МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЖИЛИЧ Володимир Андрійович

АЛГОРИТМИ БЕЗПЕКИ ДЛЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ VPN / SECURITY ALGORITHMS FOR VIRTUAL PRIVATE NETWORKS VPN

спеціальність: 125 – Кібербезпека

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБзм - 21
В.А. Жилич

Науковий керівник
к.т.н., доцент Т.Г. Цаволик

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Жиличу Володимиру Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми безпеки для віртуальних приватних мереж VPN / Security algorithms for virtual private networks vpn
керівник роботи к.т.н., доцент Т.Г. Цаволик
затверджені наказом по університету від 1 грудня 2022 року № _____
2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- проаналізувати існуючі механізми роботи віртуальних приватних мереж;
- провести аналіз потенційних загроз;
- розгляд нових методів захисту віртуальних приватних мереж;
- провести аналіз існуючих алгоритмів та протоколів віртуальних приватних мереж;
- розробка рекомендацій та стратегій безпеки.

5. Перелік графічного матеріалу у роботі:
- VPN для користувачів.
- VPN для офісів.
- Принцип роботи симетричного та асиметричного шифрування.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз предметної області	12.2022 р. – 03.2023 р.	
2	Методи та алгоритми безпеки VPN	03.2023 р. – 05.2023 р.	
3	Реалізація та дослідження алгоритмів VPN	05.2023 р. – 11.2023 р.	

Студент _____ В.А. Жилич
(підпис)

Керівник роботи _____ к.т.н., доцент Т.Г. Цаволик

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Алгоритми безпеки для віртуальних приватних мереж VPN» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 90 сторінок і містить 3 ілюстрації, 3 таблиці, 1 додаток та 32 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є аналіз засобів безпеки та алгоритмів в середовищі віртуальних приватних мереж VPN.

Методи досліджень. Для виконання поставлених задач у магістерській роботі використано методи: аналізу, синтезу та опису, абстрагування, для моделювання та проектування віртуальних приватних мереж.

Результати дослідження: порівняльна характеристика відомих протоколів безпеки, аналіз алгоритмів безпеки, концепція роботи системи віртуальних приватних мереж.

Результати роботи можуть бути використані в навчальному процесі, при створення віртуальних приватних мереж та вибору оптимальних алгоритмів і протоколів для найбільш ефективного виконання поставленої на мережі завдання.

Орієнтовні напрямки розвитку досліджень: удосконалення відомих алгоритмів безпеки; розробка алгоритмів для покращення рівня безпеки; розширення інформаційно-аналітичних систем для аналізу проблематики віртуальних приватних мереж.

Ключові слова: ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, КОМП’ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ , ІНФОРМАЦІЙНІ СИСТЕМИ, КІБЕРБЕЗПЕКА, ШИФРУВАННЯ.

ABSTRACT

The final qualifying work on the topic "Security Algorithms for Virtual Private Networks VPN" for the degree of Master's Degree in specialty 125 "Cybersecurity" of the educational and professional program "Cybersecurity" is written in 90 pages and contains 3 illustrations, 3 tables, 1 appendix and 32 sources in the list of references.

The purpose of the final qualification work is to analyze security tools and algorithms in the environment of virtual private networks VPN.

Research methods. To accomplish the tasks set in the master's thesis, the following methods were used: analysis, synthesis and description, abstraction, for modeling and designing virtual private networks.

Research results: comparative characterization of known security protocols, analysis of security algorithms, concept of virtual private networks.

The results of the work can be used in the educational process, in the creation of virtual private networks and the selection of optimal algorithms and protocols for the most efficient implementation of the task set on the network.

Indicative directions of research development: improvement of known security algorithms; development of algorithms for improving the level of security; expansion of information and analytical systems for analyzing the problems of virtual private networks.

Keywords: VIRTUAL PRIVATE NETWORKS, COMPUTER SYSTEMS AND NETWORKS, INFORMATION TECHNOLOGY, INFORMATION SYSTEM, COMPUTER SECURITY, ENCRYPTION.

ЗМІСТ

ЗМІСТ 6
ВСТУП 7
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ 9
1.1 Загальна характеристика VPN 9
1.2 Протоколи VPN 10
1.3 Функції та компоненти VPN 12
1.4 Мережа VPN та проблематика її захисту 12
2 МЕТОДИ ТА АЛГОРИТМИ БЕЗПЕКИ VPN 18
2.1 Шифрування даних 18
2.2 Протоколи безпеки 20
2.3 Протоколи аутентифікації 37
2.4 Протоколи авторизації та обміну ключами 45
3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ АЛГОРИТМІВ VPN 53
3.1 Вимоги до систем VPN 53
3.2 Характерні особливості VPN 56
3.3 Рекомендації що до захисту VPN від несанкціонованого доступу 61
ВИСНОВКИ 69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 70
ДОДАТОК А КОПІЇ ПУБЛІКАЦІЙ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ 73

ВСТУП

Virtual Private Network (VPN) – віртуальна приватна мережа, котра формується поверх інших мереж із меншим рівнем довіри. VPN формується між двома вузлами та надає можливість клієнту, який приєднався бути учасником віддаленої мережі та користуватись її сервісами (внутрішніми сайтами, базами даних, принтерами, політиками виходу в Інтернет). Безпека передачі інформації через загальнодоступні мережі реалізуються завдяки шифруванню, у результаті формується закритий для сторонніх канал обміну інформацією. Технологія VPN пов’язує мережі в єдину мережу із застосування непідконтрольних каналів. Провайдери пропонують власні послуги для розгортання власної VPN-мережі. VPN вважається клієнт - серверною технологією.

Сучасні технології обробки, передачі та збору інформації зробили свій внесок у розвиток загроз, такі як можливість втрати, модифікації та розголошення даних які надсилаються кінцевим користувачам.Програмне забезпечення інформаційної безпеки комп’ютерних систем і мереж (ІС КСМ) є одним із перспективних напрямків для розвитку ІТ. Комп'ютерні інформаційні технології (ІТ) змінює наше життя. Інформація була і буде товаром, який можна купляти, продавати чи обмінювати. Цінність інформації завжди перевищує витрати на придбання та обслуговування КСМ.

Інформаційна безпека КСМ забезпечує конфіденційність, цілісність та доступність даних, котрі обробляються, компонентів та ресурсів такої системи. При розробці КСМ варто зауважити на можливі наслідки при поломках та їх ліквідації, тому комп’ютерна безпека є надважливою, тому дана тематика є актуальною.

Заходи, які спрямовані на забезпечення комп’ютерної безпеки, які включають у собі технічні, організаційні та правові. Захист інформаційної системи від втручання, котрі шкодять власникам чи користувачам інформації, у залежності від доступності, цілісності, конфіденційності.

Метою роботи є дослідження алгоритмів безпеки та їх застосування у віртуальних приватних мережах VPN.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі:**

– Дослідження алгоритмів, протоколів та проблем VPN;

– Аналіз способів покращення дії алгоритмів для захисту корпоративної мережі та концепці побудови захищеної віртуальної мережі VPN;

– Дослідження та аналіз сучасних віртуальних мереж VPN

Об’єкт дослідження. Маршрутизація та шифрування в компютерних мережах.

Предмет дослідження. Алгоритми безпеки VPN.

Новизна роботи. Рекомендації щодо безпека та побудови віртуальних приватних мереж VPN.

Практична цінність. Аналіз, який проведено у роботі дозволить підібрати VPN з найкраще підібраними алгоритмами конкретно під ваші цілі.

Публікації та апробація результатів досліджень приведена в:

1. Жилич В.А., Цаволик Т.Г. Механізми контролю доступу та авторизації у вітруальних приватних мережах (VPN). Збірник матеріалів проблемно-наукової міжгалузевої конференції "Автоматизація та комп'ютерно-інтегровані технології" (АКІТ-2023), Тернопіль, 2023. С. 115 - 118.

2. Жилич В.А., Цаволик Т.Г. Конфігурації VPN для безпечної передачі даних. Збірник матеріалів науково-практичного симпозіуму "Захист інформації", Тернопіль, 2023. С. 72 - 75.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальна характеристика VPN

У залежності від різновидів, VPN надає можливість з’єднати три види вузлів:вузол-вузол, вузол-мережа та мережа-мережа.

Технології, що використовують Інтернет як передавач IP-трафіку.VPN повинен вирішити проблему сторони підключення кінцевого користувача до віддалених і кількох локальних мереж. До складу технології входять захищені канали глобальної мережі, спеціальні протоколи та маршрутизатори.

Приватна мережа VPN знаходиться між внутрішньою мережею та Інтернетом, на кожному кінці з’єднання є Інтернет. Під час передачі інформації через VPN інформація попадає на вхід VPN і з’являєтесь в місці призначення після проходу через мережу VPN. Цей процес вважається "тунелюванням" - формування логічного тунель, що з'єднує 2 точки в Інтернеті. Завдяки використанню «тунелювання» особиста інформація непомітна є для інших осіб, які користуються Інтернетом. Перш ніж інформація буде передана через Інтернет, вона спочатку шифрується. Це підвищує захист інформації.

Протоколи шифрування використовуються залежно від протоколу тунелювання, який підтримується рішенням VPN. Однією з унікальних властивостей рішення VPN є різноманітність протоколів, які можна підтримувати. Найпоширенішими загальними специфікаціями є сімейство стандартів X.509. Тобто, розширивши VPN за допомогою протоколу для автентифікації, ви можете посилити її захист і запобігти несанкціонованому вторгненню. Популярність технології VPN призвела до її обов'язкового включення в кожну систему захисту інформації, побудовану для роботи як в державних, так і в приватних організаціях.

Організації або структури є не тільки внутрішніми для організації, але й зовнішніми за своєю природою. Багато організацій вирішили перейти на дистанційну роботу у зв’язку зі стратегією карантину.Тому важливо захистити дані, які передаються через Інтернет чи інше використання різноманітних послуг.

VPN мають певні відмінності порівняно з іншими мережами, найважливішою з яких є доступ до мережі організації без створення виділеної лінії.

Особа, яка має доступ до Інтернету, може використовувати приватну мережу. Важливо, а також те, що вони недоступні для широкого загалу.

Захист VPN – це захист корпоративної таємниці.

Оскільки інформація передається в криптографічному форматі, доступ до неї дозволений тільки відправнику та адресату. Поширений алгоритм для шифрування це Triple DES - використання трьох ключів.

Легітимність даних підтверджується перевіркою цілісності даних,виявлення тих, хто задіяний у VPN. Це полегшує передачу інформація, яка була доставлена призначена одержувачу без пошкоджень або змін.

Алгоритми, які зазвичай використовуються для оцінки достовірності даних – MD5 і SHA1. На наступному кроці система оцінить зміни даних, коли вони переміщуються мережею, і визначає, чи це було навмисно чи випадково. Тобто створення VPN має на меті захистити вас від несанкціонованого доступу до тунелів, які з’єднують декілька локальних або віддалених мереж чи користувачів.

Для створення VPN необхідним компонентом є програма, яка кодуватиме вхідний і вихідний трафік, при цьому їх проведення може бути як систематичним, так і випадковим, обладнання та програмне забезпечення з будь-якими пов’язаними операційними системами, і це не має значення.

Це комп’ютер або портативний пристрій. У підсумку важливо зробити такий висновок - Автентифікація та шифрування даних є ключовими компонентами надійного з'єднання.

1.2 Протоколи VPN

Протокол VPN визначає, як саме система VPN взаємодіє зі всіма системами в мережі Інтернет та рівень захищеності трафіку. Тобто, протокол VPN впливає на рівень безпеки в цілому системи. Причиною є застосування шифрування між

двома кінцевими вузлами. За умови незахищеності інформації, зловмисник може перехопити ключі та розшифрувати трафік.

Щоб сформувати VPN з використанням апаратного та програмного забезпечення важливо дотримуватися стандартного механізму на базі протоколу Internet Protocol Security - IPSec. Саме він деталізує методи ідентифікації для ініціалізації тунелю, методів шифрування. Недоліками є орієнтація на використання IP-адреси.

Для створення VPN була використана наступна процедура.

Point-to-Point Tunneling Protocol - PPTP, Layer-2 Forwarding і Layer-2 Tunneling Protoco L2TP, який поєднує два згадані вище протоколи. Але їм не вистачає всебічності та не є повністю функціональними.

Інший протокол, Internet Key Exchange - IKE, відповідає за передачу ключів інформації через тунель, уникаючи зовнішнього втручання. Завдання, які поставлені на нього реагувати на проблеми та вирішувати їх стабільно та спільно із ключами безпеки, які запобігають зламу віддалених пристроїв. IKE автоматизована процедура передачі ключів методом шифрування по відкритому каналу. IKE змінює пароль, пов’язаний із підключенням, це дозволить вам збільшити конфіденційність інформації, що передається. Крім того, інкапсуляція має поєднання кількох транспортних протоколів на одному каналі.

Протокол Link Control Protocol (LCP) – Point-to-Point Protocol (PPP) описує універсальний LCP, який використовується для створення, налаштування та перевірки каналу зв’язку.

Підключення LCP залежить від протоколу інкапсуляції, розміру пакетів і залучених параметрів,параметри встановлення, відключення та автентифікації.

Протоколи керування мережею визначають конкретні параметри конфігурації, які є специфічними для певних транспортних протоколів.

PPTP, L2TP, IPsec і OpenVPN використовуються для створення VPN-тунелів.

1.3 Функції та компоненти VPN

Надійна віртуальна приватна мережа VPN — це одночасне використання локальних ресурсів із доступом до Інтернету комп’ютерів завдяки відкритому зовнішньому доступу, де гарантована передача даних в єдиній віртуальній мережі із відповідним захистом даних, які поширюються всередині організації.

Під час підключення корпоративної локальної мережі до відкритої мережі можуть виникнути такі недоліки:

– несанкціонований доступ до даних, які проходять через відкриту мережу;

– несанкціонований доступ до внутрішніх сервісів, які можна отримати після доступу до мережі.

Є основні принципи, на яких базується захист інформації під час передачі даних по відкритих каналах:

– автентифікація сервісів, які взаємодіють;

– шифрування данних, які передаються;

– аудит цілісності та незмінності переданої інформаціїї;

Для захисту комп'ютерних мереж від несанкціонованого доступу із зовнішнього середовища використовують екрани для підтримки безпеки через фільтрацію повідомлень. Міжмережевий екран розміщується між локальною та відкритою мережами. Для захисту конкретного комп’ютера, який під’єднаний до відкритої мережі, то встановлюється відповідне ПЗ міжмережевого екрану.

1.4 Мережа VPN та проблематика її захисту

Для захисту комп'ютерних мереж від несанкціонованого доступу із зовнішнього середовища використовують екрани для підтримки безпеки через фільтрацію повідомлень. Міжмережевий екран розміщується між локальною та відкритою мережами. Для захисту конкретного комп’ютера, який під’єднаний до відкритої мережі, то встановлюється відповідне ПЗ міжмережевого екрану.

Сучасний системний адміністратор вважатиме це звичайною конфігурацією. Канали VPN для віддалених співробітників, які хочуть отримати

доступ до мережі організації, наприклад, можна розглянути схему на рисунку 1.1.

Рисунок 1.1 – VPN для користувачів

Двосторонній зв'язок на дві локації мереж, (рисунок 1.2), де системи чи мережі об'єднуються, що забезпечує достовірність і секретність інформації, що передається.

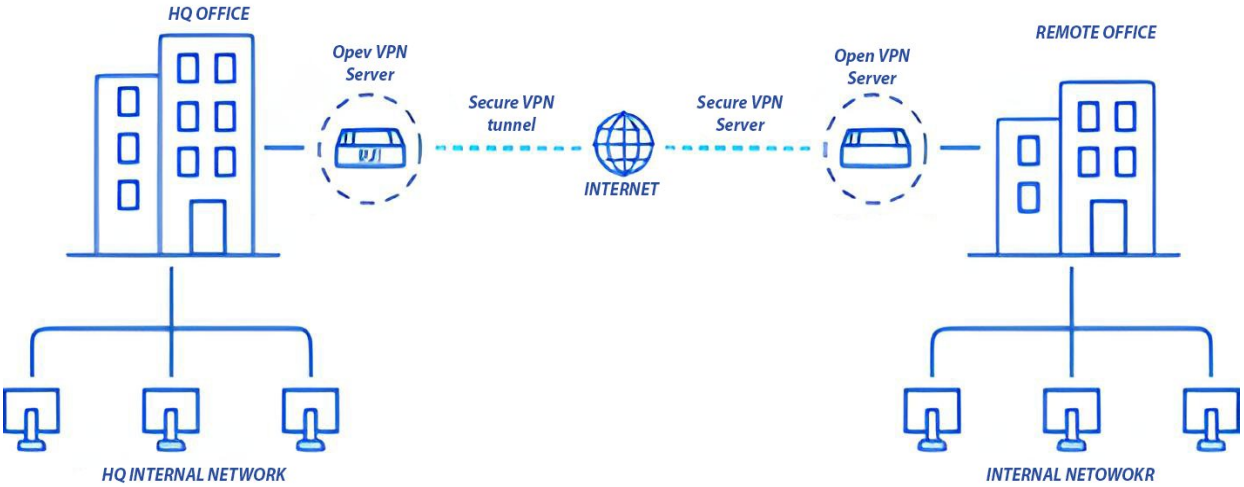

Рисунок 1.2 – VPN для офісів

Використання VPN саме по собі є вигідним порівняно з іншими методами віддаленого доступу. Тобто користувач, який має доступ до Інтернету, має можливість підключитися до мережі організації. Загальний доступ не завжди

робить інформацією незахищеною. Система безпеки для VPN надає можливість захистити корпоративну таємницю від несанкціонованого доступу.

Інформація передається тільки в зашифрованому вигляді. Ознайомившись з інформацією, власник даних підтверджує її легітимність і забезпечує достовірність інформації та ідентифікацію учасників VPN. Де перший гарантує, що дані були доставлені призначеному одержувачу в першому випадку. Популярними алгоритмами перевірки достовірності даних є MD5 і SHA1. Побудова VPN передбачає створення тунелів, захищених від санкціонованого доступу між різними локальними мережами або окремими особами.

Щоб створити VPN з обох ліній зв'язку, програма зашифрує вихідний трафік і розшифрує вхідний, які функціїонують на спеціалізованому обладнанні чи програмному забезпеченні та з будь-якими операційними системами.

VPN мають такі переваги: економія коштів, універсальність і простота використання. Завдяки VPN організації обмежені у збільшенні технічних ресурсів, включаючи модеми, сервери доступу, комутаційні плати та інші ресурси, мають можливість навадати безпечний віддалений доступ користувачам до їхніх мереж.

Ступінь безпеки та анонімності VPN залежить від реалізації та конфігурації. Високий ступінь конфіденційності досягається шляхом програмування та ефективного впровадження. Встановлення VPN дозволяє користувачам отримати анонімність у віртуальному просторі.

Структура VPN складається з двох компонентів:

– Перший рівень називають «внутрішньою мережею». Їх може бути декілька;

– Другий рівень — «Зовнішня мережа». Інтернет використовується для з'єднання між віддаленим користувачем і віртуальною мережею, це здійснюється через певний сервер. Щоб підключитися до VPN, комп'ютер пройде кілька етапів. Після того, як процес ідентифікації та автентифікації пройшов успішно, користувач отримує дозвіл на виконання певного процесу.

Авторизація дає вам повний доступ до всієї мережі. Фізичним втіленням технології VPN є здатність захищати інформаційні системи, відеоконференції, платформи електронної комерції.

Захист інформації в мережах VPN досягається кількома методами як застосовуються для втілення заходів безпеки в інформаційних мережах:

Тунелювання — це передача інформації між двома конкретними місцями. вся мережева інфраструктура між ними прихована для відправника та одержувача інформації. Транспортне середовище тунелю збирає пакети передбаченого мережевого протоколу поблизу тунелю та доставляє їх до виходу, не змінюючи їх. Створення тунелю може з’єднати дві точки Інтернету. Окрім вищезгаданих переваг є й недоліки: дані, що передаються можуть бути заздалегіть викрадені злочинцями. Оскільки вона засекречена, то виникає загроза її компрометації. Злочинці можуть змінити інформацію, щоб унеможливити перевірку її правдивості. Тоді можна зробити висновок, що тунель підходить для конкретних типів комп'ютерних мереж і не претендує на складність. Неприємності долаються сучасними методами КЗІ. Для запобігання несанкціонованим змінам пакета з даними, необхідними для проходження тунелю, використовується кваліфікований електронний підпис (КЕР), призначення методу документується додатковим блоком інформації, який створюється за допомогою асиметричного криптографічного алгоритму та унікальний склад пакету та секретний ключ відправника. Цей блок інформації є КЕР пакета, і він дає змогу одержувачу підтвердити автентичність даних, якому відомий відкритий ключ, пов’язаний із КЕР відправника. Дані, що передаються через тунель, захищені за допомогою надійних криптографічних алгоритмів.

