та кросплатформенність.

Причина, чому shadowsocks(R) користується попитом, головним чином полягає в тому, що протокол приховує трафік і GFW його важко виявити. Призначення shadowsocks — це обхід GFW, а не забезпечення безпеки в сенсі криптографії. Таким чином, протокол шифрування, розроблений shadowsocks, обмежується лише спільним ключем і не забезпечує повну конфіденційність.

Компоненти служби Shadowsocks(R) включають ss local, що працює на локальному комп’ютері, і ss server, що працює на віддаленому сервері (рис. 1.13) [9].

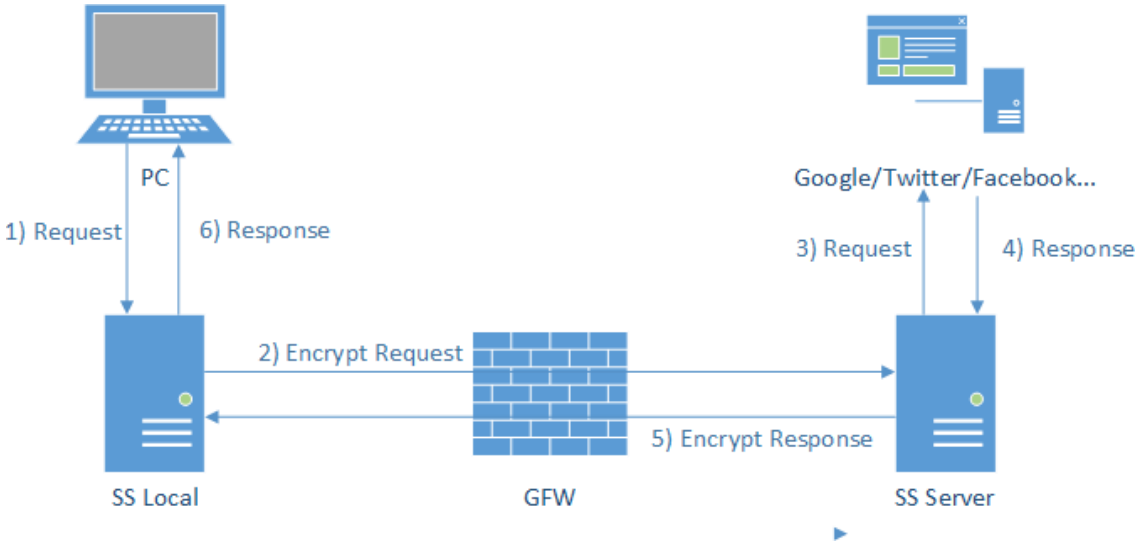

Рис. 1.13 Схема протоколу shadowsocks

Для використання shadowsocks потрібна конфігурація від користувача, яка мітить адресу сервера, порт сервера, пароль і шифрування. Після налаштування локальний клієнт SS встановлює з'єднання з портом сервера за адресою сервера для передачі даних програми, оброблених за допомогою пароля та шифрування.

Потік TCP або повідомлення UDP передається між клієнтом SS і сервером. Зашифрований текст виходить шляхом шифрування даних користувача. Перед тим, як клієнт SS перешле дані користувача на сервер SS, адреса доступу користувача буде додана перед даними користувача, і ця адреса також є зашифрованою для передачі.

Шифрування (ЦІЛЬОВА АДРЕСА||ДАНІ КОРИСТУВАЧА) відноситься до зашифрованого тексту, після шифрування об'єднаного рядка цільової адреси та даних користувача за допомогою алгоритму шифрування, вибраного параметром шифрування SS.

Варіант шифрування SS підтримує AES-128-CTR, chacha20-IETF та інші алгоритми потокового шифрування, а також AES-192-GCM, chacha20-IETF-poly1305 та інші криптографічні алгоритми AEAD. Варіанти шифрування SS вибираються по-різному, і формат зашифрованих даних користува-

ча також відрізняється. Для алгоритму потокового шифрування довжина даних до та після шифрування однакова. Для криптографічного алгоритму AEAD відкритий текст стане зашифрованим.

Генерація ключів і отримання параметрів шифрування Shadowsocks(R). Згідно з аналізом вихідного коду shadowsocks, криптографічні алгоритми, що використовуються в shadowsocks, включають два типи: алгоритм генерації ключів і алгоритм шифрування (дешифрування), який використовується різними варіантами шифрування. Коли shadowsocks налаштовує опцію шифрування, він, по суті, вибирає основний алгоритм генерації ключів і режим шифрування одночасно. Параметр шифрування шифрує дані на основі випадкового числа в потоці TCP і головного ключа, згенерованого алгоритмом генерації ключа. Довжина дорівнює 16 байтам, а значенням є 16-байтове випадкове число потоку TCP. Різні варіанти шифрування використовують випадкові числа та головні ключі по-різному.

Алгоритм генерації ключів shadowsocks генерує головний ключ на основі попереднього ключа, тобто пароля інтерфейсу налаштування shadowsocks. Коли визначається параметр шифрування, визначається довжина головного ключа.

На даний момент shadowsocks підтримує ключі довжиною 16 байтів, 24 байти та 32 байти.

1.4.5 . Захист за допомогою протоколу WireGuard

WireGuard – це сучасний та безпечний протокол VPN, призначений для забезпечення швидкого та ефективного зв'язку між одноранговими вузлами мережі. WireGuard - відносно новий VPN-протокол, що вже завоював популярність серед фахівців з кібербезпеки. Він розроблений, щоб бути швидким, сучасним та безпечним, що робить його перспективним варіантом для тих, хто шукає надійне рішення VPN. Спочатку WireGuard був випущений для ядра Linux, але тепер він є кросплатформним і широко використовується у Windows, MacOS, BSD, iOS та Android.

На відміну від деяких старих і менш безпечних протоколів WireGuard забезпечує високу швидкість, але при цьому забезпечує підвищену безпеку. Цей протокол, працює в ядрі операційної системи, яке ближче до обладнання, ніж звичайні програми. Це основна причина, через яку він може швидше шифрувати та розшифровувати дані (рис. 1.14).

В роботі WireGuard створює зашифрований тунель між двома чи більше мережевими інтерфейсами. Він використовує криптографію з відкритим ключем для автентифікації. Кожен клієнт і сервер мають закритий ключ і відкритий ключ. Відкритий ключ використовується для автентифікації клієнта або сервера під час рукостискання. WireGuard використовує алгоритм обміну ключами Діффі-Хеллмана на еліптичних кривих (ECDH) для встановлення спільного секретного кодквання між клієнтом та сервером. Цей спільне коду вання використовується для отримання сеансових ключів для шифрування та дешифрування. Протокол забезпечує досконалу пряму секретність (PFS), створюючи новий набір сеансових ключів кожного сеансу. Це означає, що навіть якщо зловмисник отримає ключі попереднього сеансу, він не зможе використовувати їх для розшифровування даних поточного сеансу. Протокол стійкий до атак типу грубої сили, диференціального та лінійного криптоаналізу.

Рис. 1.14. Схема протоколу WireGuard

Цей протокол використовує сучасну криптографію, у тому числі Curve25519 для обміну ключами, ChaCha20 для шифрування та Poly1305 для коду автентифікації повідомлень (MAC). MAC - це криптографічна контрольна сума, яка генерується з використанням секретного ключа і додається до даних, що передаються. Коли дані отримані, MAC перераховується та порівнюється з переданим MAC. Якщо дві MAC-адреси збігаються, то дані не були змінені при передачі. Загалом використання криптографії з відкритим ключем та кодів автентифікації повідомлень у WireGuard забезпечує високий рівень безпеки та гарантує безпечну та надійну передачу даних.

