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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «КОМПЛЕКСНА СИСТЕМА МЕРЕЖЕВОЇ БЕЗПЕКИ НА БАЗІ МІЖМЕРЕЖЕВОГО ЕКРАНА CISCO ASA ІЗ ЗАБЕЗПЕЧЕННЯМ ВІДДАЛЕНОГО ДОСТУПУ ЧЕРЕЗ SSL VPN»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

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

_____ *Андрій БОДНАР*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСДМ-61
Андрій БОДНАР
Ім'я, ПРІЗВИЩЕ
Керівник: Людмила АСЄЄВА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ

«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Боднар Андрій Сергійович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Комплекснасистеми мережевої безпеки на базі міжмережевого екрана Cisco ASA із забезпеченням віддаленого доступу через SSL VPN керівник кваліфікаційної роботи Людмила АСЄЄВА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10 2025р. № 467
2. Строк подання кваліфікаційної роботи «_____» _____ 2025р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, використано методи системного аналізу, моделювання мережевих топологій, експериментальний метод при налаштуванні обладнання та методи верифікації для тестування захищеності каналів зв'язку.
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Загальна характеристика технології ssl vpn
2. Розробка комплексної системи захищеного віддаленого підключення
3. Практична реалізація та верифікація комплексу захисту мережі
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.09-24.10.2025	Виконано
2	Обробка матеріалу	25.10-05.11.2025	Виконано
3	Розробка теоретичної частини	06.11-10.11.2025	Виконано
4	Розробка мережі	11.11-15.11.2025	Виконано
5	Висновки за результатами аналізу	15.11-19.11.2025	Виконано
6	Оформлення пояснювальної записки	19.11-21.11.2025	Виконано
7	Розробка презентації	21.11-29.11.2025	Виконано
8	Передзахист	01.12-02.12.2025	Виконано
9	Здача в деканат	15.12-18.12.2025	Виконано

Здобувач вищої освіти _____ Андрій БОДНАР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Людмила АСЄЄВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 65 стор., 22 рис., 1 табл., 23 джерела.

Мета дослідження – підвищення захищеності корпоративного інформаційного простору шляхом проєктування та впровадження системи безпечного віддаленого доступу на базі апаратної платформи Cisco ASA з використанням технології SSL VPN.

Об'єкт дослідження – методи конфігурації та інтеграції протоколів SSL/TLS, механізмів аутентифікації та політик доступу в середовищі Cisco ASA.

Предмет дослідження – алгоритми оцінки пропускної здатності, методи вимірювання рівня сигналу та інструменти діагностики радіочастотного середовища.

Короткий зміст роботи: У кваліфікаційній роботі проаналізовано сучасні загрози мережевій безпеці та методи їх нейтралізації за допомогою криптографічних протоколів. Розглянуто архітектурні особливості обладнання Cisco ASA та специфіку технології Clientless SSL VPN. Розроблено детальну схему мережевої топології з урахуванням філіальної структури. Виконано практичне налаштування VPN-шлюзу через графічний інтерфейс ASDM, включаючи створення користувацьких порталів, налаштування списків контролю доступу та інтеграцію з сервісами AAA.

Результати: Розгорнуто повнофункціональний шлюз безпеки, що забезпечує авторизованим користувачам захищений веб-доступ до внутрішніх ресурсів підприємства. Система пройшла успішне тестування, підтвердивши стійкість до несанкціонованого доступу та стабільність роботи каналів зв'язку..

КЛЮЧОВІ СЛОВА: CISCO ASA, SSL VPN, ІНФОРМАЦІЙНА БЕЗПЕКА, ТУНЕЛЮВАННЯ, ВІДДАЛЕНИЙ ДОСТУП, TLS, TACACS+, ASDM, МІЖМЕРЕЖЕВИЙ ЕКРАН, АВТЕНТИФІКАЦІЯ.

