DOI 10.26886/2311-4517.4(89)2023.2

УДК: 004.724.2

МЕТОДИ ПОБУДОВИ ВІРТУАЛЬНИХ ТУНЕЛІВ EXTRANET-СИСТЕМ

Верховський, бакалавр комп'ютерної інженерії

http://orcid.org/0009-0007-4648-7001

e-mail: ihor.verkhovskyi@nure.ua

Харківський національний університет радіоелектроніки, Україна, Харків

Віталій Ткачов, кандидат технічних наук, доцент

http://orcid.org/0000-0002-6524-9937

e-mail: vitalii.tkachov@nure.ua

Харківський національний університет радіоелектроніки, Україна, Харків

У статті розглядаються методи побудови віртуальних тунелів для забезпечення безпеки зв'язку в Extranet-системах. Досліджено різні протоколи та технології, такі як IPSec, SSL, TLS, SSH, та порівняно їх ефективність та можливості в різних випадках застосування. Також проаналізовано використання VPN-з'єднань та різні типи мережевих топологій для забезпечення стійкості віртуальних тунелів та максимальної продуктивності мережі. Результати досліджень можуть бути корисні для розробників Extranet-систем та адміністраторів мереж, які шукають ефективні методи захисту мережі та забезпечення стійкості тунелів.

Ключові слова: VPN, IPsec, SSL, TLS, SSH.

I. Verkhovskyi, Bachelor in Computer Engineering, V. Tkachov, Candidate in Technical Sciences, Methods of building virtual tunnels in

Extranet-systems / Kharkiv National University of Radio Electronics, Ukraine, Kharkiv

The article discusses the methods of building virtual tunnels to ensure communication security in Extranet systems. Different protocols and technologies, such as IPSec, SSL, TLS, SSH, were studied and their effectiveness and capabilities were compared in different use cases. The use of VPN connections and different types of network topologies to ensure stability of virtual tunnels and maximum network performance are also analyzed. The research results can be useful for developers of Extranet systems and network administrators who are looking for effective methods of network protection and ensuring the stability of tunnels.

Key words: VPN, IPsec, SSL, TLS, SSH.

Вступ. У сучасному світі компанії все частіше використовують різноманітні інтернет-технології, щоб поліпшити свої бізнес-процеси та співпрацювати з партнерами та клієнтами в режимі онлайн. Проте безпека даних є однією з найважливіших проблем, з якими стикаються організації, які використовують інтернет-технології для обміну інформацією. Віртуальні тунелі є одним з рішень для захисту даних під час передачі їх через інтернет. Тому тема "методи побудови віртуальних тунелів extranet-систем" є дуже актуальною. У роботі будуть розглянуті різні методи побудови віртуальних тунелів, їх переваги та недоліки, а також будуть проаналізовані можливості використання цих технологій для захисту даних в extranet-системах.

Дослідження теми "Методи побудови віртуальних тунелів extranet-систем" має великий практичний потенціал, оскільки дозволяє забезпечити безпеку даних в extranet-системах, що дозволяє організаціям знизити ризик порушення конфіденційності, цілісності та доступності даних.

Отримані результати дослідження можуть бути корисними для бізнес-організацій, які прагнуть забезпечити безпеку своїх даних у сучасному світі з високим рівнем кіберзагроз. Також результати дослідження можуть бути корисними для науковців, які працюють у галузі інформаційної безпеки та комп'ютерних мереж, оскільки вони доповнять наявні знання та методи в цій області.

Отже, дослідження теми "Методи побудови віртуальних тунелів extranet-систем" є важливим кроком у забезпеченні безпеки даних в сучасному світі, де зростають кіберзагрози та збільшується обсяг передачі даних у мережі Інтернет, має великий теоретичний та практичний інтерес, оскільки воно дозволяє розширити наявні знання в галузі інформаційної безпеки та застосувати їх на практиці для захисту даних в extranet-системах.