Проектування протоколу було здійснено таким чином, щоб бути стійким до змін мережі, тому він може підтримувати з'єднання навіть при зміні мережі, наприклад при переключенні з Wi-Fi на мобільні дані.

WireGuard має кілька ключових функцій, які роблять його привабливим VPN-протоколом як для користувачів, так і для мережевих адміністраторів. Деякі з цих функцій включають:

Швидкість та ефективність: WireGuard спроектований так, щоб бути швидким та ефективним, з мінімальним завантаженням ЦП та високою продуктивністю. Використання мінімального коду та ефективні криптографічні алгоритми роблять його більш швидким, ніж інші протоколи VPN, такі як OpenVPN та IPsec, при цьому забезпечуючи покращену безпеку.

Безпека: WireGuard використовує сучасну криптографію для забезпечення безпеки та конфіденційності зв'язку між одноранговими вузлами мережі. Він використовує досконалу пряму секретність (PFS), це означає, що навіть якщо зловмисник отримає закритий ключ, він не зможе розшифрувати попередні або майбутні повідомлення.

Легкий в налаштуванні: WireGuard спроектований таким чином, щоб його було легко налаштувати, а конфігураційні файли легко читати і розуміти. Він також підтримує аутентифікацію на основі ключів, це спрощує управління великомасштабними проектами.

Крос-платформний: WireGuard є кросплатформним і може працювати в різних операційних системах, включаючи Linux, Windows, MacOS, BSD, iOS та Android. Це робить його універсальним протоколом VPN, який можна використовувати у різних середовищах.

ВИСНОВКИ ДО РОЗДІЛУ 1

В цьому розділі було розкрито поняття та класифікації VPN мереж. Розглянуті протоколи, які використовує технологія VPN. Реалізувати VPN можно організувати захист на різних рівнях моделях OSI. Організовати VPN можно на основі мережевої ОС, МЕ, маршрутизаторів, програмних рішень.

РОЗДІЛ 2
ОСОБЛИВОСТІ ПОБУДОВИ VPN МЕРЕЖ

2.1 . Дослідження принципів роботи VPN

VPN – це сукупність мереж, на зовнішньому периметрі яких встановлені VPN-агенти.

VPN-агент - це програма або програмно-апаратний комплекс [11], який виконує настіпні дії:

1. Перед відправкою будь-якого інформаційного пакета (для визначеності тут і далі розглядатимемо IP-пакети):

• із заголовка IP-пакета виділяється інформація про його адресат. Згідно з цією інформацією на основі політики безпеки даного VPN-агента (налаштовується для кожного VPN-агента його адміністратором) вибираються алгоритми захисту та криптографічні ключі, за допомогою яких буде захищено цей пакет. У тому випадку, якщо політика безпеки VPN-агента не передбачає відправлення IP-пакета даному адресату або IP-пакета з даними характеристиками, відправка IP-пакета блокується;

• за допомогою обраного алгоритму захисту цілісності формується та додається до IP-пакету ЕЦП або імітована приставка;

• вибирається алгоритм шифрування та виконується зашифрування IP-пакету;

• за допомогою встановленого алгоритму інкапсуляції пакетів зашифрований IP-пакет поміщається в готовий для передачі IP-пакет, в заголовку кого, замість вихідної інформації про адресата та відправника містить відповідно інформацію про VPN-агент адресата та VPN-агент відправника. Це називається трансляцією мережевих адрес (NAT - Network Address Translation);

• пакет надсилається VPN-агенту адресата. У разі, якщо розмір результуючого пакета перевищує MTU (Maximum Transfer Unit - максимально мо-

жливий розмір пакета для конкретної ділянки мережі), його дроблення і почергове відправлення результуючих пакетів.

2. При отриманні IP-пакета:

• із заголовка IP-пакета виділяється інформація про його відправника. У тому випадку, якщо відправник не входить до числа дозволених (згідно з політикою безпеки) або невідомий (наприклад, при прийомі пакета з навмисно або випадково пошкодженим заголовком), пакет не обробляється та відкидається;

• відповідно до політики безпеки вибираються алгоритми захисту даного пакета та ключі, за допомогою яких буде проведено розшифрування пакета та перевірку його цілісності;

• виділяється інформаційна (інкапсульована) частина пакету та провадиться її розшифрування;

• здійснюється контроль цілісності пакета на основі вибраного алгоритму. У разі порушення цілісності пакет відкидається;

• пакет надсилається адресату згідно з інформацією, що знаходиться в його оригінальному заголовку.

VPN-агент може знаходитися безпосередньо на комп'ютері, якій захищається. У цьому випадку з його допомогою захищається інформаційний обмін лише того комп'ютера, на якому він встановлений, проте описані вище принципи дії залишаються незмінними.

VPN-агент, що захищає локальну обчислювальну мережу (ЛОМ), може бути доданий до маршрутизатором IP-пакетів, який також повинен знаходитися на виході з ЛОМ. Такий маршрутизатор зазвичай називають криптографічним. Як криптографічний маршрутизатор може використовуватися як звичайний (неспеціалізований) комп'ютер, оснащений спеціальним програмним забезпеченням та апаратурою (апаратним шифратором), так і спеціалізований маршрутизатор.

Основне правило побудови VPN: зв'язок між захищеною ЛОМ та Інтернетом повинен здійснюватися тільки через VPN-агенти, категорично забо-

роняються будь-які способи зв'язку, що проходять захисний бар'єр у вигляді VPN-агента; тобто, повинен бути визначений периметр, якій має захищатися, зв'язок з яким можлива тільки через відповідний засіб захисту.

Політика безпеки є набором правил, згідно з якими встановлюються захищені канали зв'язку між абонентами VPN. Такі канали зазвичай називають тунелями, аналогія з якими проглядається в наступному:

• вся інформація, що передається в рамках одного тунелю, захищена як від модифікації, так і від несанкціонованого перегляду;

• інкапсуляція IP-пакетів дозволяє домогтися приховування топології внутрішньої ЛОМ: з Інтернету обмін інформацією між двома захищеними ЛОМ видно як обмін інформацією тільки між їх VPN-агентами, оскільки всі внутрішні IP-адреси в IP-пакетах, що передаються через Інтернет, в цьому випадку не фігурують.

Отже, описані вище дії VPN-агентів зводяться, до забезпечення двох механізмів: тунелювання та фільтрації інформації (рис. 2.1).

Рис. 2.1. Тунелювання та фільтрація

Правила створення тунелів формуються залежно від різних параметрів IP-пакетів; наприклад, основний при побудові більшості VPN протокол IPSec буде встановлювати наступний набір вхідних даних, якими вибираються параметри тунелювання і приймається рішення при фільтрації конкретного IP-пакета:

• IP-адреса відправника. Це може бути не тільки одиночна IP-адреса, але й адреса підмережі або діапазон адрес;

• IP-адреса призначення. Також може бути діапазон адрес, що вказується явно за допомогою маски підмережі або шаблону;

• ідентифікатор користувача (відправника чи отримувача);

• протокол транспортного рівня (як, TCP/UDP);

• номер порту, з якого або на який надіслано пакет.

2.2 . Методи реалізації VPN мереж

Віртуальна приватна мережа VPN базується на трьох методах реалізації: тунелювання, шифрування та аутентифікація.

Тунелювання створює передачу даних між двома точками - закінченнями тунелю - таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, яка лежить між ними.

Транспортне середовище тунелю, як парою, підхоплює пакети використовуваного мережевого протоколу у входу в тунель і без змін доставляє їх до виходу. Створення тунелю достатньо, щоб з'єднати два мережеві вузли так, що з точки зору програмного забезпечення вони виглядають підключеними до однієї (локальної) мережі. Однак не можна забувати, що насправді потоки з даними проходить через безліч проміжних вузлів (маршрутизаторів, комутаторів) відкритої публічної мережі.