ABSTRACT

The textual part of the Master's qualification thesis: 65 pp., 22 figs., 1 tab., 23 refs.

The purpose of the study is to enhance the security of the corporate information space by designing and implementing a secure remote access system based on the Cisco ASA hardware platform using SSL VPN technology.

The object of the study is the methods of configuration and integration of SSL/TLS protocols, authentication mechanisms, and access policies within the Cisco ASA environment.

The subject of the study is algorithms for throughput estimation, methods for signal level measurement, and tools for radio frequency environment diagnostics.

Content summary: The qualification thesis analyzes modern threats to network security and methods for their neutralization using cryptographic protocols. The architectural features of Cisco ASA equipment and the specifics of Clientless SSL VPN technology are examined. A detailed network topology scheme has been developed, taking into account the branch structure. Practical configuration of the VPN gateway was performed via the ASDM graphical interface, including the creation of user portals, configuration of access control lists (ACLs), and integration with AAA services.

Results: A fully functional security gateway has been deployed, providing authorized users with secure web access to the enterprise's internal resources. The system successfully passed testing, confirming its resistance to unauthorized access and the stability of communication channels.

KEYWORDS: CISCO ASA, SSL VPN, INFORMATION SECURITY, TUNNELING, REMOTE ACCESS, TLS, TACACS+, ASDM, FIREWALL, AUTHENTICATION.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Боднар А. С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Комплекснасистеми мережевої безпеки на базі міжмережевого екрана Cisco ASA із забезпеченням віддаленого доступу через SSL VPN».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Боднар А. С. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Боднара Андрія Сергійовича на оцінку «відмінно», та присвоїти їй кваліфікацію «магістр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Людмила АСЄЄВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«_» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Боднар А. С.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Боднар Андрій Сергійович
(прізвище, ім'я, по батькові)
на тему: «Комплекснасистеми мережевої безпеки на базі міжмережевого екрана Cisco ASA із забезпеченням віддаленого доступу через SSL VPN»

Актуальність:

Кваліфікаційна магістерська робота присвячена вирішенню критично важливої для сучасного бізнесу проблеми — організації безпечного віддаленого доступу до корпоративних ресурсів. В умовах глобалізації бізнес-процесів та масового переходу на гібридні форми роботи, захист периметра мережі трансформується у захист кожного окремого підключення. Робота пропонує практичну реалізацію комплексної системи захисту на базі індустріального стандарту — обладнання Cisco ASA, що робить отримані результати безпосередньо придатними для впровадження в реальних IT-інфраструктурах.

Позитивні сторони:
1. У роботі наведено ґрунтовний аналіз теоретичної бази, зокрема детально розглянуто еволюцію протоколів TLS від версії 1.0 до 1.3, а також механізми роботи цифрових сертифікатів та інфраструктури відкритих ключів. Це свідчить про глибоке розуміння автором фундаменту мережевої безпеки.
2. Практична частина роботи вирізняється високим рівнем деталізації технічних рішень. Автор не лише спроєктував логічну топологію мережі, але й навів покроковий алгоритм налаштування Cisco ASA через ASDM, включаючи конфігурацію профілів тунелювання та політик безпеки.
3. . Вагомим плюсом є комплексний підхід до безпеки, який включає інтеграцію VPN-шлюзу з сервером централізованої аутентифікації TACACS+ та налаштування системи логування подій.

Недоліки:
1. У роботі основну увагу приділено режиму Clientless SSL VPN, проте недостатньо детально розглянуто порівняння та налаштування режиму AnyConnect , який може бути необхідним для доступу до специфічних застосунків, що не працюють через веб.
2. Бажано було б навести результати навантажувального тестування шлюзу безпеки, щоб оцінити вплив шифрування трафіку на пропускну здатність мережі та визначити максимальну кількість одночасних сесій для обраної моделі обладнання Cisco ASA..