Мета статті та завдання. Основна мета дослідження полягатиме в тому, щоб виявити оптимальний метод побудови віртуального тунелю для захисту даних в extranet-системах, що забезпечить максимальний рівень безпеки під час передачі даних через інтернет. Для досягнення мети дослідження будуть розглянуті різні підходи до побудови віртуальних тунелів, включаючи тунелі на основі технологій VPN, SSL, IPSec, а також різні методи захисту тунелів, включаючи шифрування даних, аутентифікацію та авторизацію користувачів, контроль доступу до ресурсів та інші.

Також у роботі будуть розглянуті різні сценарії використання віртуальних тунелів у extranet-системах, включаючи захист від атак з мережі Інтернет, забезпечення безпеки при з'єднанні з різних місцезнаходжень, захист конфіденційної інформації, а також інші.

Крім того, у дослідженні буде приділена увага порівнянню ефективності різних методів побудови віртуальних тунелів та їхньої придатності для захисту даних в extranet-системах. Будуть враховані

різні фактори, такі як складність налаштування, швидкість передачі даних, рівень захисту, вартість впровадження та інші.

В результаті дослідження будуть запропоновані рекомендації щодо вибору оптимального методу побудови віртуального тунелю для захисту даних в extranet-системах, а також пропозиції щодо покращення захисту даних в таких системах.

Виклад основного матеріалу. Особливості функціонування Extranet-систем. Extranet-система є інформаційною системою, яка забезпечує обмін даними між різними компаніями, підприємствами та іншими сторонами, що мають обмежений доступ до внутрішніх мереж організації [1]. За допомогою Extranet-системи, компанії можуть співпрацювати та обмінюватися даними з постачальниками, клієнтами та іншими зацікавленими сторонами, що покращує ефективність бізнес-процесів та підвищує конкурентоспроможність.

Одним з ключових аспектів забезпечення безпеки Extranet-систем є використання віртуальних тунелів [2]. Віртуальний тунель - це захищений канал зв'язку між двома вузлами мережі, що забезпечує конфіденційність, цілісність та автентичність передачі даних [3]. Віртуальний тунель може бути настроєний на рівні мережевого протоколу та забезпечувати захист від різних видів атак, таких як перехоплення, підроблення та внесення змін у передачу даних [4].

Існують різні види віртуальних тунелів, такі як:

1. IPSec тунелі: IPSec (Internet Protocol Security) - це протокол, що забезпечує безпеку передачі даних на рівні мережевого протоколу. IPSec тунелі використовують шифрування та інші заходи для захисту передачі даних між двома мережами [5].

2. SSL/TLS тунелі: SSL (Secure Sockets Layer) та його наступник TLS (Transport Layer Security) - це протоколи, що забезпечують безпеку передачі даних на рівні застосунку. SSL / TLS

тунелі використовують шифрування та інші заходи для захисту передачі даних між веб-браузером та веб-сервером [6].

3. SSH тунелі: SSH (Secure Shell) - це протокол, що забезпечує безпеку з'єднання між двома вузлами мережі. SSH тунелі можуть бути використані для захисту передачі даних між двома системами через небезпечну мережу, таку як Інтернет [7].

Віртуальний тунель може бути настроєний в різних режимах, таких як точка-точка (point-to-point) або мережа-мережі (network-to-network). У режимі точка-точка віртуальний тунель з'єднує два кінці мережі, тоді як у режимі мережа-мережа він забезпечує захист для всієї мережі [8].

Використання віртуальних тунелів дозволяє компаніям забезпечувати безпеку передачі даних між різними компаніями та іншими сторонами в Extranet-системі [9]. Крім того, віртуальні тунелі можуть бути використані для забезпечення захисту від зовнішніх загроз, таких як хакерські атаки, віруси та шкідливі програми.

Нарешті, віртуальні тунелі забезпечують високу ефективність передачі даних, оскільки вони дозволяють зменшити кількість пакетів, що передаються через мережу, та зменшити накладні витрати на захист мережі. Це робить Extranet-систему більш ефективною та зручною для використання для обміну даними між різними компаніями та іншими сторонами.