Такий стан справ містить у собі дві проблеми. Перша полягає в тому, що вся інформація, яка передається через тунель, може бути перехоплена

шахраями. Якщо вона має конфіденційність (номера банківських карток, фінансиві звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже по собі неприємно. Також, зловмисники мають можливість модифікувати передані через тунель дані так, що отримувач не зможе перевірити їх достовірність. Наслідки можуть бути не бажаними. Враховуючи сказане, ми приходимо до висновку, що тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкоджати внесенню несанкціонованих змін у пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий пакет забезпечується додатковою інформацією з блоком, що виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для змістовного пакета. Цей блок інформації є ЕЦП пакета і дозволяє виконати автентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист даних переданих через тунель від несанкціонованого впливу досягається шляхом використання сильних алгоритмів шифрування.

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

Для аутентифікації користувачів PPTP може задіяти будь-який з протоколів, які застосовуються для PPP:

EAP або Extensible Authentication Protocol;

MSCHAP або Microsoft Challenge Handshake Authentication Protocol (версії 1 та 2);

CHAP або Challenge Handshake Authentication Protocol;

SPAP або Shiva Password Authentication Protocol;

PAP або Password Authentication Protocol.

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

Аутентифікація здійснюється або відбитим тестом (clear text password), або за схемою запит/відгук (challenge/response). З прямим текстом все зрозуміло. Клієнт посилає серверу пароль. Сервер порівнює це з ідеалом і чи забороняє доступ, чи каже «ласкаво прсимо». Відкрита автентифікація мало зустрічається.

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

Схема запит/відгук набагато більш просунута. У загальному вигляді вона виглядає так:

- клієнт посилає серверу запит на автентифікацію;

- сервер повертає випадковий відгук;

- клієнт знімає зі свого пароля хеш (хешем називається результат хеш-функції, яка перетворює вхідний масив даних довільної довжини у вихідну бітову строку фіксованої довжини), шифрує;

- те саме робить і сервер, порівнюючи отриманий результат з відповіддю клієнта;

- якщо зашифрований відгук співпадає, автентифікація вважається успішною;

На першому етапі аутентифікації клієнтів і серверів VPN, L2TP поверх IPSec використовує локальні сертифікати, отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами та створюють захищене з'єднання ESP SA. Після того як L2TP (поверх IPSec) завершує процес автентифікації комп'ютера, виконується автентифікація на рівні користувача [11]. Для аунтентифікації можна задіяти будь-який протокол, навіть PAP, якій передає

ім'я користувача і пароль у відкритому вигляді. Це повністю безпечно, тому що L2TP поверх IPSec шифрує всю сесію.

PPTP змінює значення ключа шифру після кожного прийнятого пакета. Протокол MMPE розроблявся для каналів зв'язку точка-точка, в яких пакети передаються послідовно, і втрата даних дуже мала. В такій ситуації значення ключа для чергового пакета залежить від результатів дешифрації попереднього пакета. При побудові віртуальних мереж через мережі загального доступу ці умови дотримуватися неможливо, так як пакети даних часто приходять до отримувача не в тій послідовності, в якій були відправлені. Тому PPTP використовує зміни ключа шифрування порядкові номери пакетів. Це дозволяє виконувати дешифрацію незалежно від попередніх прийнятих пакетів.

Отже, використання «тунелювання + автентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу.

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

Основною проблемою мереж VPN є відсутність обміну шифрованою інформацією та стандартів аутентифікації. Ці стандарти розробляються і тому продукти різних виробників не можуть встановлювати VPN-з'єднання і

автоматично обмінюватися ключами. Дана проблема тягне за собою уповільнення поширення VPN, важко змусити різні компанії користуватися продукцією одного виробника, а тому ускладнений процес об'єднання мереж компаній-партнерів.

2.3 . VPN-рішення для побудови захищених корпоративних мереж

Потенційним клієнтам пропонується широкий спектр устаткування та програмного забезпечення для створення віртуальних приватних мереж: від інтегрованих багатофункціональних і спеціалізованих пристроїв до чисто програмних продуктів.

Можна виділити три основні види VPN-рішень: інтегровані, спеціалізовані, програмні.

Розглянемо особливості кожного з перерахованих видів.

Інтегровані VPN-рішення включають функції МЕ, маршрутизації і комутації. Головна перевага такого підходу полягає в централізації управління компонентами. Для компаній, яким не потрібна висока продуктивність корпоративної мережі, а задача зниження витрат на мережеве устаткування є однією з пріоритетних, найефективнішим буде інтегроване рішення, що дозволяє зосередити всі функції в одному пристрої. Також треба сказати, що чим більше функцій виконується одним пристроєм, тим частіше стають помітними втрати в продуктивності.

Спеціалізовані VPN-рішення. Висока продуктивність – найголовніша перевага спеціалізованих VPN-пристроїв. Вища швидкодія подібних систем обумовлена тим, що шифрування в них здійснюється спеціалізованими мікросхемами.

Об'єм обчислень, які необхідно виконати при обробці VPN-пакету, в 50-100 разів перевищує той, який потрібен для обробки звичного пакету. Якщо в корпоративній мережі проводяться різні заходи [11], які вимагають обміну ве-

ликим трафіком даних, то для ефективної обробки VPN-пакетів доцільно використовувати спеціалізовану апаратуру. Спеціалізовані VPN-пристрої забезпечують високий рівень безпеки, проте мають високу вартість.

Програмні VPN-рішення. VPN-продукти, реалізовані програмним способом, з погляду продуктивності поступаються спеціалізованим пристроям, проте мають достатню потужність для реалізації VPN-мереж. Слід зазначити, що у разі видаленого доступу вимоги до необхідної смуги пропускання невеликі. Тому чисто програмні продукти легко забезпечують продуктивність, достатню для видаленого доступу. Безперечними перевагами програмних продуктів є гнучкість і зручність в застосуванні, а також відносно невисока вартість.

Як правило, на практиці будують комбіновані VPN на базі існуючих рішень:

- мережевих операційних систем;
- маршрутизаторів;
- міжмережевих екранів;
- спеціалізованого програмного забезпечення.

Побудова VPN на базі мережевої ОС – достатньо зручний і, головне, дешевий спосіб створення інфраструктури захищених віртуальних каналів. Сьогодні найбільше розповсюдження серед мережевих систем, що дозволяють побудувати VPN штатними засобами самої системи, одержала Windows. Дане рішення виявилося популярним, завдяки загальній поширеності даної системи.

На думку фахівців, дане рішення є оптимальним для побудови VPN усередині локальних мереж або домена Windows, а також для побудови intranet- і extranet-VPN для невеликих компаній з метою захисту некритичної для їх бізнесу інформації. В той же час великий бізнес не може довірити свої секрети цьому рішенню, оскільки численні випробування VPN, показали, що протокол PPTP достатньо уразливий з погляду безпеки.

Побудова VPN на базі маршрутизаторів

Сьогодні практично всі провідні виробники маршрутизаторів і інших мережевих пристроїв заявляють про підтримку в своїх продуктах різних VPN-протоколів. В Україні безумовним лідером на цьому ринку є компанія Cisco Systems, тому побудову корпоративних VPN доцільно продемонструвати на рішеннях саме цієї компанії.

Побудова VPN-каналів на базі маршрутизаторів компанії Cisco здійснюється засобами самої ОС. Якщо па прикордонні маршрутизатори Cisco інших відділень компанії встановлена ця ОС, то є можливість сформувати корпоративну VPN, яка складається з сукупності віртуальних захищених тунелів типу «точка-точка» від одного маршрутизатора до іншого (рис. 2.2). Тут і далі як ілюстрації використовуються схеми побудови VPN мереж, одержані з Web-сайтів виробників. Для шифрування даних в каналі за умовчанням застосовується криптоалгоритм DES з довжиною ключа 56 біт.