Аутентифікація - перевірка безпеки VPN. Дані з клієнтських комп’ютерів передаються через Інтернет на сервер VPN. Сервер розташований далеко від комп'ютера клієнта, а інформація про мережу організації передається через обладнання кількох провайдерів. Щоб зберегти оригінальність даних і запобігти їх зміні або крадіжці, використовуються різні методи автентифікації та шифрування. Ефективними протоколами є MSCHAP версії 2 і EAP-TLS, оскільки вони мають спільний механізм автентифікації, який ідентифікує VPN-сервер і

клієнт. Інші протоколи, наприклад той, що використовується військовими, дозволяють серверу лише автентифікувати клієнтів.Для відкритої автентифікації: клієнт передає серверу пароль, який порівнюється зі стандартним, якщо пароль несправжній, доступ буде заборонено. Ця форма автентифікації є непопулярною.Протокол запит/відповідь більш поширений, клієнт запитує автентифікацію у сервера, сервер повертає випадкову відповідь як маркер. Клієнт забирає хеш зі свого пароля, який потім використовується для шифрування відгуку та надсилання його на сервер. Зрештою, сервер перевіряє отриманий результат на відповідь клієнта, якщо вони збігаються, процес автентифікації вважається успішним. Автентифікація VPN-клієнтів і серверів, L2TP через IPSec використовує локальні сертифіковані копії сертифіката, отримані від сертифікованої служби. Клієнт і сервер спільно використовують сертифікат і створюють надійну асоціацію безпеки ESP. Далі L2TP завершує процес перевірки легітимності комп’ютера та ідентифікує користувача, у цьому випадку використовується будь-який протокол. Це надійно і охоплює весь сеанс. Автентифікуйте користувача комп’ютера за допомогою MSCHAP, для цього буде використано інший ключ шифрування, ніж той, який використовує користувач для самоавтентифікації, що підвищить рівень безпеки.

Шифрування гарантує безпеку даних під час передачі через Інтернет. Старіші версії Windows підтримують лише шифрування з довжиною ключа 40 біт, тому в гібридному середовищі це мінімальна довжина ключа, яку слід вибрати.PPTP змінює значення ключа шифрування після того, як кожна особа отримує пакет. Протокол MMPE спочатку був призначений для зв'язку між точками, які безпосередньо підключені, однак втрати даних тепер мінімальні. У цьому випадку значення ключа для наступного пакету базується на результатах дешифрування попереднього. Під час побудови віртуальних мереж через загальнодоступні комунікаційні мережі важко дотримуватися цих умов, пакети можуть доставлятися у випадковому порядку і PPTP використовується для зміни ключа шифрування. Це дає змогу дешифрувати незалежно від попередніх пакетів інформації.

Саме тому комбінація “тунель + аутентифікація + шифрування” дає змогу передавати дані між точками через загальну мережу, імітуючи роботу приватної мережі.

Процедура впровадження VPN описується розміщенням VPN-сервера в локальній мережі комп’ютерів організації. Віддалений користувач, який використовує клієнтське програмне забезпечення VPN, ініціює процес зв’язку з сервером. Автентифікація користувача ініціюється як преамбула процесу - створення VPN-з'єднання. У разі підтвердження повноважень настає наступний етап - між клієнтом і сервером укладається домовленість про особливості підключення. Далі встановлюється VPN, це з'єднання гарантує передачу інформації між клієнтом і сервером. Далі інформація шифрується, а потім проходить аутентифікацію та перевірку даних.

Всесвітньою проблемою мереж VPN є відсутність встановлених протоколів для перевірки автентичності та обміну криптографічною інформацією. Проблема полягає в уповільненні поширення VPN, використання прогресу різних постачальників, і це складний процес об’єднання мереж асоційованих компаній.

За допомогою відповідної кількості програмного забезпечення мережа VPN може досягти високого ступеня захисту переданих даних. Завдяки правильній конфігурації та ефективній роботі всіх компонентів технологія VPN забезпечує анонімність у спілкуванні.

2.1 АЛГОРИТМИ БЕЗПЕКИ VPN

2.1 Шифрування даних

Шифрування — це процедура, яка перетворює інформацію у форму, зрозумілу лише авторизованим особам. Під час процесу шифрування звичайний текст перероблюється на зашифрований за використанням секретного ключа. Криптографічний ключ — це спільний набір числових значень, узгоджених між відправником і одержувачем.

Дешифрування або перетворення зашифрованої інформації здійснюється будь-якою особою, яка володіє відповідним ключем. Ось чому фахівці з криптографії постійно зацікавлені в створенні більш складних та інтригуючих ключів. Більш складне шифрування використовує ключі, які важко зламати, тому хакерам неможливо повністю розшифрувати текст .

Сьогодні розрізняють два типи шифрів: симетричні та асиметричні.

Алгоритми симетричного шифрування включають методи шифрування, які є ключ шифрування та ключ дешифрування ідентичні, або один із них простий походить від двох інших, і навпаки.

Алгоритми симетричного криптоаналізу розбиті на потоки та блоки.

Шифрування потоків передбачає послідовну обробку тексту повідомлення. Блоки Алгоритми використовують блоки постійного розміру. Як правило, довжина ділянки це те саме, що 64 біти, але в протоколі AES використовуються блоки довжиною 128 бітів.

Найбільш визнані блокові шифри DES, AES, Camellia, Twofish, Blowfish, IDEA, RC4 тощо.

Існують шифри для стандарту шифрування даних (DES) і розширеного стандарту шифрування (AES).

Незважаючи на те, що протокол DES було знято з експлуатації, його все ще функціональна версія з потрійним DES залишається популярною та використовується в багатьох ситуаціях,а саме: шифрування в банкоматах для збереження конфіденційності електронних комунікацій та легкий доступ до віддалених комп'ютерів.

Симетричний криптоаналіз не завжди використовується ізольовано.У сучасних криптосистемах використовуються комбінації як симетричних, так і асиметричних методів. Алгоритми в поєднанні з двома іншими схемами дозволять об’єднати переваги кожної схеми. Ці системи включають розширення безпеки, такі як SSL.

По суті, симетричні криптосистеми мають меншу обчислювальну складність ніж асиметричний. Теоретично це означає, що існують сотні чи навіть тисячі кращих асиметричних методів.У тисячі разів повільніше, ніж симетричні методи вищої якості. Недоліком є симетрична структура. Алгоритми, особистий ключ повинен мати обидві сторони передачі інформації. Отже оскільки ключі чутливі до викрадення, їх потрібно часто змінювати. Поширюйте інформацію через канали, які є безпечними та популярними під час розповсюдження.

Проблема із симетричним шифруванням полягає у необхідності транспортування ключа дешифрування даних, тому ключ може бути підроблений кимось іншим. Кожен, хто розуміє секретний пароль, може розшифрувати інформацію. В той час як асиметричне шифрування має два пов’язані ключі: пару ключів. Відкритий ключ загальнодоступний, кожен, хто хоче шифрувати, повинен мати до нього доступ.

Приватний ключ закритий, але його необхідно зберігати в секреті, доступний лише тим, хто має здатність зрозуміти інформацію.

Доступна будь-яка інформація, зашифрована відкритим ключем можна лише розшифрувати через той самий процес, але з відповідним закритим ключем. Крім того, інформацію, зашифровану за використанням закритого ключа, вийде розшифрувати використовуючи відповідний відкритий ключ.

Це означає, що немає потреби турбуватися про передачу відкритого ключа.Ключ має бути відкритим. Однак асиметричне шифрування приблизно в два рази повільніше, ніж схоже на нього симетричне. Крім того, необхідно мати метод шифрування, а також пристрій для дешифрування.

Цей підхід включає такі алгоритми, як DES і Elgamal.

Через низьку швидкість асиметричного підходу цей підхід рекомендується у поєднувати з симетричними. Щоб вирішити проблему необхідності ділитися

секретним ключем з відправником та зашифрувати інформацію, інформація спочатку є загальнодоступною. Захищена випадковим кодом, цей код потім використовується для захисту самого ключа. Асиметричний ключ одержувача, після чого відправляються повідомлення та зашифрований ключ у мережу (рисунок 2.1).

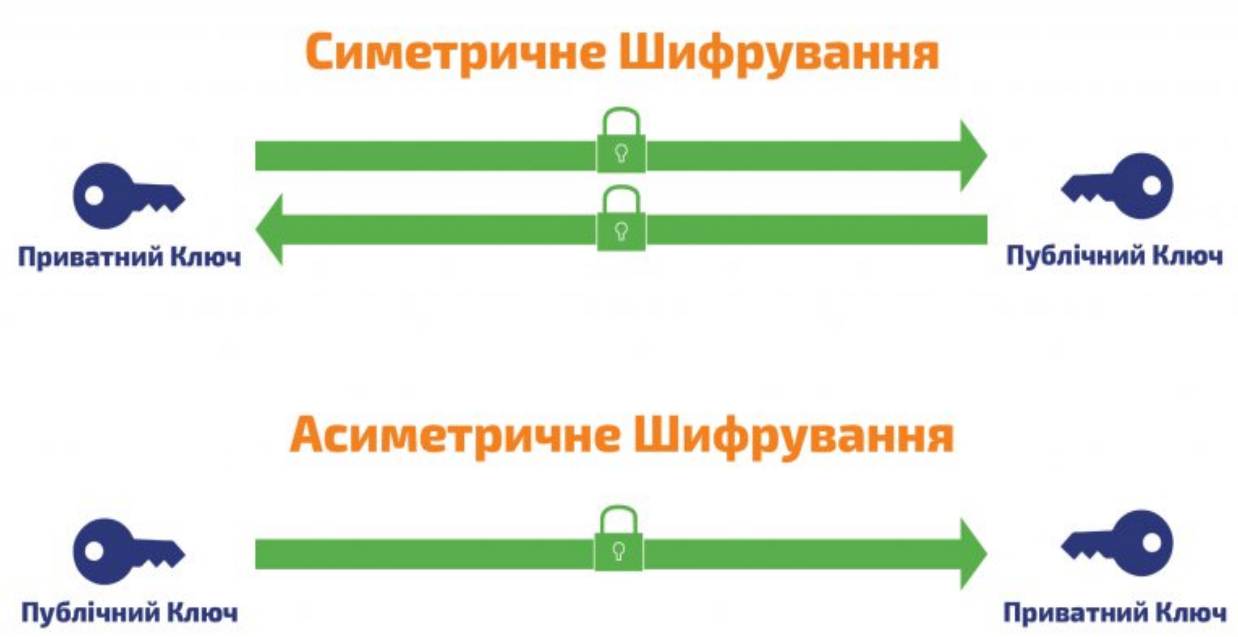

Рисунок 2.1 – Принцип роботи симетричного та асиметричного шифрування

2.2 Протоколи безпеки

На даний момент існує кілька підходів до створення VPN на основі різних протоколів, включаючи PPP, PPTP, IPSec, OpenVPN, SSTP, IKEv2, L2TP та інші. Мережі можна будувати за допомогою одного протоколу або комбінації протоколів. У цій роботі порівнюються такі варіанти, які є найпопулярнішими:

- VPN на основі протоколу IPSec;
- VPN на основі протоколу OpenVPN.
- VPN на основі протоколу PPTP;
- VPN на основі протоколу L2TP;

IPSecurity (IPSec) пропонує послідовну, довготривалу платформу для безпеки на основі мережі.

IPSec підтримує всі криптографічні алгоритми, які зараз використовуються, і навіть може підтримувати більш потужні нові алгоритми, коли вони стануть доступними.

Протоколи IPSec вирішують наступні основні проблеми безпеки:

- Автентичність даних - підтверджує, що кожне повідомлення даних було надіслано заявленим відправником.

- Цілісність даних - гарантує, що вміст дейтаграми не було змінено помилково чи навмисно.

- Конфіденційність даних – це процес приховування вмісту повідомлення, зазвичай за допомогою шифрування.

- Захист від повторного відтворення - запобігає повторному відтворенню дейтаграми зловмисником.

- Автоматизоване керування криптографічними ключами та асоціаціями

Безпека. Переконайтеся, що вашу стратегію VPN можна використовувати в розширеній мережі з мінімальною додатковою конфігурацією або без неї.

Сервіси безпеки IPsec реалізуються за допомогою двох виділених додаткових заголовків, заголовка автентифікації (AH) і інкапсуляційного корисного навантаження безпеки (ESP), а також протоколів і методів керування криптографічними ключами. Заголовок AH призначений для забезпечення легітимності та можливості перевірки IP-адреси. Він додатково пропонує додаткову послугу захисту для відтворення. Його наявність забезпечує захист від незаконних змін фіксованих IP-адрес, викрадення пакетів і потенційних дублікатів пакетів. Навпаки, ESPheader сприяє інкапсуляції даних за допомогою шифрування, яке гарантує, що лише призначений пункт може читати корисне навантаження, пов’язане з IP-адресою. Крім того, ESP може забезпечити перевірку автентичності та цілісності пакетів, а також послугу для запобігання відповіді.

AH, і ESP використовують концепцію «асоціації безпеки» (SA) під час погодження алгоритмів безпеки та параметрів, які спільно використовуються відправником і одержувачем безпечного потоку трафіку. Кожна IP-адреса пов’язана з набором асоціацій безпеки, принаймні одна асоціація для кожного

виділеного посилання. Тепер активні SA зберігаються в базі даних під назвою Security Association Database (SAD). Запис SAD відрізняється триплетом, який включає індекс параметрів безпеки (SPI), IP-адресу призначення та ідентифікатор протоколу безпеки (AH або ESP). Індекс параметрів безпеки (SPI) включено в заголовки AH і ESP, оскільки він використовується для визначення відповідного заходу безпеки.

Розшифровка та/або автентифікація пакетів. В одноадресному зв'язку SPI зазвичай вибирається об'єктом призначення та повторно отримується відправником, щойно зв'язок встановлено. У багатоадресному зв'язку SPI має бути доступним для всіх членів групи багатоадресної адреси. Кожен вузол повинен мати можливість розрізняти правильний SA шляхом поєднання SPI з адресою групової передачі. Процес узгодження є важливим компонентом протоколу безпеки для обміну ключами. Конкретні вимоги безпеки перераховані на кожному вузлі; ці вимоги зазвичай реалізуються за допомогою впорядкованого списку правил або політик, які складають базу даних політики безпеки (SPD) вузла. Захист кожного транспортного потоку, який входить або виходить із об'єкта, вирішується спільно з SPD.

Як правило, пакети вибираються для одного з трьох режимів обробки на основі IP-адреси та інформації транспортного рівня, пов'язаної із записами SPD. Вміст кожного пакета вмикав або вимикав безпеку IPsec, залежно від інформації про політику, наявної в базі даних.

IPsec використовується для захисту таких важливих даних, як банківські транзакції, медична інформація та корпоративна "таємниця", які передаються через мережу. Він також використовується для зв'язування віртуальних приватних мереж, у яких безпека на основі IPsec гарантує передачу всіх даних між двома точками. IPsec здатний шифрувати інформацію прикладного рівня і захищати безпеку маршрутизаторів, які поширюють інформацію про маршрутизацію в Інтернеті через загальнодоступний Інтернет. Крім того, його можна використовувати для автентифікації даних, отриманих від розпізнаного відправника.

Шифрування на рівнях моделі взаємозв'язку відкритих систем (OSI), які знаходяться на прикладній або транспортному рівні, може передавати дані без необхідності використання протоколу IPsec. На рівні протоколу шифрування здійснюється за допомогою протоколу передачі гіпертексту (HTTPS). На транспортному рівні протокол TLS із протоколу безпеки транспортного рівня (TLS) забезпечує безпеку. Однак процес шифрування та автентифікації на цих вищих рівнях підвищує ймовірність викриття даних і викрадення інформації протоколу злочинцями.

IPsec гарантує автентичність пакетів даних, які надсилаються через мережі IPv4 або IPv6. Заголовки IPsec розташовані в IP-заголовку пакета, ця інформація визначає, як опрацьовуються дані в пакеті, включаючи їх маршрутизацію та адресата в мережі. IPsec включає кілька компонентів в IP-адресу, ці компоненти включають інформацію про безпеку та один або кілька криптографічних методів.

Протоколи для IPsec використовують формат під назвою Request for Comments (RFC), який полегшує розробку стандартів безпеки мережі. Стандарти RFC використовуються в Інтернеті для поширення важливої інформації, яка полегшує користувачам, розробникам і менеджерам мереж створювати, керувати та підтримувати мережі.

Функціонування IPsec включає п'ять важливих кроків. А саме:

– Опізнавання хоста. Процес IPsec починається, коли хост-система розпізнає, що пакет має бути закритий і переданий за правилами IPsec. Ці пакети вважаються «цікавими» для цілей IPsec, і вони викликають активацію політик безпеки. Для пакетів, які є вихідними, це означає, що використовується відповідне шифрування та автентифікація. Коли новий пакет розпізнається як важливий, хост-система підтверджує, що він був належним чином зашифрований і перевірений.

– Узгодження, або перша фаза IKE. На другому кроці хости використовують IPsec для узгодження набору правил, які будуть застосовуватися для забезпечення безпеки каналу. Вони також автентифікують один одного та створюють спеціальний канал, який використовується для обговорення того, як протокол IPsec захистить або автентифікує інформацію, що передається через

нього. Цей процес переговорів відбувається принципово або агресивно. У базовому режимі хост, який ініціював сеанс, пропонує набір пропозицій, які визначають бажані методи шифрування та автентифікації. Процес узгодження триває, доки обидва хости не погодяться щодо протоколу IPsec, який вони використовуватимуть, і створять IKE SA, який описує особливості схеми. Цей підхід більш надійний, ніж агресивний, оскільки створює виділений канал для передачі даних. В агресивному режимі ініціатор хоста відмовляється від переговорів і вибирає систему IKE за замовчуванням. Підтвердження хоста, що відповідає, підтверджує сеанс.

– Протокол IPsec або IKE Phase 2 використовується для автентифікації та захисту зв’язку між комп’ютерами та пристроями. На третьому етапі створюється захищений канал із накладеним на нього протоколом IPsec. Хости IPsec обговорюють, як реалізувати алгоритми під час розповсюдження даних. Крім того, хости зобов’язуються та обмінюються ключами шифрування та дешифрування, які вони мають намір використовувати для зв’язку з безпечною мережею та з неї. Крім того, хости обмінюються випадковими числами, які використовуються для автентифікації сеансів.

– Протокол IPsec або IKE Phase 2 використовується для автентифікації та захисту зв’язку між комп’ютерами та пристроями. На третьому етапі створюється захищений канал із накладеним на нього протоколом IPsec. Хости IPsec обговорюють, як реалізувати алгоритми під час розповсюдження даних. Крім того, хости зобов’язуються та обмінюються ключами шифрування та дешифрування, які вони мають намір використовувати для зв’язку з безпечною мережею та з неї. Крім того, хости обмінюються випадковими числами, які використовуються для автентифікації сеансів.

– Зв'язок IPsec. На четвертому кроці хости передають фактичні дані через створений ними захищений тунель. Раніше створені AS IPsec використовуються для перетворення та декодування пакетів.

– Завершення циклу IPsec. Зрештою, тунель IPsec завершено. Зазвичай після цього йде заздалегідь визначена кількість байтів, що проходять через канал IPsec, або сеанс завершився. Коли відбувається одна з цих подій, хости

спілкуються один з одним і досягається вирішення. Після завершення завдання хости позбавляються закритих ключів,залучених до операції.

IPsec зазвичай використовується для забезпечення безпеки VPN. У той час як VPN створює персональну мережу між комп'ютером користувача та сервером VPN, протоколи IPsec реалізують безпечну мережу, яка захищає дані VPN від зовнішнього вторгнення.

По суті, режим транспортування відповідає за захист даних під час їх передачі з одного пристрою на інший, як правило, це робиться протягом одного сеансу. Крім того, тунельний режим гарантує захист усіх шляхів передачі даних від точки А до точки Б, незалежно від пристроїв між ними.

Тунельний режим. Режим роботи під назвою IPsec є загальним для безпечних мережевих шлюзів, це дозволяє хостам безпечно спілкуватися з іншими хостами. Наприклад, будь-які співробітники корпоративної системи можуть легально використовувати системи зв'язку із будь-якою системою головного офісу за умови, що філія та головний офіс мають надійні проксі-сервери, які функціонують як хост IPsec у власному офісі. Канал IPsec формується між двома учасниками, але сам канал приймає трафік від усіх інших хостів у захищених мережах. Режим тунелювання корисний для створення механізму, який захищає весь трафік між двома мережами з різних хостів на обох кінцях.

