

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи мережної безпеки на базі Cisco
ASA з реалізацією SSL VPN»

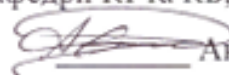
Виконав студент 4-го курсу, групи КІ-21-2
спеціальності 123 «Комп'ютерна інженерія»

 Олександр САК

Керівник: старший викладач кафедри КІ та КБ

 Ольга ДЯЧУК

Рецензент: зав. кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Сак Олександр Анатолійович

Тема роботи: «Проект системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN»

затверджена Наказом університету від 3 березня 2025 р. № 79/с

Термін здачі студентом закінченої роботи 23 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Топологія мережі
2. Протокол SSL

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7200
2. Комутатори Cisco 2960
3. Мережеві екрани Cisco ASA 5510
4. Топологія мережі

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	 15.03.2025	 15.03.2025
2	Трокоз Є. М.	 21.04.2025	 21.04.2025
3	Трокоз Є. М.	 13.05.2025	 13.05.2025

Студент  Олександр САК

Керівник  Ольга ДЯЧУК

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	15.03.2025 р.	Виконано
2	Аналіз літературних джерел	07.04.2025 р.	Виконано
3	Аналіз об'єкта дослідження	07.04.2025 р.	Виконано
4	Постановка задачі дослідження	07.04.2025 р.	Виконано
5	Розробка структурної моделі	07.05.2025 р.	Виконано
6	Розрахунок параметрів адресації	08.05.2025 р.	Виконано
7	Вибір технології для реалізації	13.05.2025 р.	Виконано
8	Розробка захищеної КМ	13.05.2025 р.	Виконано
9	Налаштування мережі	15.05.2025 р.	Виконано
10	Адміністрування мережі	21.05.2025 р.	Виконано
11	Перевірка працездатності	05.06.2025 р.	Виконано
12	Оформлення пояснювальної записки	07.06.2025 р.	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	13.06.2025 р.	Виконано
	Захист	23.06.2025 р.	Виконано

Студент  Олександр САК

Керівник  Ольга ДЯЧУК

АНОТАЦІЯ

Пояснювальна записка до дипломного проєкту на тему «Проект системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN» складається з переліку умовних скорочень, вступу, трьох розділів, висновку та списку використаної літератури. Текстова частина викладена на 66 сторінках. Список використаних джерел містить 23 найменування і займає 2 сторінки. В роботі наведено 31 рисунок. Загальний обсяг роботи – 73 сторінки.

Метою роботи є розробка та налаштування системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN.

Визначена мета обумовлює наступні завдання:

- Аналіз та дослідження існуючих технологій для захисту мережі
- Проєктування архітектури системи мережної безпеки
- Налаштування мережевих пристроїв та протоколів
- Тестування продуктивності системи

Результати дослідження показали, що використання Cisco ASA з SSL VPN забезпечує високий рівень захисту мережевих ресурсів, конфіденційність даних та ефективний захист від загроз. Проведене тестування підтвердило надійність та ефективність запропонованих рішень.

Рекомендації включають впровадження розробленої системи захисту у корпоративних мережах для безпеки передавання даних та захисту від кіберзагроз, а також можливість вдосконалення системи шляхом інтеграції додаткових засобів захисту та моніторингу.

Ключові слова: SSL VPN, CISCO ASA, SYSLOG-СЕРВЕР, STP, МАРШРУТИЗАЦІЯ, ШИФРУВАННЯ, АУДИТ.

					КІК.КР.Б – 123 – 25 – ПЗ			
					Проект системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN	Літ.	Арк.	Аркуші
Зм.	Арх.	№ докум.	Підпис	Дата				
Розроб.	Сав. О. А.			09.06.24				
Керівник	Дячук О. Ю.			09.06.24			4	73
Реценз.	Сфенішко А. А.			09.06.24		ФІКТ Гр. КІ-21-2		
Н. контр.	Дячук О. Ю.			09.06.24				
Зав. каф.	Сфенішко А. А.			09.06.24				

ANNOTATION

The explanatory note to the diploma project on the topic "Project of a network security system based on Cisco ASA with the implementation of SSL VPN" consists of a list of abbreviations, an introduction, three sections, a conclusion and a list of used literature. The text part is presented on 66 pages. The list of used sources contains 23 names and occupies 2 pages. The work contains 31 figures. The total volume of the work is 73 pages.

The purpose of the work is to develop and configure a network protection subsystem based on Cisco ASA with the implementation of SSL VPN. This goal determines the following tasks:

- Analysis and research of existing network security technologies
- Designing the architecture of the network security subsystem
- Configuring network devices and protocols
- Testing the performance of the subsystem

The results of the study showed that the use of Cisco ASA with SSL VPN provides a high level of protection of network resources, data confidentiality and effective protection against threats. The testing confirmed the reliability and effectiveness of the proposed solutions.

Recommendations include the implementation of the developed security subsystem in corporate networks for data transmission security and protection against cyber threats, as well as the possibility of improving the system by integrating additional security and monitoring tools.

Keywords: SSL VPN, CISCO ASA, SYSLOG SERVER, STP, ROUTING, ENCRYPTION, AUDIT.

		Сак О. А.			КИК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				5
Змн.3	Арк.А	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ОГЛЯД ТЕХНОЛОГІЇ SSL VPN	9
1.1 ІСТОРІЯ ТА РОЗВИТОК SSL VPN.....	9
1.1.1. Розвиток SSL VPN.....	9
1.1.2. Ключові аспекти цифрової безпеки у SSL VPN	15
1.2. ОСНОВИ VPN.	18
1.2.1. Захищені з'єднання. Протоколи та шифрування у VPN	18
1.2.2. Тунелювання VPN: Види та Реалізація.....	23
1.3. АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНІСТЬ CISCO ASA	29
1.3.1. Огляд Cisco ASA.....	29
1.3.2. Основні функціональні можливості Cisco ASA	30
РОЗДІЛ 2. ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ	33
2.1. АНАЛІЗ ВИМОГ ДО СИСТЕМИ	33
2.1.1. Вимоги до безпеки.....	33
2.1.2. Вимоги до функціональності системи	35
2.2. АРХІТЕКТУРА СИСТЕМИ	36
2.2.1. Комунікаційна модель	36
2.2.2. Компоненти системи	37
2.3. НАЛАШТУВАННЯ ТА ІНТЕГРАЦІЯ НЕОБХІДНОГО ОБЛАДНАННЯ	38
2.3.1. Використання Tacsacs-сервера	38
2.3.2. Інтеграція з існуючою мережною інфраструктурою.....	40
2.4. ПОБУДОВА СХЕМИ ТА РОЗРОБКА АДРЕСАЦІЇ	44
РОЗДІЛ 3. ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ СИСТЕМИ МЕРЕЖНОЇ БЕЗПЕКИ	52
3.1. ВПРОВАДЖЕННЯ СИСТЕМИ	52
3.1.1. Налаштування протоколу SSL VPN (Clientless SSL VPN).....	52
3.1.2 Конфігурації Syslog та DHCP серверів, STP, ACL	55
3.2. ТЕСТУВАННЯ СИСТЕМИ.....	59
3.2.1. Проведення тестових сценаріїв віддаленого доступу до серверів та логуювання	59
3.2.2. Аналіз логів	64
ВИСНОВКИ	66
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	67
ДОДАТКИ	69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ІБ – інформаційна безпека

ASA – Adaptive Security Appliance

DHCP – Dynamic Host Configuration Protocol

HTTP – Hyper Text Transfer Protocol

IP – Internet Protocol

LAN – Local Area Network

L2TP – Layer 2 Tunneling Protocol

MAC – Media Access Control

PPTP – Point-to-Point Tunneling Protocol

SNP – Secure Network Programming

SSL – Secure Sockets Layer

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UDP – User Datagram Protocol

VPN – Virtual Private Network

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми проєкту системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN визначається сучасними викликами у сфері безпеки інформації. В сучасному цифровому світі, де залежність від інтернет-ресурсів та мережевих технологій стрімко зростає, питання кібербезпеки стає вельми актуальним. Активізація кіберзлочинності та постійні загрози безпеці мережевих систем вимагають постійного удосконалення захисту та впровадження новітніх технологій. У цьому контексті, дипломна робота спрямована на вивчення та реалізацію проєкту системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN.

Мета даного дослідження полягає в розробці ефективної системи захисту, яка забезпечить високий рівень безпеки для користувачів та надійність мережевого зв'язку. Дослідження також націлене на аналіз сучасних підходів до захисту мережі та визначення оптимальних методів використання технологій Cisco ASA та SSL VPN для досягнення поставлених цілей.

У першому розділі в роботі буде вивчено основні аспекти технологій Cisco ASA та SSL VPN, здійснено огляд літературних джерел щодо захисту мережі, а також визначено структуру та зміст нашого дослідження. У подальших розділах буде розглянуто практичні аспекти впровадження захисту мережі на основі обраної технологічної бази.

Предметом дослідження є технології захисту мережі, зокрема Cisco ASA та SSL VPN, які використовуються для забезпечення високого рівня безпеки, конфіденційності та доступності мережевих ресурсів.

Об'єктом дослідження є процес захисту мережі, розроблений з використанням Cisco ASA та SSL VPN. Цей процес визначається як інтегрований комплекс технічних засобів та програмних рішень, спрямований на забезпечення конфіденційності, цілісності та доступності мережі з використанням захисту на рівні протоколів та тунелювання даних через SSL VPN.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ОГЛЯД ТЕХНОЛОГІЇ SSL VPN

1.1 ІСТОРІЯ ТА РОЗВИТОК SSL VPN

1.1.1. Розвиток SSL VPN

Система безпечної мережі даних

Протокол безпеки транспортного рівня (TLS), разом з іншими ключовими основами мережевої безпеки, виник завдяки спільній ініціативі, що стартувала в серпні 1986 року. До неї долучилися Національне агентство з безпеки, Національне бюро стандартів, Агентство оборони зв'язку та дванадцять провідних компаній у галузі телекомунікацій і комп'ютерних технологій. Ця кооперація вилилася в запуск спеціального проєкту — Система безпечної мережі даних (SDNS) [1]. Уперше програма була детально представлена у вересні 1987 року на 10-й національній конференції з комп'ютерної безпеки через серію наукових публікацій. Основний фокус інноваційної дослідницької ініціативи був на створенні нового покоління безпечних мережевих технологій та визначенні технічних специфікацій для продуктів, призначених для використання як у державних, так і приватних інтернет-мережах. Ініціатива мала підтримати нові OSI-стандарти, що активно розвивалися, та інтегруватися з GOSIP-профілями уряду США і глобальними напрацюваннями в межах ІТУ-ISO JTC1. Спершу проєкт мав назву SP4, проте пізніше його перейменували на TLS. У 1995 році він був затверджений як міжнародний стандарт ІТУ-Т X.274|ISO/IEC 10736:1995.

Secure Network Programming (SNP)

Ранні дослідницькі зусилля щодо безпеки транспортного рівня включали в себе інтерфейс програмування застосунків Secure Network Programming (SNP), який у 1993 році досліджував підхід, що передбачав наявність безпечного API транспортного рівня, що максимально наближений до Berkeley sockets, для полегшення модернізації наявних мережевих застосунків із заходами безпеки. SNP був опублікований і представлений на літній технічній конференції USENIX у 1994 році. Проєкт SNP був фінансований за рахунок гранту від Національного агентства з безпеки (NSA) професору Саймону Ламу

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		9

в Університеті Техасу в Остіні в 1991 році. Secure Network Programming отримав премію ACM Software System у 2004 році. За "створення захищених сокетів та реалізацію першого безпечного рівня сокетів — SNP — у 1993 році", Саймона Лама було включено до Зали слави Інтернету [2].

SSL 1.0, 2.0 і 3.0

Оригінальні версії SSL були створені компанією Netscape, а Тахер Ельгамаль, головний науковий співробітник Netscape Communications у 1995–1998 роках, став відомим як "батько SSL". Перша версія — SSL 1.0 — не була оприлюднена через суттєві вразливості. У лютому 1995 року з'явилася версія 2.0, яка також виявилася нестійкою: вона містила кілька критичних проблем як з безпекою, так і з практичністю використання. Протокол застосовував однакові криптографічні ключі для шифрування та автентифікації, а його MAC базувався на MD5 з додаванням секретного префікса, що робило його чутливим до атак на основі подовження довжини. До того ж, SSL 2.0 не забезпечував захист на етапі початкового рукостискання та не підтримував безпечно завершення сесії, що відкривало шлях для атак типу "людина посередині". Ще однією вадою було те, що версія підтримувала лише один доменний сертифікат, що обмежувало сумісність із віртуальним хостингом, який широко використовувався на веб-серверах. Як наслідок, багато сайтів не могли повноцінно використовувати SSL [2].

Ці численні вразливості призвели до повної переробки протоколу, результатом чого стала поява SSL 3.0. Представлена у 1996 році, ця версія була створена Полом Кохером спільно з інженерами Netscape — Філом Карльтоном і Аланом Фрейсром. Еталонну реалізацію підготували Крістофер Аллен і Тім Діркс із компанії Certicom. Саме на SSL 3.0 ґрунтуються всі подальші версії SSL/TLS. Чернетку протоколу SSL 3.0 1996 року було оприлюднено як історичний документ у RFC 6101.

SSL 2.0 офіційно визнали застарілою у 2011 році, згідно з RFC 6176. У 2014 році виявили, що SSL 3.0 піддається атаці POODLE, яка небезпечна для всіх блокових шифрів. Єдиний підтримуваний неблоковий шифр, RC4, також виявився вразливим. Через це у червні 2015 року SSL 3.0 позбавили

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		10

актуальності за допомогою RFC 7568.

TLS 1.0

Протокол TLS 1.0, що став наступником SSL 3.0, був уперше описаний у RFC 2246 у січні 1999 року. Його авторами були Крістофер Аллен і Тім Діркс з компанії Certicom. У самому RFC зазначено, що "різниця між TLS 1.0 і SSL 3.0 не є суттєвою, однак достатня для запобігання їх сумісному використанню". Тім Діркс пізніше пояснив, що зміна назви з "SSL" на "TLS" була дипломатичним кроком для Microsoft, щоб уникнути вигляду, ніби IETF просто схвалює протокол Netscape [2].

Рада з безпеки PCI рекомендувала компаніям перейти з TLS 1.0 на новіші версії — TLS 1.1 або 1.2 — до 30 червня 2018 року. У жовтні 2018 року Apple, Google, Microsoft і Mozilla одночасно оголосили про припинення підтримки TLS 1.0 і TLS 1.1, яке набуло чинності в березні 2020 року. Обидві версії були формально визнані застарілими в березні 2021 року згідно з RFC 8996.

TLS 1.1.

Ця версія протоколу була визначена в RFC 4346 у квітні 2006 року як розвиток TLS 1.0. Серед основних нововведень:

- Додано механізм захисту від атак на зв'язок блоків шифрування (CBC).
- Імпліцитний вектор ініціалізації (IV) був замінений явним IV.
- Зміни у обробці помилок доповнення.
- Підтримка реєстрації параметрів за допомогою IANA.

Ближче до 2020 року багато веб-сайтів припинили підтримку TLS 1.0 та 1.1, що обмежило доступ через старі версії браузерів, як-от Firefox до версії 24 та Chromium до версії 29.

TLS 1.2.

Протокол TLS 1.2 був офіційно описаний у RFC 5246 у серпні 2008 року як оновлення до TLS 1.1. Ключові вдосконалення включали:

- Використання SHA-256 замість комбінації MD5 і SHA-1 у псевдовипадковій функції (PRF), із можливістю налаштування PRF для конкретних шифрованих наборів.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		11

- Замість попередньої комбінації хеш-функцій MD5 і SHA-1 у повідомленні finished, введено використання SHA-256, а також дозволено застосовувати хеші, специфічні для кожного шифрованого набору. Проте, розмір хешу у цьому повідомленні має залишатися не менше ніж 96 біт.

- Комбінація MD5 та SHA-1 у цифровому підписаному елементі була замінена на один хеш, який обговорюється під час рукописання, за замовчуванням SHA-1.

- Покращення можливостей клієнта та сервера вказати, які хеш-функції та алгоритми підпису вони приймають.

- Розширено підтримку алгоритмів шифрування з аутентифікацією, що застосовуються головним чином у режимах GCM (Галуа/лічильник) і CCM з використанням AES (Advanced Encryption Standard).

- Запроваджено механізм розширень TLS та додано підтримку шифрів на основі AES.

Подальші вдосконалення всіх версій TLS були задокументовані у RFC 6176, опублікованому в березні 2011 року, який остаточно усунув можливість зворотної сумісності TLS із SSL. Відтоді жодна сесія TLS не може бути узгоджена з використанням SSL версії 2.0. На сьогодні офіційної дати припинення підтримки TLS 1.2 не встановлено [4].

TLS 1.3.

Фінальна специфікація TLS 1.3 була затверджена в серпні 2018 року у вигляді RFC 8446. Протокол розроблено на основі TLS 1.2, проте він містить суттєві покращення, серед яких:

- Відокремлення алгоритмів узгодження ключів та аутентифікації від шифрованих наборів.

- Припинення підтримки застарілих або небезпечних еліптичних кривих.

- Вилучення підтримки криптографічних хеш-функцій MD5 та SHA-224.

- Обов'язкове використання цифрового підпису навіть при попередньо узгодженій конфігурації.

- Інтегровано HKDF та передбачено підтримку напівефемерного Диффі-

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		12

Гелмана.

- Заміна продовження з PSK та квитками.
- Запроваджено 1-RTT рукостискання та підтримку 0-RTT.
- Обов'язкове забезпечення перфектної передбачуваності за допомогою використання ефемерних ключів під час узгодження ключів (EC)DH.
- Вилучено цілий набір небезпечних функцій, зокрема стиснення, повторні узгодження, шифри без AEAD, нульові шифри, обміни ключами без прямої секретності (наприклад, статичний RSA і DH), нестандартні DHE-групи, окремі формати EC-точок, протокол Change Cipher Spec, мітку часу UNIX у повідомленнях Hello та поле довжини AD у AEAD-шифрах.
- Заборонено узгодження із застосуванням SSL чи RC4 для забезпечення безпеки зворотної сумісності.
- Інтеграція використання хешу сесії.
- Відмова від використання номера версії запису та замороження номера для покращеної зворотної сумісності.
- Переміщення деяких деталей, пов'язаних з алгоритмами безпеки, з додатку до специфікації та перегляд ключа клієнта до додатку.
- Додавання потокового шифру ChaCha20 з кодом аутентифікації повідомлень Poly1305.
- Додавання цифрових алгоритмів підпису Ed25519 та Ed448.
- Додано алгоритми цифрового підпису Ed25519 і Ed448.
- Додавання підтримки відправлення кількох відповідей OCSP.
- Усі повідомлення рукостискання після ServerHello шифруються [4].

Мережеві служби безпеки (NSS), криптографічна бібліотека, розроблена Криптографічна бібліотека Network Security Services (NSS), розроблена Mozilla і що використовується в браузері Firefox, активувала TLS 1.3 за замовчуванням у лютому 2017 року. Підтримка TLS 1.3 була також включена до Firefox 52.0, випущеного в березні 2017 року, але залишалася вимкненою для деяких користувачів через проблеми сумісності. Починаючи з версії Firefox 60.0, яка вийшла у травні 2018 року, TLS 1.3 увімкнено за замовчуванням.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		13

Google Chrome тимчасово встановив TLS 1.3 як версію за замовчуванням у 2017 році. Потім він видалив її як версію за замовчуванням через несумісні посередники, такі як проксі-сервери Blue Coat.

Несумісність нової версії TLS стала прикладом так званої осифікації протоколу — коли посередники мережі "застіють" у підтримці лише певного параметра версії, ігноруючи зміни. Як наслідок, у TLS 1.3 був реалізований механізм імітації TLS 1.2, щоб обійти обмеження старих посередницьких пристроїв. Цю проблему виявили на пізньому етапі розробки, лише під час впровадження у браузерях, що змусило відмовитися від попередньої стратегії узгодження найновішої спільної версії протоколу, яка виявилась несумісною через осифікацію. Водночас з'явився підхід "greasing" (англ. "мастило") — спеціально заявляти підтримку неіснуючих або випадкових розширень протоколу, щоб забезпечити стійкість реалізацій до невідомих, але можливих розширень у майбутньому. Цей метод був розроблений спочатку для TLS, але пізніше знайшов застосування і в інших мережевих протоколах.

Під час хакатону IETF 100 у Сінгапурі (2017 рік) робоча група TLS адаптувала відкриті додатки до використання TLS 1.3. До неї входили учасники з Японії, Великої Британії та Маврикію (група cyberstorm.mu). Цю діяльність продовжили на наступних хакатонах IETF 101 у Лондоні та IETF 102 у Монреалі.