Рис. 2.2. Типова схема побудови корпоративної VPN на базі маршрутизаторів Cisco

Для організації VPN тунелю маршрутизатори компанії Cisco в даний час використовують протокол канального рівня L2TP (створений на базі фірмових протоколів L2F і PPTP) і протокол мережевого рівня IPSec.

Протокол L2TP забезпечує інкапсуляцію протоколів мережевого рівня (IP, IPX та ін.) в пакети канального рівня, які і передаються по мережах, що підтримують доставку датаграм в каналах «точка-точка». Цей протокол і претендує на рішення проблем безпеки в VPN, він ніяк не специфікує процедури шифрування, автентифікації і перевірки цілісності кожного пакету, якій передається по відкритій мережі, а також процедури управління криптографічними ключами. Основна перевага L2TP полягає в його незалежності від транспортного рівня, що дозволяє використовувати його в гетерогенних мережах. Проте «канальна природа» протоколу L2TP послужила причиною його істотного недоліку: для гарантованої передачі захищеного пакету через складові мережі всі проміжні маршрутизатори повинні підтримувати даний протокол, що, очевидно, вельми важко гарантувати [3].

На сьогоднішній день IPSec – один з досконалих, в плані безпеки Internet-протоколів. Зокрема, він забезпечує перевірку цілісності автентифікацію і шифрування повідомлень на рівні кожного пакету. IPSec дозволяє маршрутизувати зашифровані пакети мережам без додаткової настройки проміжних маршрутизаторів, оскільки зберігає стандартний IP-заголовок. А тому, IPSec включений як невід'ємна частина в Internet-протоколі IPv6, це робить його ще привабливішим для організації корпоративних VPN. Крім того, робота протоколу на мережевому рівні є однією із стратегічних переваг IPSec, оскільки VPN на його базі працюють повністю прозоро як для всіх без виключення додатків і мережевих сервісів, так і для мереж передачі даних канального рівня.

Але IPSec має в собі і деякі недоліки: підтримка тільки стека TCP/IP і досить великий об'єм технічної інформації, який може викликати істотне зниження швидкості обміну даними на низькошвидкісних каналах зв'язку.

Необхідно пам'ятати, що у разі побудови VPN на базі маршрутизаторів такий підхід не вирішує проблему забезпечення загальної інформаційної безпеки компанії, оскільки всі внутрішні інформаційні ресурси все одно залишаються відкритими для атак ззовні. Для захисту цих ресурсів, як правило, застосо-

вуються МЕ, які розташовуються за прикордонними маршрутизаторами, а отже, на каналі від маршрутизатора до МЕ і далі вся конфіденційна інформація йде в «відкритому» вигляді.

Один з істотних недоліків побудови VPN на базі маршрутизаторів полягає у тому, що рішення єдиної задачі захисту інформаційних ресурсів компанії від атак ззовні розподіляється по декількох функціонально незалежних пристроях (маршрутизатор і МЕ). Такий підхід може привести до серйозних організаційних і технічних проблем у випадках, як визначення відповідальності за порушення інформаційної безпеки мережі.

- Побудова VPN на базі міжмережевих екранів

Ряд фахівців з інформаційної безпеки вважає, що побудова VPN на базі МЕ є єдиним оптимальним варіантом з погляду забезпечення комплексної безпеки корпоративної інформаційної системи від атак з відкритих мереж. Дійсно, об'єднання функцій МЕ і VPN-шлюзу в одній точці під контролем єдиної системи управління і аудиту - не тільки технічно грамотне, але і зручне для адміністрування рішення. Як приклад розглянемо типову схему побудови корпоративної VPN на базі популярного програмного продукту Checkpoint Firewall-1/VPN-1 компанії Checkpoint Software Technologies.

Дана компанія є одним з лідерів у області виробництва продуктів комплексного забезпечення інформаційної безпеки при роботі з Internet мережою. Мережевий екран Checkpoint Firewall-1 дозволяє в рамках єдиного комплексу побудувати глибокоешелонований рубіж оборони для корпоративних інформаційних ресурсів.

Підсистема побудови VPN на базі CheckPoint FW-1 включає програмні продукти VPN:

- Gateway і VPN-1 Appliance, призначені для побудови intranet-VPN;
- VPN-1 SecureServer – для захисту виділених серверів;
- VPN-1 SecuRemote і VPN-1 SecureClient – для побудови internet/externet/ localnet-VPN.

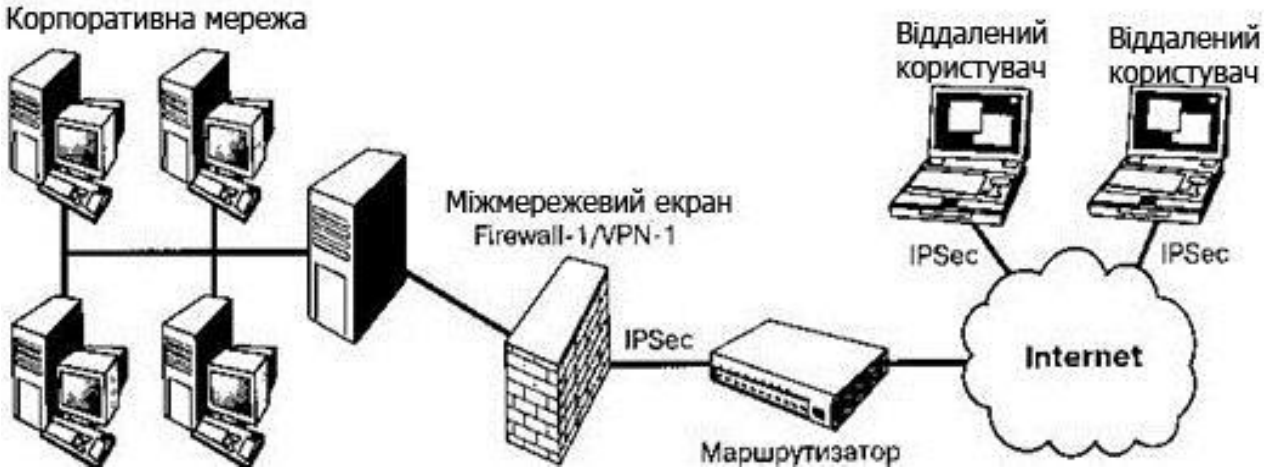

Рис. 2.3. Схема побудови мережі VPN на базі CheckPoint FW-2/VPN-1

ВИСНОВКИ ДО РОЗДІЛУ 2

В даному розділі було розглянуто, основні принципі побудови мереж VPN та протоколів, які використовуються при створенні VPN мереж. Для цього було визначено основні поняття і функції мережі VPN, описані способи для створення захищених віртуальних каналів, викладено класифікацію VPN мереж за архітектурою, та за типом технічної реалізації. Було також приділено увагу аналізу протоколів VPN мережі та описані процедури на яких рівнях моделі OSI вони функціонують.

Більш детально розглянуто протоколи, які використовуються для побудови тунелів VPN PPTP, L2TP, SSL, TLS та IPSEC. На відміну від PPTP, протокол L2TP не прив'язаний до протоколу IP, саме тому він може бути використаний в мережах з комутацією пакетів. Також, в протокол L2TP додана важлива функція управління потоками даних, та ряд відсутніх в специфікації протоколу PPTP функцій захисту. Застосування тунельного або транспортного режиму роботи залежить від ролі вузла в якому працює IPSec. Взагалі розрізняють три схеми застосування: хост-хост, шлюз-шлюз та хост-шлюз.