IPsec тунелі. IPsec (Internet Protocol Security) - це протокол, який забезпечує захист передачі даних через мережу Інтернет або будь-яку іншу небезпечну мережу. Він шифрує трафік та забезпечує аутентифікацію між двома кінцями тунелю [10].

IPsec тунелі можуть бути використані для захисту передачі даних між двома мережами, які знаходяться в різних географічних регіонах або на різних корпоративних мережах [11]. Це дозволяє компаніям

забезпечувати безпеку передачі даних між різними локаціями та захищати важливу інформацію від зовнішніх загроз.

IPsec тунелі можуть бути налаштовані в різних режимах, таких як тунелевий (tunnel mode) та транспортний (transport mode). У режимі тунелевого тунелю, весь пакет IP шифрується та вкладається в інший пакет IP, що забезпечує його безпеку. У режимі транспортного тунелю, тільки навантаження (payload) пакету IP шифрується, що дозволяє більш ефективно використовувати ресурси мережі [12].

Для встановлення IPsec тунелю, обидва кінці тунелю повинні мати встановлені IPsec протоколи та ключі шифрування. IPsec тунелі можуть бути настроєні з використанням різних протоколів, таких як ESP (Encapsulating Security Payload), AH (Authentication Header) та IKE (Internet Key Exchange) [13, 14].

IPsec тунелі забезпечують високий рівень безпеки передачі даних та можуть бути використані в Extranet-системах для забезпечення захисту між різними мережами. Крім того, вони можуть бути використані для забезпечення безпеки передачі даних між різними пристроями в корпоративній мережі, що забезпечує додатковий рівень безпеки для компаній. IPsec тунелі можуть бути настроєні для захисту від різних видів атак, таких як атаки типу "Man in the middle" та "Replay attacks" [15].

Для використання IPsec тунелей, необхідно мати відповідні знання та навички в області мережевої безпеки. Для створення IPsec тунелю можна використовувати різні програми та пристрої, такі як маршрутизатори, мережеві файрволи та програмне забезпечення VPN.

Один з найпоширеніших методів використання IPsec тунелів в Extranet-системах - це використання VPN (Virtual Private Network). VPN - це технологія, яка дозволяє створити безпечний канал зв'язку

між двома мережами чи пристроями через небезпечну мережу, таку як Інтернет [16].

VPN забезпечує шифрування даних та аутентифікацію користувачів, що дозволяє забезпечити безпеку передачі даних між різними мережами. Це дозволяє компаніям забезпечити безпеку при передачі даних між різними локаціями, включаючи віддалені офіси, робочі місця з дому та інші мережі.

У випадку використання VPN з IPsec тунелями, користувачі можуть отримати доступ до ресурсів компанії, незалежно від їх місця знаходження. Крім того, VPN забезпечує можливість забезпечення безпеки доступу до Інтернету та інших ресурсів в Інтернеті, що може забезпечити додатковий рівень безпеки для користувачів компанії [17].

Узагалі, використання IPsec тунелів та VPN забезпечує компаніям можливість забезпечення безпеки передачі даних між різними мережами та пристроями. Важливо пам'ятати, що при налаштуванні IPsec тунелей та VPN, необхідно дотримуватися відповідних процедур та практик мережевої безпеки, щоб забезпечити найвищий рівень безпеки передачі даних.

До переваг використання IPsec тунелей та VPN можна віднести:

1. Захист від несанкціонованого доступу до мережі компанії. IPsec тунелі та VPN забезпечують аутентифікацію користувачів та шифрування даних, що зменшує ризик несанкціонованого доступу до мережі компанії.

2. Забезпечення конфіденційності та цілісності даних. IPsec тунелі та VPN забезпечують шифрування даних, що дозволяє забезпечити конфіденційність та цілісність даних під час їх передачі між різними мережами та пристроями.