Бібліотека wolfSSL першою серед комерційних реалізацій включила підтримку TLS 1.3 — з версії 3.11.1, випущеної у травні 2017 року. Спочатку підтримувався чернетковий варіант Draft 18, а згодом — фінальний Draft 28. Розробники опублікували серію блогів із порівнянням продуктивності між TLS 1.2 та 1.3.

У вересні 2018 року популярний проект OpenSSL випустив версію 1.1.1 своєї бібліотеки, в якій підтримка TLS 1.3 була "головною новою функцією" [3].

Підтримка TLS 1.3 була додана до Secure Channel (schannel) для релізів загального впровадження Windows 11 та Windows Server 2022.

Транспортна безпека підприємства.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		14

Організація Electronic Frontier Foundation (EFF) позитивно оцінила впровадження TLS 1.3, однак жорстко розкритикувала Enterprise Transport Security (ETS) — варіант TLS, який навмисно обмежує функції безпеки. Спершу відомий як Enterprise TLS (eTLS), ETS був стандартизований як ETSI TS103523-3 — "Протокол безпеки Middlebox, Частина 3: Підприємницька транспортна безпека". ETS призначений виключно для внутрішнього використання у закритих корпоративних мережах, таких як банківські. Він **не** підтримує перфектну передбачуваність (Perfect Forward Secrecy) — щоб організації могли використовувати власні приватні ключі для моніторингу трафіку з метою виявлення шкідливого ПЗ чи для внутрішніх аудитів. EFF, однак, застерегла, що така практика створює серйозні ризики: у разі витоку ключа зломисники можуть розшифрувати великий обсяг раніше перехоплених даних. Експерти організації підкреслили, що існують більш безпечні альтернативи для аналізу трафіку [3].

1.1.2. Ключові аспекти цифрової безпеки у SSL VPN

Цифрові сертифікати.

Цифровий сертифікат використовується для підтвердження того, що певний публічний ключ належить конкретному власнику. Він також вказує, з якою метою можна використовувати цей ключ. Це дозволяє іншим сторонам, які покладаються на цей сертифікат, довіряти підписам або повідомленням, створеним за допомогою відповідного приватного ключа. Сертифікати й ключі можуть зберігатися у різних форматах, таких як .pem, .crt, .pfx або .jks.

Центр сертифікації

У протоколі TLS довіра до сертифікатів зазвичай базується на списку сертифікаційних центрів, які вважаються надійними. Ці довірені центри третіх сторін використовуються для перевірки автентичності сертифікатів. Такий список зазвичай вбудовується в програмне забезпечення користувача і може бути змінений за потреби стороною, що на нього покладається.

Ідповідно до досліджень компанії Netcraft, яка аналізує використання TLS-сертифікатів, компанія Symantec (раніше VeriSign) довгий час займала лідируючі позиції на ринку сертифікатів. У 2015 році на неї припадало близько

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		15

третини всіх виданих сертифікатів, а також 44% з-поміж тих, що використовувались на найпопулярніших сайтах за версією Netcraft. У 2017 році TLS/SSL-бізнес Symantec був проданий компанії DigiCert. Згідно з оновленими даними за травень 2019 року, провідними центрами сертифікації стали IdenTrust, DigiCert та Sectigo [4].

Для підтримки сертифікатів стандарту X.509 необхідна інфраструктура відкритих ключів (PKI), а також центри сертифікації, що займаються створенням, підписом і перевіркою сертифікатів. Хоча це значно зручніше, ніж перевірка особи за допомогою мереж довіри, після витоків інформації про глобальне стеження у 2013 році стало відомо, що центри сертифікації можуть стати вразливим місцем у системі безпеки. Якщо такий центр буде скомпрометовано або співпрацюватиме зі зловмисниками, це відкриває можливість для атак типу "людина посередині" (MITM).

Важливість SSL-сертифікатів

- **Шифрування:** За допомогою SSL-сертифікатів дані, що передаються між веб-браузером користувача і сервером, захищаються шляхом шифрування. Це гарантує, що жодна стороння особа не зможе перехопити або зчитати цю інформацію. Такий підхід мінімізує ризик витоку даних або хакерських атак.

- **Аутентифікація:** SSL-сертифікати не лише шифрують дані, а й виконують функцію аутентифікації — підтверджують справжність веб-сайту. Вони гарантують, що користувачі підключаються саме до справжнього сервера, а не до шахрайської копії. Такий механізм додає впевненості споживачам, що вони взаємодіють із безпечним та перевіреним сайтом.

- **Цілісність:** Ще однією важливою функцією SSL-сертифікатів є забезпечення цілісності переданих даних. Технологія SSL/TLS застосовує криптографічні алгоритми для перевірки, що інформація не була змінена під час передачі між клієнтом і сервером. Це виключає можливість того, що зловмисник втрутиться у вміст даних, зберігаючи їх точність та довіру до інформації.

Алгоритми.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		16

1. Обмін ключами або узгодження ключів

Перш ніж клієнт і сервер зможуть почати захищене спілкування через TLS, вони повинні домовитися про метод шифрування і безпечно обмінятися ключами. Серед методів обміну ключами використовуються такі підходи: використання публічних і приватних ключів, згенерованих за допомогою RSA (позначається TLS_RSA в протоколі TLS рукописання), Діффі-Хеллмана (TLS_DH), ефемерного Діффі-Хеллмана (TLS_DHE), еліптично-кривої Діффі-Хеллмана (TLS_ECDH), ефемерного еліптично-кривої Діффі-Хеллмана (TLS_ECDHE), анонімного Діффі-Хеллмана (TLS_DH_anon), попередньо узгодженого ключа (TLS_PSK) та безпечного пароля (TLS_SRP) [4].

Методи TLS_DH_anon та TLS_ECDH_anon не забезпечують аутентифікації сторін, що робить їх вразливими до атак типу "людина посередині" (MITM). З цієї причини вони майже не використовуються. Натомість, TLS_DHE та TLS_ECDHE гарантують пряму конфіденційність, що підвищує безпеку.

Публічні сертифікати, які застосовуються під час процесу обміну, можуть відрізнятися розміром ключів. Від цього безпосередньо залежить рівень криптографічного захисту. Наприклад, у 2013 році компанія Google повідомила, що відмовляється від використання 1024-бітних ключів і переходить на 2048-бітні. Це рішення було продиктовано необхідністю підвищити стійкість TLS-шифрування, яке компанія надає своїм користувачам.

2. Набір шифрів

Шифрувальний набір — це комбінація криптографічних алгоритмів, які забезпечують безпечне з'єднання між клієнтом і сервером у мережі. Найчастіше вони використовуються в протоколах TLS або його застарілій версії SSL. У типовий набір входять алгоритми для обміну ключами, масового шифрування, а також механізм перевірки цілісності даних — MAC (код аутентифікації повідомлень).

Алгоритм обміну ключами забезпечує безпечну передачу ключа між сторонами, який надалі використовується для шифрування та дешифрування повідомлень. Масове шифрування відповідає за безпосереднє кодування

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		17

інформації, що передається. MAC-алгоритм гарантує, що дані не було змінено під час передачі. Додатково, деякі шифрувальні набори можуть включати алгоритми цифрового підпису та автентифікації, що дозволяють підтвердити справжність сервера чи клієнта.

На сьогодні існують сотні варіантів шифрувальних наборів з різними комбінаціями алгоритмів, і рівень їхньої безпеки також відрізняється. Однак із впровадженням TLS 1.3 перелік доступних наборів був суттєво скорочений: офіційно підтримується лише п'ять строго визначених конфігурацій.

Особливості структури шифрувального набору й правила його використання закріплені в офіційних специфікаціях TLS. Найпоширенішою досі залишається версія TLS 1.2, проте новіша версія TLS 1.3 містить ряд змін, зокрема нові вимоги до наборів шифрів. Варто зазначити, що набори, передбачені для TLS 1.2, не сумісні з TLS 1.3, якщо це явно не передбачено в їхній специфікації. Актуальний перелік усіх визначених шифрувальних наборів можна знайти в офіційному реєстрі TLS.

3. Цілісність даних

Для забезпечення цілісності переданих даних у TLS використовується MAC. У випадку блочних шифрів у режимі CBC зазвичай застосовується HMAC, тоді як сучасні режими, засновані на автентифікованому шифруванні (AEAD), як-от GCM та CCM, вбудовують механізм MAC у сам шифр і не потребують HMAC окремо. Крім того, для реалізації TLS рукописання використовується HMAC-основний механізм PRF або його похідна версія HKDF.

1.2. Основи VPN.

1.2.1. Захищені з'єднання. Протоколи та шифрування у VPN

VPN (Virtual Private Network)

VPN або Virtual Private Network (віртуальна приватна мережа) — це технологія, яка дає змогу встановити захищене з'єднання між користувачем і іншою мережею через Інтернет. Вона може використовуватися для обходу регіональних обмежень доступу до веб-ресурсів, а також для підвищення конфіденційності під час користування публічним Wi-Fi [1].

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		18

По суті, VPN — це розширення приватної мережі, що включає передачу даних через спільні мережі, зокрема Інтернет. Через VPN організації можуть створювати канали зв'язку, які працюють подібно до прямого приватного з'єднання типу "точка-точка".

Архітектура VPN

За допомогою VPN компанії можуть ефективно захищати свій трафік, що проходить через незахищені мережі, наприклад, Інтернет. Ця технологія забезпечує процес шифрування та інкапсуляції даних для їх безпечного транспортування через проміжні мережеві середовища. Шифрування захищає інформацію, роблячи пакети, перехоплені в загальнодоступних мережах, непридатними для читання без спеціальних ключів. Крім того, дані інкапсулюються у додатковий IP-заголовок, який містить маршрутизувальну інформацію [21].

VPN також забезпечує безпечний доступ для працівників, які працюють з дому, подорожують або перебувають у філіях, дозволяючи їм підключатися до корпоративної мережі через Інтернет. З точки зору користувача VPN виглядає як пряме з'єднання між його комп'ютером і сервером організації. Навіть якщо зв'язок проходить через загальний Інтернет, для користувача це виглядає як приватний і виділений канал передачі даних.

VPN має кілька варіантів застосування. Один з найтипівіших — коли співробітник підключається до внутрішньої мережі компанії за допомогою VPN-з'єднання для віддаленого доступу. Інша поширена модель — постійне з'єднання між офісами компанії через так званий VPN-зв'язок «site-to-site» або «маршрутизатор-маршрутизатор».

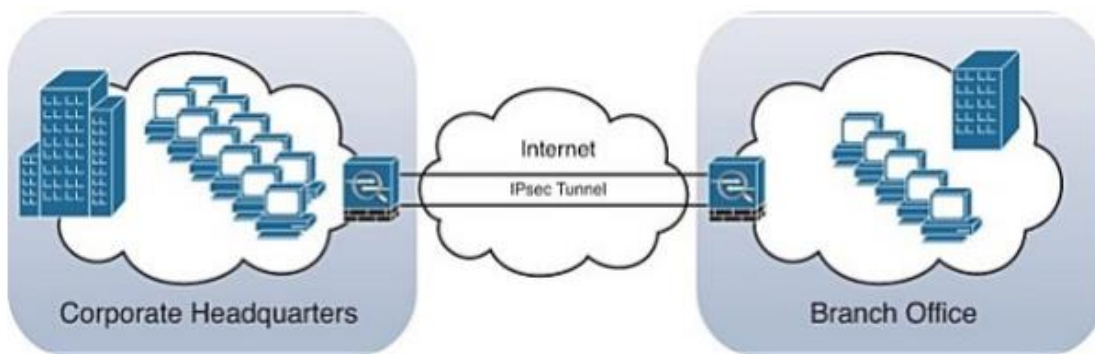


Рис. 1.1 – Приклад VPN типу Site-to-Site

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.З	Арк.А	№ докум.	Підпис	Дата		19

Обидва варіанти можуть бути реалізовані через загальнодоступні мережі (як-от Інтернет) або через приватні інтрамережі. Крім того, VPN-з'єднання можуть використовуватися в екстрамережевих сценаріях — для організації безпечної співпраці з зовнішніми партнерами. У такому разі екстранет функціонує подібно до інтрамережі, але з контрольованим доступом для обраних компаній або осіб. Використовуючи VPN-з'єднання віддаленого доступу або "site-to-site", компанія може замінити дорогі міжміські або орендовані канали на локальні підключення до Інтернету або постійні лінії зв'язку з провайдером (ISP) [21]

VPN має три основні компоненти:

1. **Протоколи безпеки.** Протоколи безпеки у VPN створюють зашифроване з'єднання між користувачем і сервером, тим самим захищаючи передані дані. Тип протоколу визначає рівень захисту та методи шифрування, які застосовуються. Хоча такі протоколи й не забезпечують абсолютної безпеки, як фізичні кабельні з'єднання, вони все ж є високонадійним засобом передачі інформації. Серед найвідоміших протоколів — OpenVPN, який вважається найбезпечнішим і найефективнішим у більшості випадків.

2. **Шифрування.** Шифрування — це процес перетворення інформації у формат, який не піддається прочитанню без спеціального ключа. Цей процес працює разом із протоколами безпеки: навіть якщо зломисник перехопить трафік, без ключа він не зможе його розшифрувати. Найчастіше VPN використовують алгоритм AES (Advanced Encryption Standard) з ключами довжиною 128 або 256 біт. Ці цифри вказують на кількість можливих комбінацій ключа: наприклад, AES-128 вважається настільки надійним, що найпотужнішим комп'ютерам знадобилися б мільярди років для повного перебору всіх варіантів. Саме тому шифрування є критичним елементом безпеки VPN.

3. **Сервери.** Велика кількість серверів у різних країнах — це не просто маркетинг. Широка географія серверів дозволяє вибирати найзручніше місце підключення, підвищує швидкість доступу та забезпечує гнучкість. Коли користувач звертається до сайту через Інтернет, дані проходять через сервер,

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		20

який відповідає на запит. При використанні VPN трафік спершу проходить через VPN-сервер, який, у свою чергу, передає запит до цільового сервера. Це означає, що кінцева точка бачить не вас, а VPN-сервер. Оскільки між вами та VPN створено зашифрований тунель, ніхто не може відстежити вашу справжню IP-адресу або місце перебування. Саме це забезпечує анонімність і дозволяє обходити регіональні блокування веб-сайтів.

VPN віддаленого доступу:

З'єднання VPN для віддаленого доступу створюється за допомогою VPN-клієнта. Це програмне забезпечення, яке запускає індивідуальний користувач на своєму комп'ютері, щоб підключитися до приватної мережі з будь-якої віддаленої локації. VPN-сервер, до якого виконується підключення, надає користувачеві доступ до внутрішніх ресурсів мережі. Весь трафік, що передається через VPN, формується безпосередньо на клієнтському пристрої.

Аутентифікація відбувається з обох сторін: клієнт підтверджує свою особу на сервері, а сервер — у відповідь на клієнті. Це забезпечує двосторонню перевірку автентичності.

Site-to-site VPN:

VPN-з'єднання типу *site-to-site* створює логічний міст між двома частинами однієї приватної мережі або між окремими приватними мережами. Наприклад, це дозволяє об'єднати головний офіс компанії з її філіями чи підрозділами інших організацій через Інтернет. Таке з'єднання працює як логічна глобальна мережа (WAN), не зважаючи на використання публічної мережі як основи. VPN-сервер у цьому випадку відповідає за маршрутизацію трафіку між мережами. Дані, що проходять через VPN-з'єднання *site-to-site*, зазвичай обробляються маршрутизаторами, але не залишають жодних слідів на них. Ініціатор з'єднання — маршрутизатор клієнта — виконує аутентифікацію на сервері, і, навпаки, сервер підтверджує свою автентичність на маршрутизаторі клієнта [23].

VPN віддаленого доступу

VPN з'єднання для віддаленого доступу дає можливість користувачеві встановити з'єднання з приватною мережею не напряду через NAS (Network

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		21

Access Server), а через звичайне підключення до Інтернету. Користувач під'єднується до локального провайдера, а потім за допомогою VPN встановлює безпечне з'єднання з сервером організації. Після встановлення VPN-тунелю, клієнт має повний доступ до ресурсів корпоративної інтрамережі так, ніби він фізично знаходиться в офісі. На ілюстрації нижче зображено типову схему такого з'єднання [21].

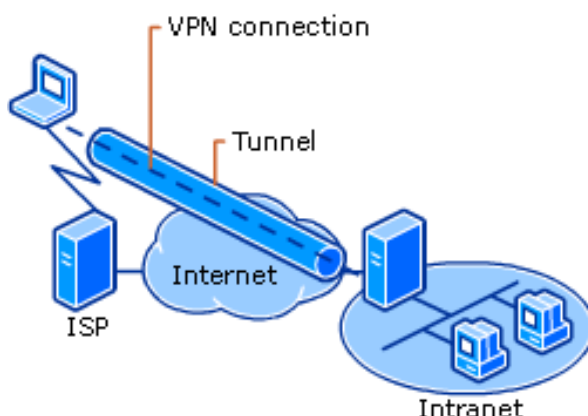


Рис. 1.2 - Схема доступу до корпоративної мережі через Інтернет за допомогою VPN

Site-to-Site VPN з'єднання через Інтернет

Коли мережі підключені через Інтернет, як показано на наступному малюнку, маршрутизатор пересилає пакети іншому маршрутизатору через з'єднання VPN. Для маршрутизаторів VPN з'єднання працює як лінк рівня каналу передачі даних [21].

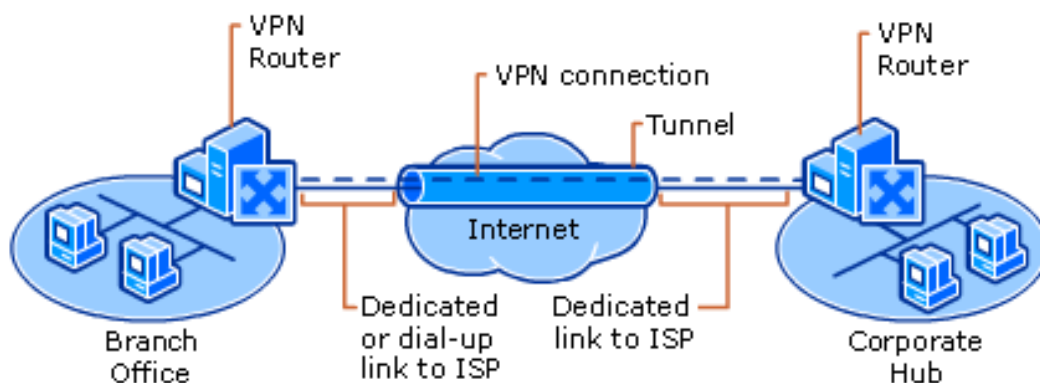


Рис. 1.3 - Безпечне з'єднання двох локальних мереж за допомогою Site-to-Site VPN

1.2.2. Тунелювання VPN: Види та Реалізація

Тунелювання — це технологія в мережевих комунікаціях, яка дає змогу загортати один тип пакету протоколу в інший. Наприклад, VPN-з'єднання в Windows можуть застосовувати протоколи тунелювання, такі як PPTP (Point-to-Point Tunneling Protocol), щоб інкапсулювати внутрішній мережевий трафік, наприклад TCP/IP, і передавати його через публічні мережі, зокрема Інтернет.

У випадку з PPTP або L2TP тунель функціонує подібно до сеансу зв'язку. Обидві його кінцеві точки повинні узгодити параметри з'єднання, такі як IP-адресація, методи шифрування або стиснення. Як правило, дані, що проходять тунелем, передаються через дейтаграмні протоколи. Управління тунелем займається окремий протокол, який забезпечує створення, підтримку та завершення тунельного каналу.

Коли тунель уже встановлений, починається передача даних. Клієнт або сервер тунелю використовує відповідний протокол для формування переданого вмісту. Наприклад, клієнт додає до даних заголовки протоколу тунелювання, після чого надсилає отриманий інкапсульований пакет у мережу. Мережеве середовище доставляє його на сервер, який розпаковує пакет, знімає заголовок і надсилає вміст у цільову мережу. Такий процес характерний і для зворотного напрямку.

Існує два основні типи тунелювання:

- Добровільне тунелювання
- Обов'язкове тунелювання

Добровільне тунелювання

У цьому випадку ініціатором створення тунелю виступає користувач або клієнтський комп'ютер. Він самостійно надсилає запит VPN на встановлення тунелю, і в такій конфігурації він виступає як одна з кінцевих точок тунельного з'єднання.

Такий тип тунелювання можливий, коли клієнт або маршрутизатор сам встановлює віртуальне з'єднання з тунельним сервером. Для цього на клієнтському ПК має бути встановлений відповідний VPN-клієнт і налаштований відповідний протокол. Для описаних у цій документації

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.З	Арк.А	№ докум.	Підпис	Дата		23

протоколів добровільне тунелювання потребує наявності IP-з'єднання (через локальну мережу або dial-up)

У випадку комутованого доступу користувач спочатку має під'єднатись до провайдера через телефонне з'єднання, щоб мати доступ до Інтернету. Лише після цього можливо ініціювати VPN-тунель. Це найбільш типовий варіант використання. Хороший приклад — користувач, який підключається до Інтернету віддалено через модем, а вже потім створює тунель до робочої мережі.