РОЗДІЛ 3
ЗАХИЩЕНА МЕРЕЖА НА БАЗІ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ТЕХНОЛОГІЇ VPN

3.1 . КОМУТОВАНІ МЕРЕЖІ

На підприємствах, які розвиваються, сучасні мережі, повинні бути легко масштабованими, керованими та надійними. Подібні завдання найпростіше можуть вирішитися у разі використання ієрархічної топології мережі, модель якої включає кілька рівнів ієрархії.

Мережі пакетної комутації зазвичай будуються з урахуванням комутаторів, які мають 12-48 портів (інтерфейсів), і деякі комутатори і більше. Якщо такої кількості портів вистачає всім користувачів, то структура мережі буде представлена найпростішою однорівневою схемою (рис. 3.1 а).

На різних рівнях моделі мережі (рис. 3.1 в) вирішуються різні завдання, виходячи з вимог, що висуваються. Ієрархічна схема мережі легко масштабується; комутатори рівня розподілу та ядра, а також їх з'єднання дублюються, що забезпечує надмірність (резервування) та підвищує надійність мережі. Комутатори різних рівнів можуть мати різну швидкодію, порівняно низьку на рівні доступу та найвищу на рівні ядра.

Рівень ядра (Core layer) є швидкодіючою магістраль мережі і дає можливість з'єднання з мережею Інтернет через маршрутизатор. Вимога високої швидкодії зумовлена тим, що цьому рівні передається сумарний потік даних всіх користувачів. Важливою властивістю ядра є надмірність.

Резервування обладнання дає змогу забезпечити високу надійність. Тому комутатори рівня ядра зазвичай дублюються (С1, С2 на рис. 3.1 в).

Рівень розподілу (Distribution layer) також характеризується запровадженням надлишкових пристроїв і з'єднань підвищення надійності. У цьому рівні формуються широкомовні домени, тобто. реалізується управління пото-

ками, що притаманно функцій мережного рівня моделі OSI, забезпечується маршрутизація між віртуальними локальними мережами.

Рівень доступу (Access layer) забезпечує доступ кінцевих вузлів до мережі. Саме на цьому рівні часто бувають спроби несанкціонованого доступу, тому питання безпеки портів комутаторів є найбільш актуальними на даному рівні. Тобто, на цьому рівні моделі (рис. 3.1 в) необхідно забезпечити безпеку портів, щоб не допустити несанкціоноване проникнення в мережу. Оскільки користувачів та портів комутаторів на цьому рівні дуже багато, то комутатори зазвичай не дублюються. Для розмежування потоків та створення широкомовних доменів порти комутатора приписуються до віртуальних локальних мереж.

Управління лише на рівні доступу задає, до яких портів комутатора може підключатися той чи інший кінцевий вузол, ідентифікація кожного вузла проводиться за його MAC-адресою. Якщо кінцеві вузли неавторизованих користувачів не матимуть доступу до комутаторів, підвищується безпека всієї мережі.

Питання гарантії якості обслуговування вирішуються всіх рівнях моделі. Якість послуг (Quality of Service-QoS) дуже важливо забезпечити в мультисервісних мережах, оскільки в них передаються як цифрові дані, так і потоки аудіо- та відеоінформації. Як правило, на рівні доступу в певний момент часу комутатор має справу з якимось одним видом інформації (аудіо-, відео-, даними). Однак на рівні розподілу та ядра комутуються агреговані потоки інформації, тому засоби цих рівнів повинні забезпечувати задану якість QoS для кожного з видів інформації, що передаються. Це реалізується за рахунок завдання різних пріоритетів повідомлень, які передаються.

Важливим питанням при проектуванні мережі ієрархічної моделі є місце розміщення серверів, баз даних, мережевих принтерів. Необхідно мінімізувати кількість проміжних пристроїв (комутаторів) між користувачем та загальномережевим обладнанням, а також оптимізувати пропускну здатність

з'єднань, оскільки до серверів та баз даних може одночасно звертатися безліч кінцевих пристроїв.

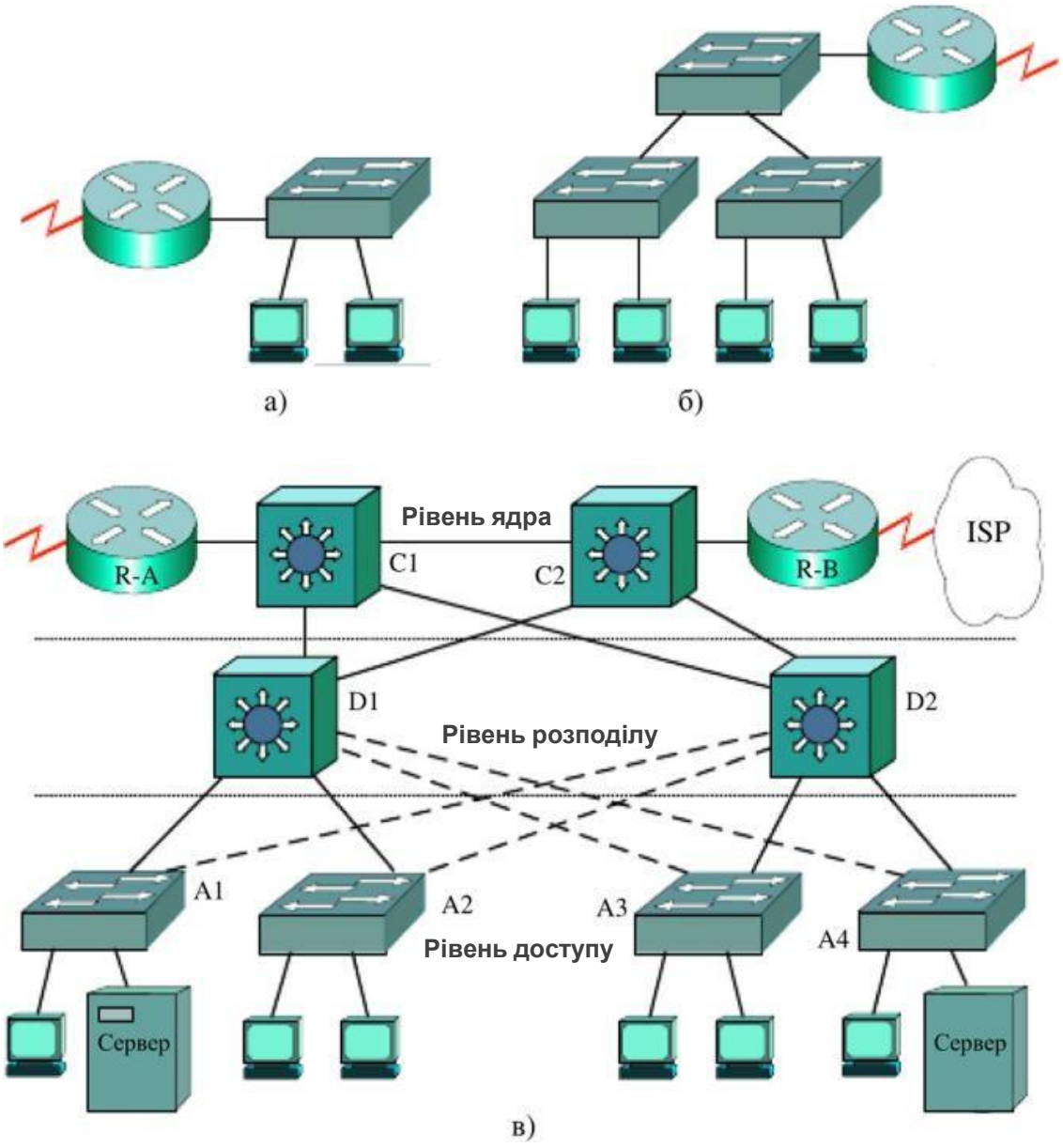

Рис. 3.1. Схеми локальних мереж з урахуванням комутаторів

Для підвищення пропускної спроможності будь-якої ділянки мережі у ряді випадків проводять об'єднання (агрегування) з'єднань, а також створюють транкові з'єднання, які характерні для всіх рівнів моделі. Принцип агрегування кількох портів комутатора забезпечення необхідної продуктивності наочно відображає схема рис. 3.2, коли доступ до сервера може одночасно

знадобитися кільком кінцевим вузлам. Для забезпечення необхідної підвищеної продуктивності з'єднання сервера з комутатором об'єднуються (агрегуються) кілька портів комутатора.