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку " відмінно", а здобувач Овдєй О. С. заслуговує присвоєння кваліфікації: магістр з комп'ютерної інженерії.*

Рецензент:
науковий ступінь, вчене звання _____ *підпис* _____ *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП 9
1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТЕХНОЛОГІЇ SSL VPN 11
1.1 Еволюція та становлення протоколів захищеного з’єднання 11
1.2 Концептуальні засади та архітектура віртуальних приватних мереж 18
1.3 Комплексні рішення мережевої безпеки на базі Cisco ASA 27
2 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ 31
2.1 Системний аналіз вимог безпеки та функціональності 31
2.2 Структурна організація та архітектурні принципи системи 34
2.3 Конфігурація мережевого обладнання та інтеграція сервісів 37
2.4 Проєктування топології та стратегія ip-адресації 44
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ВЕРИФІКАЦІЯ КОМПЛЕКСУ ЗАХИСТУ МЕРЕЖІ 52
3.1 Алгоритм розгортання та конфігурації підсистеми віддаленого доступу. 52
3.2 Комплексне тестування та діагностика налаштованих сервісів 57
ВИСНОВКИ 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 62
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 65

ВСТУП

У сучасному цифровому середовищі корпоративні мережі виходять за межі фізичних офісів, трансформуючись у складні розподілені екосистеми. Зростання попиту на дистанційну роботу та необхідність забезпечення мобільності персоналу роблять традиційні методи захисту периметра недостатньо ефективними. Передача конфіденційних корпоративних даних через публічні канали зв'язку, такі як Інтернет, створює значні ризики перехоплення інформації, атак типу «людина посередині» та несанкціонованого доступу.

Це зумовлює необхідність впровадження комплексних систем захищеного віддаленого підключення, які гарантують конфіденційність, цілісність та доступність інформаційних ресурсів. Використання технології SSL VPN на базі спеціалізованих апаратних рішень, таких як Cisco ASA, дозволяє створити надійний криптографічний бар'єр та забезпечити гранулярний контроль доступу користувачів без необхідності встановлення складного клієнтського програмного забезпечення.

Мета і завдання дослідження. Метою роботи є підвищення рівня захищеності інформаційної інфраструктури підприємства шляхом розробки та впровадження комплексної системи віддаленого доступу на основі міжмережевого екрана Cisco ASA та протоколів SSL VPN.

Для досягнення мети поставлені наступні завдання:

1. Проаналізувати еволюцію та сучасний стан протоколів захищеного з'єднання та визначити їх роль у забезпеченні мережевої безпеки.
2. Дослідити архітектурні принципи побудови віртуальних приватних мереж та особливості тунелювання трафіку.
3. Обґрунтувати вибір апаратної платформи Cisco ASA як ядра системи захисту, проаналізувавши її функціональні можливості та модельний ряд.

4. Розробити топологію захищеної мережі та стратегію IP-адресації для головного офісу та філій.

5. Реалізувати практичне налаштування сервісу Clientless SSL VPN через середовище Cisco ASDM, включаючи створення профілів, груп тунелювання та політик доступу.

6. Інтегрувати систему з сервером аутентифікації TACACS+ та забезпечити моніторинг подій безпеки.

7. Провести комплексне тестування та верифікацію налаштованих сервісів для підтвердження їх працездатності та надійності.

Об’єкт дослідження – процеси забезпечення інформаційної безпеки при організації віддаленого доступу до корпоративних мереж.

Предмет дослідження – методи, протоколи та апаратно-програмні засоби реалізації технології SSL VPN на базі платформи Cisco ASA.

Методи дослідження. У роботі використано методи системного аналізу, моделювання мережевих топологій, експериментальний метод при налаштуванні обладнання та методи верифікації для тестування захищеності каналів зв’язку.

Практичне значення. Розроблена система дозволяє забезпечити безпечний та зручний доступ віддалених співробітників до внутрішніх ресурсів компанії через веб-інтерфейс, мінімізувати ризики витоку інформації та централізувати управління політиками безпеки.