Для клієнтського комп'ютера, що знаходиться в локальній мережі, існує IP-з'єднання з мережею, яка здатна маршрутизувати інкапсульовані дані до певного тунельного сервера в LAN. Це стосується випадків, коли клієнт використовує постійне широкосмугове підключення до Інтернету. Досить часто помилково вважають, що VPN обов'язково потребує комутованого доступу, хоча насправді необхідне лише IP-з'єднання між VPN-клієнтом і сервером. Деякі пристрої (наприклад, домашні комп'ютери) справді використовують dial-up-з'єднання як транспорт для IP. Однак це лише підготовчий етап перед створенням тунелю й не є частиною самого тунельного процесу.

Обов'язкове тунелювання

У випадку примусового тунелювання саме VPN-сервер, що надає віддалений доступ, ініціює й створює тунель без участі користувача. У такому сценарії комп'ютер користувача не є одним із кінців тунелю. Натомість кінцевою точкою виступає проміжний пристрій — сервер віддаленого доступу, розташований між клієнтом і тунельним сервером, і він функціонує як VPN-клієнт.

Деякі виробники серверів віддаленого доступу впровадили функцію створення тунелю від імені користувача. Такий пристрій, який встановлює тунель для клієнта, може називатись FER (Front-End Processor) у випадку PPTP або LAC (L2TP Access Concentrator) — для протоколу L2TP. У цьому тексті термін **FER** використовується універсально — незалежно від застосованого тунельного протоколу. Щоб FER міг виконувати таку функцію, він повинен мати реалізований відповідний протокол тунелювання й уміти ініціювати

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		24

тунель під час з'єднання клієнта.

У конфігурації обов'язкового тунелювання клієнт встановлює підключення до NAS (мережевий сервер доступу), який підтримує VPN, через провайдера. Наприклад, компанія може домовитись із провайдером про надання широкої географічної мережі FEP. Ці FEP пристрої створюють тунелі до тунельного сервера, підключеного до приватної мережі компанії. Такий підхід дозволяє централізовано обробляти VPN-підключення з різних регіонів через Інтернет на єдиний корпоративний сервер.

Ця модель роботи називається примусовим тунелюванням, оскільки клієнт зобов'язаний використовувати тунель, створений FEP. Після встановлення з'єднання весь трафік клієнта автоматично передається через цей тунель. У такому випадку клієнт створює лише одне PPP-з'єднання. Коли він набирає номер NAS, тунель створюється автоматично, й уся передача даних відбувається через нього. FEP можна налаштувати на тунелювання трафіку всіх користувачів до певного тунельного сервера або здійснювати тунелювання вибірково — наприклад, за іменем користувача чи адресою призначення.

На відміну від індивідуальних тунелів, які створюються для кожного добровільного клієнта, у примусовому режимі кілька користувачів можуть передавати трафік через один спільний тунель між FEP та тунельним сервером. Якщо наступний клієнт підключається до того ж FEP і призначення таке саме, новий тунель не створюється. Дані нового користувача передаються через уже існуючий тунель. Такий тунель залишається активним доти, доки останній із підключених користувачів не завершить свою сесію.

РРТР:

Point-to-Point Tunneling Protocol (РРТР) інкапсулює кадри протоколу PPP у вигляді IP-датаграм для їх передачі через IP-мережі — наприклад, через Інтернет або внутрішню мережу компанії. Опис РРТР наведено в стандарті RFC 2637, опублікованому IETF.

Для управління тунелем РРТР використовує TCP-з'єднання, яке виконує функції встановлення, підтримки та завершення тунелю. Самі ж дані інкапсулюються за допомогою зміненої версії протоколу GRE (Generic Routing

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		25

Encapsulation), який обгортає PPP-кадри у тунельовану форму. Інкапсульовані PPP-пакети можуть бути як зашифровані, так і стиснуті, або обидві операції одночасно [12].

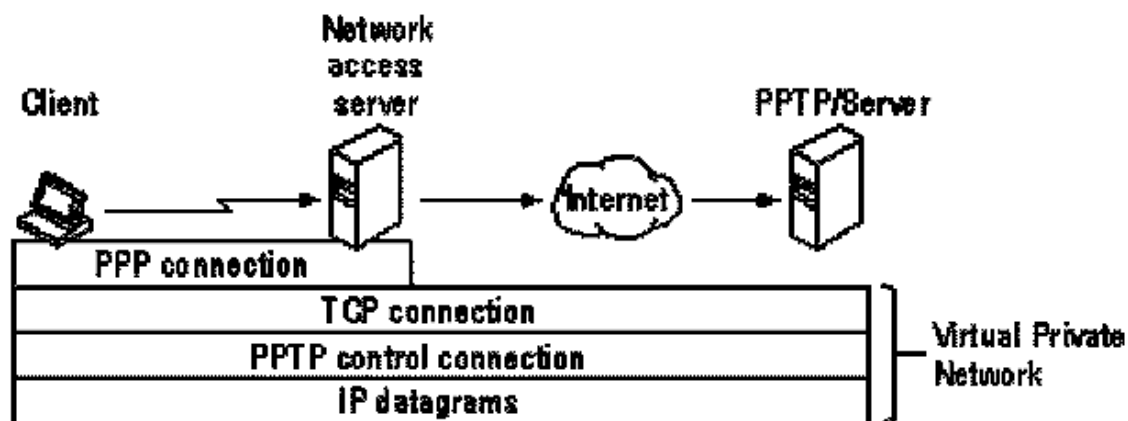


Рис. 1.4 - Схема з'єднання клієнта з сервером PPTP

Протокол PPTP потребує існування IP-мережі, яка з'єднує PPTP-клієнта (тобто користувача VPN, що використовує цей протокол) із PPTP-сервером (сервером VPN із підтримкою PPTP). Клієнт може вже перебувати в IP-мережі, яка має безпосередній доступ до сервера, або встановлює IP-з'єднання через комутовану телефонну лінію з NAS, що типово для користувачів із віддаленим доступом через Інтернет.

Процес аутентифікації при створенні VPN-з'єднання на основі PPTP використовує ті самі методи, що й у стандартному PPP-з'єднанні. Серед них: EAP (розширений протокол автентифікації), MS-CHAP і MS-CHAP v2 (версії протоколу Microsoft Challenge-Handshake), CHAP, SPAP (протокол автентифікації Shiva) та PAP (простий протокол автентифікації паролів). PPTP, як транспорт, наслідує від PPP підтримку стиснення даних, шифрування або обидва варіанти одночасно.

Щоб забезпечити шифрування даних у тунелі PPTP, використовуються методи шифрування Microsoft Point-to-Point Encryption (MPPE). Для цього потрібно, щоб клієнт застосовував EAP-TLS, MS-CHAP або MS-CHAP v2 як метод автентифікації. Тільки ці протоколи дають змогу увімкнути MPPE і, відповідно, забезпечити безпечну передачу даних у тунелі.

MPPE забезпечує лише шифрування посилань між VPN-клієнтом та VPN-сервером. Він не забезпечує наскрізного шифрування, яке є шифруванням

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		26

даних між клієнтським додатком і сервером, на якому розміщується ресурс або послуга, до якої звертається клієнтська програма. Якщо потрібно наскрізне шифрування, IPSec можна використовувати для шифрування IP-трафіку з кінця в кінець після того, як буде створено тунель PPTP.

L2TP (Протокол тунелювання другого рівня)

L2TP, або протокол тунелювання другого рівня, являє собою поєднання PPTP і технології Layer 2 Forwarding (L2F), розробленої компанією Cisco Systems, Inc. Щоб уникнути конкуренції між двома несумісними тунельними протоколами, яка створювала труднощі для користувачів, робоча група Internet Engineering Task Force (IETF) ініціювала об'єднання PPTP та L2F в єдиний протокол, який включає найкращі можливості обох.

Опис протоколу L2TP наведено в RFC 2661, опублікованому в базі IETF RFC. Протокол дозволяє інкапсулювати кадри PPP для передачі через IP-мережі, X.25, Frame Relay або ATM. При передачі через IP L2TP кадри інкапсулюються як повідомлення UDP (User Datagram Protocol).

L2TP може застосовуватись як тунельний протокол для з'єднання через Інтернет або внутрішні корпоративні мережі. Він використовує UDP-пакети для встановлення тунелів та пересилання тунельованих даних. Корисне навантаження в кадрах PPP може бути зашифроване, стиснене або обидва варіанти одночасно. Проте, L2TP-клієнти не узгоджують шифрування MPPE при з'єднаннях через L2TP. Натомість шифрування забезпечується за допомогою IPSec з використанням Encapsulating Security Payload (ESP) у транспортному режимі.

У Windows можливе створення L2TP-з'єднань без IPSec-шифрування. Такі з'єднання не можна вважати повноцінними VPN, оскільки дані, передані через тунель, не захищені. Проте незашифровані з'єднання можуть бути корисними для діагностики проблем, пов'язаних із налаштуванням L2TP через IPSec, оскільки дозволяють тимчасово виключити процес автентифікації та узгодження.

Для роботи L2TP у Windows необхідна IP-мережа, що з'єднує L2TP-клієнта (VPN-клієнт із підтримкою L2TP та IPSec) з сервером L2TP (VPN-

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		27

сервер, який також використовує L2TP та IPSec). Клієнт може вже мати доступ до мережі, або для встановлення з'єднання спершу підключитися до NAS, як у випадку з віддаленим доступом до Інтернету.

Процес аутентифікації при створенні тунелю L2TP аналогічний тому, що застосовується у PPP-з'єднаннях.

Інтернет-сервер L2TP – це сервер віддаленого доступу з підтримкою L2TP з одним інтерфейсом в Інтернеті та другий інтерфейс у приватній інтрамережі [9].

Обслуговування тунелю L2TP та тунельовані дані мають однакову структуру пакетів.

Open VPN

OpenVPN — це порівняно нова технологія з відкритим вихідним кодом, яка ґрунтується на протоколах SSLv3/TLSv1 і використовує бібліотеку OpenSSL разом з іншими технічними рішеннями для забезпечення стабільного та безпечного VPN-з'єднання. Протокол має високу гнучкість у налаштуванні та найефективніше працює через UDP-порт. Водночас його можна переналаштувати на будь-який порт, що значно ускладнює його блокування такими сервісами, як Google та іншими фільтрами.

Однією з головних переваг OpenVPN є те, що він використовує OpenSSL-бібліотеку, яка підтримує широкий набір криптографічних алгоритмів, включно з 3DES, AES, Camellia, Blowfish та CAST-128. Серед них найчастіше VPN-провайдери використовують Blowfish і AES. За замовчуванням OpenVPN застосовує 128-бітове шифрування Blowfish, яке, попри деякі відомі недоліки, вважається досить надійним.

Коли мова йде про шифрування, AES розглядається як сучасний і надійний стандарт, який не має відомих вразливостей. Його навіть було офіційно рекомендовано урядом США для захисту конфіденційних даних. Завдяки 128-бітовому блоку, AES краще справляється з великими обсягами даних порівняно з 64-бітним блоком Blowfish. Обидва алгоритми є сертифікованими NIST, і хоча деякі побоювання щодо них залишаються, серйозних загроз наразі не виявлено.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		28

Швидкодія OpenVPN прямо залежить від обраного рівня шифрування, але загалом він працює швидше, ніж IPsec. Незважаючи на те, що OpenVPN став типовим вибором для більшості VPN-сервісів, він усе ще не є нативно підтримуваним усіма операційними системами. Проте його можна запускати за допомогою стороннього програмного забезпечення, включно з клієнтами для Android та iOS.

Що стосується налаштування, то воно дещо складніше у порівнянні з протоколами L2TP/IPsec та PPTP, особливо якщо використовується стандартний OpenVPN-клієнт. Крім встановлення програми, потрібно вручну додавати конфігураційні файли та розуміти їхню структуру. Деякі VPN-провайдери спрощують це, пропонуючи вже налаштованих клієнтів.

Беручи до уваги загальну ситуацію із конфіденційністю та інформацію, оприлюднену Едвардом Сноуденом, наразі немає доказів, що OpenVPN був скомпрометований або ослаблений з боку Агентства національної безпеки США (NSA). Навпаки, використання ефемерного обміну ключами робить його стійким до подібних атак. Хоча ніхто не знає реального масштабу можливостей NSA, як математичний аналіз, так і практичні свідчення підтверджують, що OpenVPN у поєднанні з потужними шифрами є найбільш надійним VPN-протоколом.

1.3. Архітектура та функціональність Cisco ASA

1.3.1. Огляд Cisco ASA

Cisco ASA (Adaptive Security Appliance) — це одне з провідних рішень у галузі мережевої безпеки, що активно застосовується в багатьох організаціях для захисту їхньої IT-інфраструктури. Пристрій поєднує функції міжмережевого екрана, VPN-концентратора, системи запобігання вторгненням (IPS) та інші засоби кіберзахисту. ASA забезпечує ефективний захист від різноманітних загроз, зокрема шкідливого ПЗ, троянів, хробаків і вірусів. Завдяки високій надійності й універсальності, Cisco ASA стала популярним стандартом серед компаній, які шукають комплексне рішення для безпеки мереж [1].

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.З	Арк.А	№ докум.	Підпис	Дата		29

Система підтримує гнучке масштабування та високу ефективність, що дозволяє використовувати її як у малих офісах, так і у великих корпоративних мережах. Крім цього, ASA надає потужні засоби моніторингу та контролю трафіку, що дає змогу IT-адміністраторам швидко реагувати на можливі загрози. Застосування Cisco ASA дозволяє реалізувати всеохоплюючий підхід до захисту інформаційних ресурсів — від зовнішніх атак до внутрішніх інцидентів, одночасно дотримуючись вимог конфіденційності та цілісності даних.

Також Cisco ASA оснащена механізмами глибокої інспекції трафіку (DPI), які дають змогу виявляти загрози на прикладному рівні та ефективно їм протидіяти. Це робить її оптимальним вибором для організацій, які потребують захисту від складних атак, таких як DDoS та інші. Гнучка архітектура Cisco ASA дозволяє легко інтегрувати її у наявну мережеву інфраструктуру, що сприяє стабільній роботі системи та зниженню витрат на її впровадження й обслуговування [5].

1.3.2. Основні функціональні можливості Cisco ASA

Cisco ASA (Adaptive Security Appliance) — це багатофункціональний пристрій для забезпечення мережевої безпеки, який об'єднує кілька ключових функцій, необхідних для захисту IT-інфраструктури організацій. Основною його складовою є міжмережевий екран (фаєрвол), що здійснює контроль і фільтрацію трафіку відповідно до встановлених правил. ASA може аналізувати як мережеві пакети (Packet Filtering), так і трафік на рівні додатків (Application Layer Filtering), що дозволяє ефективно виявляти й блокувати різноманітні загрози.

1. Фільтрація трафіку: Пристрій Cisco ASA дає змогу адміністраторам створювати гнучкі політики безпеки для контролю проходження трафіку. Це охоплює фільтрацію за IP-адресами, портами, протоколами та іншими параметрами. Завдяки підтримці як статичних, так і динамічних списків контролю доступу (ACL), ASA дозволяє адаптуватися до змін у загрозах та зберігати ефективність захисту від несанкціонованого доступу.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		30

2. VPN-концентратор: Ще однією ключовою функцією Cisco ASA є підтримка віртуальних приватних мереж (VPN), що дозволяє забезпечити захищений віддалений доступ до внутрішніх ресурсів компанії. ASA підтримує декілька протоколів VPN, включаючи IPsec та SSL VPN, що забезпечує шифрування даних, автентифікацію користувачів і контроль доступу. Це гарантує безпечну передачу інформації навіть у незахищених мережах, таких як Інтернет

3. Система запобігання вторгненням (IPS): Cisco ASA також інтегрує функціональність IPS, яка дозволяє в режимі реального часу виявляти та блокувати підозрілу активність. Ця система аналізує трафік на наявність шкідливих шаблонів, таких як дії вірусів, троянів, хробаків та інших загроз. При виявленні таких атак IPS автоматично блокує трафік, запобігаючи проникненню [22].

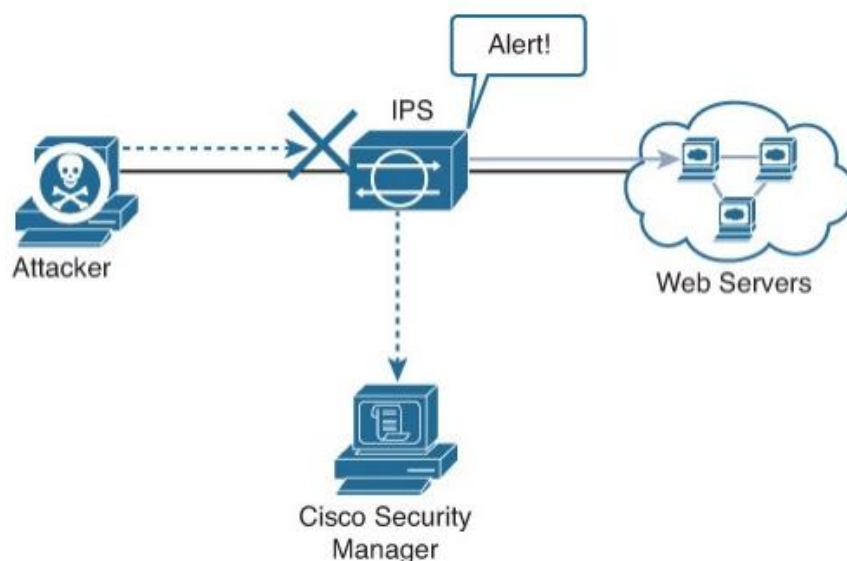


Рис. 1.5 - Приклад роботи IPS

4. Моніторинг та логування: Cisco ASA має розвинені інструменти для спостереження за станом мережі та фіксації подій. Адміністратори можуть налаштувати збір, перегляд та зберігання журналів активності. Ці журнали можна аналізувати як у візуальному інтерфейсі, так і за допомогою зовнішніх систем, що дозволяє швидко виявляти порушення безпеки та реагувати на інциденти. Дані можуть зберігатися локально або передаватися на централізовані сервери логування для подальшого аналізу.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		31

5. Контроль доступу: Cisco ASA підтримує різноманітні методи аутентифікації користувачів, зокрема локальні облікові записи, а також зовнішні сервіси, такі як LDAP, RADIUS і TACACS+. Це надає можливість гнучко керувати доступом до ресурсів мережі. Адміністратори мають змогу встановлювати індивідуальні політики доступу для окремих користувачів або груп, визначаючи, які саме сервіси та ресурси будуть їм доступні.

6. Масштабованість та висока продуктивність: Пристрій Cisco ASA розроблений із урахуванням потреб організацій, яким важлива висока пропускна здатність та стабільна робота під значним навантаженням. Його функціональність можна розширювати за допомогою модулів і оновлень ПЗ, що дозволяє адаптувати систему до нових вимог. Крім того, ASA підтримує режими високої доступності та балансування навантаження, що сприяє надійності та безперервності роботи мережевої інфраструктури.

Ці ключові можливості роблять Cisco ASA ефективним і універсальним рішенням для побудови безпечного мережевого середовища в організаціях різного розміру. Завдяки поєднанню гнучкості, стабільності та високої продуктивності, ASA продовжує залишатися популярним вибором серед засобів захисту мереж.

Висновок до першого розділу:

У першому розділі було здійснено загальний огляд технології SSL VPN, включаючи її історичний розвиток. Розглядалися основні компоненти цифрової безпеки, з акцентом на захист інформації та алгоритми шифрування. Також описано фундаментальні принципи роботи VPN — захищене з'єднання та методи тунелювання, які забезпечують цілісність і конфіденційність даних під час їх передачі. Таким чином, перший розділ формує базове розуміння SSL VPN, її еволюції, особливостей безпеки та принципів функціонування.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		32

РОЗДІЛ 2. ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

2.1. Аналіз вимог до системи

2.1.1. Вимоги до безпеки

Вимоги до безпеки є ключовим елементом у реалізації системи захищеного віддаленого доступу до кінцевих та комунікаційних пристроїв мережі за допомогою SSL VPN. Через постійний розвиток кіберзагроз важливо не лише дотримуватись актуальних вимог, а й своєчасно впроваджувати відповідні захисні механізми:

1. Аутентифікація: Різні підходи до автентифікації є основою надійного захисту. Використання складних паролів із вимогою їх регулярної зміни зміцнює класичну парольну автентифікацію. Двофакторна автентифікація (наприклад, через одноразові коди або пари відкритого/закритого ключів) значно підвищує рівень захисту доступу.

2. Шифрування: Надійне шифрування трафіку через SSL VPN забезпечує конфіденційність передаваних даних. Застосування сучасних криптографічних алгоритмів і регулярне оновлення налаштувань шифрування є необхідним для підтримання високих стандартів безпеки. Також важливо постійно відслідковувати безпеку використовуваних алгоритмів і своєчасно усувати виявлені вразливості.