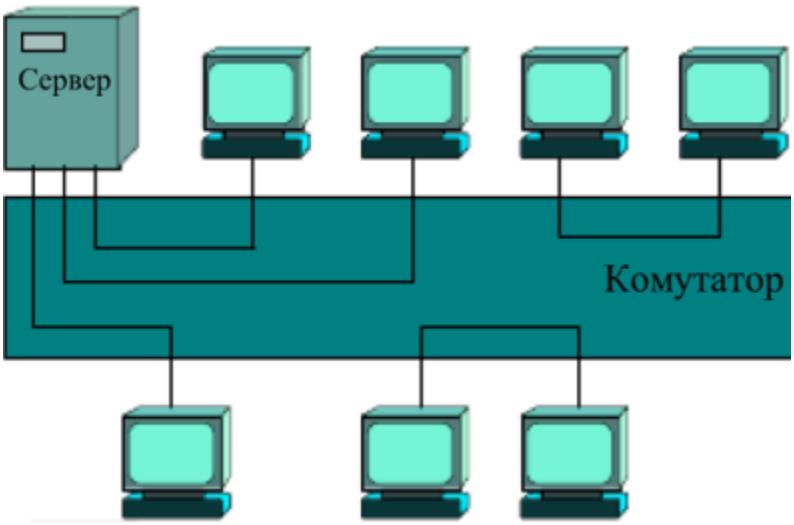

Рис. 3.2. Агрегування портів комутатора

Швидкість передачі порту комутатора визначається двома технічними характеристиками: швидкістю фільтрації і швидкістю просування. Фільтрація кадрів відбувається у тому випадку, коли адресат призначення перебуває у тому сегменті, як і джерело переданих даних. При цьому немає необхідності передавати кадр через комутатор, тому після прийому кадру в буфер і визначення адресата призначення комутатор знищує кадр, що знаходиться в буфері, копія якого вже надійшла адресату. Сегменти утворюються пристроями фізичного рівня (повторювачами, концентраторами). Двоточкове з'єднання комп'ютера з інтерфейсом комутатора утворює мікросегмент.

Комутатори можуть працювати в кількох режимах, при зміні яких змінюються затримка та надійність. Для забезпечення максимальної швидкодії (мінімальної затримки) комутатор може розпочинати передачу кадру відразу, як тільки отримає MAC-адресу вузла призначення. Такий режим отримав назву наскрізної комутації або комутації на льоту (cut-through switching), він за-

безпечує найменшу затримку при проходженні кадрів через комутатор. Однак у цьому режимі неможливий контроль помилок, оскільки поле контрольної суми наприкінці кадру. Отже, цей режим характеризується низькою надійністю. У цьому режимі мережа засмічується пошкодженими кадрами, вони знижують її продуктивність.

У другому режимі комутатор отримує кадр повністю, поміщає його в буфер, перевіряє поле контрольної суми і потім пересилає адресату. Якщо отримано кадр з помилками, він відкидається комутатором. Оскільки кадр перед відправкою адресату призначення запам'ятовується в буферній пам'яті, такий режим комутації отримав назву комутація з проміжним зберіганням або буферизацією. Таким чином, у цьому режимі забезпечується висока надійність, але порівняно низька швидкість комутації.

3.2 . ЗАХИЩЕНА МЕРЕЖА ЗАСОБОМ ПРОГРАМНО-АПАРАТНОГО ЗАХИСТУ ІНФОРМАЦІЇ ШИФР-VPN

На теперішній час, для вже існуючих інформаційних систем, забезпечення безпечної та конфіденційної передачі даних з використанням мережі Інтернет вирішується за допомогою технологій віртуальних приватних мереж VPN.

При побудові VPN рекомендують звернути увагу на:

- Зручність експлуатації та інтеграції.
- Гнучкість та зручність керування ключами.
- Гнучкість та зручність налаштування мережі.
- Перспективність (підтримувані алгоритми).
- Орієнтація на хмарні технології.
- Швидкість передачі даних.
- Широкий спектр підтримуваних апаратних платформ та операційних систем [21].

Система криптографічного захисту каналів зв'язку «Шифр-VPN» програмний чи програмно-апаратний комплекс, що базується на протоколі OpenVPN з підтримкою SSL/TLS, для забезпечує конфіденційность при передачі даних в комп’ютерних мережах.

СКЗКЗ «Шифр-VPN» дозволяє забезпечити конфіденційність (шифрування) між:

- Мережа-Мережа (Сервер-Сервер). Такий підхід дозволяє будувати VPN з’єднання між різними мережами, де весь трафік буде захищений.
- Користувач-Мережа (Клієнт-Сервер). Такий підхід дозволяє будувати VPN з’єднання між комп’ютером користувача та мережею, яка розміщена за VPN Сервером.

Для забезпечення конфіденційності використовуються криптографічні алгоритми:

- Реалізовані в бібліотеках криптографічних примітивів «Шифр+» v 2.1 (наявний чинний позитивний експертний висновок).
- З урахуванням великого досвіду компанії Сайфер [21].

СКЗКЗ Шифр-VPN можна будувати навколо інфраструктури відкритих ключів:

- Ключі видані АЦСК/КНЕДП. У цьому випадку для авторизації користувачів в захищеній мережі, можуть використовуватися:
  - Перевірка статусу сертифікату за протоколом OCSP.
  - Ведення списку довірених ЦСК на сервері VPN.
  - Ведення списку дозволених користувачів на сервері VPN.
- Ключі видані внутрішнім ЦСК. У цьому випадку розгортається власна інфраструктура ключів, використовуючи власні рішення.

У якості криптографічних алгоритмів допускається використовувати:

- Національні криптографічні алгоритми:
  - ДСТУ 4145:2002.
  - ГОСТ 34.311-95, ДСТУ 7564:2014.
  - ГОСТ 28147-89, ДСТУ 7624:2014.

- Міжнародні криптографічні алгоритми:
  - RSA, ECDSA.
  - SHA-1, SHA-2.
  - AES, DEA, TDEA [21].

Ключі користувачів та серверів можуть використовуватись:

- У вигляді файлу – файлового ключового контейнеру
  - PFX/PKCS#12.
  - JKS (АЦСК Приватбанк).
  - Key-6.dat (ЦСК побудовані на основі АТ ІІТ).
  - ZS2 (аналог PFX/PKCS#12 АЦСК Україна).
- На захищеному носії
  - В пасивному режимі.
    - Aladdin/SafeNet/Gemalto eToken.
    - Автор SecureToken-337.
    - Авест AvestKey.
    - Ефіт EfitKey.
    - Та інші.
  - В активному режимі.
    - ІІТ Алмаз-1К.
    - Автор SecureToken-337.
    - Авест AvestKey.
    - Ефіт EfitKey [21].