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТЕХНОЛОГІЇ SSL VPN

1.1 Еволюція та становлення протоколів захищеного з'єднання

Фундамент сучасної мережевої безпеки, зокрема протокол захисту транспортного рівня (TLS), почав закладатися ще в серпні 1986 року. Це стало можливим завдяки масштабній кооперації між ключовими державними установами США, такими як Національне агентство з безпеки та Національне бюро стандартів, Агентством оборони зв'язку, а також дюжиною провідних корпорацій у сфері телекомунікацій та обчислювальної техніки. Результатом цієї співпраці став запуск проєкту під назвою «Система безпечної мережі даних» (SDNS) [1]. Офіційна презентація напрацювань відбулася у вересні 1987 року під час 10-ї національної конференції з комп'ютерної безпеки, де було оприлюднено низку наукових статей. Головною метою цієї ініціативи була розробка специфікацій для продуктів нового покоління, здатних гарантувати безпеку як у державних, так і в комерційних мережах. Проєкт мав на меті доповнити нові стандарти OSI та інтегруватися з профілями GOSIP і напрацюваннями ITY-ISO JTC1. Спочатку відома як SP4, ця технологія згодом трансформувалася в TLS і в 1995 році отримала статус міжнародного стандарту ITU-T X.274|ISO/IEC 10736:1995.

Технологія безпечного програмування мереж (SNP) Важливим етапом у розвитку безпеки транспортного рівня стала поява інтерфейсу прикладного програмування Secure Network Programming (SNP). У 1993 році було запропоновано підхід, що передбачав створення безпечного API, який за своєю логікою нагадував сокети Berkeley. Це дозволило б значно спростити процес інтеграції механізмів захисту в наявні мережеві застосунки. Результати досліджень SNP були оприлюднені на технічній конференції USENIX влітку 1994 року. Фінансову підтримку проєкту забезпечило Національне агентство з

безпеки (NSA) через грант, наданий професору Саймону Ламу з Університету Техасу в Остіні ще у 1991 році. Вклад цієї технології був настільки вагомим, що у 2004 році SNP відзначили премією ACM Software System, а Саймона Лама було включено до Зали слави Інтернету за розробку перших захищених сокетів [2].

Розвиток версій протоколу SSL (1.0, 2.0 та 3.0) Витоки протоколу SSL пов'язані з компанією Netscape, а його творцем вважають Тахера Ельгамаля. Перша ітерація протоколу, SSL 1.0, так і не побачила світ через виявлені критичні вразливості ще на етапі розробки. У лютому 1995 року було випущено SSL 2.0, проте і ця версія виявилася недосконалою. Вона мала низку серйозних недоліків як у площині безпеки, так і в зручності експлуатації. Зокрема, для шифрування та аутентифікації використовувалися ідентичні криптографічні ключі, а алгоритм перевірки цілісності повідомлень базувався на MD5 із секретним префіксом, що робило систему вразливою до атак на подовження повідомлення. Більше того, SSL 2.0 не захищав процес початкового узгодження з’єднання та не гарантував безпечного закриття сесії, що створювало передумови для атак типу «людина посередині». Ще одним суттєвим обмеженням була неможливість використання різних сертифікатів для віртуального хостингу, що гальмувало впровадження SSL на багатьох веб-ресурсах [2].

Наявність критичних дірок у безпеці змусила розробників повністю переглянути архітектуру протоколу, що призвело до створення SSL 3.0 у 1996 році. Над цією версією працювали Пол Кохер разом з інженерами Netscape Філом Карльтоном та Аланом Фрейєром, а еталонну реалізацію виконали фахівці Certicom. Саме третя версія стала базисом для всіх подальших розробок у сімействі TLS. Проте з часом і цей стандарт застарів: у 2011 році було офіційно відмовлено від підтримки SSL 2.0, а в 2015 році, після виявлення вразливості POODLE, що загрожувала всім блоковим шифрам, було визнано неактуальним і SSL 3.0.