Режим транспортування. Режим транспортування, який використовує IPsec, називається режимом транспортування IPsec. Цей режим використовується двома хостами для прямого підключення через IPsec. Наприклад, цей тип схеми може бути розроблений для того, щоб дозволити спеціалісту служби підтримки інформаційних технологій входити на віддалений сервер і виконувати технічне обслуговування.

Протокол IPsec використовується, коли два різні хости повинні спілкуватися один з одним. Хости безпосередньо спілкуються один з одним через канал IPsec, який зазвичай припиняється після завершення сеансу.

Безпека є однією з найбільш швидкозростаючих областей комп'ютерних мереж, тому що важливо зберегти дані та забезпечити економічну життєздатність за допомогою електронної комерції. IP-безпека не є винятком із загального

правила: було запропоновано нові розширення для режимів автентифікації IKE та ISAKMP, які вирішують проблему безпечного віддаленого доступу та намагаються запровадити кілька методів автентифікації на основі користувача в IPsec. Концептуальна модель мережевого середовища на основі політики безпеки описана для IPsec разом із протоколом, який призначений для виявлення та вирішення політик щодо протоколу Ipsec. Досі IPsec був ефективним у статичних конфігураціях мереж і, загалом, у мережах, які є частиною спільного адміністрування. Нові методи керування політикою, засновані на IPsec, дозволяють застосовувати цю технологію для різноманітних загальних цілей і можуть сприяти її широкому поширенню в Інтернеті. Загальна перевага полягає в тому, що на мережевому рівні вже буде присутній більший рівень безпеки, в результаті програми можуть зосередитися на різних аспектах безпеки, включаючи авторизацію та відмовостійкість.

OpenVPN — це протокол для створення безпечного каналу між двома мережами. Повсякденною мовою цей термін означає, що це надійна технологія, яка використовується багатьма віртуальними приватними мережами, щоб гарантувати, що будь-яка інформація, що передається через Інтернет, є зашифрованою та конфіденційною. Коротше кажучи, це, мабуть, найнадійніший протокол VPN з моменту його створення.

Коли ви отримуєте доступ до Інтернету, особливо в загальнодоступній мережі, є шанс, що ваші дані будуть передані через Інтернет. Ось чому не рекомендується входити у свій банк через загальнодоступну Wi-Fi. І навпаки, коли ви об’єднуєтеся з віртуальною спільнотою.

У вашій персональній мережі або VPN, яка використовує протокол OpenVPN, ваша інформація захищена за допомогою високоякісного шифрування. Якщо кіберзлочинець контролює вашу мережу, у нього не буде засобів для обходу протоколу безпеки.

Жоден інструмент або віртуальна приватна мережа не може забезпечити вашу безпеку та конфіденційність, а OpenVPN також не має спеціальних атрибутів. Однак є законні підстави вважати його одним з найнадійніших з'єднань, про які мова піде нижче.

OpenVPN спочатку був створений у 2001 році як безкоштовний “opensource” проект, це означає, що кожен вправі використовувати та аналізувати його код. Це призвело до спільноти розробників, які часто оцінюють, змінюють і оновлюють протокол.

Це головна перевага будь-якого вільного програмного забезпечення. Оскільки це загальнодоступний код, міжнародні експерти з безпеки мають доступ до нього без обмежень. Подібно до Вікіпедії, успіх OpenVPN пояснюється здатністю спільноти шукати та виправляти помилки.

Ви можете використовувати функції OpenVPN, якщо дотримуєтеся умов ліцензійної угоди на програмне забезпечення, яке є відкритим кодом. Незважаючи на те, що код доступний безкоштовно, важливо зазначити, що він потребує значного ручного втручання. Жодна офіційна програма не доступна для завантаження або сервери з усього світу доступні для вас.

Незважаючи на ці характеристики, типовий користувач зазвичай використовує протокол через окремого постачальника VPN, який ліцензує програмне забезпечення та оплачує його самостійно через щомісячну плату.

VPN сприймає це як два протоколи: OpenVPN UDP і OpenVPN TCP.

- OpenVPN UDP присвячений протоколу дейтаграм користувача та містить правила, які дозволять вам підключатися швидше. Часто це буде підключення за замовчуванням, оскільки воно забезпечуватиме вищу швидкість Інтернету.

- OpenVPN TCP призначений для протоколу керування передачею, цей протокол призначений для більшого контролю над даними, що передаються. Це призводить до нижчих швидкостей, але, як правило, є більш надійним.

OpenVPN використовує секретні ключі, яким можна довіряти, тому цей протокол вважається надійним. Крім того, його можна регулювати, що дозволяє змінювати параметри відповідно до ваших уподобань. Цим займаються багато служб у сфері VPN. Багато експертів з безпеки вважають, що OpenVPN достатньо для захисту від державного моніторингу.

Є сенс згадати атрибути, які забезпечують безпеку:

а) OpenVPN універсальний: одна версія в основному відрізняється від іншої. Як результат, він підходить для багатьох цілей. Ваш постачальник VPN може використовувати інший протокол, ніж інший постачальник.

б) OpenVPN випущено за ліцензією Creative Commons: якщо програмне забезпечення не є власністю, у його розробці зазвичай бере участь велика спільнота. Коли вони знаходять проблему, вони виправляють її, а також намагаються доповнити новими функціями. Це головна причина універсальності OpenVPN.

в) OpenVPN здатен взаємодіяти із різними стандартами шифрування: Однак OpenVPN зазвичай використовує 256-бітне шифрування, яке не є обов’язковим.

г) OpenVPN є гнучким: він може працювати в різних конфігураціях мережі. Таким чином, незалежно від того, як ваш провайдер VPN налаштовує свої сервери та з’єднання, OpenVPN буде відповідним для них.

ґ) OpenVPN не має прив'язки до конкретної платформи: існують протоколи, які не залежать від пристроїв. PPTP не може працювати на Mac. І навпаки, OpenVPN можна використовувати на комп’ютерах, планшетах, телефонах та інших пристроях.

OpenVPN має численні сторонні доповнення та сценарії, які розширюють його можливості. OpenVPN залишається найпопулярнішим безпечним протоколом VPN.

Протокол тунелювання «точка-точка» (PPTP) — це протокол, який забезпечує передачу безпечних даних від віддаленого клієнта до серверу приватного підприємства шляхом створення віртуальної приватної мережі через мережі передачі даних, які базуються на TCP/IP. PPTP полегшує багатопротокольну віртуальну приватну мережу на вимогу через звичайні віртуальні мережі, такі як Інтернет. PPTP — це протокол, який розширює віддалений доступ «точка-точка». Крім того, PPTP можна використовувати в окремих мережах LAN-to-LAN.

Одним із унікальних аспектів протоколу PPTP є його підтримка віртуальних приватних мереж, які використовують телефонні мережі загального користування (PSTN). PPTP зменшує витрати та ускладнює розгортання рішення віддаленого

доступу для мобільних або віддалених користувачів, забезпечуючи безпечний і зашифрований зв’язок через загальнодоступні телефонні лінії та Інтернет. PPTP усуває необхідність виділених, дорогих або приватних серверів для зв’язку із зовнішнім світом, оскільки ви можете використовувати PPTP через стандартні телефонні лінії.

Як правило, кожен екземпляр PPTP включає три комп’ютери:

- клієнт PPTP;

- сервер доступу;

- сервер PPTP.

Типове налаштування PPTP починається з віддаленого або мобільного клієнта PPTP, якому потрібен доступ до локальної мережі приватної компанії через постачальника послуг Інтернету в місцевому регіоні. Клієнти, користуючись ПК під системами рівнем не нижче Windows NT використовують віддалену мережу та PPP для з’єднання з провайдерами Інтернету.

Клієнт підключається до сервера доступу до мережі Інтернет провайдера на місці. Після з'єднання клієнт може як надсилати, так і отримувати пакети через Інтернет. Сервер, який отримує доступ до мережі, використовує протокол TCP/IP для всього онлайн-трафіку в Інтернеті. Після того, як клієнт підключився до провайдера через початковий протокол PPP, другий виклик до мережі здійснюється через існуючий протокол. Інформація, що передається по цьому другому каналу, має форму IP-пакетів, які містять кадри PPP, які називаються інкапсульованими кадрами PPP. Наступний виклик ініціалізує підключення віртуальної приватної мережі до сервера PPTP у приватній корпоративній мережі, це називається тунелем.

Тунелювання — це надсилання пакетів до комп’ютера в персональній мережі через іншу мережу, наприклад Інтернет. Інші мережеві маршрутизатори не мають доступу до комп’ютера в персональній мережі. Однак тунелювання дозволяє мережі направляти пакет на вторинний комп’ютер, наприклад сервер.

PPTP, який пов’язаний як з мережею для маршрутизації, так і з особистою мережею. І клієнт, і сервер використовують тунелювання, щоб забезпечити

передачу пакетів на комп’ютер у приватній мережі без знання адреси приватної мережі.

Коли сервер PPTP отримує повідомлення від мережі, призначеної для роумінгу, він передає його на комп’ютер призначення через приватну мережу. Сервер PPTP використовує цей метод для обробки пакета PPTP, який містить особисту інформацію про мережевий комп’ютер або адресу, яка міститься в інкапсульованому протоколі PPP. Пакет PPP, інкапсульований, може містити багатопротокольні дані, наприклад TCP/IP, IPX або NetBEUI. Оскільки сервер PPTP призначений для зв’язку через приватну мережу за допомогою приватних протоколів, він може отримувати кілька протоколів.

Повідомлення від клієнта PPTP до сервера PPTP проходить тунель PPTP до кінцевого комп’ютера в персональній мережі. Пакети PPTP інкапсулюються та передаються через Інтернет так, ніби це звичайні пакети. Ці IP-пакети передаються через Інтернет на сервер PPTP, який підключено до Інтернету та приватної мережі. Сервер PPTP інтерпретує IP-адресу в протокол PPP, який потім розшифровується за допомогою протоколу приватної мережі.

Комп’ютер, який використовує PPTP, спроможний встановлювати з'єднання із сервером PPTP такими способами:

- використовуючи сервера доступу до мережі Інтернет-провайдера, який полегшує вхідні PPP-з’єднання;

- використання фізичного мережевого підключення за допомогою TCP/IP для з'єднання із PPTP-сервером.

Абоненти PPTP, які використовують провайдера ISP, повинні мати окреме з’єднання з провайдером і сервером PPTP через модем. Перше з’єднання — це комутоване PPP-з’єднання, яке використовує модем для з’єднання з Інтернетом. Друге з’єднання – це з’єднання VPN, яке використовує PPTP через модем і постачальника послуг Інтернету, щоб обійти Інтернет і отримати доступ до пристрою VPN через PPTP на сервері. Друге з’єднання потребує першого з’єднання, оскільки тунель між пристроями VPN будується за допомогою модему та PPP-з’єднання з Інтернетом.

Одним винятком із вимог для двох з’єднань є наявність протоколу PPTP для ініціалізації віртуальної приватної мережі між комп’ютерами, які фізично підключені до локальної мережі приватної мережі. У цьому контексті PPTP-клієнт уже підключений до мережі, але використовує лише віддалену мережу з пристроєм VPN для підключення до PPTP-сервера в локальній мережі.

Пакети PPTP, отримані від віддаленого клієнта PPTP і локального клієнта PPTP, обробляються по-різному. Повідомлення від клієнта віддаленого доступу надсилається через фізичний мережевий шлях телекомунікаційного пристрою, тоді як повідомлення від клієнта локальної мережі надсилається через фізичний мережевий шлях мережевого адаптера.

Інтернет-провайдери використовують сервери доступу, які реалізують такі протоколи, як SLIP або PPP, для доступу до Інтернету. Однак сервер доступу до мережі повинен сприяти наданню послуг PPP клієнтам з підтримкою PPTP. Сервери, які мають доступ до Інтернету через мережу провайдера, призначені та створені для розміщення великої кількості клієнтів, підключених до Інтернету.

Надійне з’єднання, яке створюється за допомогою протоколу PPTP, зазвичай складається з трьох кроків, кожен з яких вимагає виконання попереднього кроку:

- Взаємодія та комунікація між PPP. Клієнт PPTP використовує PPP для підключення до постачальника послуг Інтернету через стандартну телефонну лінію або лінію ISDN. Ця асоціація використовує протокол PPP для зв’язування та захисту пакетів даних.

- Регулювання зв'язку між Control і PPTP. Через доступ до Інтернету, встановлений PPP, PPTP створює зв’язок між клієнтом PPTP і сервером PPTP через FTP.

- Тунелювання PPTP. Зрештою, протокол PPTP створює IP-пакети, зашифровані за допомогою PPP, які потім передаються через тунель PPTP на сервер PPTP. Сервер PPTP інтерпретує IP-пакети, розшифровує протокол PPP, а потім передає розшифровані пакети в приватну мережу.

PPP — це протокол віддаленого доступу, який використовується PPTP для передачі даних, які підтримують кілька протоколів, через мережі на основі

TCP/IP. PPP охоплює пакети IP, IPX і NetBEUI, які знаходяться між різними кадрами PPP, і вони надсилаються як є, створюючи пряме з'єднання «точка-точка» між комп'ютерами-відправниками та приймаючими.

Багато сеансів PPTP ініціюються клієнтом, який підключається до сервера доступу до мережі Інтернет-провайдера. Протокол PPP використовується для створення прямого з'єднання між клієнтом і мережевим сервером, який забезпечує доступ до Інтернету, він функціонує наступним чином:

- Встановлює та розриває логічне з'єднання. Протокол PPP дотримується послідовності, визначеної в RFC 1661, для створення та підтримки з'єднань між віддаленими комп'ютерами;

- Створює пакети PPP, зашифровані за протоколом IPX, NetBEUI або TCP/IP. PPP створює пакети даних, які або зашифровані за допомогою TCP, IPX або NetBEUI, або вони складаються з кількох таких пакетів. Оскільки пакети в мережі зашифровані, трафік між клієнтом і сервером захищений.

Безпеку мережі можна підвищити, зробивши активним фільтрацію на сервер PPTP. Коли фільтрацію PPTP активовано, сервер PPTP у приватній мережі прийматиме та направлятиме пакети PPTP лише від авторизованих користувачів. Це запобігає досягненню іншого трафіку до PPTP-сервера та персональної мережі. У поєднанні з шифруванням PPP цей протокол гарантує, що лише авторизовані зашифровані дані залишають або потрапляють у приватну мережу.

Протокол PPTP сумісний із більшістю брандмауерів і комп'ютерів, що дозволяє перенаправляти трафік, спрямований на порт 1723. Брандмауери запобігають доступу до корпоративної мережі для людей у приватному секторі, а також запобігають доступу Інтернету до корпоративної мережі. Сервер отримує пакети PPTP, які надсилаються в персональну мережу від брандмауера, він витягує пакет PPP з IP-адреси, виконується розшифровка пакета, а потім він надсилається на комп'ютер у персональній мережі.

У комп'ютерних мережах тунельний протокол рівня 2 (L2TP) — це протокол, який полегшує створення віртуальних приватних мереж. Цей протокол також використовується провайдерами Інтернет-послуг для надання послуг. Він використовує шифрування лише з метою контролю отриманих повідомлень, не

забезпечує жодної безпеки чи конфіденційності самого вмісту. Замість цього він служить проходом для другого рівня, який може передаватися через протокол для шифрування рівня 3, наприклад Ipsec.

Опублікований у 2000 році як запропонований RFC 2661, L2TP в основному походить від двох старих протоколів, які є за своєю природою «точка-точка»: L2F, розробленого Cisco, і PPTP, створеного Microsoft. Нова версія протоколу, L2TPv3, була запропонована як формальний стандарт RFC 3931 у 2005 році. L2TPv3 додає протоколу додатковий захист, покращує інкапсуляцію протоколу та дозволяє передавати додаткові дані через Інтернет.

Весь пакет L2TP, включаючи корисне навантаження та заголовок L2TP, передається через протокол дейтаграм користувача (UDP). Перевага передачі через UDP (на відміну від TCP) полягає в тому, що вона обходить «проблему збою TCP». Зазвичай розмови PPP передаються через канали L2TP.

Сам по собі L2TP не забезпечує безпеки чи конфіденційності. IPsec часто використовується для захисту пакетів L2TP, які призначені для захисту, це забезпечує конфіденційність, автентичність і надійність. Комбінацію цих двох протоколів часто називають L2TP/Ipsec.

Дві кінцеві точки тунелю L2TP називаються концентратором доступу L2TP (LAC) і мережевим сервером L2TP мережевим сервером L2TP (LNS). LNS очікує на нові тунелі. Після встановлення тунелю мережевий трафік між одноранговими вузлами стає двонаправленим. Щоб бути корисними для роботи в мережі, протоколи більш високого рівня потім проходять через тунель L2TP. Щоб полегшити це, в тунелі створюється сеанс L2TP для всіх протоколів вищого рівня, такого як PPP. Ініціювати сеанси може або LAC, або LNS. Трафік для кожного сеансу ізолюється L2TP ізолює трафік для кожної сесії, тому можна створити більше однієї віртуальної мережі через той самий тунель.

Пакети, якими обмінюються в каналі L2TP, поділяються на пакети керування та пакети даних.

L2TP пропонує підвищену надійність для контрольних пакетів, але не має надійності для пакетів даних. Надійність вимагається від протоколів, які виконуються в кожному сеансі L2TP.

L2TP дає змогу створити віртуальну приватну мережу з комутованим доступом (VPDN), це дає змогу підключити віддаленого клієнта до вашої корпоративної мережі через спільну інфраструктуру, це може бути Інтернет або мережа провайдера.

Тунель L2TP може передавати весь час PPP або лише його частину. Це можна виразити чотирма різними сценаріями тунелювання:

- добровільний тунель;
- примусовий тунель — вхідний виклик;
- примусовий тунель — вихідний виклик;
- L2TP мультихоп з'єднання.

Під час створення з'єднання L2TP між сервером і клієнтом відбувається обмін багатьма пакетами, які використовуються для створення тунелю та сеансу для кожного напрямку. Один одноранговий сервер запитує іншого про конкретне призначення тунелю та пов'язаний з ним ідентифікатор сеансу, використовуючи ці пакети для контролю. Потім тунель використовується для обміну даними у вигляді стиснутих кадрів PPP як корисного навантаження.

Через відсутність конфіденційності, пов'язаної з протоколом L2TP, його зазвичай поєднують з IPsec. Це відомо як L2TP/IPsec і задокументовано в IETF RFC 3193. Процедура створення L2TP/IPsec VPN така:

а) Типова процедура зв'язку безпеки IPsec SA здійснюється за допомогою протоколу IKE для обміну ключами в Інтернеті. Це виконується через протокол UDP 500 і зазвичай передбачає використання спільного пароля, відкритого ключа або сертифіката X.509 з обох сторін, хоча можливі й інші методи шифрування;

б) Створення корисного навантаження безпеки, інкапсульованого в транспорті. Адреса для ESP – 50. На цьому етапі встановлюється прямий канал, який є безпечним, але криптоаналіз не виконується;

в) Процес створення тунелю та узгодження з другим шаром. Фактичне обговорення параметрів відбувається через виділений канал безпеки, це досягається за допомогою використання IPsec для включення IPsec. L2TP використовує протокол UDP 1701.

Після завершення процедури зв’язок L2TP між точками вирішується за допомогою IPsec. Оскільки пакет протоколу L2TP прихований у пакеті протоколу IPsec, вихідні адреси джерела та призначення зашифровані в останньому. Крім того, немає необхідності відкривати UDP-порт 1701 на брандмауерах між точками контакту, внутрішні пакети не оцінюються, доки дані IPsec не будуть розшифровані та видалені, це відбувається лише в точках контакту.

Можливою плутаниною в L2TP/IPsec є різниця між термінами «тунель» і «захищений канал». Термін тунельний режим використовується для опису каналу, який полегшує передачу цілих пакетів з однієї мережі в іншу. У контексті L2TP/PPP це означає, що пакети L2TP/PPP передаються через Інтернет. Захищений канал – це канал, який гарантує конфіденційність всієї інформації. У L2TP/IPsec першим компонентом є IPsec, який створює безпечний канал, а потім L2TP, який створює тунель. Крім того, IPsec має протокол, який є специфічним для тунелів: він не використовується, коли використовується протокол L2TP.