3. Забезпечення безпеки під час передачі даних між різними

мережами. IPsec тунелі та VPN дозволяють забезпечити безпеку передачі даних між різними мережами, що може зменшити ризик злому та витоку даних.

4. Можливість отримання доступу до ресурсів компанії незалежно від місця знаходження. IPsec тунелі та VPN дозволяють користувачам компанії отримувати доступ до ресурсів компанії незалежно від їх місця знаходження, що може збільшити продуктивність роботи та зменшити витрати на організацію та обслуговування робочих місць [18].

Узагалі, IPsec тунелі та VPN є важливими елементами мережевої безпеки, що дозволяють компаніям забезпечити безпеку при обміні даними між різними мережами та пристроями. При налаштуванні IPsec тунелів та VPN необхідно дотримуватися відповідних процедур та практик мережевої безпеки, таких як використання сильних паролів, шифрування ключів, захист пристроїв від злому та вірусів, оновлення програмного забезпечення та оперативної системи, та інші [19].

Для налаштування IPsec тунелів та VPN зазвичай використовують спеціальне програмне забезпечення, яке може бути встановлене як на мережевих пристроях, так і на пристроях користувачів. Деякі операційні системи, такі як Windows та MacOS, мають вбудовані засоби для налаштування IPsec тунелів та VPN, що дозволяє скористатися цими функціями без необхідності встановлення додаткового програмного забезпечення.

Узагалі, використання IPsec тунелів та VPN є важливою складовою мережевої безпеки, що дозволяє компаніям забезпечити безпеку при обміні даними між різними мережами та пристроями. При налаштуванні IPsec тунелів та VPN необхідно дотримуватися відповідних процедур та практик мережевої безпеки, щоб забезпечити

максимальний рівень безпеки передачі даних.

SSL/TLS тунелі. SSL (Secure Sockets Layer) та його наступник TLS (Transport Layer Security) є протоколами шифрування даних, що використовуються для забезпечення безпеки передачі даних через Інтернет. SSL/TLS тунелі дозволяють шифрувати трафік між веб-сайтами та веб-браузерами, щоб забезпечити конфіденційність та цілісність даних [20].

У контексті Extranet-систем, SSL/TLS тунелі можуть бути використані для забезпечення безпеки під час обміну даними між різними мережами та пристроями. Зазвичай, використання SSL/TLS тунелів включає в себе встановлення сертифікатів SSL на сервері, що дозволяє забезпечити безпеку при з'єднанні між веб-браузером та веб-сервером. Крім того, можна використовувати SSL/TLS тунелі для захисту інших мережевих пристроїв, таких як маршрутизатори та комутатори, при обміні даними [21].

SSL/TLS тунелі забезпечують безпеку передачі даних за допомогою шифрування трафіку та використання сертифікатів SSL. Це дозволяє забезпечити конфіденційність та цілісність даних, що передаються через мережу. Крім того, SSL/TLS тунелі можуть бути використані для аутентифікації користувачів та пристроїв, що забезпечує додатковий рівень безпеки [22].

Для налаштування SSL/TLS тунелів зазвичай використовують SSL-сертифікати, що можуть бути виписані відповідними видачами, такими як Symantec, Comodo, GeoTrust тощо. Крім того, можна використовувати відкриті SSL/TLS сертифікати, такі як Let's Encrypt, які є безкоштовними та підтримують автоматичне оновлення [23].

Взагалі, при використанні SSL/TLS тунелів важливо враховувати деякі нюанси, зокрема:

1. Налаштування криптографії: важливо використовувати

надійні шифри та протоколи шифрування для забезпечення максимальної безпеки передачі даних.

2. Перевірка сертифікатів: важливо перевіряти SSL/TLS сертифікати на достовірність та не використовувати недійсні сертифікати, що можуть створити вразливості в системі.

3. Автоматичне оновлення: важливо встановлювати автоматичне оновлення SSL/TLS сертифікатів, щоб уникнути проблем з безпекою.