3. Ідентифікація та авторизація: Чіткий контроль ідентифікації користувачів і надання їм доступу лише до дозволених ресурсів знижує ризик стороннього втручання. Це досягається через використання цифрових сертифікатів, рольової моделі доступу, обмеження повноважень та реалізацію механізмів блокування після кількох невдалих спроб входу.

4. Моніторинг та аудит: Неперервний контроль дій користувачів у рамках SSL VPN допомагає своєчасно виявляти й усувати потенційні інциденти безпеки. Аналіз логів доступу, виявлення нетипових дій, створення систем оповіщення та швидке реагування на інциденти дозволяють ефективно протидіяти загрозам і посилити захист мережевої інфраструктури.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		33

Забезпечення вищезазначених вимог до безпеки є складним завданням, яке потребує комплексного підходу. Крім базових принципів, як-от аутентифікація, шифрування, ідентифікація та авторизація, слід враховувати й додаткові аспекти безпеки:

1. Протидія атакам «людина посередині» (MITM): Щоб уникнути несанкціонованого перехоплення трафіку, система SSL VPN має використовувати надійні механізми перевірки автентичності, зокрема сертифікати та криптографічні алгоритми. Це критично для запобігання MITM-атакам.

2. Захист від витоку інформації: Захист переданої інформації передбачає впровадження політик контролю доступу, шифрування даних у русі, а також суворе дотримання корпоративних політик безпеки.

3. Захист від вірусів та шкідливих програм: Інтеграція з антивірусними рішеннями або наявність вбудованих механізмів протидії вірусам і шпигунським програмам допомагає уникнути зараження користувацьких пристроїв та запобігає розповсюдженню загроз у корпоративній мережі.

4. Захист від переповнення буфера: Реалізація захисту від експлоїтів, які використовують переповнення буфера, дозволяє знизити ризики компрометації системи або несанкціонованого доступу до ресурсів.

5. Моніторинг та реагування на інциденти: Система має бути здатна фіксувати, аналізувати та реагувати на підозрілу активність. Доцільно використовувати логування, інструменти аналізу подій і системи автоматичного реагування на загрози.

6. Оновлення та патчі безпеки: Оперативне встановлення оновлень і виправлень для компонентів SSL VPN допомагає усувати відомі вразливості, зменшуючи ймовірність експлуатації слабких місць у системі.

Ці додаткові аспекти доповнюють основні вимоги до безпеки SSL VPN та допомагають створити повноцінну та надійну систему для захищеного віддаленого доступу.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		34

2.1.2. Вимоги до функціональності системи

Функціональні вимоги до системи захищеного доступу на основі SSL VPN мають вирішальне значення для забезпечення її ефективної та стабільної роботи. Основний акцент робиться на клієнтське програмне забезпечення, яке має бути зручним для користувача, сумісним з різними платформами та функціонально гнучким.

1. Простота встановлення та налаштування. Клієнт повинен бути легким у розгортанні — як для технічних фахівців, так і для звичайних користувачів. Інсталяція має проходити швидко, із мінімальною кількістю кроків, а конфігурація зводиться до вибору профілю чи сервера.

2. Інтуїтивне керування та збереження налаштувань. Користувач повинен мати можливість зберігати параметри підключення (логін, сервер, сертифікат тощо) у профілі. Простий та зрозумілий інтерфейс дозволить швидко перемикатися між обліковими записами або серверами.

3. Кросплатформність. Клієнтське ПЗ повинно працювати на більшості поширених платформ: Windows, macOS, Linux, Android та iOS. Це дозволяє забезпечити доступ як із персональних комп'ютерів, так і з мобільних пристроїв.

4. Автоматичне перепідключення. У разі втрати з'єднання або зміни мережі (наприклад, при переході між Wi-Fi і мобільною мережею) клієнт має автоматично відновлювати VPN-з'єднання без участі користувача..

5. Вбудовані засоби моніторингу та діагностики. Базові функції перегляду стану підключення, журналу подій, діагностики збоїв у з'єднанні дозволять оперативно виявляти та усувати проблеми без залучення технічної підтримки.

Додаткові функції, такі як підтримка декількох протоколів шифрування, приховування IP-адреси, обмеження пропускної здатності або інтеграція з системами багатофакторної аутентифікації, є бажаними і підвищують загальну гнучкість та безпеку рішення.

Врахування цих функціональних вимог забезпечує не лише зручність користувачам, а й стабільність та надійність системи у різних мережесих умовах.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		35

2.2. Архітектура системи

2.2.1. Комунікаційна модель

Принципи комунікації в системі SSL VPN:

Взаємодія між клієнтськими та серверними компонентами VPN ґрунтується на ретельній системі принципів комунікації. Ці принципи, в основі своїй, визначають правила та обмеження, за якими відбувається обмін даними між цими компонентами.

Перш за все, принцип ефективності полягає в оптимізованій передачі інформації - зменшенні затримок і мінімізації обсягу обміну для досягнення стабільного з'єднання навіть у нестабільних мережах.

Другий принцип - прозорість. Всі етапи обміну мають бути зрозумілими та доступними для контролю, що дозволяє здійснювати моніторинг, виявляти збої та підтримувати стабільність роботи VPN.

Третій принцип стосується надійності: дані повинні передаватися точно й повністю, без втрат або спотворень. Це критично для підтримки цілісності інформації, особливо у випадках передачі важливих або конфіденційних даних.

Четвертий принцип - безпека. Уся комунікація між клієнтом і сервером має бути зашифрована та захищена від перехоплення або несанкціонованого доступу.

І, нарешті, принцип сумісності гарантує, що система працює з різними пристроями, операційними системами та версіями протоколів, забезпечуючи зручність і гнучкість для користувачів незалежно від платформи.

Протоколи комунікації:

Протоколи комунікації визначають стандарти та правила обміну даними між клієнтськими і серверними компонентами VPN. Вони забезпечують захист, сумісність і стабільність у процесі передачі інформації. Нижче наведені основні протоколи, що використовуються в SSL VPN:

1. TLS/SSL (Transport Layer Security / Secure Sockets Layer): Ці протоколи забезпечують шифрування каналу зв'язку та аутентифікацію сторін. Вони є базовою технологією для безпечного з'єднання між клієнтом і сервером через відкриті мережі [1].

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		36

2. HTTP/HTTPS: HTTP використовується для обміну гіпертекстовими даними, тоді як HTTPS доповнює його захистом через TLS/SSL. Це дозволяє забезпечити конфіденційність і цілісність інформації під час передавання [6].

3. IPsec (Internet Protocol Security): Протокол функціонує на мережевому рівні й забезпечує захист трафіку шляхом шифрування та аутентифікації IP-пакетів. Широко використовується для створення безпечних VPN-з'єднань.

4. OpenVPN: Популярне відкриття рішення, що реалізує VPN через TLS/SSL. OpenVPN підтримує як високий рівень шифрування, так і гнучку конфігурацію, завдяки чому є надійним вибором для побудови захищених тунелів [1].

5. L2TP/IPsec (Layer 2 Tunneling Protocol/Internet Protocol Security): Ця комбінація протоколів дозволяє створювати захищені тунелі для передавання даних. L2TP забезпечує тунелювання, тоді як IPsec виконує шифрування та аутентифікацію.

Застосування цих протоколів дозволяє гарантувати безпечний, надійний і масштабований обмін інформацією в рамках інфраструктури SSL VPN.

2.2.2. Компоненти системи

У цьому розділі розглянуто основні компоненти, що формують систему захищеного доступу на базі SSL VPN. Нижче наведено опис кожного з них:

1. Сервер VPN: Основним елементом системи є VPN-сервер, який забезпечує безпечне підключення користувачів до внутрішньої мережі. Він виконує функції автентифікації, управління сесіями, шифрування переданих даних та реалізує інші заходи безпеки.

2. VPN-шлюзи: Ці пристрої працюють як проміжна ланка між зовнішніми та внутрішніми мережами. Вони відповідають за захист, обробку трафіку та його правильну маршрутизацію до внутрішніх ресурсів.

3. Системи аутентифікації: Системи аутентифікації призначені для перевірки достовірності користувачів, які ініціюють з'єднання з VPN. Серед методів автентифікації можуть бути паролі, сертифікати, токени або інші засоби підтвердження особи.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		37

4. Модулі шифрування: Ці системи відповідають за захист переданої інформації, забезпечуючи її конфіденційність у відкритих мережах. Вони застосовують сучасні алгоритми шифрування для захищеного обміну даними між сервером і клієнтом.

5. Системи моніторингу та логування: Вони дозволяють контролювати дії користувачів у мережі VPN. До таких дій належать спроби входу, сеанси передачі даних та інші події, які реєструються з метою аналізу, контролю та аудиту.

Усі ці складові формують технічну основу SSL VPN-системи, забезпечуючи її безпечну та стабільну роботу в умовах захищеного віддаленого доступу.

2.3. Налаштування та інтеграція необхідного обладнання

2.3.1. Використання Тасас-сервера

Використання Тасас-сервера для централізованої аутентифікації та авторизації відіграє ключову роль у підвищенні безпеки та ефективності функціонування мережевої інфраструктури. Нижче наведено детальну інформацію про цей процес:

1. Аутентифікація: Тасас-сервер використовується для централізованої перевірки користувачів, які намагаються підключитися до мережевого обладнання. Він приймає запити на аутентифікацію від клієнтів і звіряє їхні облікові записи та паролі в базі даних. Це дозволяє точно визначити особу користувача та запобігти несанкціонованому доступу.

2. Авторизація: Після успішної аутентифікації Тасас-сервер визначає, які дії дозволено виконувати конкретному користувачу. Система перевіряє рівень доступу користувача і визначає відповідні привілеї для виконання різних операцій, таких як налаштування параметрів, керування ресурсами та інші дії.

3. Централізоване керування: Тасас-сервер дозволяє адмініструвати аутентифікацію та доступ до пристроїв з одного місця. Це полегшує керування користувачами та їхніми правами, роблячи політику безпеки послідовною по всій мережі.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.З	Арк.А	№ докум.	Підпис	Дата		38

4. Інтеграція з існуючими системами: Тасас-сервер легко поєднується з такими сервісами, як LDAP або Active Directory, що дає змогу синхронізувати облікові записи й автоматизувати процеси управління доступом.

5. Аудит та журналювання: Тасас-сервер проводить аудит та журналює всі дії користувачів на мережевих пристроях. Це дає змогу відслідковувати активність користувачів, виявляти потенційні загрози безпеки та забезпечує відповідність з регуляторними вимогами.

Spanning Tree Protocol (STP)

Протокол Spanning Tree Protocol (STP) є мережевим протоколом, який діє на другому рівні моделі OSI, створений Радьєю Перлманом для запобігання утворенню петель в комутаторах. Його принцип роботи базується на логічному блокуванні всіх надлишкових каналів між комутаторами, логічно створюючи топологію у вигляді дерева (математичного графа).

Для досягнення своїх функцій STP використовує два типи повідомлень:

BPDU, яке містить інформацію про комутатори, і TCN, що передає повідомлення про зміни у топології. Після активації протоколу STP комутатори починають обмінюватись BPDU-повідомленнями. У процесі аналізу обирається кореневий комутатор на основі інформації з BPDU-повідомлень, такої як ідентифікатор відправника, ідентифікатор кореневого маршрутизатора, ідентифікатор інтерфейсу та вартість маршруту до кореневого маршрутизатора.

Після визначення кореневого комутатора він регулярно надсилає BPDU-повідомлення для створення топології. У цьому процесі інтерфейсам комутатора надаються різні стани, такі як:

- Blocking (блокування): Інтерфейс не передає жодних повідомлень і використовується для запобігання петлям.

- Listening (слухання): Інтерфейс передає лише BPDU-повідомлення під час вибору кореневого комутатора.

- Learning (навчання): Інтерфейс приймає BPDU-повідомлення, але не відправляє нічого, зберігаючи отриману інформацію про MAC-адреси комутатора.

– Forwarding (пересилання): Основний стан інтерфейсу, під час якого відбувається пересилання інформаційних пакетів [7].

Для перевірки стану мережі, кореневий комутатор періодично надсилає BPDU повідомлення кожні 2 секунди, і цей таймер відомий як Hello Timer. Інші комутатори, прийнявши ці повідомлення, пересилають їх далі. Якщо будь-який комутатор не отримує це повідомлення протягом таймера Max Age (20 секунд за замовчуванням), це розглядається як втрата зв'язку з кореневим комутатором, що спричиняє повторний вибір кореневого комутатора.

Коли звичайний комутатор виявляє зміни в топології, такі як включення або виключення підключення нового пристрою, використовуються повідомлення TCN. TCN повідомлення містять інформацію про зміни в топології, і ці повідомлення пересилаються на кореневий комутатор. Звичайні некореневі комутатори єдині, хто пересилає TCN повідомлення для спілкування з кореневим комутатором [11].

RSTP представляє сучасний варіант протоколу STP, який не використовує таймери і дозволяє всім комутаторам передавати BPDU повідомлення. Для виявлення змін використовується механізм іксації втрат BPDU, а завдяки Proposal/Agreement інтерфейси можуть переходити в робочий стан без затримок. Проте, коли до мережі підключається пристрій, який не підтримує RSTP, використовується класичний алгоритм STP.

2.3.2. Інтеграція з існуючою мережною інфраструктурою

Інтеграція з маршрутизаторами та комутаторами:

Інтеграція SSL VPN із маршрутизаторами та комутаторами становить важливу складову у побудові безпечного доступу до внутрішніх ресурсів мережі. У середовищах для тестування, наприклад, GNS3, можливо задіяти віртуальні маршрутизатори й комутатори, які підтримують VPN-рішення, зокрема IPsec або SSL VPN. Розгортання SSL VPN на подібному обладнанні дає змогу підвищити рівень захищеності та убезпечити мережу від несанкціонованого проникнення.

Після налаштування SSL VPN на маршрутизаторах і комутаторах відкривається можливість формування захищених з'єднань із користувачами,

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		40

які підключаються віддалено. Це забезпечує надійне шифрування трафіку та перевірку автентичності користувачів перед передачею критичної інформації по мережі, що значно підвищує рівень конфіденційності.

Додатково, конфігурування SSL VPN на цих пристроях створює умови для розширюваності та адаптивності системи, адже маршрутизатори й комутатори здатні одночасно обробляти значну кількість з'єднань та реалізовувати контроль доступу до різних частин інфраструктури. Таким чином, інтеграція SSL VPN із цим обладнанням дозволяє сформувати ефективне та надійне середовище для взаємодії з віддаленими користувачами й посилити захист мережі [13].

Отже, інтеграція SSL VPN з маршрутизаторами та комутаторами дає можливість створити захищене та ефективне середовище для роботи з віддаленими користувачами та забезпечити високий рівень захищеності мережі.

Інтеграція з фаєрволами:

Інтеграція SSL VPN із фаєрволами підсилює загальний рівень безпеки мережі та забезпечує ефективне управління доступом до її ресурсів. У середовищах для віртуального моделювання, наприклад GNS3, можливо використовувати віртуальні фаєрволи, як-от Cisco ASA або Palo Alto Networks, що мають підтримку технології SSL VPN.

Розгортання SSL VPN безпосередньо на фаєрволах дає змогу реалізувати потужний захист мережевого периметра та точно налаштовувати політики доступу. Це відкриває можливість створення правил, які обмежують доступ користувачів до окремих сегментів мережі чи конкретних ресурсів, що значно підвищує рівень інформаційної безпеки.

Також використання SSL VPN у поєднанні з фаєрволами дає змогу реалізувати надійне шифрування переданих даних, аутентифікацію користувачів і точний контроль доступу до внутрішніх сервісів через захищені канали. Такий підхід унеможливорює несанкціонований доступ та захищає критично важливу інформацію.

Таким чином, інтеграція SSL VPN із фаєрволами не лише зміцнює безпеку мережі, а й дозволяє надійно керувати правами доступу користувачів, гарантуючи високий рівень захисту.

Інтеграція з Тасас-сервером:

Інтеграція SSL VPN з Тасас-сервером забезпечує централізоване управління процесами аутентифікації та авторизації користувачів, дозволяючи ефективно контролювати їхній доступ до мережевих сервісів. Тасас-сервер виконує функцію перевірки облікових даних та визначення рівня доступу для кожного користувача згідно з установленими адміністративними політиками.

У процесі налаштування взаємодії між SSL VPN та Тасас-сервером необхідно сконфігурувати параметри автентифікації як на серверній стороні, так і на пристроях, що працюють з SSL VPN. Тасас підтримує декілька варіантів перевірки — це можуть бути локальні облікові записи, а також підключення до зовнішніх джерел, як-от LDAP або Active Directory, залежно від потреб організації.

Після успішної автентифікації Тасас-сервер передає інформацію щодо прав користувача, відповідно до яких формується доступ до визначених мережевих ресурсів. Такий підхід дозволяє гнучко розмежовувати права доступу згідно з функціональними обов'язками користувачів та рівнем їхньої відповідальності.

Таким чином, застосування Тасас у зв'язці з SSL VPN створює надійний, централізований механізм управління доступом, що відповідає сучасним вимогам до безпеки інформаційних систем.

Успішні впровадження подібних систем:

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		42

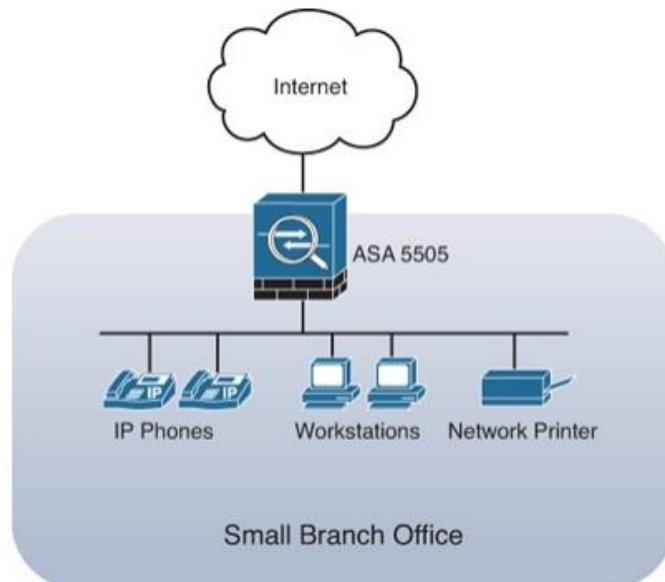


Рис. 2.1 - Розгортання Cisco ASA у малих філіях

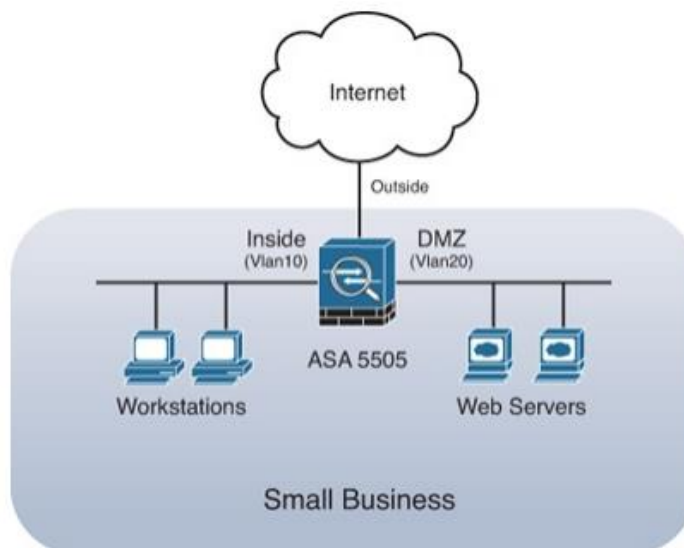


Рис. 2.2 - Розгортання Cisco ASA для малого бізнесу з окремими захищеними мережами

Впровадження системи мережної безпеки на базі Cisco ASA з реалізацією SSL VPN стало ключовим елементом для багатьох організацій, які мають велику потребу у безпеці, доступності та ефективності своїх інформаційних ресурсів. Розглянемо конкретні приклади впровадження таких рішень, що ілюструють реальні приклади вигід та відмінностей в їх використанні.

Таблиця 1.1 – Кейси впровадження подібних систем

Сектор	Виклик	Рішення	Результат
Фінансовий сектор	Організації фінансового сектору мають потребу в високому рівні безпеки фінансових операцій та інформації.	Впровадження Cisco ASA разом з SSL VPN для захищеного доступу.	Зниження ризику фінансових шахрайств, підвищення репутації та впевненості клієнтів.
Глобальна корпорація з ІТ-сервісів	Компанія з управління ІТ-інфраструктурою	Використання Cisco ASA та SSL VPN для	Підвищення продуктивності, скорочення часу
Глобальна корпорація з ІТ-сервісів	має завдання об'єднання різноманітних мережевих ресурсів та забезпечення безпечного зв'язку.	створення захищеного корпоративного каналу.	на вирішення проблем, розширення глобальної доступності.
Освітній сектор	Університетська мережа має завдання забезпечити безпеку електронних ресурсів та надати студентам та викладачам захищений віртуальний доступ.	Використання Cisco ASA та SSL VPN для безпечного віддаленого доступу.	Підвищення рівня безпеки електронної освіти, гнучкість та зручність для учасників освітнього процесу.