L2TP часто використовується Інтернет-провайдерами для продажу пропускної здатності через ADSL або кабель. Від кінцевого користувача пакети проходять через мережу оптового постачальника послуг до сервера, який називається сервером широкосмугового віддаленого доступу (BRAS) — процесор протоколу та маршрутизатор в одному флаконі. У застарілих мережах шлях від обладнання кінцевого користувача до BRAS може проходити через мережу банкоматів. Звідти протокол L2TP працює через IP-мережу, BRAS і LNS служать кінцем діапазону протоколу на межі IP-мережі провайдера.

Однак L2TP також піддався критиці та обмеженням, про які слід пам’ятати при використанні протоколу:

- Продуктивність: L2TP має вищі накладні витрати, спричинені процесом інкапсуляції та шифрування, цей процес може дещо негативно вплинути на продуктивність мережі;

- Уразливості безпеки: L2TP без IPSec не має шифрування, тому дані можуть стати вразливими для спостереження. У результаті пропонується поєднати L2TP з IPSec для підвищення безпеки;

- Доступність портів: L2TP вимагає, щоб порти UDP 500 і 1701 були доступні на брандмауерах і маршрутизаторах. У деяких мережах ці порти навмисно вимкнено, що перешкоджає встановленню L2TP VPN;

- Брандмауери: трафік від L2TP може погіршуватися брандмауерами та іншими пристроями безпеки мережі. Для забезпечення успішного підключення може знадобитися правильна конфігурація брандмауерів і мережевих компонентів.

Як наслідок, L2TP є широко використовуваним протоколом для тунелювання, який використовується у VPN. Незважаючи на відсутність окремого шифрування, у поєднанні з IPSec L2TP може забезпечити надійну та безпечну VPN на різних платформах і середовищах (таблиця 2.1).

Таблиця 2.1 – Порівняльний аналіз популярних алгоритмів та протоколів

	PPTP	SSTP	L2TP/IPSec	OpenVPN
1	2	3	4	5
Розробник	Microsoft	Microsoft	L2TP - спільна розробка Cisco і Microsoft, IPsec - The Internet Engineering Task Force	OpenVPN Technologies
Ліцензія	Пропріетарна	Пропріетарна	Пропріетарна	GNU GPL
Встановлення	Windows, macOS, iOS, деякий час GNU/Linux. Працює "з коробки", не вимагаючи встановлення додаткового ПЗ	Windows. Працює "з коробки", не вимагаючи встановлення додаткового ПЗ	Windows, Mac OS X, Linux, iOS, Android. Багато ОС (включно з Windows 2000/XP +, Mac OS 10.3+) мають вбудовану підтримку, немає необхідності ставити додаткове ПЗ.	Windows, Mac OS, GNU/Linux, Apple iOS, Android і маршрутизатори. Необхідне встановлення спеціалізованого ПЗ, що підтримує роботу з цим протоколом

Продовження таблиці 2.1

1	2	3	4	5
Шифрування	Використовує Microsoft Point-to-Point Encryption (MPPE), який реалізує RSA RC4 з максимум 128-бітними сеансовими ключами	SSL (шифруються всі частини, крім TCP- і SSL-заголовків)	3DES або AES	Використовує бібліотеку OpenSSL (реалізує більшість популярних криптографічних стандартів)
Порти	TCP-порт 1723	TCP-порт 443	UDP-порт 500 для першопочаткового обміну ключами і UDP-порт 1701 для першої конфігурації L2TP, UDP-порт 5500 для обходу NAT	Будь-який UDP- або TCP-порт
Недоліки безпеки	Має серйозні вразливості. MSCHAP-v2 вразливий для атаки за словником, а алгоритм RC4 піддається атаці Bit-flipping	3DES вразливий недоліків безпеки поки не зафіксовано	3DES вразливий для MITH і Sweet32, але AES не має відомих вразливостей. Однак є думка, що стандарт IPsec скомпрометований АНБ США	Серйозних недоліків безпеки не було виявлено

2.3 Протоколи аунтентифікації

У віртуальних приватних мережах VPN використовуються різні протоколи для аутентифікації, щоб підтвердити ідентичність певного користувача або пристрою, що зробив запит на отримання доступу до мережі.Їх є доволі багато, зокрема вищезгадані IKE,L2TP та SSL/TLS. Вони частково можуть виконувати дані функції але це не їх основна мета, під цю мету є спеціально створені протоколи які працюють конкретно із цим пунктом безпеки VPN. Такими протоколам є Radius (Remote Authentication Dial-In User Service) та TACACS+ (Terminal Access Controller Access-Control System Plus), за них і буде йти мова у цій дипломній роботі в даному пункті.

Щоб централізувати керування автентифікацією, авторизацією та обліком (AAA) для ресурсів локальної мережі, таких як маршрутизатори та комутатори, у 1990-х роках було створено протокол RADIUS, призначений для мережі.

Однак, оскільки протокол продемонстрував свою ефективність у багатьох сценаріях, хмарні провайдери намагаються використовувати RADIUS для полегшення доступу до мережі без довіри (ZTNA) і зниження ризику, пов'язаного з повітряними атаками на бездротові мережі та віртуальні приватні мережі VPN.

Будь-хто, хто займається адмініструванням мережі, повинен мати повне розуміння RADIUS, оскільки він є невід'ємною частиною розробки багатьох ефективних рішень безпеки для мереж. Оскільки RADIUS — це протокол, який базується на стандартах, він визначається специфікаціями IETF.

RADIUS-клієнт запитує підключення до RADIUS-сервера, коли він бажає підключитися до нього. Після того, як сервер RADIUS ідентифікує кінцевого користувача, йому дозволяється підключитися до клієнта RADIUS. Клієнт RADIUS може бути будь-яким пристроєм, який підключено до мережі та використовується для автентифікації користувачів на рівні пристрою.

Протоколом для транспортування в RADIUS є UDP.

Протокол UDP не має з'єднання, що означає, що кожен пакет надсилається окремо, без попереднього встановлення з'єднання. Оскільки він може обслуговувати велику кількість клієнтів, не вимагаючи великої кількості серверних ресурсів, ось чому RADIUS є особливо надійним. RADIUS використовує корекцію помилок, щоб забезпечити правильну передачу пакетів.

Оскільки витрати на створення та підтримку серверної інфраструктури RADIUS делегуються третій стороні, яка укладена з організацією, модель RADIUS, яка базується на хмарі, може зменшити капітальні витрати організації (CapEx).

Інтернет-протокол під назвою RADIUS відповідає за централізовану автентифікацію, нагляд і керування IP-адресами для віддалених користувачів у розподіленій мережі, яка підключена за телефоном.

Сервер доступу до мережі (NAS) схожий на сервер RADIUS, який функціонує як клієнт для RADIUS. Стандартний протокол RADIUS, визначений у

RFC 2865, використовується NAS для передачі інформації про користувача та підключення до вибраного сервера RADIUS. Сервери RADIUS відповідають на запити на підключення, автентифікуючи користувача, а потім повертаючи до мережевого сховища (системи) будь-яку конфігураційну інформацію, необхідну для мережевого сховища для надання авторизованих послуг автентифікованому користувачеві.

Система може направляти запити на автентифікацію на інший сервер, якщо з RADIUS-сервером неможливо зв'язатися. Це полегшує надання комутованого доступу користувачам транснаціональних корпорацій. Точка доступу не має значення для надання доступу до цієї інформації.

Як працює RADIUS: Сервер RADIUS оцінює запит на автентифікацію після його отримання, а потім розшифровує дані, щоб отримати ім'я користувача та пароль. Відповідна система захисту отримує дані. Це може бути система безпеки, створена для бізнесу, спеціальна система на основі Kerberos, файл паролів у стилі UNIX або комерційна система. Сервер RADIUS повторно отримує будь-які служби, які авторизованому користувачеві дозволено використовувати, наприклад IP-адресу. Подібні методи використовуються для обробки запитів на облік RADIUS. Зазначений сервер RADIUS для обліку може отримувати облікові дані від зовнішніх користувачів. RFC 2866 описує типовий спосіб реалізації RADIUS. Записуючи дані із запиту автентифікації RADIUS, сервер RADIUS відповідає на вхідні запити автентифікації.

RADIUS дозволяє компанії відстежувати профілі користувачів в єдиній базі даних, яка використовується спільно для всіх віддалених серверів. Централізована база даних забезпечує більший рівень безпеки, що дозволяє компанії створювати політики, які можна впроваджувати в одному адміністративному місці в мережі. Центральна база даних також полегшує зберігання мережевих даних і запис статистики використання, пов'язаної з вашим доступом до мережі або постачальником послуг Інтернету. Провідні виробники мережевих продуктів використовують RADIUS, який вважається стандартом де-факто в галузі з 1991 року, створений колишнім постачальником мережевого обладнання Livingston Enterprises.

Як задокументовано в RFC 2865, протокол RADIUS був офіційно визнаний як запропонований стандарт робочою групою з розвитку Інтернету в 2000 році. Спочатку RADIUS був призначений для допомоги багатьом клієнтам у віддаленому підключенні до Інтернет-провайдерів (ISP) або бізнес-мереж через кластери модемів або інші з'єднання «точка-точка», які є послідовними. Сьогодні RADIUS часто використовується для доступу до віддалених ресурсів у кількох мережах, включаючи бездротові мережі, мережі Ethernet і віддалений доступ через Інтернет.

Процес аутентифікації через RADIUS: користувачі віддалених мереж підключаються до своїх мереж через протокол RADIUS через сервер, який забезпечує доступ до мережі (NAS). Щоб отримати інформацію про автентифікацію, авторизацію та конфігурацію для віддаленого користувача, NAS зв'язується з сервером автентифікації. Клієнти RADIUS — це системи, які використовують мережу як точку доступу, на відміну від інших клієнт-серверних програм, якими зазвичай користується одна особа. Сервери RADIUS служать засобом аутентифікації. У протоколі RADIUS сервери, які мають доступ до ресурсів, роблять це так, ніби вони є клієнтами сервера RADIUS. Користувачі, які мають віддалений доступ до мережі через сервери, використовують для автентифікації протокол RADIUS.

Доступно кілька різновидів серверів віддаленої автентифікації користувачів, у тому числі

- Сервери, які підключаються до Інтернету через модем, який об'єднує ресурси кількох клієнтів;

- Сервери, які сприяють створенню віртуальних приватних мереж, які отримують запити від віддалених користувачів для встановлення надійного з'єднання з приватною мережею;

- Точки доступу для бездротових мереж, які дозволяють клієнтам бездротових мереж запитувати підключення;

- Контролери, які використовуються для доступу до мережі через протокол 802.1x, який використовується для автентифікації доступу до мережі.

Під час перевірки у віддаленій мережі користувачі мають лише непряму взаємодію з сервером RADIUS через сервер доступу до мережі. Коли користувач потрапляє у віддалену мережу, мережевий диск починає розмову RADIUS із сервером автентифікації. Запит може містити ідентифікатор віддаленого користувача, пароль і адресу, коли віддалений користувач входить до системи через мережеве сховище. Потім RADIUS-сервер отримує запит на автентифікацію від мережевого сховища.

RADIUS використовує два засоби аутентифікації.

– Протокол аутентифікації паролів (PAP). Ідентифікатор користувача та пароль віддаленого користувача передаються клієнтом RADIUS на сервер автентифікації RADIUS. Сервер перевіряє легітимність користувача, якщо облікові дані правильні, а клієнт RADIUS дозволяє віддаленому користувачеві отримати доступ до мережі.

– Протокол аутентифікації за допомогою рукостискань (CHAP). Автентифікація CHAP, яка також відома як тристороння угода, залежить від того, чи клієнт і сервер спільно використовують зашифрований ключ. Оскільки його можна налаштувати на автентифікацію кілька разів протягом сеансу та шифрування передачі інформації автентифікації, CHAP вважається більш надійним, ніж PAP.

Ви можете створити RADIUS-клієнт, який надсилатиме запити автентифікації іншим RADIUS-серверам. Централізована перевірка можлива у великих або розгалужених мережах через сервери RADIUS. Програмне забезпечення служби каталогів поєднується з протоколом RADIUS, який є визнаним засобом автентифікації, який використовується багатьма мережевими компонентами для авторизації та обліку. Наприклад, сервер мережевої політики Microsoft, який використовує Microsoft Active Directory, використовує RADIUS.

Керування доступом користувачів значно полегшується завдяки єдиній платформі RADIUS, яка аутентифікує як користувача, так і систему. Через централізований характер RADIUS кілька IT-менеджерів можуть легко досліджувати одну мережу. Крім того, той факт, що кожен користувач у середовищі RADIUS має унікальний набір облікових даних, усуває необхідність

частої зміни паролів. У результаті недоліки традиційного захисту паролів зменшуються. Мабуть, найважливіше те, що RADIUS гарантує безпеку мережевих з'єднань, які є законними для користувачів. Кожен користувач, підключений до мережі, перевіряється адміністраторами, чи він є тим, за кого себе видає, і має необхідні рівні авторизації.

Проблеми RADIUS: через традиційну власну реалізацію може бути важко налаштувати та підтримувати, це може зайняти час. Впровадження та підтримка можуть бути простішими за допомогою хмарних технологій. Процедура інсталяції нового RADIUS-сервера та його інтеграції в існуючу систему ще більше ускладнюється численними доступними параметрами конфігурації. Ці перешкоди можуть негативно вплинути на ефективність і продуктивність. Крім того, кількість рішень RADIUS, ймовірно, буде великою. Щоб вибрати найбільш відповідний сервер RADIUS, важливо врахувати вимоги організації та оцінити різні варіанти. Цей процес повільний.

TACACS+ (Terminal Access Controller Access Control System Plus) — це протокол, створений компанією Cisco Systems і опублікований у чернетці RFC.. TACACS+ надає послуги автентифікації, авторизації та обліку через безпечне з'єднання TCP, яке використовує протокол порту 49.

Подібно до RADIUS, TACACS+ використовує модель клієнт/сервер, яка включає сервер доступу до мережі (NAS) як клієнта та оснащений TACACS+ пристрій (демон у термінології TACACS+), який функціонує як сервер. Для цілей поточної реалізації Oracle Enterprise Session Border Controller служить клієнтом TACACS+. На відміну від RADIUS, який поєднує автентифікацію та авторизацію, TACACS+ надає три окремі програми, які забезпечують більш точний контроль доступу.

Як правило, автентифікація базується на простій комбінації імені користувача та пароля, але інші, більш складні методи стають все більш популярними. Поточна реалізація підтримує такі підходи автентифікації: простий пароль, PAP (протокол автентифікації протоколу) і CHAP (протокол автентифікації рукостискання).

TACACS+ може запропонувати надзвичайно детальний контроль доступу до системних ресурсів. Сьогодні TACACS+ контролює доступ до ресурсів адміністрування системи.

TACACS+ гарантує безпеку зв'язку між клієнтом і сервером шляхом шифрування всіх пакетів. Шифрування базується на спільному ключі, який відомий лише клієнту та серверу. Пакети повністю закриті шифруванням, за винятком звичайного трейлера TACACS+.

Заголовок простого тексту містить поля, окрім номера версії, порядкового номера та ідентифікатора сеансу. Відправник криптографічно кодує оригінальне текстове повідомлення, багаторазово виконуючи хеш MD5 над комбінацією ідентифікатора сеансу, ключа, номера версії та порядкового номера, що призводить до віртуального, одноразового блокнота, ідентичного тілу повідомлення, а також ключу сесії. Відправник криптографічно кодує текст за допомогою операції XOR, вхідними даними для цієї операції є сам текст і віртуальна одноразова панель.

Дуже важливо оцінити ефективність служби TACACS+ перед її повним впровадженням. Залежно від процедури та параметрів, які ви використовуєте для налаштування та тестування автентифікації TACACS+ у вашій мережі, ви можете не мати доступу до комутатора для всіх користувачів, включаючи себе. Незважаючи на те, що відновлення є простим, воно може призвести до непотрібних ускладнень. Щоб запобігти випадковому блокуванню комутатора, скористайтеся процедурою, яка налаштовує та перевіряє безпеку TACACS+ через Telnet, залишаючи інший тип доступу відкритим на випадок, якщо безпеку комутатора буде порушено через проблеми з конфігурацією.

Загалом TACACS+ пропонує більш надійний засіб автентифікації користувача, ніж RADIUS. TACACS+ використовує TCP як транспортний протокол замість UDP, цей протокол більш надійний і менш чутливий до помилок мережевого рівня.

TACACS+ також виділяє послуги автентифікації, авторизації та обліку, тоді як RADIUS надає профіль для користувачів, який описує всі конкретні параметри, які вони мають, разом із автентифікацією. Цей розподіл служб дозволяє

TACACS+ використовувати інші методи автентифікації, такі як Kerberos, на додаток до власного.

TACACS+ використовує попередньо встановлений секретний ключ для автентифікації транзакцій. TACACS+ охоплює весь трафік, який сервер автентифікації та пристрій хочуть використовувати для автентифікації. Інформація про користувачів захищена за допомогою алгоритму дайджесту повідомлень MD5.

Сервери автентифікації TACACS+ можуть обробляти адреси IPv4 і IPv6 (таблиця 2.2).

Таблиця 2.2 – Порівняння популярних протоколів аунтефікації

Протокол	RADIUS	TACACS+
1	2	3
Основне застосування	Автентифікація та реєстрація віддалених користувачів мережі	Надання доступу адміністратора до мережевих пристроїв, таких як маршрутизатори та комутатори
Аутентифікація та авторизація	Автентифікація та перевірка авторизації пов'язані між собою. Коли клієнтський пристрій запитує автентифікацію у сервера, сервер відповідає як атрибутами автентифікації, так і атрибутами авторизації. Ці функції не можуть виконуватися окремо.	Всі три функції AAA (автентифікація, авторизація та облік) можна використовувати незалежно. Тому для автентифікації можна використовувати один метод, наприклад, kerberos, а для авторизації - окремий метод, наприклад, TACACS+.

Продовження таблиці 2.2

1	2	3
Протокол	User Datagram Protocol (UDP)/IP з найкращими зусиллями використовується для доставки на портах 1645/1646, 1812/1813	TCP використовується для доставки через порт 49. Також має мультипротокольну підтримку протоколів AppleTalk Remote Access (ARA), NetBIOS Frame Protocol Control, Novell Asynchronous Services Interface (NASI) і X.25 PAD з'єднання.
Шифрування застосовується до	Пароль	Ім'я користувача та пароль
Застосування 802.1X	Не підтримується	Підтримується
Модель	клієнт/сервер	клієнт/сервер
Рекомендоване середовище	Напівдовірене	довірене

2.4 Протоколи авторизації та обміну ключами

Протоколи обміну ключами або Key Exchange Protocols у мережах VPN використовуються для того, щоб спільний ключ ділився між двома чи більше сторонами, цей ключ потім використовується для шифрування та дешифрування інформації під час безпечного обміну інформацією. У даній роботі буде йти мова про такі популярні протоколи як: протокол Діффі – Геллмана, TLS/SSL, протокол авторизації типу “Точка-Точка” (PPP).

Що таке обмін ключами Діффі-Хеллмана (експоненціальний обмін ключами).Обмін ключами Діффі-Хеллмана - це метод цифрового шифрування, який забезпечує безпечний обмін криптографічними ключами між двома сторонами через публічний канал без передачі їхньої розмови через Інтернет. Дві сторони використовують симетричну криптографію для шифрування і розшифрування своїх повідомлень. Опублікована в 1976 році Вітфілдом Діффі та Мартіном Хеллманом, вона стала одним з перших практичних прикладів криптографії з відкритим ключем.

Метод обміну ключами Діффі-Хеллмана передбачає збільшення потужності чисел для отримання ключів шифрування. Складові частини ключів ніколи не передаються безпосередньо, це ускладнює для потенційного зловмисника код математичний розв'язок проблеми. Метод не вимагає обміну інформацією під час обміну ключами. Обидві сторони не мають попередньої інформації одна про одну, але обидві сторони створюють весь ключ разом.

Яка мета методу узгодження ключів Діффі-Хеллмана. Метою обміну ключами Діффі-Хеллмана є забезпечення безпечних засобів генерації та спільного використання ключів для симетричного криптоаналізу. Зазвичай він використовується для транзакцій на основі паролів, а також для безпеки користувачів. Ключові з’єднання, які використовують автентифікацію пароля, використовуються для запобігання атакам посередників (MithM). Протоколи на основі пересилання захищають від критичних атак шляхом створення нових ключів для кожного сеансу зв’язку.

Обмін ключами Діффі-Хеллмана поширений у протоколах, метою яких є безпека, наприклад Transport Layer Security (TLS), SSH і IPsec. Наприклад, в IPsec метод шифрування використовується для створення та ротації ключів.