Стандарт TLS 1.0 Наступником SSL 3.0 став протокол TLS 1.0, описаний у RFC 2246 у січні 1999 року. Автори стандарту, Крістофер Аллен і Тім Діркс, зазначали, що, хоча технічні відмінності між TLS 1.0 і SSL 3.0 були незначними, їх було достатньо для унеможливлення прямої сумісності. Зміна назви з SSL на TLS мала здебільшого політичний характер, щоб задовольнити Microsoft і не створювати враження, що IETF просто легітимізує продукт Netscape [2]. Згодом, через виявлені ризики, провідні технологічні гіганти та регулятори (PCI, Apple, Google, Microsoft) ініціювали процес відмови від TLS 1.0, який остаточно завершився визнанням протоколу застарілим у березні 2021 року.

Версія протоколу TLS 1.1 У квітні 2006 року в документі RFC 4346 було представлено версію TLS 1.1. Це оновлення привнесло низку важливих змін для підвищення стійкості до атак. Зокрема, було впроваджено захист від атак на зчеплення блоків шифру (CBC), неявний вектор ініціалізації замінено на явний, а також перероблено процедуру обробки помилок доповнення. Додатково було реалізовано підтримку реєстрації параметрів через IANA. Незважаючи на покращення, до 2020 року більшість веб-ресурсів припинили підтримку цієї версії.

Особливості специфікації TLS 1.2 Значним кроком уперед стала поява TLS 1.2 у серпні 2008 року (RFC 5246). У цій версії розробники суттєво посилили криптографічну складову. Замість комбінації MD5 та SHA-1 у псевдовипадковій функції почали використовувати надійніший SHA-256. Аналогічні зміни торкнулися повідомлень завершення рукостискання та цифрових підписів, де також було впроваджено SHA-256 та можливість вибору хеш-функцій, при цьому розмір хешу обмежили мінімумом у 96 біт. Протокол розширив можливості сторін узгоджувати допустимі алгоритми шифрування та підпису. Важливим нововведенням стала підтримка шифрування з аутентифікацією (AEAD), зокрема режимів GCM та CCM для алгоритму AES, а також механізму розширень протоколу. Станом на сьогодні TLS 1.2 залишається актуальним стандартом [4].

Специфікація протоколу TLS 1.3 Найактуальніша специфікація, TLS 1.3, була затверджена у серпні 2018 року (RFC 8446). Ця версія стала результатом докорінного переосмислення протоколу з метою підвищення швидкодії та безпеки. Основні зміни включають чітке розмежування алгоритмів узгодження ключів та аутентифікації, відмову від застарілих еліптичних кривих та небезпечних хеш-функцій типу MD5 і SHA-224. У новій версії використання цифрового підпису стало обов'язковим навіть за наявності попередньої конфігурації. Також було інтегровано HKDF і передбачено підтримку напівефемерного протоколу Діффі-Гелмана.

Для прискорення встановлення з'єднання було запроваджено процедуру рукостискання за один цикл (1-RTT) та опцію нульового циклу (0-RTT) для відновлення сесій. Безпека була посилена шляхом забезпечення цілковитої прямої секретності (Perfect Forward Secrecy) через використання ефемерних ключів. З протоколу було вилучено цілу низку потенційно вразливих елементів: стиснення даних, статичні обміни ключами RSA та DH, застарілі шифри без аутентифікації та інші рудименти попередніх версій. Окрім того, було додано підтримку потокового шифру ChaCha20 з кодом аутентифікації Poly1305 та алгоритмів цифрового підпису Ed25519 і Ed448. Усі повідомлення рукостискання після етапу ServerHello тепер шифруються [4].