2.4. Побудова схеми та розробка адресації

Конфігурація IP-адрес та підмереж є необхідним етапом для забезпечення зв'язку між різними компонентами системи.

Під час конфігурації IP-адрес слід враховувати наступні аспекти:

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		44

1. Підбір IP-адресного простору: Необхідно обрати відповідний діапазон IP-адрес, враховуючи вимоги проєкту та сумісність із наявною мережею. Зазвичай орієнтуються на технічну документацію обладнання або рекомендації щодо безпеки мереж.

2. Розподіл адрес на підмережі: Адресний простір варто структурувати, розбивши його на підмережі відповідно до кількості пристроїв і специфіки окремих сегментів. Це спрощує адміністрування, підвищує безпеку та забезпечує гнучкість для майбутнього розширення.

3. Налаштування IP-адрес на мережевих пристроях: Після призначення IP-адрес та підмереж, необхідно налаштувати ці адреси на мережевих пристроях, таких як маршрутизатори, комутатори та сервери. Це забезпечить правильну маршрутизацію та взаємодію між усіма елементами системи.

4. Перевірка налаштувань: Важливо перевірити правильність конфігурації IP-адрес та підмереж шляхом проведення тестів зв'язку між компонентами системи. Це допоможе переконатися в правильності конфігурації та виявити можливі проблеми до запуску системи в експлуатацію.

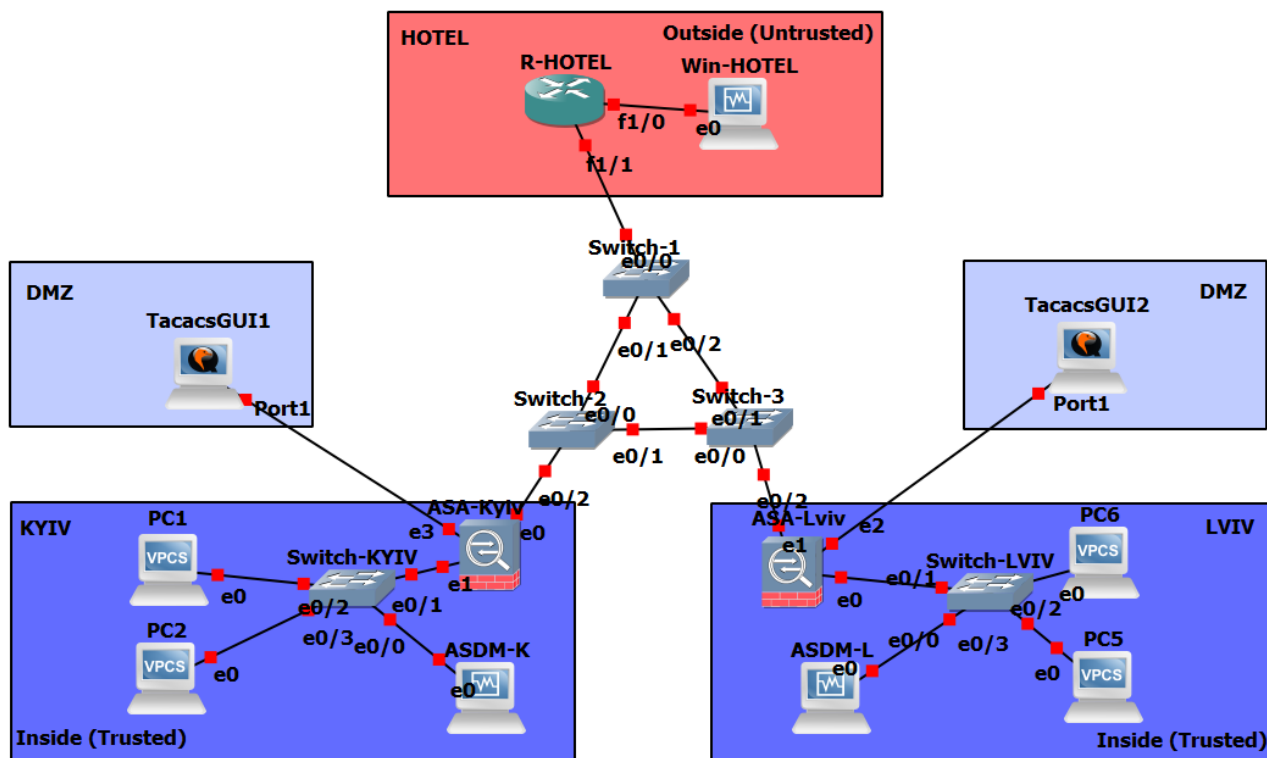


Рис. 2.3 - Проєкт мережі

Таблиця 1.2 – Адресація мережі

Параметри адресації мережі

Мережа/ Пристрій	Інтерфейс	ІР-адреса	Маска	Пре- фікс
Підмережа HOTEL	-	10.10.10.0 145.1.1.0	255.255.255.0	/24
Підмережа KYIV	-	192.168.1.0	255.255.255.0	/24
Підмережа LVIV	-	10.10.10.0	255.255.255.0	/24
Підмережа DMZ- KYIV	-	192.168.2.0	255.255.255.0	/24
Підмережа DMZ- LVIV	-	10.10.20.0	255.255.255.0	/24
ASA-KYIV	Gig0/0	192.168.1.1	255.255.255.0	/24
	Gig0/1	192.168.2.1	255.255.255.0	/24
	Gig0/2	145.1.1.3	255.255.255.0	/24
ASA-LVIV	Gig0/0	10.10.10.1	255.255.255.0	/24
	Gig0/2	10.10.20.1	255.255.255.0	/24
	Gig0/1	145.1.1.1	255.255.255.0	/24
R-HOTEL	Fa0/0	145.1.1.2	255.255.255.0	/24
	Fa1/0	10.10.30.1	255.255.255.0	/24
Win-HOTEL	E0	10.10.30.2	255.255.255.0	/24
ASDM-K	E0	192.168.1.2	255.255.255.0	/24
	Шлюз за замовч.	192.168.1.1	255.255.255.0	/24
ASDM-L	E0	10.10.10.2	255.255.255.0	/24
	Шлюз за замовч.	10.10.10.1	255.255.255.0	/24
Tacsacs-1	Port1	192.168.2.2	255.255.255.0	/24
	Шлюз за замовч.	192.168.2.1	255.255.255.0	/24

Tacacs-2	Port1	10.10.20.2	255.255.255.0	/24
	Шлюз за замовч.	10.10.20.1	255.255.255.0	/24
VPCS-K-1	Fa0/0	192.168.1.3	255.255.255.0	/24
VPCS-K-2	Fa0/0	192.168.1.4	255.255.255.0	/24
VPCS-L-1	Fa0/0	10.10.10.3	255.255.255.0	/24
VPCS-L-2	Fa0/0	10.10.10.4	255.255.255.0	/24

Конфігурація IP-адрес та підмереж є ключовим етапом у проектуванні системи мережної безпеки, оскільки саме вона забезпечує стабільну та безпечну комунікацію між різними компонентами системи.

Використане обладнання для проєкту мережної безпеки

Компанія Cisco, вивчивши потреби ринку, розробила лінійку пристроїв захисту серії ASA, орієнтуючись на можливості масштабування та модернізації, що забезпечує довгострокову ефективність будь-якої обраної конфігурації. На сьогодні компанія пропонує три моделі ASA.

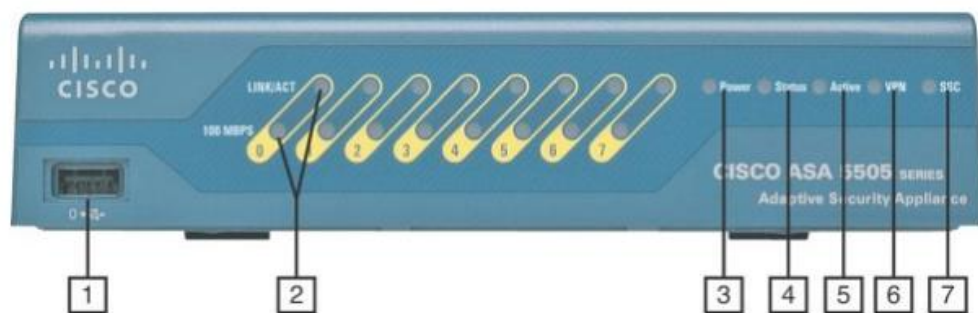


Рис. 2.4 - Cisco ASA 5505 вигляд спереду

Передня панель складається з таких компонентів:

1. Порт USB: Зарезервований для майбутнього використання.
2. Індикатори швидкості та активності з'єднання: Cisco ASA 5505 має світлодіодний індикатор швидкості та окремий світлодіодний індикатор активності каналу для кожного з восьми портів. Коли індикатор швидкості не світиться, це означає, що мережевий трафік передається зі швидкістю 10 мегабіт на секунду (Мбіт/с). Якщо індикатор швидкості

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		47

світиться зеленим кольором, це означає, що мережевий трафік передається зі швидкістю 100 Мбіт/с. Коли індикатор активності з'єднання світиться зеленим кольором, це означає, що фізичне мережеве з'єднання встановлено; коли він блимає, це означає, що є мережева активність.

3. Індикатор живлення: Постійне зелене світіння вказує на те, що пристрій увімкнено.
4. Індикатор стану: Миготливий зелений вказує на те, що система завантажується і проходять тести ввімкнення. Постійне світіння зеленим кольором означає, що системні тести пройдено і система працює. Янтарне світіння вказує на те, що системні тести не пройшли.
5. Індикатор Active: Зелений колір вказує на те, що Cisco ASA активний, коли налаштований на обхід відмов. У разі роботи як автономний пристрій — індикатор також світиться зеленим.
6. Індикатор VPN: Світиться зеленим кольором, вказуючи на те, що один або декілька VPN-тунелів активні.
7. Індикатор SSC: Горить зеленим кольором, якщо в гнізді SSC встановлена картка служби безпеки (SSC).

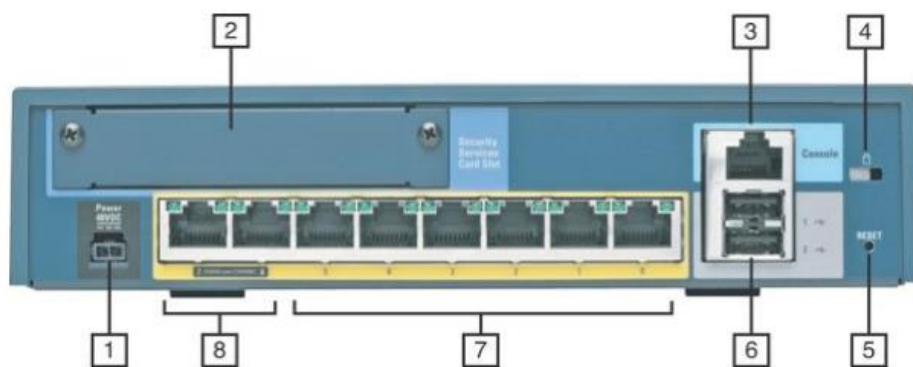


Рис. 2.5 - Cisco ASA 5505 вигляд ззаду

Задня панель містить такі основні елементи:

1. Роз'єм живлення.
2. Слот SSC: призначений для модуля Cisco AIP-SSC-5 (модуль більше не підтримується та знятий з продажу).
3. Послідовний консольний порт: Консольний порт RJ-45 дозволяє фізично підключитися до пристрою для доступу до його інтерфейсу командного

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		48

рядка (CLI) для початкового налаштування.

4. Фізичне блокування: замок для унеможливлення несанкціонованого доступу до пристрою.
5. Кнопка скидання: Зарезервована для майбутнього використання.
6. Два порти USB версії 2.0: також зарезервовані для майбутніх функцій.
7. Порти комутатора Ethernet з 0 по 5: порти комутатора 10/100 Fast Ethernet.
8. Порти комутатора Ethernet 6 і 7: порти комутатора 10/100 Fast Ethernet з підтримкою PoE [5].

Модель Cisco ASA 5510 - ідеальний для малих і середніх компаній із обмеженим бюджетом. Забезпечує базовий рівень захисту та продуктивності на стартовому етапі розвитку.

Модель Cisco ASA 5520 - підходить для організацій із зростаючими потребами — пропонує більше інтерфейсів, підтримку Gigabit Ethernet і вищу пропускну здатність. Оптимальний варіант для середніх і великих мережевих середовищ. (Рис. 2.6.)

Модель Cisco ASA 5540 - орієнтований на великі підприємства з високими вимогами до безпеки. Забезпечує масштабовану та стійку інфраструктуру захисту. [1]

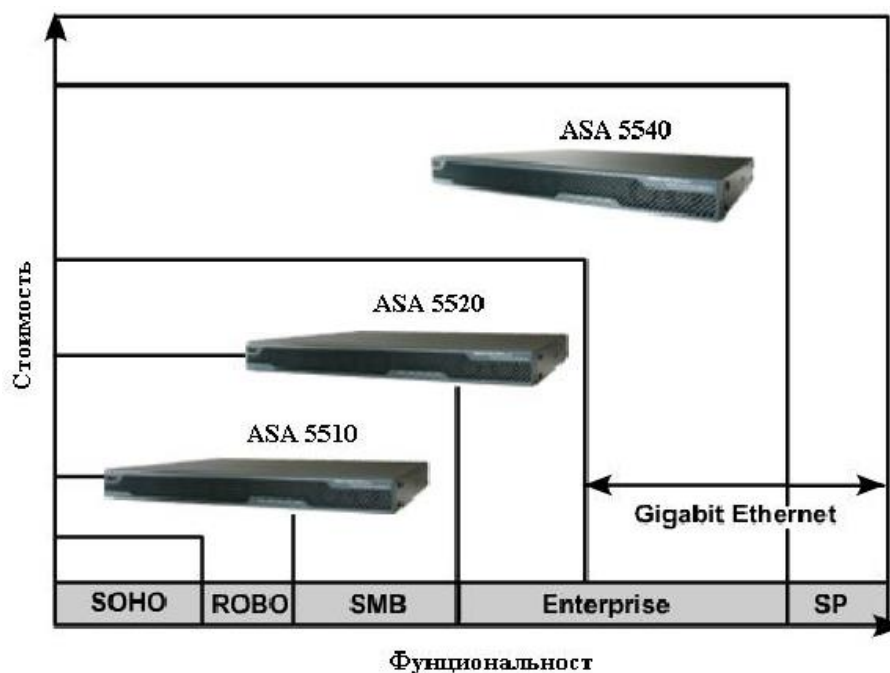


Рис. 2.6 - Залежність функціональності від ціни продукції ASA

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		49

В усіх моделях передбачена можливість додавання інших служб захисту, таких як модулі адаптивної перевірки (Рис. 2.7) та запобігання атакам (AIP-SSM), а також забезпечення безпеки вмісту (CSC-SSM).



Рис. 2.7 - SSM слот

Завдяки гнучкій архітектурі пристрої Cisco ASA можуть адаптуватися до динамічного ландшафту загроз, забезпечуючи довгострокову ефективність захисту.

В таблиці 3 наведені характеристики приладів захисту ASA:

Табл. 1.3 – Характеристики моделей Cisco ASA

	ASA 5510	ASA 5520	ASA 5540
Продуктивність фаєрволу, Мбіт/с	До 300	До 450	До 650
Продуктивність віжраження атак, Мбіт/с	150 з AIP SSM-10 300 с AIP SSM-20	225 з AIP-SSM-10 375 з AIP-SSM-20 450 з AIP-SSM-40	500 з AIP-SSM-20 650 з AIP-SSM-40
Продуктивність VPN, Мбіт/с	До 170	До 225	До 325
Число одночасно підтримуваних сеансів	32 000/64 000	130 000	280 000
Число тунелів IPsec VPN	50/150	300/750	500/2000/5000
Число тунелів SSL VPN	50/150	300/750	500/1250/2500
Віртуальні фаєрволи	0	2/10	2/50

Продовження таблиці 1.3 – Характеристики моделей Cisco ASA

Відмовостійкість	Active/Standby	Active/Active та Active/Standby	Active/Active та Active/Standby
Кластеризація та балансування VPN	Ні	Так	Так
Підтримувані фізичні інтерфейси	3 FastEthernet + 1 порт керування/5 FastErhernet	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet
Підтримувані логічні інтерфейси VLAN 802.1q	0/10	25	100

Висновок до другого розділу:

У цьому розділі розглянуто вимоги до безпеки та функціональних можливостей системи захищеного віддаленого доступу на основі технології SSL VPN. Проведено детальний аналіз архітектури та ключових елементів системи, включаючи комунікаційну модель. Описано процес налаштування та інтеграції обладнання, зокрема підключення Тасас-сервера та взаємодію з наявною інфраструктурою мережі. За підсумками аналізу встановлено, що використання SSL VPN забезпечує ефективний захист і зручність доступу для віддалених користувачів у корпоративних мережах.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ ТА ТЕСТУВАННЯ СИСТЕМИ МЕРЕЖНОЇ БЕЗПЕКИ

3.1. Впровадження системи

3.1.1. Налаштування протоколу SSL VPN (Clientless SSL VPN)

Для забезпечення віддаленого доступу користувачів до мережевих ресурсів через протокол SSL VPN було налаштовано пристрій Cisco за допомогою графічного інтерфейсу Cisco ASDM (Adaptive Security Device Manager).

Кроки налаштування:

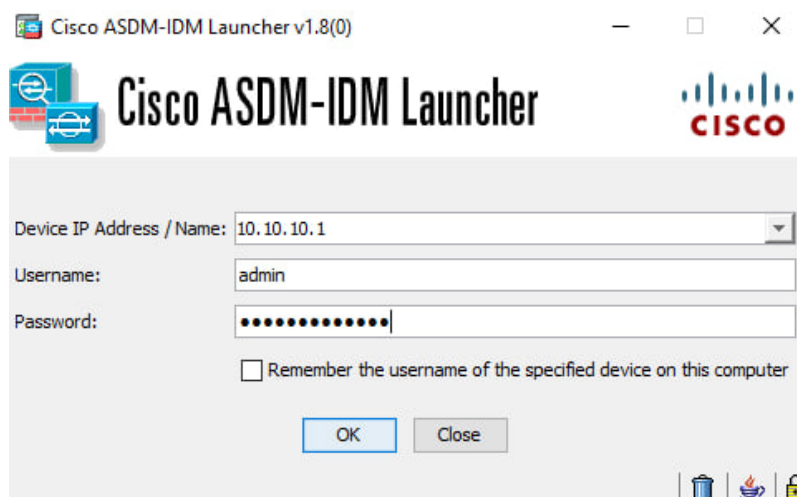


Рис. 3.1 - Сторінка входу в Cisco ASDM Launcher

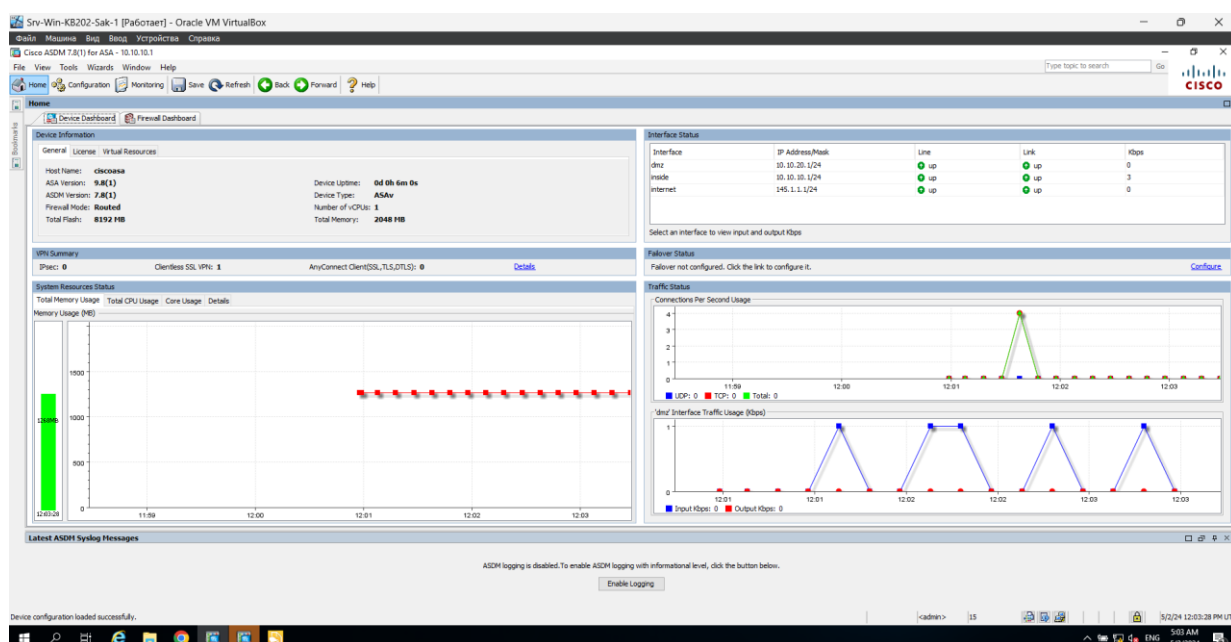


Рис. 3.2 - Домашня сторінка ASDM

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк. 52
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		

1. Створення профілю SSL VPN:

- За допомогою майстера налаштування Clientless SSL VPN в Cisco ASDM було створено новий профіль SSL VPN.
- У профілі були задані такі параметри, як ім'я профілю, діапазон IP-адрес, перелік доступних ресурсів параметри безпеки.