4. Використання захисту паролів: важливо використовувати надійні паролі для доступу до SSL/TLS тунелів та періодично змінювати їх для забезпечення максимальної безпеки [24].

SSL/TLS тунелі можуть бути використані в Extranet-системах для забезпечення безпеки під час обміну даними між різними мережами та пристроями. Зазвичай використовуються SSL/TLS сертифікати, що забезпечують шифрування трафіку та аутентифікацію користувачів та пристроїв. При належному налаштуванні та використанні SSL/TLS тунелів можна забезпечити високий рівень безпеки передачі даних [25].

SSH тунелі. SSH (Secure Shell) - протокол для безпечного доступу до віддалених систем та безпечної передачі даних. SSH також може використовуватися для створення безпечних тунелів для передачі даних між двома вузлами [26].

SSH тунель - це механізм, який дозволяє перенаправляти трафік між двома вузлами через SSH-канал. При цьому весь трафік буде шифруватися і захищатися від перехоплення та аналізу. Іншими словами, SSH тунель дозволяє безпечно передавати дані через незахищені мережі.

SSH тунель може бути використаний в Extranet-системах для безпечного доступу до різних ресурсів та систем в мережі. Наприклад,

якщо ви хочете безпечно підключитися до бази даних, яка знаходиться на віддаленому сервері, ви можете створити SSH тунель, щоб зашифрувати трафік між вашим комп'ютером та сервером [27].

Створення SSH тунелю може бути здійснене через командний рядок або за допомогою графічного інтерфейсу. Основна ідея полягає в тому, що ми налаштовуємо SSH-клієнт на тунелювання певного порту на локальному комп'ютері до порту на віддаленому сервері. SSH тунелі дозволяють забезпечити високий рівень безпеки передачі даних між різними мережами.

Крім того, SSH тунелі дозволяють уникнути блокування різних протоколів та портів в мережі. Наприклад, якщо ви хочете отримати доступ до веб-сайту, який блокується в мережі, ви можете створити SSH тунель, щоб обійти блокування. Для цього необхідно налаштувати SSH-клієнт на перенаправлення порту 80 на локальному комп'ютері до порту 80 на віддаленому сервері [28].

Крім створення SSH тунелю для одного порту, SSH також дозволяє створювати тунелі для цілих мереж, включаючи VPN-підключення. Наприклад, можна створити SSH тунель, щоб підключити дві мережі між собою через захищену SSH-з'єднання.

Використання SSH тунелю має деякі переваги перед іншими методами захисту мережі, такими як IPsec або SSL/TLS [29]:

1. Шифрування даних: SSH тунелі забезпечують шифрування даних на рівні пакетів, що забезпечує їх безпеку під час транспорту.

2. Інтеграція з багатьма протоколами: SSH тунелі можуть бути використані для створення безпечного каналу для будь-якого протоколу, який може бути транспортований через TCP.

3. Перенаправлення портів: SSH тунелі дозволяють перенаправляти порти між різними мережами, що дає можливість

підключатися до різних ресурсів у безпечному режимі.

4. Простота використання: SSH тунелі легко створюються та налаштовуються через командний рядок або графічний інтерфейс.

Однак, SSH тунелі мають свої недоліки, зокрема, вони не є підходом масштабованого застосування для великих мереж, і для захисту великих мереж варто використовувати ін ші методи, такі як VPN на базі IPsec.

Також варто зазначити, що SSH тунелі можуть бути більш повільними за інші методи тунелювання, такі як IPsec або SSL/TLS, оскільки SSH використовує більш складні методи шифрування та аутентифікації [30].

Узагалі, SSH тунелі - це простий та ефективний спосіб забезпечити безпеку мережі та перенаправлення трафіку між мережами через безпечне SSH-з'єднання. Якщо потрібно перенаправити декілька портів або створити безпечний канал між двома мережами, SSH тунель може бути хорошим вибором. Однак, якщо вам потрібно забезпечити безпеку для великої мережі, може бути краще використовувати більш розширені методи, такі як VPN на базі IPsec.