Незважаючи на те, що обмін ключами Діффі-Хеллмана можна використовувати для створення відкритих і закритих ключів, алгоритм Ріввеста-Шаміра-Адлемана або алгоритм RSA також здатний підписувати документи з відкритими ключами. Обмін ключами Diffie-Hellman є вразливим. Найбільше занепокоєння щодо базової конструкції Діффі-Хеллмана викликає відсутність автентифікації. Зв'язок, що використовує протокол Діффі-Хеллмана, за своєю суттю чутливий до MitM. В ідеалі функція Діффі-Хеллмана повинна поєднуватися з визнаним методом автентифікації, таким як цифровий підпис, для автентифікації особи користувачів у публічному віртуальному просторі.

Крім того, метод обміну ключами Діффі-Хеллмана сприйнятливий до атак, які викликають перевантаження, ці атаки особливо поширені в TLS. Атаки перевантаження руйнують протокол TLS до 512-бітного рівня безпеки, що дозволяє зловмиснику читати та змінювати інформацію, що передається через посилання. Протокол Діффі-Хеллмана все ще життєздатний, якщо він

виконується правильно. Наприклад, атаки перевантаження не будуть ефективними з 2048-бітним ключем.

Приклад обміну ключами Діффі-Хеллмана: якщо два користувачі, користувач-1 і користувач-2, хочуть поділитися секретними даними через відкриту загальнодоступну мережу, але хочуть уникнути хакерів або підслуховування, вони можуть використовувати метод Діффі-Хеллмана для обміну ключами для шифрування. Ця загальнодоступна онлайн-мережа доступна, наприклад, у кафе.Користувач-1 і користувач-2 кожен вибирає секретний ключ, який є закритим, функція буде запущена на цих ключах для створення відкритого ключа. Розголошуються результати, але не процес. Навіть якщо третя сторона спостерігає за розмовою, вона не матиме всіх залучених цифр, що ускладнить висновок про процес, з якого були отримані цифри.

Далі користувач-1 і користувач-2 обчислюють нову функцію, використовуючи інформацію, яку вони отримали від іншої сторони, власне секретне число та початкове просте значення. Після цього користувач-1 і користувач-2 отримують спільний ключ, який не може обчислити третя сторона. Тепер користувач-1 і користувач-2 можуть спілкуватися один з одним, не турбуючись про треті сторони.

Secure Sockets Layer (SSL) — це протокол, який забезпечує безпечне спілкування в Інтернеті. Він використовує як стандартні криптографічні методи, так і асиметричні методи. Протокол SSL гарантує автентичність сервера та автентичність клієнта.

Процес автентифікації для клієнта ініціюється, коли клієнт підключається до сервера. Після першого привітання сервер видає клієнту свій цифровий сертифікат. Клієнт перевіряє сертифікат сервера або ланцюжок сертифікатів.

Процес перевірки автентичності клієнта виконується, коли сервер запитує сертифікат від клієнта під час рукостискання. Якщо сертифікат клієнта перевірено та отримано повідомлення, яке підтверджує сертифікат клієнта, з’єднання продовжиться. Додаткова автентифікація виконується шляхом перевірки загального імені в сертифікаті на повне ім’я домену сервера за допомогою

зворотного запиту сервера доменних імен (DNS), після чого отримується повне ім’я домену сервера.

У сертифікації SSL підтримуються два типи довіри:

– Довіра центру сертифікації – це довіра на основі основного сертифіката, який використовується для видачі інших сертифікатів. Це типова модель довіри, пов’язана з ліцензіями SSL.

– Пряма довіра – довіра, яка постачається разом із підписаними сертифікатами, які передаються за допомогою безпечних позасмугових методів. Пряма довіра та самосертифіковані підписи не є частиною стандартів SSL, але вони часто використовуються в окремих комерційних спільнотах. Використання сертифікатів SSL. Щоб спілкуватися через SSL, переконайтеся, що задіяні системи можуть підтримувати автентифікацію на стороні сервера або автентифікацію клієнт-сервер. Щоб автентифікувати сервер, ви повинні мати центр сертифікації (CA), який має кореневий сертифікат, який потрібно перевірити, а також набір проміжних сертифікатів, необхідних для процесу автентифікації або, якщо сервер використовує самопідписаний сертифікат - сертифікат, дублікат самопідписаного сертифіката. Щоб полегшити автентифікацію клієнт-сервер, ви повинні мати сертифікат ЦС або самопідписаний сертифікат разом із системним сертифікатом. Ви можете отримати сертифікат SSL від довіреного ЦС, надіславши запит на підписання сертифіката (CSR). Сертифікат SSL надає відкритий ключ серверу або клієнту SSL (таблиця 2.3).

Таблиця 2.3 – Способи авторизації та аутентифікації користувачів у VPN

Метод	Опис	Переваги	Недоліки
1	2	3	4
Ідентифікатор на основі пароля	Найпростіший та найпоширеніший метод: користувачі вводять свої ідентифікаційні дані, після чого сервер надає доступ.	Простота використання та підтримка багатьох пристроїв	Вразливість до атак, слабка безпека

Продовження таблиці 2.3

1	2	3	4
Аутентифікація на основі сертифікатів	Кожен користувач має власний цифроваий сертифікат, який видається центром сертифікації. Користувачі відправляють свій сертифікат при підключенні до VPN, сервер перевіряє його валідність. Рівень безпеки вищий ніж у попередньому методі, оскільки пароль не передається по мережі.	Висока безпека, важко підробити	Втрата або крадіжка, додаткові витрати на фізичні носії
Аутентифікація на основі інтеграції з існуючою інфраструктурою	В деяких випадках VPN може використовувати існуючу інфраструктура аутентифікації, таку як сервер доменів або служби каталогів, для перевірки ідентичності користувачів	Централізоване управління, одна точка входу	Складність налаштування, залежність від існуючої інфраструктури
Аутентифікація на основі двофакторної перевірки	Після введення логіна та пароля потрібен додатковий елемент ідентифікації - одноразовий код, який відправляється на телефон чи пошту користувача.	Вищий рівень безпеки, захист від втрат пароля	Додаткові кроки, проблеми із сумісністю

Протокол TLS походить від протоколу SSL, який спочатку був задуманий у Netscape як засіб підвищення безпеки онлайн-покупок. Протокол SSL було реалізовано на прикладному рівні, безпосередньо над TCP (протокол керування передачею), цей протокол дозволяє використовувати протоколи вищого рівня без додаткових змін. Якщо SSL налаштовано належним чином, сторонній спостерігач

може лише визначити параметри з’єднання, а також частоту просування вперед і приблизний обсяг даних, але він не може змінити ці параметри.

Після того, як IETF (Internet Engineering Task Force) стандартизувала протокол для SSL, його перейменували в TLS. Незважаючи на те, що назви SSL і TLS є синонімами, вони все ж відрізняються, оскільки кожна описує різну версію протоколу. Перший публічний випуск протоколу називався SSL 2.0, але за ним швидко пішов SSL 3.0 через очевидні небезпеки. Як згадувалося раніше, SSL був створений Netscape як частина їхніх зусиль із впровадження безпечного браузера, це призвело до офіційного прийняття IETF терміну TLS 1.0 у січні 1999 року. Пізніше, у квітні 2006 року, була випущена версія TLS 1.1, цей протокол збільшив початкові можливості протоколу та вирішив відомі проблеми. Поточна версія протоколу - TLS 1.2, яка була випущена в серпні 2008 року.

Через історичні та комерційні причини алгоритм RSA зазвичай використовується в TLS: клієнт генерує секретний ключ, ідентичний в обох напрямках, підписує його відкритим ключем сервера, а потім надсилає на сервер.

На сервері інформація клієнта розшифровується за допомогою особистого ключа. Після цього процес шифрування вважається завершеним. У цього алгоритму є одне застереження: для автентифікації серверів використовується та сама пара відкритих і закритих ключів. У результаті, якщо злодій отримує закритий ключ сервера, він може розшифрувати весь сеанс зв'язку. Крім того, зловмисник може просто взяти весь сеанс зв’язку та перетворити його в зашифровану версію, а потім розпочати дешифрування пізніше, отримавши закритий ключ сервера. Крім того, процес обміну ключами Diffie-Hellman виглядає більш надійним, оскільки встановлений симетричний ключ ніколи не залишає клієнта чи сервера, отже, його не може перервати зловмисник, навіть якщо зловмисник знає закритий ключ сервера.

Це основа протоколу, яка знижує ризик розкриття попередніх сеансів зв’язку: для кожного послідуючого сеансу зв’язку використовується новий «тимчасовий» ідентичний ключ. У результаті, навіть якщо зловмисник має приватний ключ сервера, він не може розшифрувати раніше записані сесії.

Наразі всі браузери, які встановлюють з’єднання TLS, віддають перевагу

комбінації алгоритму Діффі-Хеллмана та використання тимчасових ключів для підвищення безпеки з’єднання. Важливо ще раз зазначити, що криптографія з відкритим ключем використовується лише під час рукостискання TLS під час початкового налаштування з’єднання. Після того, як тунель побудовано, симетрична криптографія бере на себе перевагу, і зв’язок між сеансами тепер здійснюється з однаковими точними симетричними ключами. Це важливо, оскільки для реалізації криптографії з відкритим ключем потрібна додаткова обчислювальна потужність.

PPP (протокол «точка-точка»), визначений у RFC 1661, — це протокол, який встановлює пряме з’єднання між двома точками через WAN або LAN. Це полегшує передачу кількох потоків даних протоколу через пряме з’єднання «точка-точка». Інкапсуляція протоколу PPP забезпечує одночасну передачу кількох рівнів протоколу по одному каналу.

PPP — це найпоширеніший протокол, який використовується для підключення хоста до постачальника послуг Інтернету (ISP).

PPP було створено Інженерною робочою групою Інтернету (IETF) як засіб передачі даних, які містять більше одного протоколу для зв’язку через одне з’єднання «точка-точка». Це стандартний, незалежний від постачальника підхід до передачі даних, який містить кілька протоколів для зв'язку.

PPP полегшує прямий зв’язок як через синхронне, так і через асинхронне середовище. PPP використовує кілька рівнів протоколу в мережі, включаючи IPv6 та IP. Крім того, PPP має такі протоколи безпеки, як PAP (протокол автентифікації пароля), CHAP (протокол рукостискання автентифікації) і EAP (розширюваний протокол автентифікації).

Протокол PPP складається з таких основних компонентів:

- Процедура включення даних через послідовний або інший первинний механізм зв'язку. HDLC (High-level Data Link Control), L2TP (Layer 2 Tunneling Protocol) і PPPoE (Point-to-Point Protocol over Ethernet) — це протоколи, які забезпечують цю функцію;

- Протокол керування зв'язками (LCP), який використовується для створення, налаштування та тестування каналів передачі даних;

- Сімейство протоколів, які реалізують і налаштовують різні протоколи мережевого рівня. PPP дозволяє одночасне використання кількох рівнів протоколу в мережі. Найпоширенішим NCP є протокол керування протоколом Інтернету (IPCP).

Метод, який PPP використовує для передачі інформації про мережу, полягає у створенні короткого каналу зв’язку. Після формування каналу мережеві дані передаються з мінімальними додатковими витратами.

Трафік передається як послідовність інформаційних пакетів без міток, що означає, що підтвердження підключення не потрібне, і повторні спроби не використовуються. Після формування зв'язку PPP функціонує як прямий канал передачі даних для протоколів, які знаходяться на вищому рівні.

Визначення розширюваного LCP у PPP включає протокол, який дозволяє визначати процес автентифікації протоколами мережевого рівня, які будуть передаватися по каналу зв’язку. RFC 1334 описує два протоколи автентифікації.

PAP простий і передбачає двосторонній зв’язок. Це не передбачає шифрування. Ім'я користувача та пароль передаються в явному вигляді. Якщо на них застосовано санкції, заставу затверджують.

Етап автентифікації сеансу PPP є необов’язковим. Якщо це використовується, LCP зможе автентифікувати однорангового вузла після встановлення з’єднання та вибору протоколу для автентифікації LCP для однорангового вузла. Якщо це використовується, процес автентифікації відбувається до початку фази налаштування протоколу мережевого рівня.

Параметри автентифікації вимагають від сторони, яка бере участь у перенаправленні, введення інформації щодо автентифікації. Це полегшує процес забезпечення того, щоб користувач отримав дозвіл від менеджера мережі на здійснення телефонного дзвінка. Однорангові маршрутизатори спілкуються один з одним за допомогою повідомлень автентифікації. Однією з найвидатніших особливостей PPP є те, що він має додаткові рівні автентифікації, шифрування, контролю доступу та загальної безпеки.

3. РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ АЛГОРИТМІВ VPN

3.1 Вимоги до систем VPN

Основною причиною, чому компанії виступають за безпечні VPN, є можливість передавати приватну інформацію через Інтернет, не турбуючись про те, хто її побачить. Все, що проходить через захищену VPN, криптографічно зашифровано на такому рівні, що навіть якщо хтось отримає копію трафіку, він не зможе його розшифрувати, навіть якщо він використовує комп'ютери, вартість яких становить 200 мільйонів доларів або більше. Крім того, використання захищеної VPN дає змогу корпорації знати, що зловмисник не матиме можливості змінити вміст їхніх передач, включаючи вартість фінансових операцій. Захищені мережі VPN особливо корисні для віддаленого доступу, коли користувач підключений до Інтернету в місці, яке не контролюється адміністратором мережі, наприклад у готельному номері, на стійці в аеропорту чи вдома.

Компанії, які використовують захищені VPN, роблять це тому, що хочуть бути в курсі руху даних за шляхами, які мають певні властивості та контролюються лише одним постачальником або надійною коаліцією постачальників. Це полегшує власні персоналізовані схеми адресації клієнта та потенційне керування їхнім власним шляхом. Клієнт вважає, що шляхи будуть проходити згідно з домовленістю, і що люди, яким він не довіряє, наприклад зловмисники, не матимуть можливості змінити шляхи в VPN або ввести трафік у VPN. Важливо зазначити, що клієнт не може знати маршрути, які використовуються в надійних VPN, або перевірити наявність надійної VPN; він повинен покладатися на довіру свого постачальника.

Захищені VPN забезпечують безпеку, але не гарантують шляхи. Довірені VPN забезпечують шляхи з такими властивостями, як QoS, але вони не захищають від прослуховування чи перенаправлення. Через ці переваги та недоліки почали розробляти гібридні VPN, хоча список ситуацій, у яких вони корисні, продовжує розширюватися. Звичайним явищем для гібридної VPN є те, що компанія вже має надійну VPN, і додаткові частини компанії повинні бути захищені через частину VPN. На щастя, жодна з загальнодовірених технологій

VPN не забороняє створення гібридних VPN, деякі виробники створили системи, які спеціально підтримують створення гібридних служб VPN.

Однією з важливих вимог, яка поділяється всіма захищеними, надійними та гібридними VPN, є вимога до менеджера VPN знати про сферу дії VPN. Незалежно від типу VPN, який використовується, VPN має мати атрибути, яких не має типова мережа. У результаті адміністратор VPN повинен мати можливість знати, яка інформація буде, а яка ні, буде присутня в VPN.

Кожен із чотирьох типів VPN має додаткові вимоги, які є унікальними. Вимоги до захищеного VPN. Весь трафік, що проходить через захищену VPN, має бути зашифрований і перевірений. Багато протоколів, які використовуються для створення безпечних VPN, мають компонент автентифікації, але не мають засобів шифрування. Незважаючи на підвищену безпеку мережі, яка не має автентичного підпису, вона не є VPN, оскільки їй бракує конфіденційності.

Функції безпеки VPN повинні бути визнані всіма сторонами, залученими до VPN. Захищені VPN мають принаймні один або кілька тунелів, кожен з яких має дві кінцеві точки. Менеджери обох кінців кожного тунелю повинні мати можливість приймати рішення щодо безпеки тунелю.

Ніхто, крім самої VPN, не може змінити властивості безпеки VPN. Зловмисник не може змінити властивості безпеки будь-якої частини VPN, зокрема послабити шифрування чи змінити ключі, що використовуються для шифрування.

Вимоги до надійної VPN: лише надійний постачальник VPN може змінити або створити шлях VPN. Вся цінність надійної VPN полягає в тому, що клієнт може довіряти постачальнику створення та керування VPN. Як наслідок, ніхто, крім кордону довіри, не може змінити будь-яку частину VPN. Важливо розуміти, що деякі мережі VPN мають кілька постачальників, які покриваються, у цьому сценарії клієнт вважає, що всі постачальники є одним постачальником.

Лише надійний постачальник VPN може змінювати дані, вставляти дані або видаляти дані під час роботи VPN. Надійна мережа VPN — це більше, ніж просто ряд маршрутів: він також містить дані, які проходять ці маршрути. Незважаючи на те, що шляхи зазвичай використовуються кількома клієнтами провайдерів, сам шлях має бути призначений для VPN, і ніхто інший не може змінити дані на

цьому шляху. Ця зміна, внесена третьою стороною, вплине на характеристики шляху, наприклад на обсяг трафіку на шляху.

Вимоги до гібридної VPN: межі адреси безпечної довіреної VPN мають бути дуже конкретними. У гібридній VPN захищена VPN може бути частиною довіреної VPN, наприклад, якщо один відділ у корпорації використовує власну захищену VPN поверх корпоративної довіреної VPN. Для будь-якої пари адрес, пов'язаної з гібридною VPN, менеджер VPN повинен мати можливість розрізняти трафік між двома адресами та вважати його частиною безпечної VPN.

3.2 Характерні особливості VPN

Оскільки доступно так багато різних служб VPN, важко зрозуміти, яку з них вибрати. Хоча постачальники VPN мають веб-сайти, які допомагають підкреслити важливі функції, часто це більше, ніж те, що розкриває веб-сайт.

Немає єдиного найкращого способу використання VPN: це залежить від того, ким ви є і що хочете робити. Наприклад, наявність кількох серверів, розташованих по всьому світу, збільшує ймовірність того, що ви не зможете транслювати онлайн-фільми та телевізійні шоу, як Netflix USA. Однак це відбувається за рахунок зниження безпеки, оскільки ваш Інтернет-провайдер має більше серверів, які виділяють для безпеки.

1) Розташування сервера.

VPN охоплює інформацію користувача, шифруючи її через тунель, створений між пристроєм користувача та веб-сайтом VPN. Після цього користувач отримує IP-адресу веб-сервера а не свою фактичну адресу, що призводить до переваги VPN: користувач може виглядати в іншому місці, ніж він є насправді.

Це може мати кілька цілей, включаючи доступ до потокових сервісів, таких як Netflix, або магазинів, таких як Amazon, націлених на певну країну, в обхід так званого геоблокування.

Важливо пам'ятати, що будь-який ефективний постачальник має широке охоплення в багатьох країнах, що розширює ваші можливості. Це також є

перевагою для онлайн-сервісів, які намагаються запобігти блокуванню IP-адрес відомих серверів VPN. Що більша кількість варіантів у вас є в країні, то більша ймовірність того, що ви зможете споживати вміст.

Однак щодо вашої особистої конфіденційності ви можете цінувати якість більше, ніж кількість. Якщо провайдер VPN бере простір на сервері від третьої сторони, щоб надати вам послугу, це означає, що він повинен відмовитися від своїх даних цій третій стороні.

Ось чому провайдери VPN, як-от ProtonVPN, намагаються контролювати самі головні сервери, використовуючи повне шифрування диска та хостинг на голому металі. Незважаючи на вищу вартість, ви маєте більшу ймовірність зберегти конфіденційність своєї інформації, якщо натомість використовуєте власні сервери замість VPN.

2) Мобільні додатки

Будь-які VPN мають програмне забезпечення, яке клієнти використовують на своїх ПК. Однак справжня цінність VPN полягає в її підтримці мобільних пристроїв і безпеці доступу до публічної мережі Wi-Fi, коли ви не вдома.

Вибираючи VPN, переконайтеся, що він відповідає платформам, які ви використовуєте в мобільному пристрої. У багатьох провайдерів є програми, які дозволяють користуватися Інтернетом у дорозі, але вони також мають сторінки з інструкціями щодо налаштування мобільної віртуальної приватної мережі. У ExpressVPN є інструкції щодо налаштування посібників для використання з Windows Phone, Blackberry, електронними пристроями для читання, Linux та іншими платформами.

Золотим стандартом для будь-якої програми, пов’язаної з безпекою, наприклад VPN-клієнта, є відкритий вихідний код: це означає, що код є загальнодоступним і спільнота може перевіряти його для виявлення проблем із безпекою чи прогалин.