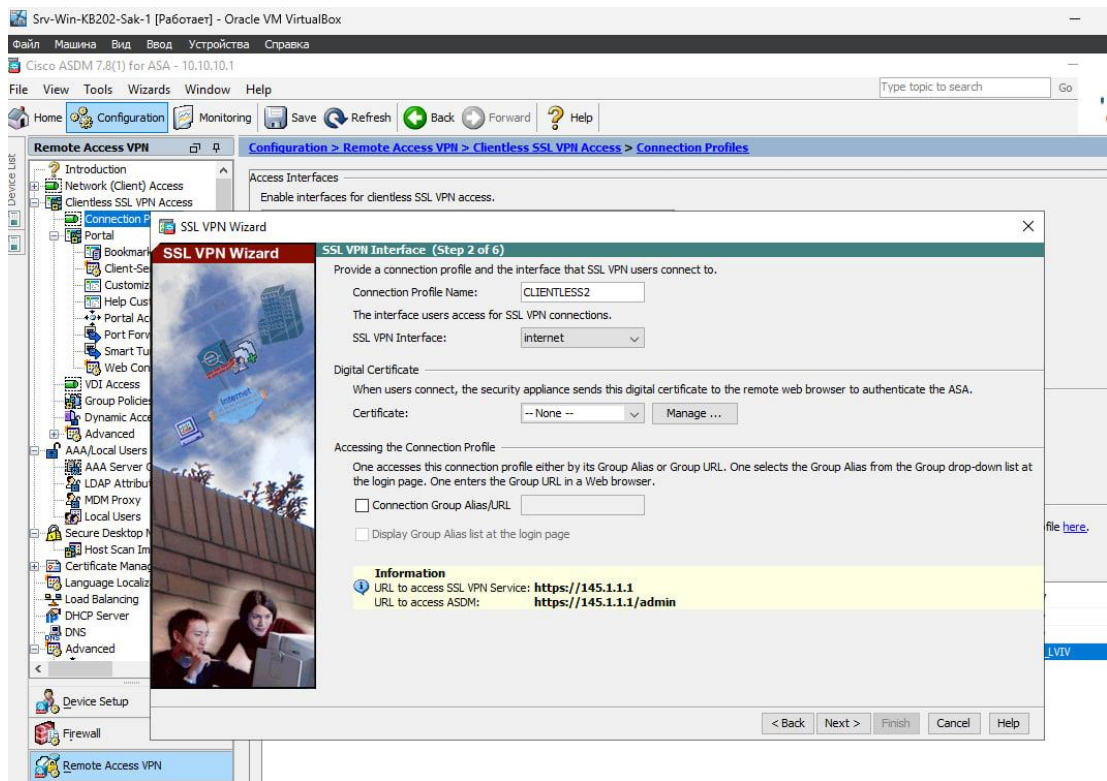


Рис. 3.3 - Сторінка налаштувань SSL VPN

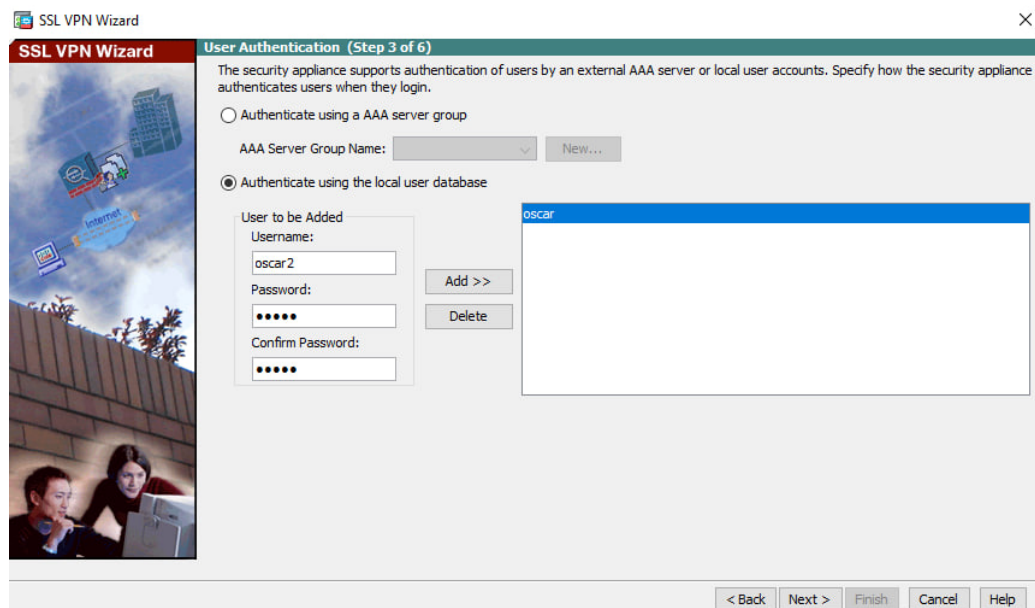


Рис. 3.4 - Процес створення користувача для входу на веб-портал SSL VPN

Service

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		53

2. Налаштування доступу до ресурсів:

- У розділі "**Bookmarks**" було визначено перелік веб-сайтів, файлів і мережевих ресурсів, доступних через SSL VPN-портал.

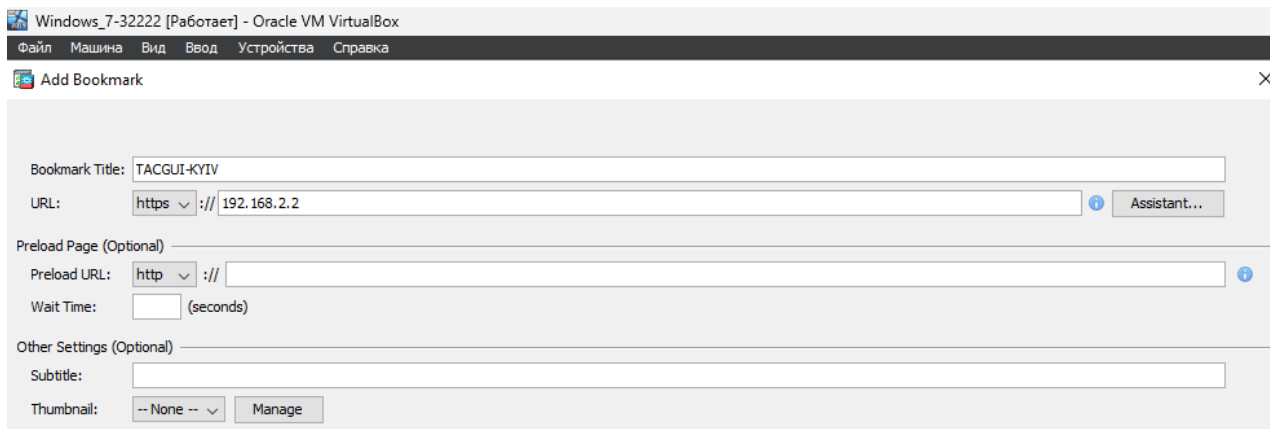


Рис. 3.5 - Додавання закладки до TACGUI-KYIV

3. Налаштування безпеки:

- Для забезпечення захищеної передачі даних через Інтернет були налаштовані параметри безпеки, зокрема шифрування SSL-трафіку та перевірка цифрових сертифікатів.

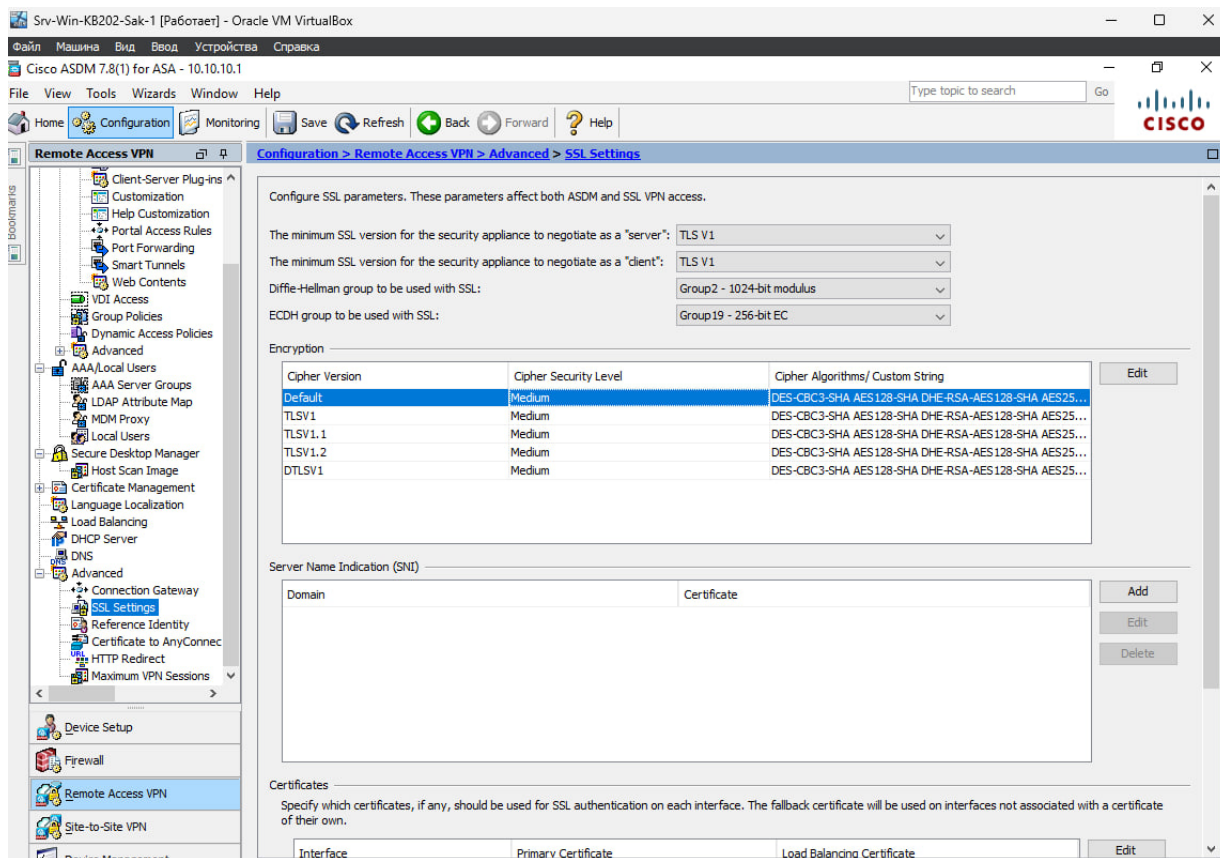


Рис. 3.6 - Основні налаштування безпеки SSL VPN

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		54

4. Перегляд та збереження налаштувань:

- Після завершення налаштування було здійснено перевірку всіх параметрів та внесених змін.
- За допомогою функцій "**Apply**" та "**Save Configuration**" зміни було застосовано й збережено у конфігурації.

У результаті було успішно реалізовано налаштування SSL VPN за допомогою Cisco ASDM, що забезпечило безпечний віддалений доступ користувачів до мережевих ресурсів через веб-браузер.

3.1.2 Конфігурації Syslog та DHCP серверів, STP, ACL

Конфігурація Kiwi Syslog Server виконується з метою централізованого збору, зберігання та аналізу системних журналів подій від різноманітних мережевих пристроїв. Цей інструмент забезпечує гнучкі можливості фільтрації, сортування та візуалізації логів, що значно полегшує адміністрування інфраструктури та своєчасне виявлення проблем.

Основні етапи налаштування Kiwi Syslog Server:

1. Завантаження та встановлення Kiwi Syslog Server на комп'ютер або сервер, який виступатиме центральним вузлом для збору логів.

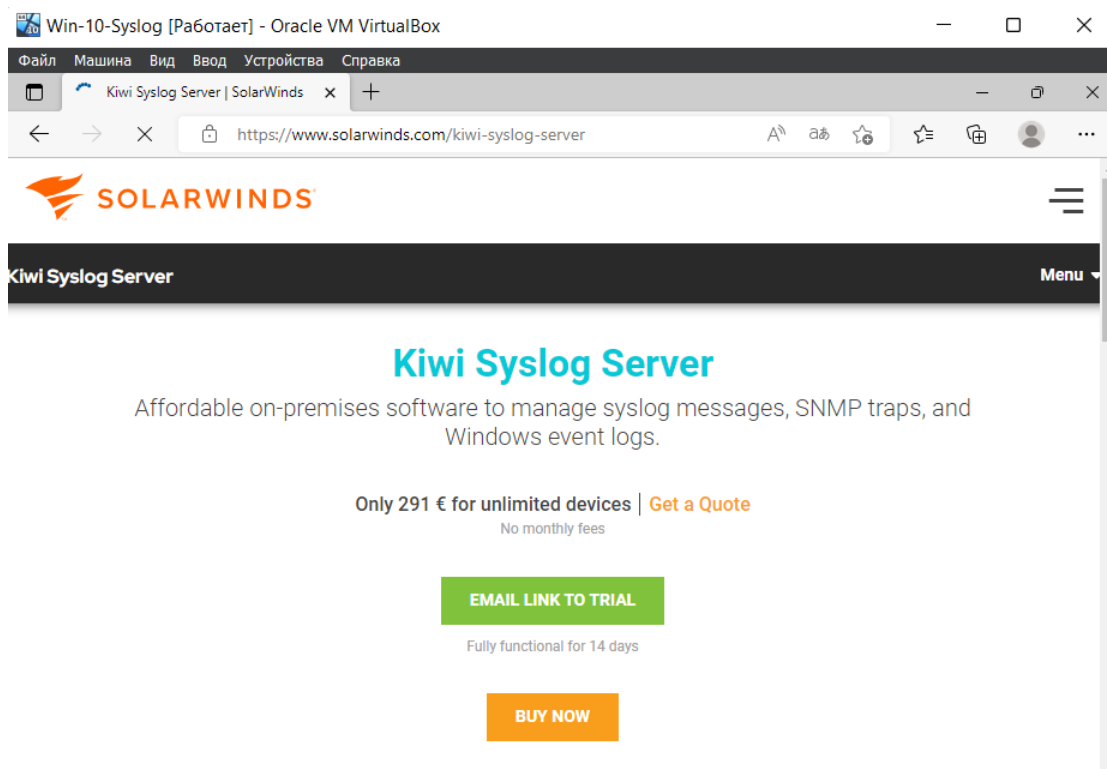


Рис. 3.7 - Офіційний сайт Kiwi Syslog Server. (посилання для завантаження)

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		55

2. Конфігурація збору логів. Визначення переліку пристроїв (за IP-адресами або DNS-іменами), з яких надходитимуть журнали. При потребі додаються фільтри та правила для сортування подій за категоріями або рівнями важливості.

3. Налаштування збереження. Вказується каталог або база даних для збереження логів, встановлюється частота архівації або обмеження на обсяг файлів журналів.

4. Після збереження налаштувань запускається служба збору подій.

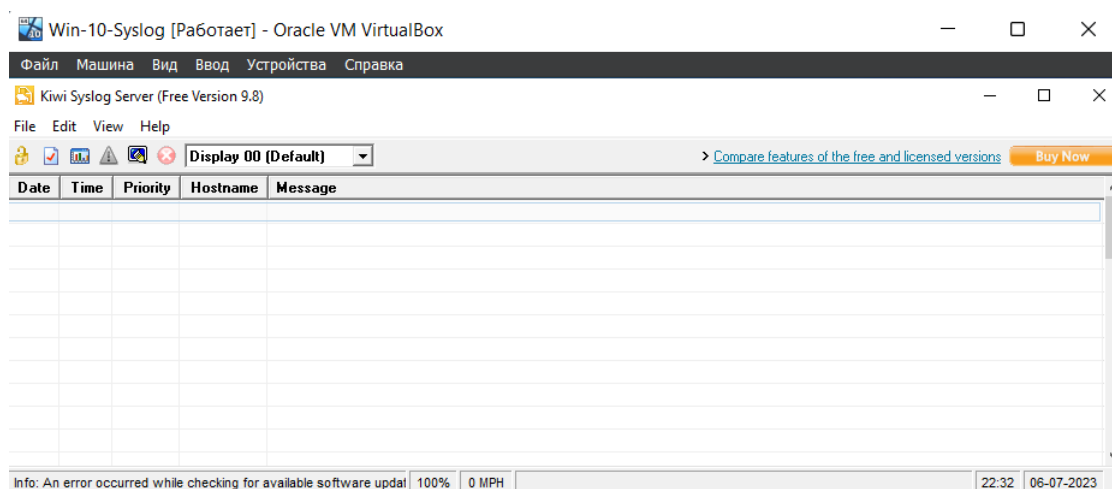


Рис. 3.8 - Головне вікно Kiwi Syslog Server

Переконалися, що він почав збирати журнали з налаштованих пристроїв (результат буде надано в наступному розділі)

Після успішного запуску Kiwi Syslog Server починає отримувати дані з налаштованих джерел. Це дозволяє в режимі реального часу відслідковувати стан мережевих компонентів, оперативно реагувати на інциденти та підвищувати загальний рівень інформаційної безпеки інфраструктури.

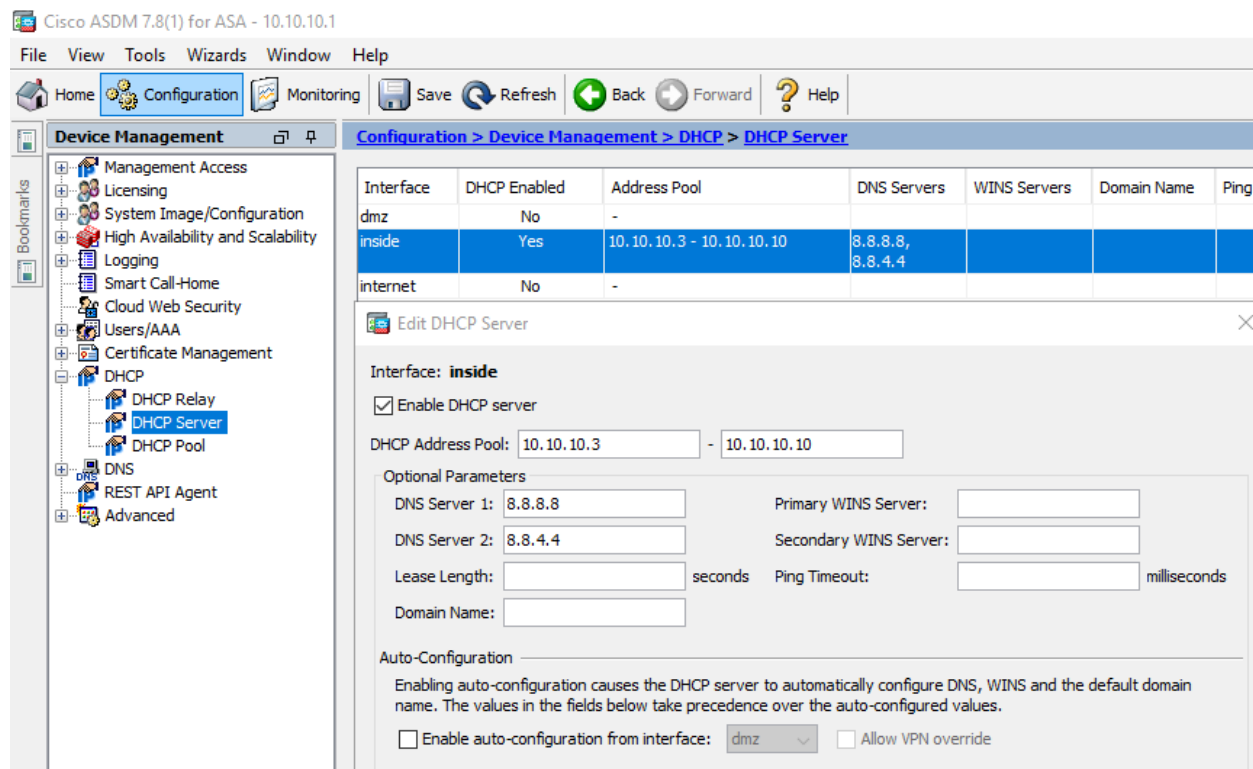


Рис. 3.9 - Основні налаштування DHCP на ASDM-L (ASA-LVIV)

```
PC1> ip dhcp
DORA IP 192.168.1.10/24 GW 192.168.1.1

PC5> ip dhcp
DORA IP 10.10.10.10/24 GW 10.10.10.1
```

Рис. 3.10 - Результат налаштування DHCP сервера

Налаштування STP

Для гарантування безперебійної роботи мережевої інфраструктури та запобігання виникненню мережеских петель на яdroвому рівні було впроваджено протокол **Spanning Tree Protocol (STP)**. Основні команди для налаштування STP були виконані наступним чином:

Встановлення пріоритету кореневого комутатора (Switch-1):

Switch-1(config)# spanning-tree vlan 1 priority 4096

Налаштування комутаторів Switch-2 та Switch-2 для зменшення пріоритету, щоб вони не стали корневими:

Switch-2(config)# spanning-tree vlan 1 priority 8192

Switch-3(config)# spanning-tree vlan 1 priority 12288

Налаштування PortFast та BPDU Guard для інтерфейсів підключення кінцевих пристроїв:

```
Switch-1(config)# interface range e0/0 – 2
Switch-1(config-if-range)# spanning-tree portfast
Switch-1(config)# interface e0/0
Switch-1(config-if-range)# spanning-tree bpduguard enable
Switch-2(config)# interface range e0/0 – 2
Switch-2(config-if-range)# spanning-tree portfast
Switch-2(config)# interface e0/2
Switch-2(config-if-range)# spanning-tree bpduguard enable
Switch-3(config)# interface range e0/0 – 2
Switch-3(config-if-range)# spanning-tree portfast
Switch-3(config)# interface e0/2
Switch-3(config-if-range)# spanning-tree bpduguard enable
```

У результаті налаштувань комутатор **Switch-1** було призначено кореневим (root bridge), тоді як **Switch-2** і **Switch-3** виконують функції резервних вузлів. Додатково були активовані функції **PortFast** та **BPDU Guard** для прискореного підключення кінцевих пристроїв і захисту від можливих петель, які можуть виникнути через неправильне підключення користувацьких пристроїв.