Впровадження TLS 1.3 супроводжувалося певними труднощами через так звану «осифікацію» протоколу, коли проміжне мережеве обладнання некоректно обробляло нові параметри. Для вирішення цієї проблеми розробники застосували механізм імітації структури пакетів TLS 1.2, а також методику «greasing», що передбачає додавання випадкових даних для перевірки гнучкості системи. Підтримка нових стандартів поступово впроваджувалася у популярні програмні продукти, такі як бібліотека NSS від Mozilla, браузери Firefox та Chrome, а також бібліотеки wolfSSL та OpenSSL.

Корпоративні стандарти безпеки та ETS Окрему увагу варто приділити появі специфікації Enterprise Transport Security (ETS), відомої також як eTLS. Цей варіант протоколу, призначений для внутрішніх корпоративних мереж,

викликав гостру критику з боку організації Electronic Frontier Foundation (EFF). Основна претензія полягає у відмові від принципу прямої секретності, що дозволяє організаціям дешифрувати та аналізувати власний трафік. Експерти наголошують, що такий підхід створює значні ризики: компрометація ключа може призвести до розкриття всього масиву раніше перехоплених даних, тому для моніторингу рекомендується використовувати більш безпечні альтернативні методи [3].

Сутність та формати цифрових сертифікатів Цифровий сертифікат виступає фундаментальним елементом довіри в сучасних мережах, виконуючи роль електронного посвідчення. Його основне завдання — беззаперечно підтвердити приналежність конкретного відкритого (публічного) ключа певному власнику, будь то веб-сервер, організація чи приватна особа. Окрім ідентифікації власника, сертифікат чітко регламентує сферу застосування ключа, визначаючи дозволені операції. Завдяки цьому механізму, треті сторони, які покладаються на даний сертифікат, можуть бути впевненими у легітимності цифрових підписів та зашифрованих повідомлень, створених за допомогою парного приватного ключа. З технічної точки зору, для зберігання та транспортування ключів і сертифікатів використовується низка стандартизованих форматів файлів. Найпоширенішими серед них є текстові формати з кодуванням Base64, такі як .pem та .crt, а також бінарні контейнери .pfx або специфічні для Java-середовища сховища .jks.

Інфраструктура центрів сертифікації та довіри У межах протоколу TLS модель безпеки побудована на ланцюжку довіри, ключовою ланкою якого є центри сертифікації (CA). Програмне забезпечення кінцевого користувача, наприклад веб-браузер або операційна система, містить попередньо встановлене сховище кореневих сертифікатів від організацій, які мають статус довірених третіх сторін. Саме ці центри відповідають за верифікацію даних заявників перед видачею сертифікатів. Користувачі або адміністратори систем мають можливість керувати цим списком, додаючи або відкликаючи довіру до певних кореневих центрів за необхідності.

Ринок сертифікації є динамічним середовищем. Згідно з аналітичними звітами компанії Netcraft, яка здійснює моніторинг використання TLS, довгий час беззаперечним лідером галузі була корпорація Symantec (що раніше поглинула бізнес VeriSign). Станом на 2015 рік ця компанія контролювала близько третини світового ринку сертифікатів і забезпечувала захист 44% найбільш відвідуваних веб-ресурсів. Однак ландшафт змінився у 2017 році, коли підрозділ безпеки Symantec був придбаний компанією DigiCert. Оновлена статистика за травень 2019 року демонструє нову розстановку сил: провідні позиції зайняли IdenTrust, DigiCert та Sectigo [4].

Функціонування сертифікатів стандарту X.509 неможливе без розгалуженої інфраструктури відкритих ключів (PKI), яка забезпечує повний життєвий цикл сертифіката: від генерації та підпису до перевірки статусу та відкликання. Така централізована модель є значно ефективнішою за децентралізовані «мережі довіри», проте вона не позбавлена ризиків. Після викриттів глобального стеження у 2013 році стало очевидно, що центри сертифікації можуть бути слабкою ланкою. Компрометація центру або його примусова співпраця зі зловмисниками чи спецслужбами створює загрозу випуску підроблених сертифікатів, що дозволяє реалізовувати атаки типу «людина посередині» (MITM) навіть на захищених каналах.