СКЗКЗ Шифр-VPN підтримує широкий спектр апаратних платформ та операційних систем:

- Апаратні платформи:
  - x86, x86-64 (AES NI, CLMUL, SSE, AVX). Підтримується апаратне прискорення.
  - ARMv6, ARMv7, ARMv8.
- Операційні системи:
  - Сервер: Windows, Linux, FreeBSD.

- Клієнт: Windows, Linux, MacOS.
- Клієнт: Android, iOS.

Зручність використання СКЗКЗ Шифр-VPN забезпечується:

- Розвинутою системою керування серверами VPN.
- Розвинутою системою моніторингу сервера VPN побудованою на базі агентів та розширень для Zabbix.
- Можливість гнучкого налаштування сервера та клієнтів. Налаштування здійснюється завдяки розповсюдженню серед клієнтів раніше підготовлених файлів налаштувань [21].

Одним з найскладніших питань застосування VPN, є інтеграція зі вже існуючими системами з мінімальними змінами:

- Шифр-VPN забезпечує балансування трафіку. У цьому випадку, кілька Серверів VPN працюють, як єдине ціле та з'єднання від клієнтів розповсюджується менш навантаженим Серверам VPN (найменшою кількістю підключень).
- За необхідності, Шифр-VPN дозволяє захищати мережеві підключення з більшою пропускною здатністю, за рахунок агрегації віртуальних мережевих інтерфейсів. У цьому випадку обчислювальна система, може бути завантажена оптимальним чином.
- Агрегація трафіку досягається за рахунок паралельної роботи кількох Серверів VPN на одній обчислювальній машині [21]. У цьому випадку Сервера VPN прив'язані до різних портів та/чи адрес.
- Застосовані в Шифр-VPN підходи до побудови Сервера VPN, забезпечують ефективну можливість роботи, як на фізичному, так і на віртуальному обладнані.

Існують варіанти побудови Сервера VPN:

- Віртуальна машина. Рекомендується для забезпечення конфіденційності при підключенні до хмарних ресурсів.
- Docker контейнер. Рекомендується для забезпечення конфіденційності при підключенні до хмарних ресурсів.

- Архів з дистрибутивом для самостійного встановлення.
- Може виконуватися в захищеному апаратному виконанні (попереднє замовлення) [21].

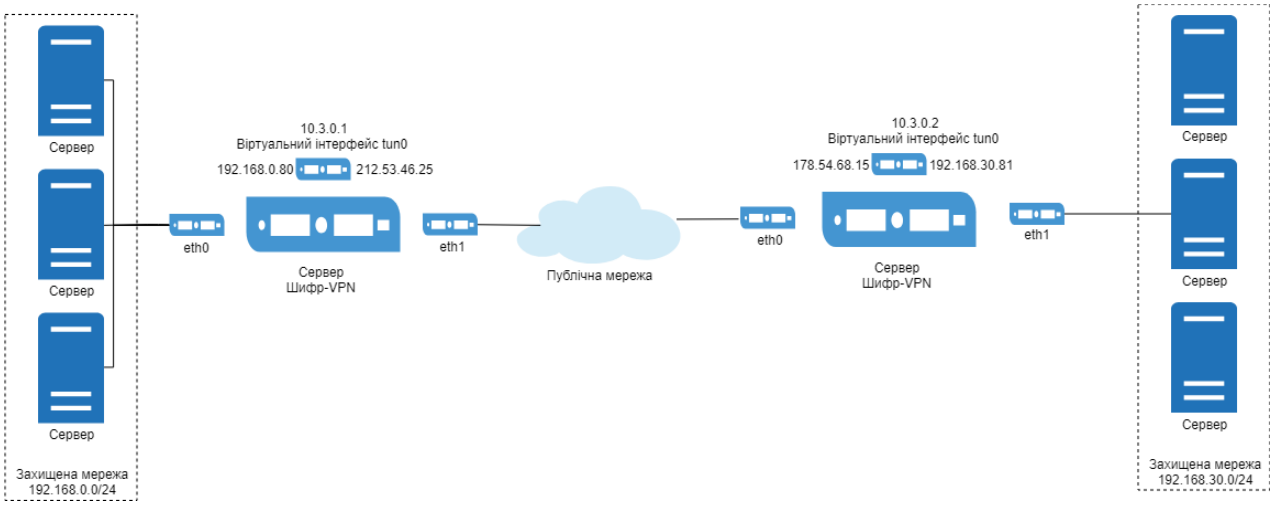

Рис 3.3. Побудова захищеного каналу між двома мережами

Однією з типових задач, які можуть бути успішно вирішуватися СКЗКЗ «Шифр-VPN» [21], є побудова захищеного каналу між двома мережами.

З обох сторін розгорнутий Сервер VPN, який може:

- Керувати трафіком між мережами, які знаходяться за VPN.
- Шифрувати чи не шифрувати трафік.
- Можливість проходження трафіку через фаєрволи та HTTP-proxy.
- Агрегувати трафік з кількох мережевих інтерфейсів, а також виконувати зворотнє перетворення.
- На цих серверах використовуються статичні ідентичні ключі у PKCS контейнері.

Однією з типових задач, які можуть успішно вирішуватися СКЗКЗ «Шифр-VPN» [21], є побудова захищеного каналу між користувачем та мережею.

З одного боку, розгорнуто Сервер VPN, а у користувача Клієнт VPN.

На стороні Сервера VPN:

- Керувати трафіком між двома мережами, які знаходяться за VPN.
- Можливість проходження трафіку через фаєрволи та HTTP-proxy.
- Шифрувати чи не шифрувати (а тегувати) трафік.
- Агрегувати трафік з кількох мережевих інтерфейсів, а також виконувати зворотнє перетворення.
- На цих серверах використовуються статичні ідентичні ключі у PKCS#12 контейнері.
- Паралельна робота кількох Серверів VPN.
- Балансування підключень між пулом Серверів VPN.
- Автентифікація користувача за різними ознаками.
- Підтримка роботи з ЦСК за протоколами OCSP over HTTP, для перевірки статусу сертифікату [21].

На стороні Клієнта VPN:

- Можливість використання конфігураційних файлів виконанням налаштувань для даного Сервера VPN.
- Можливість підключення до пулу Серверів VPN, за принципом «хто перший відповість».
- Шифрувати чи не шифрувати (а тегувати) трафік
- Можливість проходження трафіку через фаєрволи та HTTP-proxy.
- Керувати трафіком між мережами, які знаходяться за VPN.
- Можливість зберігати ключ у файлових контейнерах та на захищених носіях.
- Зберігати пароль в пам’яті до захищеного носія, чи вимагати його вводити кілька разів.
- Підтримка роботи з ЦСК за протоколами OCSP over HTTP, для перевірки статусу сертифікату [21].