Налаштування ACL

З метою контролю доступу та підвищення рівня інформаційної безпеки мережі були налаштовані списки контролю доступу (ACL) на міжмережевих екранах Cisco ASA у містах Київ та Львів.

Налаштування на ASA-KYIV

```
ASA-KYIV(config)# access-list OUTSIDE_IN permit tcp any host 145.1.1.3
eq 22
```

```
ASA-KYIV(config)# access-list OUTSIDE_IN permit tcp any host 145.1.1.3
eq 80
```

```
ASA-KYIV(config)# access-list OUTSIDE_IN permit tcp any host 145.1.1.3
eq 443
```

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		58

```
ASA-KYIV(config)# access-list OUTSIDE_IN permit udp any host 145.1.1.3  
eq 53
```

```
ASA-KYIV(config)# access-list OUTSIDE_IN permit icmp any any
```

```
ASA-KYIV(config)# access-list OUTSIDE_IN deny ip any any
```

```
ASA-KYIV(config)# access-group OUTSIDE_IN in interface outside
```

Конфігурація ACL передбачає дозвіл лише необхідного трафіку ззовні до внутрішньої мережі — таких сервісів, як **SSH, HTTP, HTTPS, DNS** та **ICMP**. Весь інший трафік блокується, що дозволяє ефективно захищати мережу від несанкціонованого доступу.

Таким чином, імплементація STP та ACL забезпечила високу надійність мережевої інфраструктури, запобігла формуванню петель і встановила чіткі правила доступу до критичних ресурсів.

3.2. Тестування системи

3.2.1. Проведення тестових сценаріїв віддаленого доступу до серверів та логування

У цьому розділі було проведено тестування налаштованого протоколу Clientless SSL VPN на Cisco ASA, а також перевірка роботи Kiwi Syslog Server. VPN-рішення дозволяє користувачам поза межами корпоративної мережі безпечно підключатися до внутрішніх ресурсів через звичайний веб-браузер. Перевірка охоплювала коректність сертифікатів, політик доступу, параметрів шифрування та стабільність з'єднання з різних пристроїв і мереж.

Особливу увагу приділено роботі веб-інтерфейсу Cisco ASA, де були створені закладки для швидкого доступу до веб-ресурсів, зокрема до інтерфейсу Tacsacs-сервера. Це спрощує користувачам взаємодію з інфраструктурою без необхідності встановлення додаткового клієнтського програмного забезпечення.

Було також протестовано інтеграцію з Kiwi Syslog Server для збору та аналізу логів. Перевірка включала тестування налаштувань логування, аналіз подій для виявлення потенційних аномалій та оцінку ефективності оповіщень про інциденти безпеки. Симульовано кілька сценаріїв підключення та обробки помилок для забезпечення надійного логування.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		59

Отримані результати підтверджують, що налаштування Clientless SSL VPN працюють коректно, забезпечуючи надійний та захищений доступ. Kiwi Syslog Server успішно виконує функції моніторингу та зберігання логів, що підвищує загальний рівень контролю та безпеки мережі.

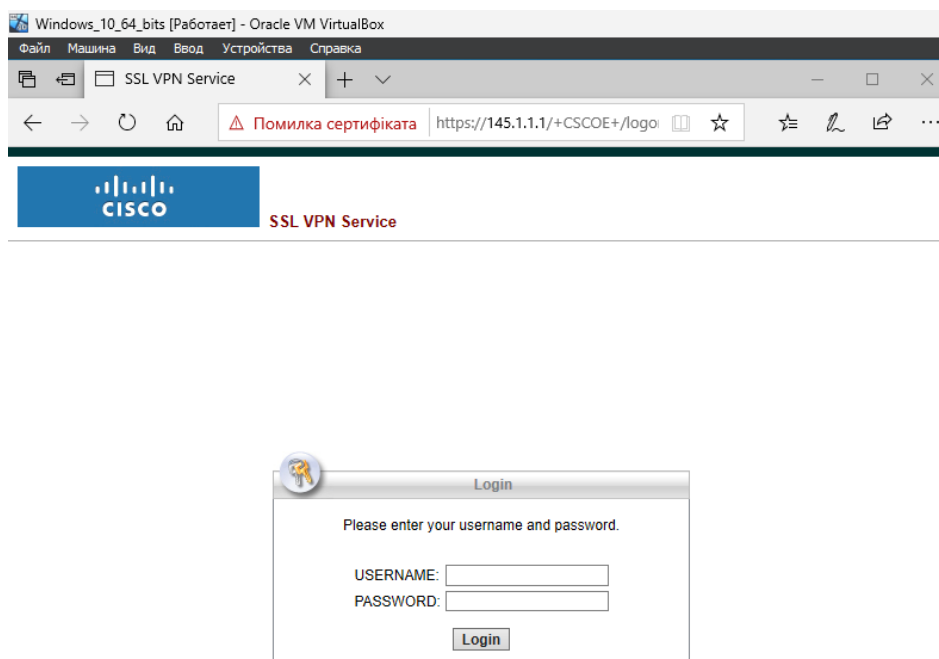


Рис. 3.11 - Результат підключення до SSL VPN Service (LVIV)

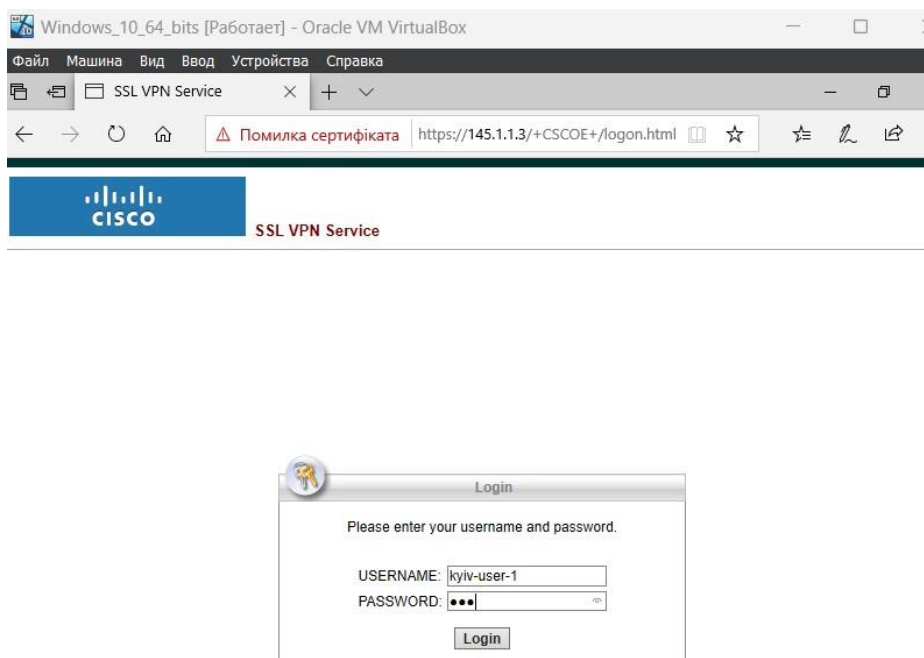


Рис. 3.12 - Результат підключення до SSL VPN Service (KYIV)

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				60
Змн.3	Арк.А	№ докум.	Підпис	Дата		

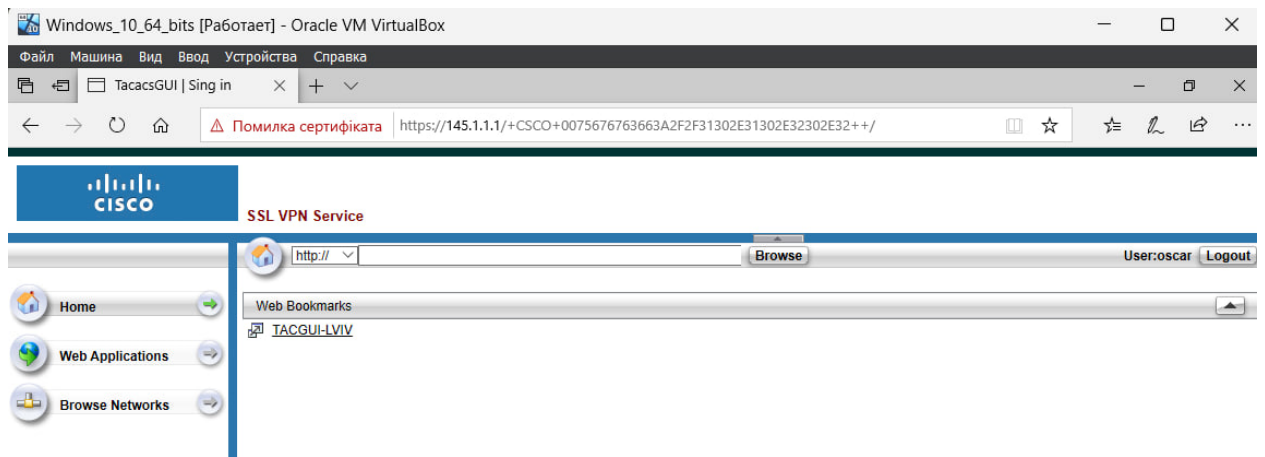


Рис. 3.13 - Сторінка веб-інтерфейсу SSL VPN з наявною закладкою TACACS-сервера (LVIV)

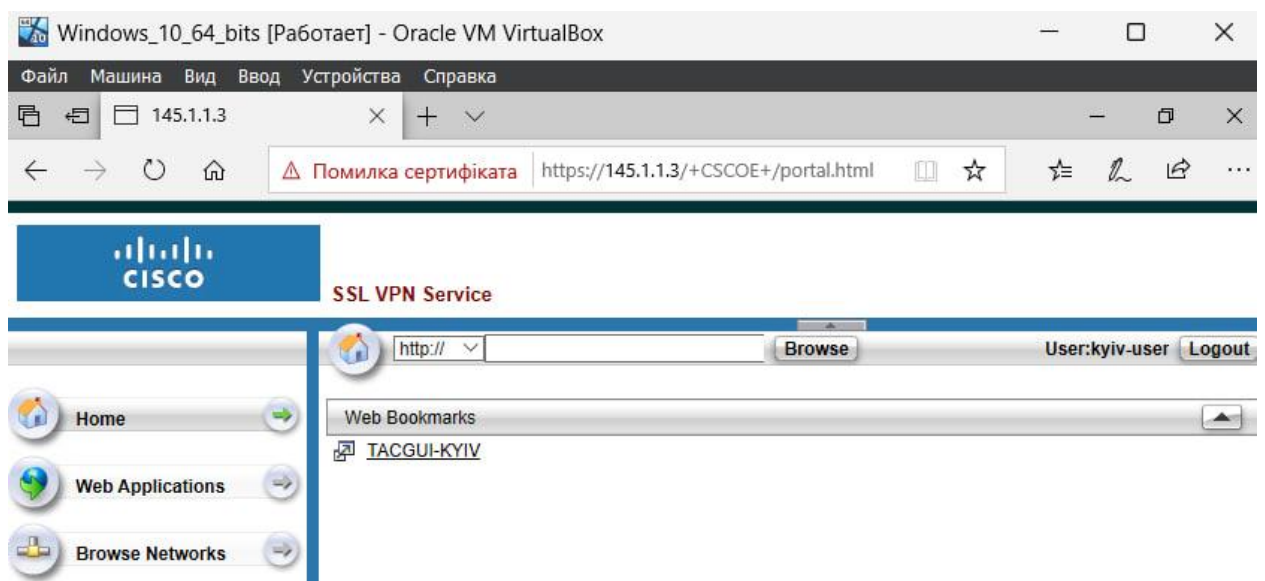


Рис. 3.14 - Сторінка веб-інтерфейсу SSL VPN з наявною закладкою до TACACS-сервера (KYIV)

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		61

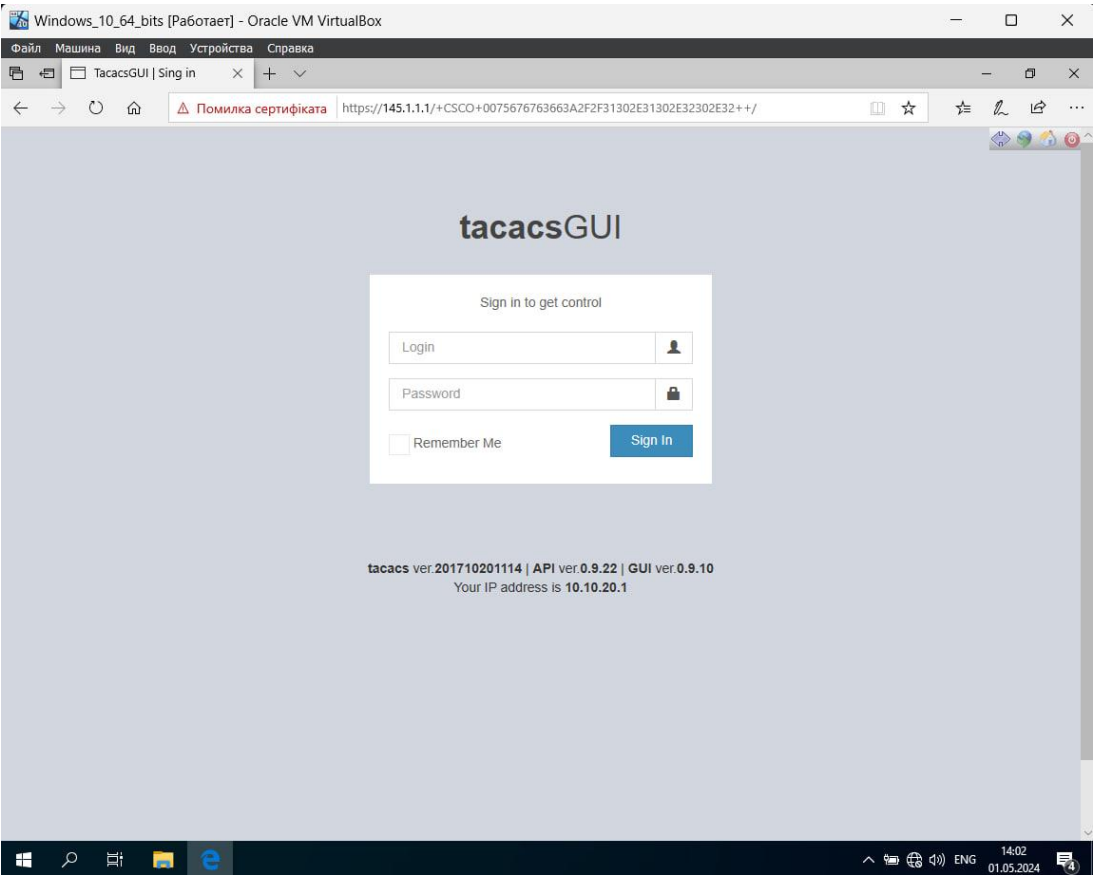


Рис. 3.15 - Аутентифікація до TACACS-GUI (LVIV)

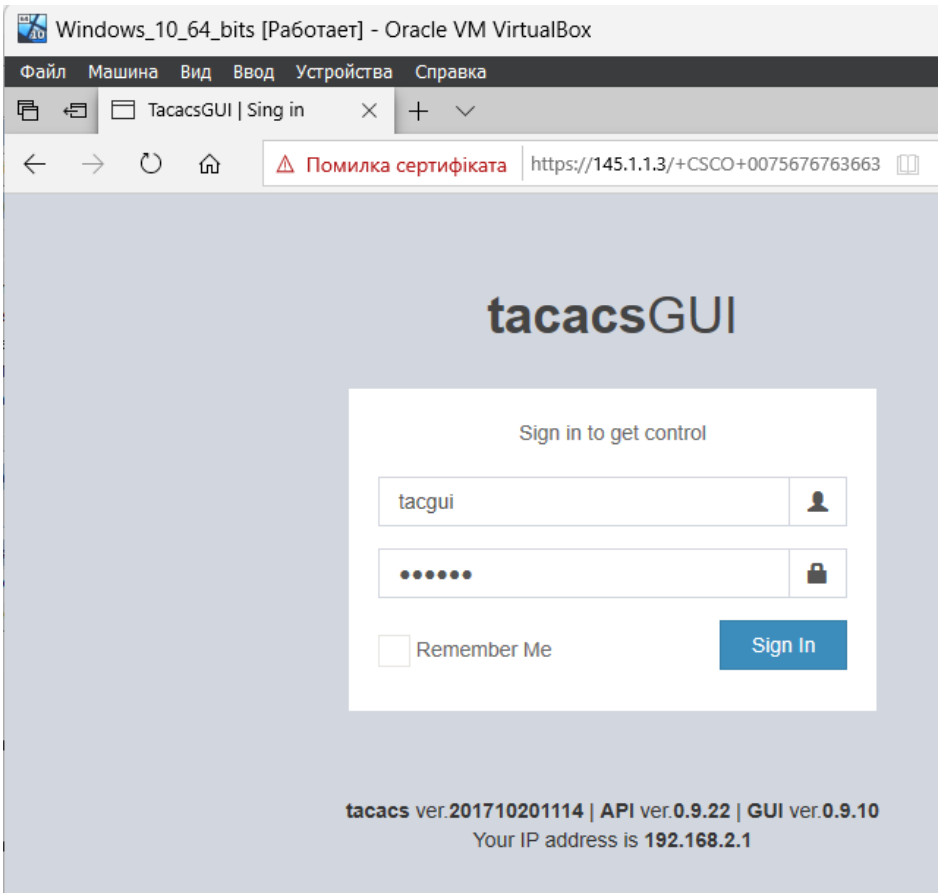


Рис. 3.16 - Автентифікація до TACACS-GUI (KYIV)