Якщо ваш провайдер VPN не має цієї опції, це не обов’язково означає, що ваша інформація в небезпеці. Це простіше перевірити. Зв’яжіться зі своїм постачальником послуг Інтернету та запитайте, чи підтримує він такі протоколи, як Wireguard або OpenVPN. Якщо це так, ви можете використовувати VPN-

клієнти з відкритим кодом, такі як Wireguard або OpenVPN, щоб підключитися до особистої VPN.

3) Інтегрований перемикач

Жодна служба VPN не є повністю безпечною, і вона може піддаватися витоку IP-адреси, яка розкриває вашу фактичну IP-адресу, коли ви в Інтернеті. Це більш імовірно, коли служба VPN зайнята.

Це не завжди відповідальність вашого інтернет-провайдера: якщо VPN-з'єднання втрачено з вашого боку без належних налаштувань, ваш пристрій повернеться до звичайного Інтернету. Що ще гірше, Інтернет-провайдер не завжди інформує вас про це, а це означає, що у вас є можливість отримати доступ до особистої інформації, яка є конфіденційною, не знаючи, що ви більше не захищені.

Відповіддю на цю проблему є комутатор VPN, який може спостерігати, коли з'єднання розривається, ваша справжня адреса буде виявлена. У цьому випадку комутатор заборонить передачу даних.

Загалом, як видно з назви, він розриває з'єднання, запобігаючи передачі незашифрованої інформації (і приховуючи ваш справжній IP).

Хоча не всі служби VPN мають можливість відмовитися, деякі мають. Він включений в програмне забезпечення для клієнтів цих сервісів. Знайдіть комбінований автоматичний вимикач VPN, який є частиною послуги, і переконайтеся, що ввімкнули його в налаштуваннях програми VPN; багато параметрів увімкнено за умовчанням.

Найефективніше зв'язатися зі своїм постачальником VPN, щоб дізнатися, чи ця послуга сумісна. Наприклад, клієнтська версія NordVPN для iOS має вбудований перемикач, який за замовчуванням увімкнено, це означає, що вам не потрібно його активувати.

Пам'ятайте, що якщо перемикач увімкнено, ви не зможете використовувати жодні інтернет-програми. Якщо ваш VPN-клієнт підтримує цю функцію, після активації комутатора переконайтеся, що він має атрибут «автоматичне підключення», це дозволить вам використовувати Інтернет одразу після ввімкнення пристрою.

4) Анонімні DNS-сервери

Розпізнавання DNS – це процес, який перетворює адресу, яку ви вводите в адресний рядок веб-переглядача, наприклад TechRadar.com, на IP-адресу, яку використовує Всесвітня мережа для спрямування трафіку до користувача. Багато користувачів за умовчанням встановлюють роздільну здатність DNS через свого Інтернет-провайдера, хоча це можна легко змінити.

Звичайно, під час використання VPN конфіденційність є пріоритетом, тому ми хочемо, щоб конфігурація VPN захищала нас від потенційно проникливих очей постачальника послуг Інтернету (ISP).

Незважаючи на те, що DNS-адреса Google часто використовується через її швидкість, це не чудовий варіант з точки зору конфіденційності. Натомість існують служби DNS, призначені для забезпечення анонімності, наприклад FreeDNS або DNSWatch, ваш постачальник послуг VPN повинен використовувати власну анонімну DNS, щоб ефективніше зберегти вашу конфіденційність.

Хоча кожен поважний провайдер VPN робить це, є багато інших, які можуть захистити ваше з’єднання, дозволяючи вашому провайдеру запитувати DNS на своїх власних серверах. Це означає, що будь-хто, хто має дозвіл переглядати записи вашого провайдера, може спостерігати, які веб-сайти ви відвідуєте, це називається витоком DNS.

Аби не допустити цього, спочатку підключіться до вибраного вами постачальника VPN. Потім відкрийте веб-браузер і відвідайте веб-сайт тестування на витік DNS, наприклад IP Leak. Це продемонструє вашу IP-адресу та DNS-сервери в Інтернеті: вони мають відповідати даним вашого постачальника VPN, а не вашого особистого постачальника послуг Інтернету.

5) Відсутність офіційної політики логування.

Служби VPN мають інші правила щодо входу. Наприклад, деякі VPN мають можливість зберігати онлайн-активність протягом періоду часу, який може тривати місяці, потім ці дані передаються органам влади, якщо вони про це запитують.

Вам потрібна VPN із політикою «без журналу», але будьте обережні щодо деяких постачальників, які стверджують, що пропонують такий тип політики,

хоча насправді вони можуть зберігати дані про сеанси (наприклад, файли журналів).

Корисно детально прочитати політику конфіденційності постачальника VPN і переконатися, що немає прихованих небезпек. Крім того, важливо звернути увагу на найбільш персоналізовані доступні VPN.

Варто пам’ятати, що золотим стандартом для будь-якого провайдера VPN, який стверджує, що не має журналів, є той, який регулярно перевіряється третьою стороною, якій довіряють, щоб перевірити легітимність своїх заяв. Наприклад, ExpressVPN і NordVPN регулярно перевіряють сервери, щоб переконатися, що на них не зберігається особиста інформація.

6) Підтримка маршрутизатора

Замість встановлення VPN на кожному окремому пристрої інша стратегія полягає в тому, щоб просто встановити VPN на маршрутизатор вашої домашньої мережі, і тоді кожен пристрій, підключений до мережі, матиме захист від VPN.

Хоча ця стратегія зазвичай є кращою, вона потребує двох компонентів: сумісного комп’ютера та служби VPN, яка її підтримує.

Ви можете створити VPN на своєму маршрутизаторі як проміжну форму мережі. Після встановлення конфігурації вам не доведеться встановлювати спеціальне програмне забезпечення на окремих пристроях, щоб використовувати VPN: ви можете просто підключити їх до мережі Wi-Fi маршрутизатора.

Крім того, це чудовий спосіб обійти обмеження певної VPN: наприклад, NordVPN забороняє використовувати певну кількість пристроїв одночасно. Однак якщо у вас є маршрутизатор із підтримкою VPN, він вважатиметься одним пристроєм незалежно від кількості інших пристроїв, підключених через бездротове з’єднання.

З міркувань безпеки спробуйте знайти маршрутизатор із загальнодоступною конфігурацією прошивки, наприклад DD-WRT. Окрім надання засобів доступу до VPN, спільнота розробників програмного забезпечення часто може перевірити код на наявність помилок.

7) Підтримка OpenVPN

Незважаючи на те, що всі VPN захищають вашу конфіденційність, створюючи зашифрований перехід між клієнтом і сервером VPN, існують численні протоколи, які сприяють цьому.

Чим більше протоколів має VPN, тим краще, але вам особливо потрібна служба, яка підтримує протокол OpenVPN.

Це один із найпоширеніших протоколів для VPN, він вважається дуже безпечним, і зазвичай ваша власна VPN матиме параметри як для TCP, так і для UDP.

Якщо ваш інтернет-провайдер підтримує OpenVPN, ви можете використовувати його функції за допомогою клієнтів із відкритим кодом, таких як OpenVPN connect. Ви також можете підключитися до служби VPN через бездротовий маршрутизатор DD-WRT.

Якщо VPN має додаткові протоколи, окрім OpenVPN, як-от ExpressVPN Lightway або «Nordlynx» NordVPN, не обов'язково викликати підозру. Більш сучасні протоколи мають специфіку. Наприклад, Wireguard зазвичай швидше, ніж OpenVPN. Вас має турбувати поведінка постачальника VPN, лише якщо він наполягає на використанні свого протоколу, не пропонуючи альтернативу під назвою OpenVPN.

Під час створення конфігурації OpenVPN ваш постачальник послуг Інтернету повинен буде надати вам файли для конфігурації (OpenVPN). Вам також доведеться імпортувати файли конфігурації для кожного сервера, якщо ваш постачальник послуг Інтернету не пропонує інший метод, наприклад, надаючи «OpenVPN» як параметр підключення в програмному забезпеченні клієнта.

8) Співвідношення ціни та якості

Це може здатися очевидним, але сюди додана ця інформація, тому що важливо розуміти, що з мережами VPN пов'язано багато різних планів і цін.

Зазвичай ви матимете набагато нижчий тариф, якщо зареєструєтеся принаймні на рік, а деякі постачальники запропонують вам справді вигідні пропозиції.

Крім того, пам'ятайте, що іноді в найпростіших планах відсутній повний набір функцій, і ви можете втратити щось корисне (наприклад, власний протокол,

який уникає виявлення VPN-з’єднання, цей протокол дозволяє обійти блокування або обмеження).

Ви також повинні переконатися, що обраний вами провайдер VPN підходить для того, що ви хочете робити в Інтернеті. Наприклад, непрактично платити за річну передплату постачальнику, який пропонує телебачення, лише для того, щоб виявити, що веб-сайт потокового передавання відключив усі його сервери.

Усі законні постачальники VPN пропонують 30-денну безкоштовну пробну версію або місячну підписку. Скористайтеся цією можливістю, щоб спробувати послугу протягом кількох тижнів і перевірити, чи підходить вона вам.

Ми вже обговорювали ризики нібито безкоштовних VPN. Зрештою, будьте обережні, вони повинні заробляти гроші будь-яким способом, і цілком ймовірно, що вони роблять це, ділячись вашою особистою інформацією третім особам.

Навіть чесні «безкоштовні» служби VPN можуть зменшити обсяг трафіку, який ви завантажуєте, або заблокувати певні типи трафіку, наприклад потокове відео. Через це ваші дані знаходяться під загрозою, коли ви користуєтеся послугою, оскільки вам потрібно контролювати з’єднання.

3.3 Рекомендації що до захисту VPN від несанкціонованого доступу

Захист даних сьогодні є одним із головних обов’язків організацій у всьому світі. Інформаційна безпека в першу чергу стосується запобігання несанкціонованому доступу до інформації. Саме це забезпечує захист даних.

Очікується, що до 2025 року послуги, пов’язані з безпекою, як-от управління інформацією про безпеку та подіями (SIEM), становитимуть майже половину всіх витрат на кібербезпеку. Це означає, що компанії все більше піклуються про кібербезпеку та впроваджують більш просунуті та надійні методи запобігання несанкціонованому доступу хакерів або зловмисників.

Кілька важливих принципів безпеки, яких має дотримуватися кожна компанія, щоб захистити свої дані від зловмисного доступу. Ось кілька порад, які можуть допомогти вам уникнути несанкціонованого доступу до ваших даних.

1) Завжди перевіряти останні оновлення.

Першим кроком для будь-якої організації, яка бажає запобігти несанкціонованому доступу до даних, є збереження всіх прогалин у безпеці на поточну дату.

Патчі безпеки виправляють вразливості програмного забезпечення, операційних систем, драйверів тощо, якими можуть скористатися зловмисники, щоб отримати доступ до ваших пристроїв і даних. Патчі безпеки для таких операційних систем, як Windows, Linux, Android, iOS тощо, надзвичайно важливі, оскільки вразливість операційної системи може мати серйозні наслідки. Крім того, оновлюйте драйвери та програмне забезпечення, коли з'являться нові виправлення.

Вірус WannaCry пошкодив понад 400 000 комп'ютерних систем у 150 країнах і став однією з найгірших атак за останні роки. Він атакує вразливість у протоколі Windows SMB V1 (Server Message Block) і запускається, використовуючи вразливість EternalBlue.

Використовуючи оновлені патчі безпеки, користувачі можуть запобігти несанкціонованому доступу до своїх систем для здійснення атак.

Дуже важливо переконатися, що ви інсталюєте найновіші виправлення безпеки та оновлення для свого комп'ютера та іншого програмного забезпечення, це захистить його від кібер-вторгнення. Ви також можете ввімкнути автоматичні оновлення, щоб система автоматично встановлювала їх щоразу, коли виходить патч або оновлення безпеки.

Завжди залишаючись готовими та актуальними, ви можете запобігти неавторизованому доступу до своїх даних.

2) Швидко виявляти вторгнення та реагувати на них.

Звичайно, ви хочете залишатися спостережливими та запобіжними, щоб запобігти несанкціонованому доступу хакерів до вашої інформації.

Але що, якщо вам не вистачає здатності сприймати вторгнення?

Як рухатися вперед?

Чим швидше ви розпізнаєте вторгнення, тим швидше зможете його вирішити. Профілактика має вирішальне значення, але опитування про дії

користувачів, спроби входу, журнали та інші дії також можуть надати інформацію про безпеку вашої системи.

Існує кілька методів швидкого виявлення вторгнень і реагування на них:

IDS/IPS (система виявлення вторгнень/система запобігання вторгненням)

IDS використовує відомі симптоми вторгнення або моделі поведінки, щоб оцінити інтернет-трафік на наявність аномальної поведінки.

Виявлення вторгнення — це спостереження та аналіз активності вашої мережі або системи, щоб визначити, чи існує загроза вторгнення, наприклад потенційне порушення вашої політики безпеки або загроза вашій мережі.

І навпаки, SPP служить доповненням до IDS, активно досліджуючи трафік, що надходить до системи, для виявлення зловмисних запитів. SPP запобігає атакам, запобігаючи неавторизованим або шкідливим IP-адресам, запобігаючи зловмисним даним та інформуючи персонал служби безпеки про можливі атаки.

SIEPM (Планувальник заходів безпеки)

Менеджер подій безпеки (SIEM) — це метод управління безпекою, який передбачає спостереження за діями в інформаційній системі. Програмне забезпечення SIEM отримує та аналізує дані журналу, згенеровані технологічною інфраструктурою компанії, включаючи програми, хости, мережі та пристрої безпеки.

Потім програмне забезпечення визначає та класифікує інциденти та події та оцінює їх. перш за все, є дві основні цілі SIEM:

Спостерігайте та повідомляйте про випадки й інциденти, пов’язані з безпекою, зокрема про невдалі й успішні входи, зловмисне програмне забезпечення чи будь-яку іншу підозрілу активність.

Повідомте персонал служби безпеки, якщо буде помічена будь-яка підозріла поведінка, яка свідчить про загрозу безпеці.

Застосовуйте аналіз поведінки та подій (UEBA) для реалізації поведінки користувачів.

Щоб запобігти несанкціонованому доступу до даних, ви повинні володіти аналітичною грою.

Поведінка користувачів і аналітика подій допомагають виявити будь-яку незвичну поведінку або випадки відхилення від типової поведінки користувачів. Наприклад, якщо користувач зазвичай завантажує 10 Мб файлів щодня, але зараз він завантажує гігабайти файлів, система розпізнає це як аномалію; адміністратор буде негайно повідомлений.

Поведінка користувачів і аналіз подій використовують алгоритми, статистичні процедури та машинне навчання для виявлення випадків відхилення від встановлених шаблонів, ця інформація відображається у формі аномальної поведінки та потенційної загрози, яку вона становить. Це дозволить вам отримувати сповіщення про несанкціонований доступ до даних.

Цей тип аналізу зосереджується як на користувачах, так і на організаціях у вашій системі, особливо на тих, хто може скористатися своїми привілеями для здійснення намічених атак або шахрайства.

3) Реалізація принципу найменших привілеїв (мінімізація доступу до інформації)

Концепція найменших привілеїв — це практика надання обліковим записам, користувачам і процесам обмеженого доступу до ресурсів, які є специфічними для їхніх посадових інструкцій і необхідні для виконання повсякденних завдань. У Глобальному звіті про захист даних за 2019 рік зазначено, що типовий працівник має доступ до 17 мільйонів документів.

Реалізація концепції найменших привілеїв може допомогти вам захистити ваші дані від несанкціонованого доступу. Принцип найменших привілеїв (POLP) вимагає, щоб користувачі мали найменшу кількість привілеїв для доступу до ресурсів, які доступні лише користувачам, які мають відповідні привілеї. Це зменшує ймовірність використання неавторизованих користувачів, програм або систем без негативного впливу на загальну продуктивність організації.

Хоча мінімальні привілеї забезпечують найбільший рівень повноважень над ресурсами, необхідними для поточної роботи, вони також сприяють більш ефективним методам безпеки та зменшують ймовірність того, що ваша організація стане жертвою кібератаки.

4) Використовуйте багатофакторну автентифікацію

Для компаній надзвичайно важливо використовувати надійні методи автентифікації, які включають надійне застосування політики паролів на додаток до багатофакторної автентифікації. Це може значно зменшити доступ неавторизованих осіб до даних.

Як відомо, багатофакторна автентифікація вимагає від користувача надання кількох фрагментів інформації, які система оцінить, перш ніж хтось зможе отримати доступ до мережі. Це ускладнює хакерам зламати облікові записи користувачів, оскільки для цього потрібно більше зусиль, ніж просто зламати пароль.

Для багатофакторної автентифікації може використовуватися одноразовий пароль, який надсилається за допомогою зовнішнього каналу зв'язку, як-от автоматичний телефонний дзвінок або текстове повідомлення на авторизований пристрій користувача, таємне запитання, на яке користувач відповідає, або біометрична автентифікація. Хоча це ускладнює автентифікацію, воно забезпечує більш потужний рівень безпеки та змушує зловмисника не лише зламати пароль, але й відхилитися від другого фактора. Це ускладнює зловмисникам зламати автентифікацію.

Хоча багатофакторна автентифікація безумовно використовується, ви також можете використовувати фрази замість паролів.

5) Застосуйте білі списки IP-адрес

Ще один спосіб запобігання несанкціонованому доступу до даних – це внесення IP-адрес авторизованих користувачів до білого списку.

Білі списки IP полегшують обмеження та контроль доступу лише для авторизованих користувачів. Це полегшує створення списку авторизованих і надійних IP-адрес, з яких користувачі можуть отримати доступ до вашої мережі. Як правило, корпорація використовує Інтернет через певний набір IP-адрес, тому вона може створити список усіх дозволених IP-адрес.

За допомогою білого списку IP-адрес ви можете дозволити лише авторизованим користувачам із певного діапазону IP-адрес отримувати доступ до ресурсів у мережі, таких як URL-адреси, програми, електронні листи тощо.

Якщо хтось із невідомої IP-адреси спробує отримати доступ до вашої мережі, йому буде відмовлено в доступі. Крім того, білі списки IP-адрес дозволяють організаціям захистити віддалений доступ до Інтернету, включаючи протокол Bring Your Own Device (BYOD), який дозволяє співробітникам використовувати власні пристрої на роботі.

6) Шифрування мережевих даних у системі.

Шифруючи мережевий трафік, ви можете гарантувати, що він не буде контролюватися зловмисником, який може стежити за трафіком.

Однак трафік між серверами та всередині центрів обробки даних часто не має криптографічного підпису. Якщо зловмисник отримує доступ до цієї мережі, він може спостерігати за даними, що передаються між серверами в кластері з кількох машин.

Щоб запобігти неавторизованому доступу до даних, організації все частіше перевіряють власний трафік у мережі з метою виявлення вторгнень. Компанії можуть зберігати копії мережевого трафіку протягом тривалого часу у своїх системах моніторингу.

Для всіх мереж надзвичайно важливо використовувати шифрування, якщо вони зберігають важливі дані. Це стосується як авторизованих користувачів, яким надано доступ до системи через зовнішні засоби, так і внутрішніх з'єднань між комп'ютерами в багатосерверній системі.

Ви можете використовувати рівень VPN між собою та системою або застосувати SSL/TLS для шифрування мережевого трафіку. Усередині системи зв'язок можна захистити за допомогою IPsec, SSL/TLS або іншої технології, пов'язаної з VPN.

7) Шифрування даних під час неактивного стану

Шифрування даних у спокої використовується для безпечного зберігання даних, а не в оригінальній формі. Коли дані записуються на диск, вони криптографічно підписуються за допомогою секретного набору ключів, які знають лише авторизовані адміністратори.

Доступ до цих приватних ключів обмежений і заздалегідь визначений, це робиться для того, щоб запобігти неавторизованим користувачам отримати

доступ і використовувати зашифровану інформацію. Цей підхід захищає дані від хижаків, які можуть спробувати отримати віддалений доступ до системи, і зберігає дані від пошкодження.

Це вигідний спосіб захисту ваших даних від будь-кого, хто вживе несанкціонованих дій. Шифрування в стані спокою передбачає перевірку всіх місць, де зберігаються дані, включно з тимчасовими серверами або пристроями зберігання, призначеними для кешування.

8) Забезпечте захист від зловмисного програмного забезпечення/білого списку додатків

Зловмисне ПЗ – це програмне забезпечення, призначене для проникнення або атаки на комп'ютери без дозволу чи згоди користувача. Троянські коні, комп'ютерні віруси, хробаки, відлякувальні та шпигунські програми — лише деякі з найпоширеніших типів шкідливого програмного забезпечення. Вони можуть міститися в електронних листах і на веб-сайтах або бути прихованими у вкладеннях, відео та фотографіях.