Висновки. У статті проаналізовано методи побудови тунелів в Extranet-системах такі, як IPsec, SSL/TLS та SSH..

Докладно розглянуто принципи роботи обраних методів, визначено переваги та недоліки. Аналіз показав, що такі тунелі є важливим інструментом для забезпечення безпеки передачі даних між різними вузлами мережі, що знаходяться у різних місцях.

Під час аналізу було виявлено, що кожен з досліджених протоколів має свої переваги та недоліки, але загалом вони є досить ефективними для захисту передачі даних в Extranet-системах.

Також було виявлено, що важливою складовою безпеки

віртуальних тунелів є правильне налаштування параметрів, таких як ключі шифрування та аутентифікації. Невірно налаштовані параметри можуть призвести до вразливостей тунелів та загрози для безпеки передачі даних.

В цілому, аналіз віртуальних тунелів в Extranet-системах є важливим етапом в забезпеченні безпеки та ефективності передачі даних. Рекомендується проводити періодичний аналіз тунелів та їх параметрів для забезпечення найвищої можливої рівня безпеки та ефективності передачі даних в Extranet-системах.

Література:

1. Brooks, C. J., Grow, C., Craig, P. A., & Short, D. (2018). Protecting the Perimeter.

2. Sadiku, M. N., & Akujuobi, C. M. (2022). Intranets and Extranets. In *Fundamentals of Computer Networks* (pp. 71-77). Cham: Springer International Publishing.

3. Kovalenko, A., Kuchuk, H., & Tkachov, V. (2021). Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. *Системи управління, навігації та зв'язку. Збірник наукових праць*, *1*(63), 90-95.

4. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 161-165). IEEE.

5. Обозний, Д. М., & Поштацька, К. В. (2020). Автоматизація розгортання та налаштування програмного забезпечення інфраструктури створеної в середовищі хмарних обчислень. *Науковий огляд*, *7*(70), 7–9.

6. Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN's protocols and security. *International Journal of*

Scientific Research in Computer Science, Engineering and Information Technology, *3*(5), 919-932.

7. Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. *IEEE Access*, *8*, 139567-139586.

8. Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 309-319.

9. Pudelko, M., Emmerich, P., Gallenmüller, S., & Carle, G. (2020, June). Performance analysis of VPN gateways. In *2020 IFIP Networking Conference (Networking)* (pp. 325-333). IEEE.

10. Lopez-Millan, G., Marin-Lopez, R., & Pereniguez-Garcia, F. (2019). Towards a standard SDN-based IPsec management framework. *Computer Standards & Interfaces*, *66*, 103357.

11. Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018, May). Decrypting SSL/TLS traffic for hidden threats detection. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*(pp. 143-146). IEEE.

12. Liu, A., Alqazzaz, A., Ming, H., & Dharmalingam, B. (2019). Iotverif: Automatic verification of SSL/TLS certificate for IoT applications. *IEEE Access*, *9*, 27038-27050.

13. Garre, J. T. M., Pérez, M. G., & Ruiz-Martínez, A. (2021). A novel Machine Learning-based approach for the detection of SSH botnet infection. *Future Generation Computer Systems*, *115*, 387-396.

14. Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. *CMC-Computers Materials & Continua*, *68*(1), 887-901.

15. Agghey, A. Z., Mwinuka, L. J., Pandhare, S. M., Dida, M. A., & Ndibwile, J. D. (2021). Detection of Username Enumeration Attack on SSH Protocol: Machine Learning Approach. *Symmetry*, *13*(11), 2192.

16. Sadiku, M. N., & Akujuobi, C. M. (2022). Virtual Private Networks. In *Fundamentals of Computer Networks* (pp. 79-86). Cham: Springer International Publishing.

17. Forbacha, S. C., & Agwu, M. J. A. (2023). Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet). *American Journal of Technology*, *2*(1), 1-36.