Функціональне значення SSL-сертифікатів Впровадження SSL-сертифікатів вирішує три критичні завдання інформаційної безпеки. По-перше, забезпечується конфіденційність шляхом шифрування трафіку між клієнтом і сервером. Це унеможливлює перехоплення та прочитання інформації сторонніми особами, мінімізуючи ризики витоку чутливих даних. По-друге, реалізується сувора аутентифікація, яка підтверджує, що користувач взаємодіє саме з легітимним сервером, а не з фішинговим ресурсом. По-третє, гарантується цілісність даних: завдяки криптографічним алгоритмам будь-яка несанкціонована зміна інформації під час транзиту буде миттєво виявлена, що забезпечує точність і надійність обміну даними.

Механізми узгодження ключів Ініціалізація захищеного з'єднання TLS починається з процедури узгодження параметрів шифрування та безпечного обміну сесійними ключами. Для цього застосовується широкий спектр алгоритмів. Класичний підхід базується на асиметричному шифруванні RSA (TLS_RSA), де ключ шифрується публічним ключем сервера. Альтернативою є протокол Діффі-Хеллмана в різних варіаціях: статичний (TLS_DH), ефемерний (TLS_DHE), а також їхні аналоги на еліптичних кривих (TLS_ECDH та TLS_ECDHE). Також існують методи з використанням попередньо узгодженого ключа (TLS_PSK) та захищеного віддаленого пароля (TLS_SRP) [4].

Важливо зазначити, що анонімні версії протоколів (TLS_DH_anon, TLS_ECDH_anon) не передбачають аутентифікації учасників, що робить їх вразливими до перехоплення, тому на практиці вони майже не застосовуються. Натомість ефемерні режими (DHE, ECDHE) набули популярності завдяки властивості прямої досконалої секретності (Forward Secrecy), яка гарантує, що компрометація довгострокового ключа у майбутньому не дозволить розшифрувати записаний раніше трафік. Рівень захисту також залежить від довжини ключів. Показовим є приклад компанії Google, яка ще у 2013 році ініціювала перехід з 1024-бітних на 2048-бітні ключі RSA, підвищивши планку криптографічної стійкості для всієї індустрії.

Архітектура наборів шифрів Поняття «набір шифрів» (cipher suite) описує комбінацію алгоритмів, необхідних для встановлення та підтримки захищеного каналу. Типовий набір включає три компоненти: алгоритм обміну ключами (для безпечної передачі секрету), алгоритм симетричного шифрування (для захисту основного потоку даних) та функцію коду автентифікації повідомлень (MAC) для контролю цілісності. Деякі набори додатково специфікують алгоритми цифрового підпису для ідентифікації сторін.

Існує величезна кількість варіацій наборів шифрів, що відрізняються рівнем безпеки та продуктивністю. Проте з виходом специфікації TLS 1.3

підхід до цього питання радикально змінився: кількість дозволених наборів було скорочено до п’яти найбільш надійних комбінацій. Важливою деталлю є те, що набори шифрів для TLS 1.2 не сумісні з TLS 1.3 (якщо це окремо не зазначено), а повний перелік актуальних параметрів ведеться в офіційному реєстрі.

Забезпечення цілісності та автентичності даних Для гарантування того, що дані не були модифіковані в дорозі, TLS використовує механізми MAC. У класичних схемах із застосуванням блокових шифрів у режимі зчеплення блоків (CBC) стандартом є використання HMAC. Однак у сучасних реалізаціях перевага надається алгоритмам автентифікованого шифрування з приєднаними даними (AEAD), таким як GCM (Galois/Counter Mode) або CCM. Особливість AEAD полягає в тому, що контроль цілісності вбудовано безпосередньо в процес шифрування, що усуває потребу в окремому обчисленні HMAC і підвищує продуктивність. Крім того, на етапі рукостискання для генерації ключового матеріалу використовуються псевдовипадкові функції (PRF) на базі HMAC або спеціалізовані функції формування ключа (HKDF).