Цей тип шкідливого програмного забезпечення легко зламати та надає хакерам несанкціонований доступ до інформації.

Захист від зловмисного програмного забезпечення має вирішальне значення, оскільки він є основою безпеки ваших пристроїв. Використовуйте ефективне антивірусне програмне забезпечення, не клацайте підозрілі електронні листи та не отримуйте вкладення з невідомих джерел і завжди перевіряйте свій пристрій на наявність шкідливих програм.

Іншим варіантом контролю є використання білих списків програм. Він здатний запобігти несанкціонованому доступу до інформації.

Цей метод залишає вам відомі та надійні програми, які можна інсталювати на ваших комп'ютерах, тоді як усі інші програми відхиляються. Навіть якщо хтось отримає неавторизований доступ, він не зможе запустити зловмисне програмне забезпечення на ваших комп'ютерах, якщо програмі не надано спеціальний дозвіл.

9) Слідкуйте за ризиками та регулюйте їх

Ризиком може бути будь-що, що може негативно вплинути на ефективність, бюджет або графік проекту. Якщо ці небезпеки стають серйозними, вони перетворюються на кібератаки, яких слід уникати, щоб уникнути атак кіберзлочинців.

Вкрай важливо, щоб організації визнавали, класифікували, зосереджували та пом’якшували ризики ефективним і своєчасним способом. Визнаючи ризики до того, як вони стануть проблемами, ви можете запобігти цьому. Крім того, повинен бути створений план по негайному усунення небезпек.

ВИСНОВКИ

На сьогоднішній день віртуальні приватні мережі VPN є однією з найбільш затребуваних областю кібербезпеки. Відомі методи та протоколи мають не багато недоліків і показують достатньо високу ефективність у комбінації один з одним. Завдяки даній роботі було проаналізовано та встановлено особливості віртуальних приватних мереж, які показали, що попит користування віртуальними приватними мережами неухильно росте, кількість підключених пристроїв значно зросла, що спонукає до удосконалення та розробки нових методів та протоколів забезпечення безпеки у мережі.

Розглянувши літературні джерала було охарактеризовано загальні методи та алгоритми безпеки віртуальних приватних мереж, встановленні переваги та недоліки конкретних підходів, що дозволило сконцентуватися у подальшій роботі над найбільш поширеними та дієвих методами.

Описані відомі алгоритми для працездатності та збільшення безпеки віртуальних приватних мереж, показали великий засобів для боротьби із несанкціонованим доступом, які реалізовані на різних підходах для їх запобіганнях.

Враховуючи складність роботи алгоритмів безпеки віртуальних приватних мереж було встановлено вимоги до систем вцілому, їхнє завдання та структурні компоненти, описані особливості до таких систем, встановлено нормативи, правила та постулати, яких вона має дотримуватися щоб забезпечити якумога вищий рівень безпеки мережі та її користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Securing Remote Access in Palo Alto Networks.Practical techniques to enable and protect remote users, improve your security posture, and troubleshoot next-generation firewalls, by Tom Piens (Author),Packt Publishing, Limited, 2021,336 pages

2. VPNs Illustrated: Tunnels, VPNs, and IPsec 1st Edition, Kindle Edition by Jon C. Snader,by Jon C. Snader (Author),Pearson Education,482 pages

3. Into The VPN Tunnel: An eye-opening guide that emphasizes the value of Virtual Private Networks to protect your internet privacy, by Peter Merchant,July 12, 2017,17 pages

4. Firewall Policies and VPN Configurations 1st Edition, by Syngress (Author), Dale Liu (Author), Stephanie Miller (Author), Mark Lucas (Author), Abhishek Singh (Author),Syngress,October 5, 2006,657 pages

5. Network & Internet Technology & Design Kindle Edition by Dileep Keshava Narayana (Author), 9781731515735, November 17, 2018, 431 pages

6. VPNs and NAT for Cisco Networks (Cisco CCIE Routing and Switching v5.0 Book 3) Kindle Edition by Stuart Fordham (Author), CreateSpace Independent Publishing Platform May 28, 2015, 258 pages

7. NIST SP 800-113 Guide to SSL VPNs by National Institute of Standards and Technology (Author), CreateSpace Independent Publishing Platform July 31, 2008, 84 pages

8. How To Install A VPN by Marquis Shamsid-Deen (Author), B0BRM7TQQ4, January 30, 2023, 15 pages

9. The Purpose of a VPN: The main purpose of a VPN is to hide your online activity by ABHI RAJ (Author), B09WQRV63F, March 28 2022, 11 pages

10. What is a VPN? Paul Ferguson,Geoff Huston April 1998 Revision 1. URL: https://www.potaroo.net/papers/vpn.pdf

11. Proper Virtual Private Network (VPN) Solution [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1109/NGMAST.2008.18.

12. Virtual Private Network (VPN) [Електронний ресурс]. Режим доступу: https://www.academia.edu/1343134/Virtual_Private_Network_VPN_

A. Strom and A. Robertson, "The MITRE Corporation," 3 March 2020. [Електронний ресурс]. Режим доступу: https://medium.com/MITRE-attack/2020-attack-roadmap-4820d30b38ba.

13. Virtual Private Networks.Raj Jain, Washington University in Saint Louis,Saint Louis, MO 63130 [Електронний ресурс]. Режим доступу: https://www.cse.wustl.edu/~jain/cse571-09/ftp/l_17vpn.pdf

14. Virtual Private Network (VPN) Profile image of Robin GuptaRobin Gupta [Електронний ресурс]. Режим доступу: https://www.academia.edu/38802764/Virtual_Private_Network_VPN

15. IPSec, VPN, and Firewall Concepts [Електронний ресурс]. Режим доступу: https://www.cs.unh.edu/~it666/reading_list/Networking/firewall_concept_terms.pdf

16. Long M, Peng F, Li HY (2018) Separable reversible data hiding and encryption for HEVC video. J Real-Time Image Process 14(1):171–182

17. Guide to IPsec VPNs [Електронний ресурс]. Режим доступу: https://csrc.nist.rip/library/alt-SP800-77.pdf

18. Cisco IOS VPN Configuration Guide [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg.pdf

19. VPN SECURITY.February 2008 [Електронний ресурс]. Режим доступу: https://books-library.net/files/download-pdf-ebooks.org-1489587735Qk6Y7.pdf

20. VIRTUAL PRIVATE NETWORK(VPNS) [Електронний ресурс]. Режим доступу:https://www.idconline.com/technical_references/pdfs/data_communications/Virtual_Private_Network_VPNs.pdf

21. THE REERADIUS TECHNICAL GUIDE by Networkradius. https://networkradius.com/doc/FreeRADIUS-Technical-Guide.pdf

22. (Oreilly) Radius airo Seas, https://www.academia.edu/29281736

23. Design of RADIUS server on server network internet faculty of computer science universoityMuhannadyahMetro https://www.researchgate.net/publication/364173711_DESIGN_OF_RADIUS_SERVE

R_ON_SERVER_NETWORK_INTERNET_FACULTY_OF_COMPUTER_SCIENCE_UNIVERSITY_MUHAMMADIYAH_METRO

24.Local RADIUS Server.Feature Overview and Configuration Guide https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/local_radius_server_feature_overview_guide.pdf

25.TACACS+ Configuration Guide by Cisco https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book.pdf

26.tacacs.administration.https://www.cisco.com/en/US/docs/ios/security/command/reference/sec_t1.pdf

27.The Advantages of TACACS+ for dministrator Authentication [Електронний ресурс]. – Режим доступу: https://tacacs.net/docs/TACACS_Advantages.pdf

28.TACACS+.University of Oregon [Електронний ресурс]. – Режим доступу: https:/nsrc.org/workshops/2013/pacnog14-sns/raw-attachment/wiki/Agenda/tacacs+.pdf

29.Document history for the Site-to-Site VPN User Guide https://docs.aws.amazon.com/vpn/latest/s2svpn/WhatsNew.html

30.National Security Agency | Cybersecurity Information configuring IPsec Virtual Private Networks October 2020 ver. 1.2

31.Жилич В.А., Цаволик Т.Г. Механізми контролю доступу та авторизації у вітруальних приватних мережах (VPN). Збірник матеріалів проблемно-наукової міжгалузевої конференції "Автоматизація та комп'ютерно-інтегровані технології" (АКІТ-2023), Тернопіль, 2023. С. 115 - 118.

32. Жилич В.А., Цаволик Т.Г. Конфігурації VPN для безпечної передачі даних. Збірник матеріалів науково-практичного симпозіуму "Захист інформації", Тернопіль, 2023. С. 72 - 75.

ДОДАТОК А Копії публікацій результатів дослідження

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2023)

23—25 лютого 2023 року

Тернопіль

Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2023), Тернопіль, 2023. -178 с.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:
Західноукраїнський національний університет
кафедра спеціалізованих комп'ютерних систем
вул. Олени Теліги 8, м. Тернопіль 46003

Контактний телефон
тел. (0352) 50-17-87

Лущевський Б.Л.
АЛГОРИТМИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ АТАК НА МЕРЕЖЕВУ ІНФРАСТРУКТУРУ 109

Жмурко І.І.
АНАЛІЗ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ЗАХИСТУ ІНТЕРНЕТ-РЕЧЕЙ 112

Жилич В.А., Цаволик Т.Г.
МЕХАНІЗМИ КОНТРОЛЮ ДОСТУПУ ТА АВТОРИЗАЦІЇ У ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ (VPN) 115

Волянський А.І., Абизов І.С., Павлюк Р.Я.
ДОСЛІДЖЕННЯ НАЛАШТУВАННЯ СИСТЕМИ МОНІТОРИНГУ SURICATA 118

Бараннік Б.О., Цаволик Т.Г.
АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ КРИПТОВАЛЮТИ 123

Доліновський Р. М.
ВРАЗЛИВОСТІ XSS: ВАЛІДАЦІЯ ВВЕДЕНИХ ДАНИХ 127

Присяжнюк А.Ю., Павлюс В.П., Кузик В.М.
РОЗРОБКА КРИПТОГРАФІЧНОЇ БІБЛІОТЕКИ НА МОВІ ПРОГРАМУВАННЯ PYTHON ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБМІНУ ДАНИМИ 130

Гнатик А.І., Посвятовська О.Б., Гавришків Н.Г.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ VPN ДЛЯ ВСТАНОВЛЕННЯ БЕЗПЕЧНОГО ЗЄДНАННЯ 133

Максимчук Р.О., Цаволик Т.Г.
АНАЛІЗ ТА ОЦІНКА ПОШИРЕНИХ ПРОГРАМ ПО ЗБОРУ ІНФОРМАЦІЇ ТРАНЗАКЦІЙ З КРИПТОВАЛЮТАМИ 137

Баранюк В.В., Николишин В.І., Лизун Я.І
НАЛАШТУВАННЯ СИСТЕМ ШИРОКОСМУГОВОГОЗВ'ЯЗКУ WI-FI І WIMAX 139

Колінець Р.Б., Цаволик Т.Г.
АНАЛІЗ ПОШИРЕНИХ ВРАЗЛИВОСТЕЙ У ВЕБ-ЗАСТОСУНКАХ 143

Дживра П.І., Івасьєв С.В.
ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ MIKROTIK 146

Духницький Р.В., Стефупак Н.А.
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ ЗА ДОПОМОГОЮ DLP СИСТЕМ 150

Гамера М.А.
РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ СЕРВЕРІВ З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON 154

Коршшко Д.Г., Антонюк І.В.
АНАЛІЗ МЕРЕЖЕВИХ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ WIRESHARK 157

УДК 004.738.5

Жилич В.А.[1], *Цаволик Т.Г.*[1]

[1]*Західноукраїнський національний університет*

МЕХАНІЗМИ КОНТРОЛЮ ДОСТУПУ ТА АВТОРИЗАЦІЇ У ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖАХ

Вступ.Віртуальні приватні мережі (VPN) стали невід'ємною складовою сучасної мережевої інфраструктури. VPN забезпечують безпечне та конфіденційне з'єднання між віддаленими мережами або користувачами через публічну інтернет-мережу.

Зважаючи на значну кількість конфіденційних даних, які передаються через VPN, необхідні надійні механізми контролю доступу та авторизації, які забезпечать захист мережі від несанкціонованого доступу та недозволених дій.

Мета: Дослідження механізмів контролю доступу та авторизації в віртуальних приватних мережах та їх ролі у забезпеченні безпеки і конфіденційності мережевих комунікацій.

1. Аутентифікація та авторизація доступу користувачів

Цей механізм перевіряє ідентичність користувача, який намагається отримати доступ до VPN. Аутентифікація може базуватися на різних факторах, таких як ім'я користувача та пароль, сертифікати, біометричні дані тощо. Це дозволяє впевнитись, що тільки дійсні користувачі мають право підключатися до VPN (Таблиця 1) [1, 4].

Таблиця 1 - Способи аутентифікації користувачів у VPN

Метод	Опис	Переваги	Недоліки
1	2	3	4
Ідентифікація на основі пароля	Цей метод є найпоширенішим і простим у використанні. Користувачі вводять свої ідентифікаційні дані (логін та пароль), які перевіряються на вірність сервером VPN перед наданням доступу	Простота використання та підтримка багатьох пристроїв	Вразливість до атак, слабка безпека
Аутентифікація на основі сертифікатів	У цьому методі кожен користувач має власний цифровий сертифікат, який видається центром сертифікації. Користувачі презентують свій сертифікат при підключенні до VPN, і сервер перевіряє його валідність. Цей метод забезпечує більшу безпеку, оскільки пароль не передається по мережі	Висока безпека, важко підробити	Втрата або крадіжка, додаткові витрати на фізичні носії

Аутентифікація на основі інтеграції з існуючою інфраструктурою	В деяких випадках VPN може використовувати існуючу інфраструктуру аутентифікації, таку як сервери доменів або служби каталогів, для перевірки ідентичності користувачів	Централізоване управління, одна точка входу	Складність налаштування, залежність від існуючої інфраструктури
Аутентифікація на основі двофакторної перевірки	Цей метод вимагає від користувачів введення не тільки логіна та пароля, але й додаткового елемента ідентифікації, наприклад, одноразового коду, який надсилається на мобільний пристрій користувача. Це робить аутентифікацію більш надійною, оскільки зловмисникам важко отримати обидва фактори ідентифікації	Вищий рівень безпеки, захист від втрат пароля	Додаткові кроки, проблеми із сумісністю

Авторизація доступу у VPN відбувається після успішної аутентифікації користувача і визначає, які ресурси та служби він має право використовувати в межах VPN [2, 3]. Для авторизації доступу розглянемо наступні методи: Ролева базована авторизація (Role-Based Access Control, RBAC). У цьому підході користувачам призначаються ролі, які визначають їх права доступу до різних ресурсів мережі. Наприклад, можуть бути визначені ролі адміністратора, користувача з обмеженими правами, гостя тощо. Кожній ролі надається відповідний набір дозволених дій та доступу до ресурсів; Авторизація на основі групових політик. Цей підхід полягає в тому, що користувачам призначаються групові політики, які визначають їх доступ до ресурсів залежно від їхньої членості у певній групі. Наприклад, можуть бути створені групові політики для відділів організації, і користувачі, які належать до цих відділів, отримують відповідні права доступу; Правила доступу на основі IP-адрес. У цьому випадку можуть бути встановлені правила доступу до ресурсів, що базуються на IP-адресах користувачів. Наприклад, може бути обмежений доступ до певного сервера або мережного сегмента лише з деяких визначених IP-адрес; Авторизація на основі атрибутів користувача. У цьому підході доступ користувача до ресурсів визначається на підставі його атрибутів, таких як роль, відділ, рівень дозволу тощо. Наприклад, атрибути користувача можуть бути отримані з існуючої інфраструктури, такої як сервери доменів або служби каталогів.

2. Керування правами доступу

Керування правами доступу у VPN включає в себе набір політик та механізмів, які визначають, які ресурси можуть бути доступні користувачам і які дії вони можуть виконувати. Основна мета полягає в обмеженні доступу до ресурсів лише для авторизованих користувачів з необхідними правами.

Основні компоненти керування правами доступу у VPN:

1. Ролі та привілеї: Встановлюються різні ролі для користувачів в межах VPN, такі як адміністратор, користувач з обмеженими правами, гість і т.д. Кожна роль має свій набір привілеїв, які визначають дозволені дії та рівень доступу до ресурсів. Це дозволяє гнучко налаштовувати доступ для різних категорій користувачів.

2. Політики керування доступом (Access Control Policies): Встановлюються правила та обмеження для кожної ролі або групи користувачів. Ці політики визначають, які ресурси, такі як файли, папки, додатки, сервери і т.д., можуть бути доступні для кожної ролі. Такі політики можуть базуватися на IP-адресах, портах, протоколах, групах користувачів, часових інтервалах і багатьох інших параметрах.

3. VPN Firewall: Встановлення брандмауера на VPN-сервері або інших вузлах мережі дозволяє контролювати трафік, що входить та виходить з VPN. Брандмауер може блокувати небажаний трафік, реалізувати правила фільтрації пакетів і дозволяти доступ до ресурсів лише для визначених IP-адрес або портів.

4. Журналювання та аудит доступу: Для забезпечення безпеки і контролю доступу до ресурсів важливо вести журнал подій, що стосуються авторизації та доступу користувачів. Це дозволяє виявляти потенційні загрози та проводити аналіз безпеки.

5. Автоматичне управління: Деякі VPN-системи можуть мати механізми автоматичного управління правами доступу, такі як управління життєвим циклом користувача (наприклад, автоматичне призначення ролей та доступу при включенні до домену або групи користувачів), управління засобами аутентифікації (наприклад, автоматичне відкриття або блокування доступу на основі певних умов) та інші.

Висновок. Механізми контролю доступу та авторизації у віртуальних приватних мережах (VPN) відіграють ключову роль у забезпеченні безпеки та захищеності комунікацій. Вони гарантують, що лише автентифіковані та авторизовані користувачі мають доступ до мережі і її ресурсів. Загалом, механізми контролю доступу та авторизації в VPN виконують критичну роль у забезпеченні безпеки та захищеності мережевих комунікацій. Їх використання допомагає забезпечити віртуальну приватність, конфіденційність та інтегрітет переданих даних, а також контролювати доступ до мережевих ресурсів згідно з встановленими політиками та правами користувачів.

Перелік використаних джерел.

1. Сєдих, В. (2018). Віртуальні приватні мережі. Інформаційні технології у науці, освіті, виробництві: збірник тез І Всеукраїнської науково-практичної Інтернет-конференції здобувачів вищої освіти і молодих учених, м. Маріуполь, 26 квітня 2018 р./Маріупольський державний університет; уклад. Тимофєєва ІБ, Дяченко ОФ–Маріуполь: МДУ, 2018.–186 с., 168.

2. Капустін, М. О. Порівняльний аналіз протоколів віртуальних приватних мереж. 2023.

3. Ferguson, Paul, and Geoff Huston. "What is a VPN?." (1998): 01-22.

4. SINGH, Kuwar Kuldeep VV; GUPTA, Himanshu. A New Approach for the Security of VPN. In: Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies. 2016. p. 1-5.


Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»
2023

ГРОМАДСЬКЕ ОБЄДНАННЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2023
Тернопіль

У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. - 195 с.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадське об'єднання «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: entmkd.scs@gmail.com

ВСТУП

Даний збірник праць представляє результати науково-практичного симпозіуму "Захист інформації", що відбувся 30 листопада 2023 року в рамках Міжнародного дня захисту інформації. Обрання саме цієї дати для проведення заходу не є випадковим рішенням, оскільки вона має історичне значення.

У цей день 1988 року відбулася перша масова комп'ютерна епідемія, ініційована вірусом Morris Worm. Ця подія визначила новий етап в розвитку інформаційної безпеки, відкривши двері для вивчення та впровадження комплексного підходу до захисту інформації в умовах поширення вірусів через мережу Інтернет. Зазначений інцидент підкреслив необхідність та актуальність поглибленого розгляду питань інформаційної безпеки для ефективного захисту комп'ютерних систем у всесвітньому контексті.

Метою науково-практичного симпозіуму «Захист інформації» є не лише відзначити важливі історичні моменти у сфері комп'ютерної безпеки, але й у спонукати бути уважними та відповідальними у обробці особистих даних у віртуальному просторі. Закликати усіх захищати свою інформацію, підтримувати конфіденційність та сприяти створенню безпечного цифрового оточення для всіх користувачів. Захід спрямований на підвищення обізнаності та практичних навичок у сфері кібербезпеки.

Міжнародний День захисту інформації – це час для усвідомлення та об'єднання зусиль у вирішенні актуальних проблем сучасного світу.