18. Angelo, R. (2019). Secure Protocols And Virtual Private Networks: An Evaluation. *Issues in Information Systems*, *20*(3).

19. Wen, B., Fioccola, G., Xie, C., & Jalil, L. (2018). *A YANG data model for layer 2 virtual private network (L2VPN) service delivery*(No. rfc8466).

20. Patni, S., Sambudas, M., & Sharma, S. A Conceptual Survey of Sturucture, Security and Advantages in Virtual Private Network. *International Journal of Computer Applications*, *975*, 8887.

21. AL-Dhief, F. T., Sabri, N., Latiff, N. A., Malik, N. N. N. A., Abbas, M., Albader, A., ... & Ghani, A. (2018). Performance comparison between TCP and UDP protocols in different simulation scenarios. *International Journal of Engineering & Technology*, *7*(4.36), 172-176.

22. Faisal, A., & Zulkernine, M. (2021). A secure architecture for TCP/UDP-based cloud communications. *International Journal of Information Security*, *20*, 161-179.

23. Kartvelishvili, I., & Todua, T. (2022). ACTUAL ISSUES OF BUILDING SECURE COMMUNICATION CHANNEL CONSIDERING MODERN TECHNOLOGICAL CHALLENGES. *Globalization & Business.*

24. Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 58-65.

25. Vitalii, B., & Anatoly, E. (2022). MPLS VPN TECHNOLOGY. *EDITORIAL BOARD*, 430.

26. Zakaria, M. I., Norizan, M. N., Isa, M. M., Jamlos, M. F., & Mustapa, M. (2022). Comparative analysis on virtual private network in the internet of things gateways. *Indones. J. Electr. Eng. Comput. Sci*, *28*(1), 488-497.

27. Raj, J. R., & Srinivasulu, S. (2022, March). Design of IoT based VPN gateway for home network. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*(pp. 561-564). IEEE.

28. Dharma, F. W. (2021). Enhancing branch office network availability using cloud EoIP gateway. *Procedia Computer Science*, *179*, 574-581.

29. Zhu, R., Li, T., & Song, T. (2021, July). iGate: NDN Gateway for Tunneling over IP World. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-9). IEEE.

30. Arashloo, M. T., Shirshov, P., Gandhi, R., Lu, G., Yuan, L., & Rexford, J. (2018). A scalable vpn gateway for multi-tenant cloud services. *ACM SIGCOMM Computer Communication Review*, *48*(1), 49-55.

References:

1. Brooks, C. J., Grow, C., Craig, P. A., & Short, D. (2018). Protecting the Perimeter.

2. Sadiku, M. N., & Akujuobi, C. M. (2022). Intranets and Extranets. In *Fundamentals of Computer Networks* (pp. 71-77). Cham: Springer International Publishing.

3. Kovalenko, A., Kuchuk, H., & Tkachov, V. (2021). A method for ensuring the survivability of a computer network based on VPN tunneling. *Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats, 1*(63), 90-95 [in Ukrainian].

4. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 161-165). IEEE. [in English].

5. Oboznyi, D. M., & Poshtatska, K. V. (2020). Automation of deployment and configuration of infrastructure software created in a cloud computing environment. *Naukovyi ohliad*, *7*(70), 7–9 [in Ukrainian].

6. Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN's protocols and security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(5), 919-932.

7. Hauser, F., Häberle, M., Schmidt, M., & Menth, M. (2020). P4-ipsec: Site-to-site and host-to-site vpn with ipsec in p4-based sdn. *IEEE Access*, *8*, 139567-139586.

8. Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 309-319.

9. Pudelko, M., Emmerich, P., Gallenmüller, S., & Carle, G. (2020, June). Performance analysis of VPN gateways. In *2020 IFIP Networking Conference (Networking)* (pp. 325-333). IEEE.

10. Lopez-Millan, G., Marin-Lopez, R., & Pereniguez-Garcia, F. (2019). Towards a standard SDN-based IPsec management framework. *Computer Standards & Interfaces*, *66*, 103357.

11. Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018, May). Decrypting SSL/TLS traffic for hidden threats detection. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*(pp. 143-146). IEEE.

12. Liu, A., Alqazzaz, A., Ming, H., & Dharmalingam, B. (2019). Iotverif: Automatic verification of SSL/TLS certificate for IoT applications. *IEEE Access*, *9*, 27038-27050.

13. Garre, J. T. M., Pérez, M. G., & Ruiz-Martínez, A. (2021). A novel Machine Learning-based approach for the detection of SSH botnet infection. *Future Generation Computer Systems*, *115*, 387-396.

14. Park, J., Kim, J., Gupta, B. B., & Park, N. (2021). Network log-based SSH brute-force attack detection model. *CMC-Computers Materials & Continua*, *68*(1), 887-901.

15. Agghey, A. Z., Mwinuka, L. J., Pandhare, S. M., Dida, M. A., & Ndibwile, J. D. (2021). Detection of Username Enumeration Attack on SSH Protocol: Machine Learning Approach. *Symmetry*, *13*(11), 2192.

16. Sadiku, M. N., & Akujuobi, C. M. (2022). Virtual Private Networks. In *Fundamentals of Computer Networks* (pp. 79-86). Cham: Springer International Publishing.

17. Forbacha, S. C., & Agwu, M. J. A. (2023). Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet). *American Journal of Technology*, *2*(1), 1-36.

18. Angelo, R. (2019). Secure Protocols And Virtual Private Networks: An Evaluation. *Issues in Information Systems*, *20*(3).

19. Wen, B., Fioccola, G., Xie, C., & Jalil, L. (2018). *A YANG data model for layer 2 virtual private network (L2VPN) service delivery*(No. rfc8466).

20. Patni, S., Sambudas, M., & Sharma, S. A Conceptual Survey of Sturucture, Security and Advantages in Virtual Private Network. *International Journal of Computer Applications*, *975*, 8887.

21. AL-Dhief, F. T., Sabri, N., Latiff, N. A., Malik, N. N. N. A., Abbas, M., Albader, A., ... & Ghani, A. (2018). Performance comparison between TCP and UDP protocols in different simulation scenarios. *International Journal of Engineering & Technology*, *7*(4.36), 172-176.

22. Faisal, A., & Zulkernine, M. (2021). A secure architecture for TCP/UDP-based cloud communications. *International Journal of Information Security*, *20*, 161-179.

23. Kartvelishvili, I., & Todua, T. (2022). ACTUAL ISSUES OF BUILDING SECURE COMMUNICATION CHANNEL CONSIDERING MODERN TECHNOLOGICAL CHALLENGES. *Globalization & Business.*

24. Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 58-65.

25. Vitalii, B., & Anatoly, E. (2022). MPLS VPN TECHNOLOGY. *EDITORIAL BOARD*, 430.

26. Zakaria, M. I., Norizan, M. N., Isa, M. M., Jamlos, M. F., & Mustapa, M. (2022). Comparative analysis on virtual private network in the internet of things gateways. *Indones. J. Electr. Eng. Comput. Sci*, *28*(1), 488-497.

27. Raj, J. R., & Srinivasulu, S. (2022, March). Design of IoT based VPN gateway for home network. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*(pp. 561-564). IEEE.

28. Dharma, F. W. (2021). Enhancing branch office network availability using cloud EoIP gateway. *Procedia Computer Science*, *179*, 574-581.

29. Zhu, R., Li, T., & Song, T. (2021, July). iGate: NDN Gateway for Tunneling over IP World. In *2021 International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-9). IEEE.

30. Arashloo, M. T., Shirshov, P., Gandhi, R., Lu, G., Yuan, L., & Rexford, J. (2018). A scalable vpn gateway for multi-tenant cloud services. *ACM SIGCOMM Computer Communication Review*, *48*(1), 49-55.