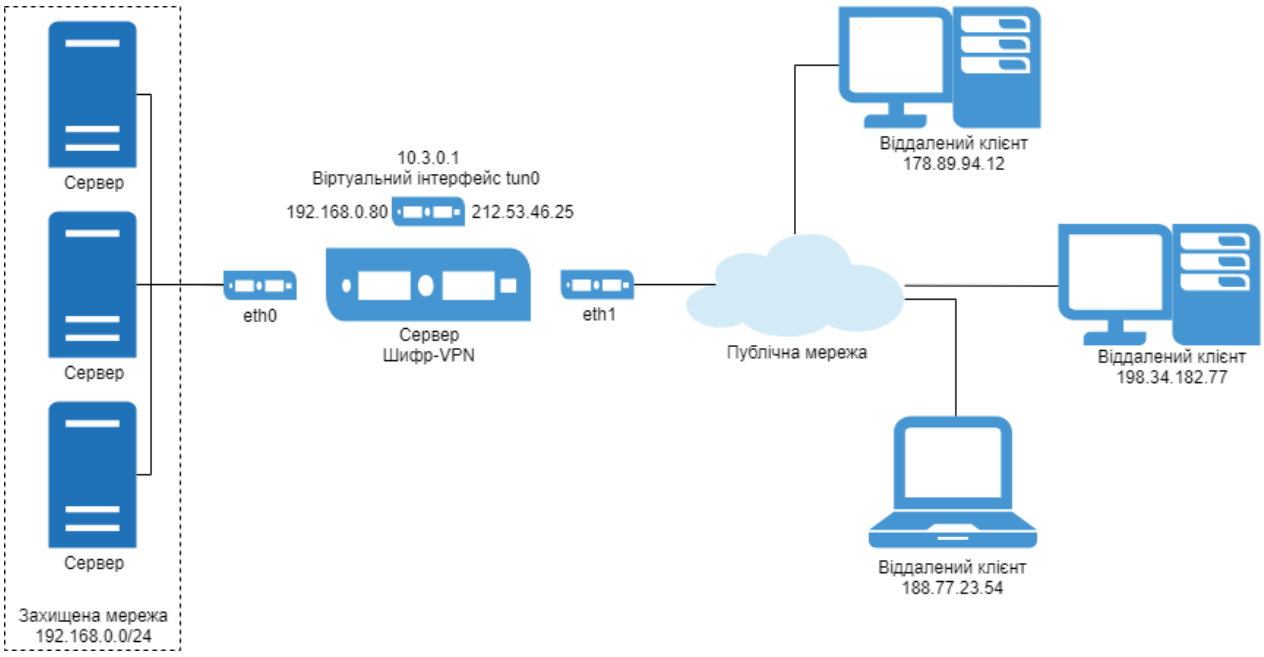

Рис. 3.4. Побудова захищеного каналу між користувачем та мережею

Однією з типових задач, що можуть успішно вирішуватися комплексом «Шифр-VPN», є побудова захищеного каналу між користувачем та мережею.

З одного боку розгорнутий Сервер VPN, а з іншого, у користувача Клієнт VPN. На стороні Сервера VPN можливе управління трафіком від клієнтських підключень між різними мережами.

Існує велика кількість підходів до побудови VPN, у залежності від рівня:

- Мережевий (IP/IPSec).
- Транспортний (TCP/UDP).

Вказані підходи мають як позитивні, так і негативні сторони [21].

Серед існуючих рішень та підходів, виділяють протокол OpenVPN з підтримкою SSL/TLS, який дозволяє забезпечити:

- Прозорість проходження Firewall, Proxy, NAT у порівнянні з LT2P/IPsec.

- Більш високу продуктивність при меншому об’ємі спожитих обчислювальних ресурсів у порівнянні з LT2P/IPsec.
- Підтримку протоколів транспортного рівня TCP, UDP.
- Стискання трафіку за допомогою алгоритмів LZO, ZIP.
- Гнучкість налаштування на стороні клієнтів, завдяки попередньо встановлених конфігураційних файлів [21].

Для того, щоб зменшити навантаження на процесор зі сторони фізичного сервера, де запущено Сервер VPN, обов’язково рекомендується використовувати процесори з підтримкою інструкцій AES NI.

ВИСНОВКИ ДО РОЗДІЛУ 3

На підприємствах сучасні мережі, повинні бути легко масштабованими, керованими та надійними. Подібні завдання можуть вирішуватися у разі використання ієрархічної топології мережі, модель якої включає кілька рівнів ієрархії. В цьому розділі роботи було проаналізовано, побудову комутованої мережі, в якої буде працювати мережа VPN. Розглянуто її види, складові частини. За допомогою VPN також визначено способи організації VPN наділені певними перевагами та недоліками. Розглянуто та проаналізовано вже існуючий VPN від Сайфер, який має експертні висновки в Україні.

ВИСНОВОК

Ефективне використання інформаційних технологій є важливим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств та організацій. Технологія віртуальної приватної мережі VPN забезпечує зв'язок між мережами, а також вирішення різних проблем через захищений канал Інтернет між віддаленим користувачем та корпоративною мережею.

У кваліфікаційній роботі було розглянуто різні технології VPN, різновиди протоколів для побудови VPN, сутність технології VPN.

Використовуючи VPN можна організувати захист на різних рівнях моделях OSI. На канальному рівні, засоби VPN, дозволяють забезпечити інкапсуляцію різних видів трафіку та побудову віртуальних тунелів типу «точка-точка». На мережевому рівні виконується інкапсуляція IP в IP, а на сеансовому використовується метод «circuit proxy», який ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet. Реалізувати VPN можна на основі мережевої операційної системи, міжмережевого екрану, маршрутизаторів, програмних рішень або спеціалізованих апаратних засобів з вбудованими шифропроцесорами.

Було розглянуто захищену мережу за допомогою протоколів PPTP, L2TP, SSL, TLS та IPSEC. Протокол L2TP не прив'язаний до протоколу IP, на відміну від PPTP, тому він може бути використаний в мережах з комутацією пакетів. Також, в протокол L2TP додана важлива функція управління потоками даних, а також ряд відсутніх в специфікації протоколу PPTP функцій захисту. В залежності від ролі вузла в якому працює IPSec застосовується тунельний або транспортний режим. Взагалі розрізняють три схеми застосування IPSec: хост-хост, шлюз-шлюз та хост-шлюз. Система IPSec займає лідируючі позиції в наборі стандартів для створення VPN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ютерні мережі: підручник / Азаров О.Д., Захарченко С.М., Кадук О.В., Орлова М.М., Тарасенко В.П. – Вінниця: ВНТУ. – 2020. –378 с.

2. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1 / Буров Є.В., Митник М.М.; За заг. ред. Пасічника В.В. Львів: Магнолія 2006, 2019. – 334 с

3. Микитишин А.Г. Комп'ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.

4. Andrew S. Tanenbaum. Computer Networks / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall; 5 edition (October 7, 2010). – 960 p.

5. Larry L. Peterson. Computer Networks, Fifth Edition: A Systems Approach (The Morgan Kaufmann Series in Networking) / Larry L. Peterson, Bruce S. Davie. – Morgan Kaufmann; 5 edition (March 25, 2011). – 920 p.

6. Комп'ютерні мережі / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В., 2016. – 256 с.

7. Комплексні системи захисту банківських інформаційних технологій / Петренко О. Є., – Харків, 2014. – 78 с.

8. Комп'ютерні мережі: навчальний посібник /Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П., Вінниця: ВНТУ, 2013 р. – 374 с.

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

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

11. Pure hardware VPNs uale high-availability tests [Електронний ресурс] – Режим доступу до ресурсу:

https://web.archive.org/web/20070923013848/http://www.networkworld.com/reviews/2000/1211rev.html

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

13. Комп'ютерні мережі: навчальний посібник / Азаров О.Д., Захарченко С.М., Кадук О.В., Орлова М.М., Тарасенко В.П. – Вінниця: ВНТУ. – 2013. – 371 с.

14. Комп'ютерні мережі: підручник / Азаров О.Д., Захарченко С.М., Кадук О.В., Орлова М.М., Тарасенко В.П. – Вінниця: ВНТУ. – 2020. – 378 с.

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

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

17. Дудикевич В.Б. Квінтесенція безпеки кіберфізичних систем / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець // Інформаційні системи і мережі. – 2018. – № 887.

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

19. Городецька, О. С. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.

20. Что такое WireGuard? [Електронний ресурс] – Режим доступу до ресурсу: https://www.websiterating.com/ru/vpn/glossary/what-is-wireguard/

21. Шифр-VPN [Електронний ресурс] – Режим доступу до ресурсу: https://cipher.com.ua/uk/products/cipher-vpn

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

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

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

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