Проведений захід присвячений тим, хто працює в сфері інформаційної безпеки, а також кожному, хто зберігає та обмінюється інформацією в цифровому форматі. Інтернет сьогодні став невід'ємною частиною нашого життя, але разом з цим зростає кількість кіберзлочинців, які використовують його для своїх цілей.

ЗМІСТ

АНТОНЮК О.О., КРУК О.В.
СТРУКТУРНА СХЕМА ФУНКЦІОНУВАННЯ ТА ІНТЕРФЕЙС СИСТЕМИ МОНІТОРИНГУ СТАНУ БАНКОМАТІВ..... 9

БАРАНЮК В.
МЕХАНІЗМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ШИРОКОСМУГОВОГО ЗВ'ЯЗКУ WI-FI І WIMAX..... 12

БОНДАРЬ І.В.
ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СТЕГАНОГРАФІЇ..... 15

ВАСИЛЕНКО Я.С.
КОНЦЕПЦІЯ ЗАХИСТУ В КІБЕРФІЗИЧНИХ СИСТЕМАХ..... 19

ВАСИЛЬКІВ В.О., БАСІСТИЙ В.П., СИДОРЧУК Р.В.
БЛОКЧЕЙН-ПЛАТФОРМА HYPERLEDGER FABRIC..... 22

ВІТВІЦЬКИЙ А.О., МАСЛОВСЬКИЙ С.В., БАЗИЛЕВСЬКИЙ Д.В.
ДОСЛІДЖЕННЯ СТІЙКОСТІ АЛГОРИТМІВ ШИФРУВАННЯ ДАНИХ... 25

ГЛАДЕНЬКИЙ П.
ПАКЕТИ МОБІЛЬНОЇ КРИПТОГРАФІЇ..... 29

ГОЛЕМБЙОВСЬКИЙ М.П., ГОЛЕМБЙОВСЬКИЙ П.М.
РЕАЛІЗАЦІЯ ТАБЛИЧНОГО ПЕРЕТВОРЕННЯ «ЧИТАННЯ ЗІ ЗМІЩЕННЯМ» ДЛЯ S-BOX НА МІКРОКОНТРОЛЕРАХ ATMEL..... 36

ГОЛОД Ю.В., ГАРМАТЮК В.Р., ВОЛОС І.П.
МЕРЕЖЕВІ АТАКИ НА ІНТЕРНЕТ-РЕЧЕЙ..... 39

ДАВЛЕТОВА А.Я., ЖМУРКО І.І.
ВИЯВЛЕННЯ ЗАГРОЗ ТА ЗАХИСТ ІНТЕРНЕТ РЕЧЕЙ..... 43

ДІЛАЙ С.Я., КОНДРАТЮК В.М., ПОМОГАЄВ С.О.
ВИКОРИСТАННЯ ДОКАЗІВ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ..... 48

ДМИТРІВ О., ХОМЯК Р.Д., СЛОБОДЯН В.Р.
СИСТЕМА КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ ДЕЦЕНТРАЛІЗОВАНОЇ МЕРЕЖІ..... 50

ДМИТРІВ Ю.
ОГЛЯД СУЧАСНИХ DDOS-АТАК, МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ.. 54

ДОЛЮК В.І.
МЕТОД ПОПЕРЕДЖЕННЯ ПОЛОМОК НА ЕЛЕВАТОРІ НА ОСНОВІ КОНТРОЛЮ ТЕМПЕРАТУРИ ПІДШИПНИКІВ..... 58

ДОРОШ В.Ю.
РОЗРОБЛЕННЯ МІНІМАЛЬНО РОБОЧОГО ПРОДУКТУ ГОЛОСОВОГО БОТУ IP-ТЕЛЕФОНІЇ..... 61

ДРАПАК В.І., ПИТЕЛЬ Р.О., РОМАНІВ А.М., ШАКОВ В.Ю.
ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОПРАЦЮВАННЯ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ..... 67

ЖИЛИЧ В.А.
КОНФІГУРАЦІЇ VPN ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ДАНИХ..... 72

ЗАЛУЖНИЙ В.В., МОЦНИЙ В.О.
МОДЕЛЮВАННЯ АТАКИ НА СИСТЕМУ «РОЗУМНИЙ БУДИНОК»..... 75

ІВАЩЕНКО М.В., КОНДРАТЮК В.М.
АЛГОРИТМ ВПРОВАДЖЕННЯ WAZUH У ХМАРНОМУ СЕРЕДОВИЩІ..... 78

ІГНАТЄВ І.В., КМЕТИК В.В.
РЕАГУВАННЯ НА АТАКУ ПРОГРАМ-ВИМАГАЧІВ..... 80

ЙОВБАК А.П., ОСАДЧУК О.Й., КАСЯНЧУК В.М.
МОДЕЛЮВАННЯ ПРОЦЕСУ АУТЕНТИФІКАЦІЇ ДЛЯ ДОСЛІДЖЕННЯ ЇЇ НАДІЙНОСТІ ТА БЕЗПЕКИ РЕЗУЛЬТАТІВ..... 82

КАВКА В.І.
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ..... 86

КЛІМОВ П.Я., ГАРТУНГ В.А.
СТЕГАНОГРАФІЯ В МЕРЕЖЕВИХ ПРОТОКОЛАХ: ОГЛЯД ТА НОВІ ПЕРСПЕКТИВИ ЗАХИСТУ ІНФОРМАЦІЇ..... 89

КОВАЛЬСЬКИЙ О.
ЕЛІПТИЧНІ КРИВІ НАД СКІНЧЕННИМИ ПОЛЯМИ..... 92

КОГУТ В.
ЗАХИСТ ВІД ПІДМІНИ DNS ДЛЯ ЗАПОБІГАННЯ АТАК..... 96

КОНДРАТЮК А.В., КМЕТИК В.В.
ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ..... 100

КОСТЮК О.В.
КЛЮЧОВІ АСПЕКТИ ТА ПЕРЕВАГИ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ ТА ЗБЕРЕЖЕННЯ ЖУРНАЛІВ РОБОТИ ІНФРАСТРУКТУРИ..... 102

КУРТЯК А.М., САВРІЙ С.В.
ФОРМУВАННЯ ВИМОГ ДО КРИПТОГРАФІЧНИХ АЛГОРИТМІВ НА ОСНОВІ ДИНАМІЧНОГО ХАОСУ..... 105

КУСМАРЦЕВ В.І.
НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО ВЕБ-РЕСУРСІВ ТА ЙОГО ОСОБЛИВОСТІ..... 108

ЛУЩЕВСЬКИЙ Б.,СИРОТЮК О.Б.
ІНДИКАТОРИ ЗАГРОЗ МЕРЕЖЕВІЙ ІНФРАСТРУКТУРІ, СТВОРЕНІ ШТУЧНИМ ІНТЕЛЕКТОМ..... 111

МАКАР М.О., БОХНАТ Н.І., КОЦІЙ О.В., СЛОБОДЯН В.Р., ХОМЯК Р.
МЕТОДИ ВИЯВЛЕННЯ ВБУДОВАНИХ ПОВДОМЛЕНЬ..... 114

МАЛЕНКО Д.А.
ОСНОВНИЙ ПРИНЦИП РОБОТИ NFC-ПРИСТРОЇВ ТА ЇХНЯ БЕЗПЕКА..... 118

МАРКІВ А.П., ГОНЧАРИК Г.Я., ТВЕРДУН Б.С..
СХЕМА АУТЕНТИФІКАЦІЇ, СТІЙКА ДО DDOS АТАК..... 121

МЕЛЬНИК А.І.
ІНОВАЦІЙНІ ПІДХОДИ ДО АВТОМАТИЗАЦІЇ ПРОЦЕСУ СТЕРЕЛІЗАЦІЇ У ХАРЧОВІЙ ПРОМИСЛОВОСТІ..... 124

МЕЛЬНИК П.
АСПЕКТИ БЕЗПЕКИ ОБРОБКИ ДАНИХ У ХМАРНИХ СХОВИЩАХ.... 127

МОТРОНЮК.Н.Б
АРХІТЕКТУРА ТА АЛГОРИТМ РОБОТИ ТЕЛЕГРАМ-БОТА..... 130

НЕМЕШ І.В., ДОДЬ О.А., ЛИСОБЕЙ Л.В.
МЕТОД ВИЗНАЧЕННЯ ЧАСУ ТА СЕРЕДНЬОГО ЧИСЛА ІТЕРАЦІЙ АПРОКСИМУЮЧОГО k-АРНОГО АЛГОРИТМУ ЕВКЛІДА..... 132

ПАСТУХ Т.І., ДЗІВАК О.А., ПОНЕДЄЛЬНІКОВ Г.М.
АВТЕНТИФІКАЦІЯ ТА ПЕРЕВІРКА ЦІЛІСНОСТІ ЗОБРАЖЕНЬ НА ОСНОВІ ХЕШУ..... 135

ПЕЛЕХ Т.В.
ПОБУДОВА МОДЕЛЕЙ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У СКЛАДІ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ... 138

ПОДЗВІННИЙ В.В.
СИСТЕМИ КАРДІОМОНІТОРИНГУ СПОРТСМЕНІВ..... 141

ПРАЧКОВСЬКИЙ І.П., ГРИЦЬКІВ А.В.
АКТУАЛЬНІСТЬ ТА ПРОБЛЕМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ.. 145

ПРИСЯЖНЮК А.
ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ КРИПТОБІБЛІОТЕКИ ДЛЯ БЕЗПЕЧНОГО ОБМІНУ ДАНИМИ..... 148

РАЇНЧУК В.В.
АЛГОРИТМ ВИКОНАННЯ SQL-ІН'ЄКЦІЙ..... 151

РУДЧЕНКО В., ХОМОЛЮК М.І., СЛОБОДЯН В.Р., ПАВЛОВСЬКИЙ С.М.
АЛГОРИМТ ВИДІЛЕННЯ ОЗНАК СИМВОЛІВ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ..... 155

РУДЧЕНКО М., ЯКУБЕЦЬ Ю.М., КОЦІЙ О.В., ПОЦІЛУЙКО М.Б., ГРИЦАЙ Н.М.
ПРОГРАМНА СИСТЕМА КРИПТОАНАЛІЗУ НА ОСНОВІ ПРИРОДНИХ АЛГОРИТМІВ..... 162

САВЧУК К.В.
ПІДХОДИ ДО ОЦІНКИ РИЗИКІВ..... 170

СИГИДЕНКО М.М., БАСІСТИЙ В.П.
МЕТОД ЗАХИЩЕНОЇ МАРШРУТИЗАЦІЇ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ..... 172

ФРАНКІВ І.П.
КЛЮЧОВІ ЕЛЕМЕНТИ ІНТЕРНЕТУ РЕЧЕЙ..... 175

ШЕСТЕРИНА С. В.
СТРУКТУРА ЗАХИЩЕНОЇ СИСТЕМИ ЗБЕРІГАННЯ ДАННИХ..... 177

ШУМКА М.І., ГОЛЕМБЙОВСЬКИЙ М.П., ЧЕРНЯК В.А
МЕТОД ПОБУДОВИ МОДЕЛІ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ..... 181

ЯКУБЕЦЬ Ю.М.
НЕЙРОМЕРЕЖЕВІ МОДЕЛІ І МЕТОДИ ПРОТИДІЇ АТАКАМ..... 185

ЯНІК І.І.
ГЕНЕРАЦІЯ СИМЕТРИЧНОГО КЛЮЧА В КРИПТОГРАФІЧНІЙ СИСТЕМІ БЕЗПЕКИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ..... 189

ЯЦКІВ Н.Г., СМІРНОВ Д.С., ХОТИНСЬКИЙ В.А.
АЛГОРИТМ ВИКОРИСТАННЯ MITRE ATT&CK У ЦЕНТРІ БЕЗПЕКИ ОПЕРАЦІЙ..... 193

Алгоритм допомагає мінімізувати час очікування задач в черзі завдяки розумному розподілу навантаження. Задачі розподіляються на ОР з урахуванням їхнього стану та віддаленості від СД, що зменшує середній час очікування. *Він також* сприяє покращенню якості обслуговування завдяки раціональному вибору ОР для виконання задач. Врахування параметрів ОР дозволяє вибирати найбільш потужні ресурси для максимізації продуктивності.

Висновки.

Застосування запропонованого алгоритму дозволить оптимізувати використання своїх ОР, що забезпечить підвищення продуктивності та призведе до зниження витрат на обладнання та електроенергію. Врахування віддаленості ресурсів і поточної завантаженості допоможе уникнути перевантажень та покращити надійність систем розподіленої обробки даних.

Перелік використаних джерел.

1. Bagirov A.M., Gaudioso M., Karmitsa N., Makela M.M., Taheri S.(eds.) Numerical Nonsmooth Optimization: State of the Art Algorithms.- New York: Springer, 2020. — 700 p.

2. Klemm M., Cownie J. High Performance Parallel Runtimes: Design and Implementation.-De Gruyter Oldenbourg, 2021. - 356 p.

УДК 004.056

ЖИЛИЧ В.А.

[1]Західноукраїнський національний університет

КОНФІГУРАЦІЇ VPN ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ДАНИХ

Вступ. Використання віртуальних приватних мереж VPN є ключовим елементом для забезпечення безпеки передачі даних в сучасному цифровому світі. VPN дозволяють створювати безпечне тунельне з'єднання через інтернет, що захищає дані від несанкціонованого доступу та шифрує їх для забезпечення конфіденційності.

Мета: Дослідження можливих конфігурацій VPN для передачі данних та шляхи підвищення безпеки.

1. Аналіз роботи протоколів для забезпечення безпеки даних

Захист інформації у процесі передачі відкритими каналами ґрунтується на основі здійснення функцій:

- автентифікації взаємодіючих сторін;
- криптографічному закритті даних, що передаються;
- перевірці достовірності та цілісності доставленої інформації.

Для вищеописаних функцій характерний взаємозв'язок «один до одного», реалізація ґрунтується на використанні КЗІ, ефективність яких забезпечується за рахунок спільного застосування симетричних та асиметричних криптографічних

систем.Захист даних в процесі передачі ґрунтується на побудові захищених віртуальних каналів зв'язку це є тунелі VPN.

Тунелювання не захищає дані від НСД чи модифікації, але забезпечує можливість повного КЗІ, котрі інкапсулюються. Тунелювання застосовується для забезпечення конфіденційності цілісності та автентичності, де можна застосувати КЕП, окрім цього, вирішуються проблеми переходів між мережами з різними протоколами.

Організовується взаємодія кількох різних типів мереж, щоб забезпечити цілісність і конфіденційність переданих даних які передаються та завершують подолання невідповідностей зовнішніх протоколів чи схем адресації. Для тунелювання використовуються протоколи канального рівня PPTR і L2TP і протокол мережевого рівня IPSec.

Безпека інформаційного обміну забезпечує об'єднання локальних мереж та доступ до локальних мереж виділених або мобільних користувачів. При проектуванні VPN розглядаються схеми:

- «мережа-мережа». Заміна виділених ліній між офісами, які віддалені один від одного та сформувати захищені канали між ними, шлюз служить інтерфейсом між тунелем та локальною мережею; користувачі локальних мереж застосовують тунель для спілкування один з одним.
- «користувач-мережа». Встановлення з'єднань з віддаленими чи мобільними користувачами. Створення тунелю ініціює клієнт для зв'язку зі шлюзом, який захищає віддалену мережу, запускаючи спеціальне ПЗ користувача.

Для забезпечення безпеки даних, передаються у VPN, які вирішують задачі мережевої безпеки:

- взаємна автентифікація користувачів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності й автентичності інформації, що передається;
- авторизація та управління доступом.

Порівняльний аналіз протоколів L2TP, IPSec та SSL, котрі претендують для розв'язку проблем, які стосуються безпеки в VPN мають певні результати:

- переваги L2TP ґрунтуються на незалежності від транспортного рівня, який надає можливість застосовувати його в гетерогенних мережах;
- через «канальну природу» протоколу складно гарантувати, зможуть підтримувати мережі та проміжні маршрутизатори;
- IPSec забезпечує автентифікацію, перевірку цілісності та шифрування повідомлень на рівні кожного пакету;
- протокол має бути прозорим;
- робота між мережами з протоколами IPv4 та IPv6;
- важливе встановлення VPN клієнта на робочу станцію користувача та надсилання досить великого об'єму службової інформації знизить швидкість обміну даними на низькошвидкісних каналах зв'язку;
- SSL забезпечує захист даних між сервісними та транспортними протоколами, які у зашифрованому вигляді передаються із застосуванням асиметричних ключів для закодування/розкодування інформації;
- протокол здійснює «розпізнавання» серверу та клієнта;

- характеризується відсутністю завищеного навантаження на сервер;
- замість VPN-клієнта застосовується браузер

2. Порівняння популярних конфігурацій VPN

У світі віртуальних приватних мереж (VPN) два основних протоколи: OpenVPN та IPSec, стоять на передньому краї технологій забезпечення безпеки та конфіденційності під час передачі даних через мережі.

Порівняння цих двох протоколів стає важливим завданням для визначення їхніх переваг, недоліків та відповідності конкретним потребам користувачів наведено в таблиці 1.

Таблиця 1 – Порівння конфігурацій OpenVPN та IPSec

Конфігурація	Опис	Переваги	Недоліки
OpenVPN	Відкритий та гнучкий протокол VPN, використовує SSL/TLS для шифрування та забезпечення безпеки передачі даних; підтримується на різних платформах та дозволяє легко налаштовувати безпечні віртуальні приватні мережі.	Гнучкість налаштувань	Швидкість
		Прохід через NAT	Складність конфігурації
		Широкий спектр платформ	
IPSec	Стандартний протокол безпеки для VPN, забезпечує криптографічні функції шифрування, аутентифікації та управління ключами, забезпечуючи безпеку передачі даних в мережах; широко використовується в корпоративних середовищах для захисту конфіденційності та цілісності інформації.	Інтегрована безпека	Несумісність з деякими мережевими конфігураціями
		Швидкість	Обмежена гнучкість
		Широке використання	Проблеми з NAT

OpenVPN відзначається гнучкістю та універсальністю, надаючи ефективний шлях для забезпечення безпеки та конфіденційності через віртуальні приватні мережі, особливо на різних платформах. У той час як IPSec стандартизований та інтегрує широкий спектр безпекових функцій, забезпечуючи

комплексний підхід до захисту передачі даних в корпоративних мережах. Вибір між OpenVPN та IPSec залежить від конкретних потреб користувача, таких як гнучкість налаштувань, ефективність та сумісність з існуючими інфраструктурами.

Висновки.

Конфігурації VPN для безпечної передачі даних мають ключове значення для комплексного підходу до безпеки, які включають в себе вибір правильного протоколу, встановлення сильного шифрування, належну аутентифікацію користувачів та налагодження контролю доступу. Ці заходи допомагають у забезпеченні конфіденційності, цілісності та доступності переданих даних, що є критичними для безпечного обміну інформацією в сучасному інтернет-просторі.

Перелік використаних джерел.

1. VPN protocols expained and compared. [Електронний ресурс].- Режим доступу: https://www.comparitech.com/vpn/protocols/

2. VPN Protocols: Are you using the right one?. [Електронний ресурс].- Режим доступу: https://www.g2.com/articles/vpn-protocols

3. VPN Types and Protocols of VPN: Are you using the right one?. [Електронний ресурс].- Режим доступу: https://ipcisco.com/lesson/vpn-types-and-protocols-of-vpn-2/

4. User VPN (P2S) client configuration. [Електронний ресурс].- Режим доступу: https://learn.microsoft.com/uk-ua/azure/virtual-wan/vpn-client-certificate-windows

5. Клієнт OpenVPN. [Електронний ресурс].- Режим доступу: https://help.keenetic.com/hc/uk/articles/3600000632239

УДК 004.056.53

ЗАЛУЖНИЙ В.В., МОЦНИЙ В.О.

Західноукраїнський національний університет

МОДЕЛЮВАННЯ АТАКИ НА СИСТЕМУ «РОЗУМНИЙ БУДИНОК»

Вступ. В даний час бурхливий розвиток переживає технологія «розумних середовищ» [1]. Хоча поки що відсутнє загальновизнане визначення, однак можна виділити ряд положень, що характеризують такі середовища – це використання сенсорів та обчислювальних пристроїв, що взаємодіють у динамічному децентралізованому середовищі для досягнення єдиної мети, такої, як забезпечення безпеки чи ефективного управління.

Такі середовища в першу чергу знаходять своє застосування в різних системах автоматизації, надаючи хорошу основу для побудови інфраструктури. Одним з найбільш поширених прикладів використання «розумних середовищ» є системи «розумного будинку», що є розвитком автоматичних систем керування спорудами. Системи «розумного будинку» призначені для забезпечення зручності