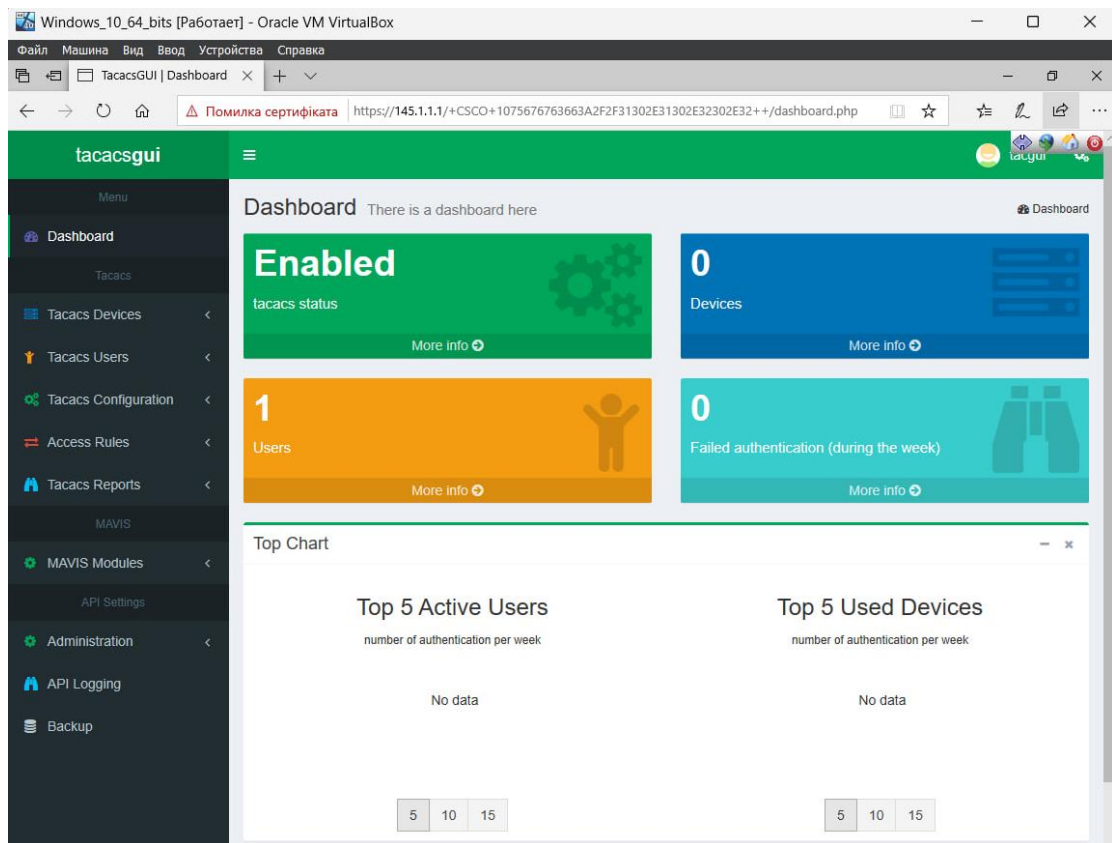


Рис. 3.17 - Результат вдалого підключення до tacacsGUI (LVIV)

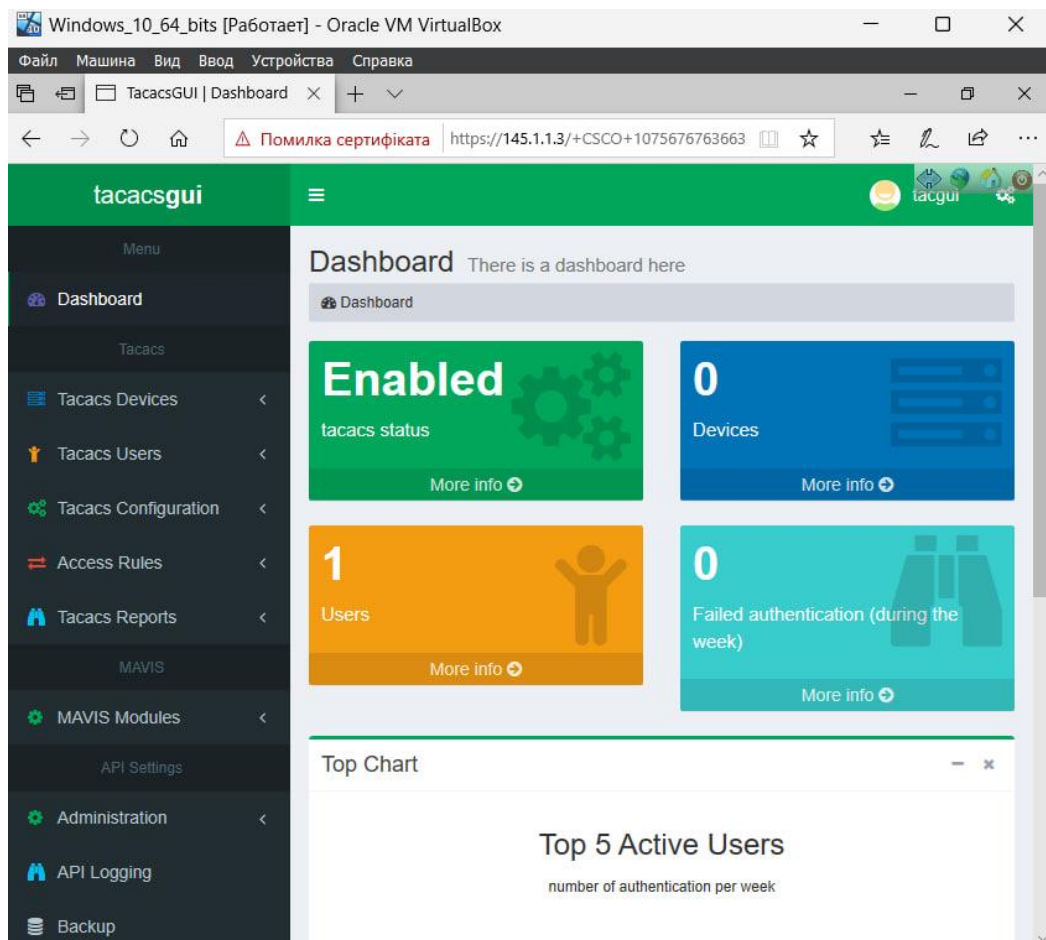
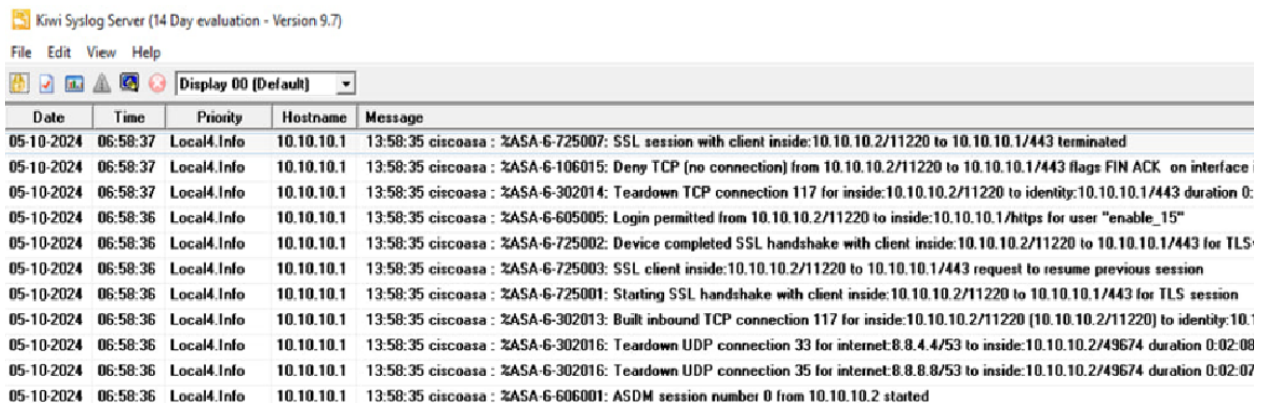


Рис. 3.18 - Результат вдалого підключення до tacacsGUI (KYIV)

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				63
Змн.3	Арк.А	№ докум.	Підпис	Дата		

3.2.2. Аналіз логів

Було перевірено працездатність Syslog-сервера, і підтверджено, що журналювання подій функціонує належним чином.



Kiwi Syslog Server (14 Day evaluation - Version 9.7)

File Edit View Help

Display 00 (Default)

Date	Time	Priority	Hostname	Message
05-10-2024	06:58:37	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-725007: SSL session with client inside:10.10.10.2/11220 to 10.10.10.1/443 terminated
05-10-2024	06:58:37	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-106015: Deny TCP (no connection) from 10.10.10.2/11220 to 10.10.10.1/443 (flags FIN ACK) on interface
05-10-2024	06:58:37	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-302014: Teardown TCP connection 117 for inside:10.10.10.2/11220 to identity:10.10.10.1/443 duration 0:
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-605005: Login permitted from 10.10.10.2/11220 to inside:10.10.10.1/https for user "enable_15"
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-725002: Device completed SSL handshake with client inside:10.10.10.2/11220 to 10.10.10.1/443 for TLS
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-725003: SSL client inside:10.10.10.2/11220 to 10.10.10.1/443 request to resume previous session
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-725001: Starting SSL handshake with client inside:10.10.10.2/11220 to 10.10.10.1/443 for TLS session
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-302013: Built inbound TCP connection 117 for inside:10.10.10.2/11220 (10.10.10.2/11220) to identity:10.1
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-302016: Teardown UDP connection 33 for internet:8.8.4.4/53 to inside:10.10.10.2/49674 duration 0:02:08
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-302016: Teardown UDP connection 35 for internet:8.8.8.8/53 to inside:10.10.10.2/49674 duration 0:02:07
05-10-2024	06:58:36	Local4.Info	10.10.10.1	13:58:35 ciscoasa : %ASA-6-606001: ASDM session number 0 from 10.10.10.2 started

Рис. 3.19 - Результат роботи Kiwi Syslog сервера

На основі зібраних логів зроблено такі висновки щодо стану мережі та її безпеки:

1. Аналіз з'єднань та їх завершення:

- Подія з кодом 725007 вказує на завершення SSL-сесії між клієнтом 10.10.10.2/11220 та сервером 10.10.10.1/443.
- Подія 302014 свідчить про завершення TCP-з'єднання з внутрішнього адреса 10.10.10.2/11220 до ідентифікатора 10.10.10.1/443.
- Ці логи підтверджують стабільність роботи ммережі без збоїв та несанкціонованих розривів з'єднань.

2. Виявлення та блокування підозрілої активності:

- Лог з кодом 106015 фіксує відмову у встановленні TCP-з'єднання з адреси 10.10.10.2 до порту 443, що може вказувати на спробу несанкціонованого доступу.
- Подія 302016 демонструє завершення UDP-з'єднання з зовнішньої IP-адреси 8.8.8.4 до 10.10.10.2 — можливе сканування або тестування портівсканування.

3. Дозволені з'єднання та успішна аутентифікація:

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.З	Арк.А	№ докум.	Підпис	Дата		64

- Лог з кодом 605005 підтверджує успішний дозвіл HTTPS-з'єднання з 10.10.10.2/11220 до 10.10.10.1 для користувача з правами "enable_15".
- Подія 725003 свідчить про успішне SSL-рукоостискання з клієнтом, що означає правильно налаштоване захищене з'єднання.

4. Запуск сесій та процесів:

- Лог 606001 інформує про запуск сесії ASDM з адреси 10.10.10.2, що вказує на адміністративний доступ до пристрою для проведення налаштувань або моніторингу.

На основі цих логів можна дійти висновку, що мережа працює стабільно, а впроваджені засоби безпеки ефективно фіксують як легітимну активність, так і потенційні загрози. Регулярний аналіз подібних логів дозволяє оперативно виявляти аномалії та зберігати високий рівень захисту інфраструктури.

Висновки до третього розділу:

У даному розділі була розглянута система мережної безпеки на базі Cisco ASA з реалізацією SSL VPN та Syslog-сервера. Проведений аналіз засвідчив, що використання Clientless SSL VPN не лише гарантує конфіденційність і безпечну передачу даних, але й забезпечує зручний доступ до корпоративних ресурсів через Інтернет. Такий підхід надає можливість працювати з важливою інформацією з будь-якого місця та пристрою, що має підключення до мережі. Додатково, конфігурація системи Syslog була виконана з особливою увагою для забезпечення збору, збереження та аналізу журналів подій, що дозволяє ефективно здійснювати моніторинг і підвищувати рівень мережевої безпеки. Такий підхід свідчить про те, що увага до деталей та використання сучасних технологій допомагає забезпечити стабільність та безпеку мережі компанії.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		65

ВИСНОВКИ

Дипломний проєкт присвячений налаштуванню мережевих сервісів, зокрема Clientless SSL VPN та Cisco ASA, що є важливими складовими для створення безпечної та ефективної мережевої інфраструктури. У ході виконання роботи було розглянуто основні аспекти конфігурації цих сервісів

Було розглянуто технологію SSL VPN у контексті її історії, розвитку та ключових аспектів цифрової безпеки. Проведений аналіз стосується захисту даних та протоколів шифрування, а також основ VPN, включаючи різні методи тунелювання та захищені з'єднання. Цей розділ надає загальне уявлення про функціонування технології SSL VPN та її важливість у забезпеченні безпеки мережі.

Ретельно проаналізовано вимоги до безпеки та функціональності системи захищеного віддаленого доступу на основі SSL VPN. Виявлено, що SSL VPN є ефективним інструментом для забезпечення безпеки та зручності роботи з віддаленими користувачами в мережевих середовищах.

Була налаштована система мережної безпеки на базі Cisco ASA та SSL VPN та Syslog-сервера. Встановлено, що використання безклієнтського SSL VPN дозволяє забезпечити конфіденційність та безпеку передачі даних і зручний доступ до корпоративних ресурсів через Інтернет.

Загальною метою цієї дипломної роботи було налаштування Clientless SSL VPN на основі Cisco ASA та Syslog-сервера. У результаті вдалося досягти високого рівня безпеки та конфіденційності мережевих з'єднань, забезпечити зручний доступ до корпоративних ресурсів через Інтернет і централізоване журналювання подій. Отримані результати можуть бути практично застосовані для створення безпечної мережевої інфраструктури в організаціях, що потребують надійного віддаленого доступу.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		66

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Джазіб Ф. Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services / Д. Фрахім, О. Сантос, А. Оссіпов., 2014. – 1248 с.
2. Штейнберг Д. SSL VPN: Understanding, evaluating and planning secure, web-based remote access / Д. Штейнберг, 2005. – 327 с.
3. Столлінгс У. Network Security Essentials: Applications and Standards / Столлінгс Уільям., 2016. – 464 с.
4. Фрахім Д. SSL Remote Access VPNs / Д. Фрахім, Ц. Хуанг., 2008. – 349 с.
5. Дон Р. Кроулі Cisco ASA for Accidental Administrators: An Illustrated Step-by-Step ASA Learning and Configuration Guide / Р Кроулі Дон., 2015. – 258 с.
6. Реріс Д. Securing VoIP: Keeping Your VoIP Network Safe / Джонс Реріс., 2014. – 220 с.
7. Штуттард Д. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws / Дафід Штуттард., 2011. – 1232 с.
8. Network Security Essentials: Applications and Standards [Книга, авторства Уільяма Столлінгса]
9. Курос Д. Computer Networking: A Top-Down Approach / Джеймс Ф. Курос., 2022. – 864 с.
10. Фолл К. TCP/IP Illustrated: The Protocols, Volume 1 / К. Фолл, Р. Стівенс., 2011. – 1056 с
11. Уайт Р. Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks / Рус Уайт., 2017. – 1431 с.
12. Донахью Г. Network Warrior / Гері Донахью., 2007. – 504 с.
13. Ламмл Т. CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125 / Тодд Ламмл., 2016. – 1069 с.
14. Столлінгс В. Network Security Essentials: Applications and Standards / Вільям Столлінгс., 2016. – 464 с.
15. Чапелл Л. Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide / Лаура Чапелл., 2014. – 986 с.
16. Едельман Д. Network Programmability and Automation: Skills for the Next-Generation Network Engineer / Д. Едельман, М. Освальт., 2023. – 825 с.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		67

17. Дойл Д. Routing TCP/IP: CCIE Professional Development: CCIE Professional Development / Джефф Дойл., 2016. – 1125 с.

18. Столлінгс В. Data And Computer Communications 10Th Edition / Вільям Столлінгс., 2017. – 912 с.

19. Григорик І. High Performance Browser Networking: What every web developer should know about networking and web performance / Ілля Григорик., 2013. – 653 с.

20. Пітерсон Л. Computer Networks: A Systems Approach / Л. Пітерсон, Б. Дейві., 2011. – 920 с.

21. Хупер Г. CCNP Security VPN 642-647 Official Cert Guide / Говард Хупер., 2011. – 725 с.

22. Андреа Г. Cisco ASA Firewall Fundamentals - 3rd Edition: Step-By-Step Practical Configuration Guide Using the CLI for ASA v8.x and v9.x / Гарріс Андреа., 2014. – 296 с.

23. Андреа Г. Cisco VPN Configuration Guide: Step-By-Step Configuration of Cisco VPNs for ASA and Routers / Гарріс Андреа., 2014. – 260 с.

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		68

Додатки

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		69

Лістинг конфігураційних файлів всіх пристроїв мережі

Конфігурація Cisco ASA (ASA-LVIV):

```

Serial Number: 9A0C5S86E54
Hardware: ASAv, 2048 MB RAM, CPU
Pentium II 2495 MHz
ASA Version 9.8(1)
!
hostname ASA-LVIV
enable                                     password
$sha512$5000$J+Gj41sqXN8SuEvvhquVB
A == $Yy2QnF1/iVm6a1znUHI7sA ==
pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq
domain
xlate per-session deny udp any4 any6 eq
domain
xlate per-session deny udp any6 any4 eq
domain
xlate per-session deny udp any6 any6 eq
domain
names
!
interface GigabitEthernet0/0
nameif inside
security leve
ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif internet
security-level 0
ip address 145.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif dmz
security-level 50
ip address 10.10.20.1 255.255.255.0
!
ftp mode passive
object network obj_any
subnet 10.10.10.0 255.255.255.0
object network obj_dmz
subnet 10.10.20.0 255.255.255.0
access-list outside_access_in extended
permit icmp any any
access-list OUTSIDE_IN extended permit
tcp any host 145.1.1.1 eq ssh
access-list OUTSIDE_IN extended permit
tcp any host 145.1.1.1 eq www
access-list OUTSIDE_IN extended permit
tcp any host 145.1.1.1 eq https
access-list OUTSIDE_IN extended permit
udp any host 145.1.1.1 eq domain
access-list OUTSIDE_IN extended deny ip
any any
pager lines 23
mtu inside 1500
mtu internet 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
!
object network obj_any
nat (inside, internet) dynamic interface
object network obj_dmz
nat (dmz, internet) dynamic interface
access-group OUTSIDE_IN in interface
internet
route inside 192.168.1.0 255.255.255.0
10.10.10.0 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-
invite 0:03:00 sip-disconnect 0:02:00

```

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		70

```

timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddow 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ca trustpoint
_SmartCallHome_ServerCA
no validation-usage
crl conf igure
crypto ca trustpool policy
auto-import
crypto ca certificate chain
_SmartCallHome_ServerCA
certificate ca
18dad19e267de8bb4a2158cdcc6b3b4a
...
crypto isakmp identity address
crypto ikev1 policy 10
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy
CLIENTLESS_POLICY_KYIV internal
group-policy
CLIENTLESS_POLICY_KYIV attributes
vpn-tunne1-protocol ssl-clientless
webvpn
url-list value BOOKMARKS-KYIV

```

```

dynamic-access-policy-record Df
ltAccessPolicy
username kyiv-user1 password
$sha512$5000$eog0GPdyHTsEzhn1ZP6cH
A == $Bx0HzYu3cKyam 522kkjAAA ==
pbkdf2 privilege 0
username kyiv-user1 attributes
vpn-group-policy
CLIENTLESS_POLICY_KYIV
username kyiv-user password
$sha512$5000$dA8fWEoDmUbYTvOwtTF
f Bw == $AtMC1+3zssc7GL e7rCQGFg ==
pbkdf2 privilege 0
username kyiv-user attributes
vpn-group-policy
CLIENTLESS_POLICY_KYIV
tunne1-group CLIENTLESS-KYIV type
remote-access
tunne1-group CLIENTLESS-KYIV general-
attributes
default-group-policy
CLIENTLESS_POLICY_KYIV
tunne1-group CLIENTLESS2 type remote-
access
tunne1-group CLIENTLESS2 general-
attributes
default-group-policy
CLIENTLESS_POLICY KYIV
tunne1-group CLIENTLESS-KYIV1 type
remote-access
tunne1-group CLIENTLESS-KYIV1
general-attributes
default-group-policy
CLIENTLESS_POLICY_KYIV
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns
migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection

```

```

netbios
!
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
policy-map type inspect dns
migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
service-policy global_policy global
no call-home reporting anonymous

```

```

call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
destination address email
callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic
monthly
subscribe-to-alert-group configuration
periodic monthly
subscribe-to-alert-group telemetry periodic
daily
profile License
destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
destination transport-method http
Cryptochecksum:8829bf06b2e76dcfcdb2a05db158d7c8
: end

```

Конфігурація Switch-1:

```

Switch-1#show run
Building configuration...
Current configuration : 1689 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch-1
!
boot-start-marker
boot-end-marker
!

```

```

logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id

```

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		72

```

spanning-tree vlan 1 priority 4096
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
duplex auto
spanning-tree portfast
spanning-tree bpduguard enable
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
duplex auto
spanning-tree portfast
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
duplex auto
spanning-tree portfast
!
...
!
interface Vlan1
no ip address
shutdown
!
no ip http server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

		Сак О. А.			КІК.КР.Б – 123 – 9 – ПЗ	Арк.
		Дячук О. Ю.				
Змн.3	Арк.А	№ докум.	Підпис	Дата		73