1.2 Концептуальні засади та архітектура віртуальних приватних мереж

Технологія віртуальних приватних мереж (VPN) являє собою механізм створення захищеного логічного з'єднання поверх незахищених мереж загального користування, таких як Інтернет. Основна ідея полягає в тому, щоб забезпечити безпечну передачу даних між кінцевим користувачем та цільовою мережею, імітуючи властивості фізично виділеної лінії. Спектр застосування цієї технології досить широкий: від обходу регіональних блокувань контенту до забезпечення конфіденційності даних під час роботи в публічних зонах Wi-

Fi [1]. Фактично, VPN розширює межі приватної корпоративної мережі, використовуючи публічну інфраструктуру для транспортування інформації. Це дозволяє організаціям будувати канали комунікації, які за своїми характеристиками нагадують прямі з’єднання типу «точка-точка». Візуалізацію такого підходу, зокрема для об’єднання офісів, наведено на рис. 1.1.

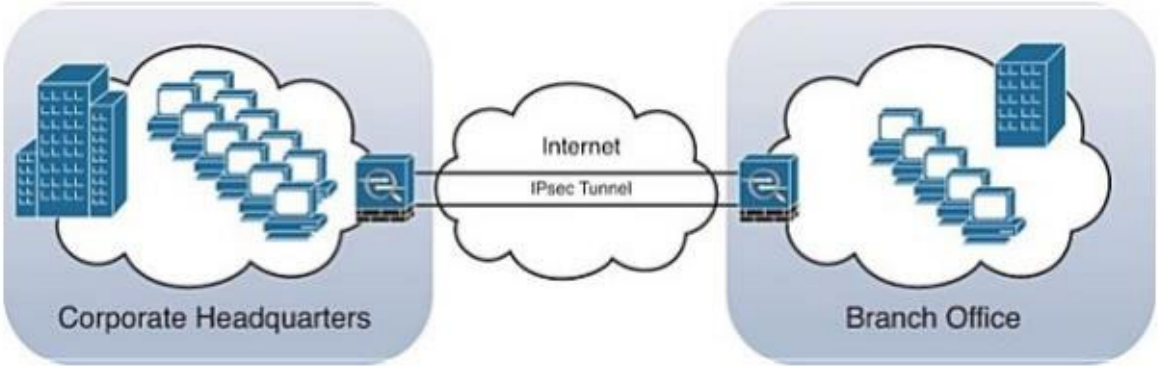


Рисунок 1.1. Ілюстрація об’єднання мереж за технологією Site-to-Site

Впровадження VPN дозволяє підприємствам ефективно нівелювати загрози, пов'язані з передачею конфіденційної інформації через відкриті канали зв'язку. Фундаментом цієї безпеки є процеси інкапсуляції та шифрування. Інкапсуляція передбачає поміщення оригінальних пакетів даних у додаткову оболонку (новий IP-заголовок), що містить необхідну маршрутну інформацію для проходження через тунель. Паралельно з цим, застосування криптографічних методів робить перехоплені дані абсолютно нечитабельними для зловмисників, оскільки для їх дешифрування необхідні унікальні ключі [21].

Для кінцевого користувача, будь то віддалений працівник, співробітник у відрядженні або фахівець філії, робота через VPN виглядає прозорою. Комп'ютер сприймає з'єднання з корпоративним сервером як пряме, незважаючи на те, що фізично сигнал проходить через безліч проміжних вузлів глобальної мережі.

Існує кілька ключових моделей розгортання VPN. Найпоширенішою є організація віддаленого доступу, коли окремі працівники підключаються до внутрішніх ресурсів компанії ззовні. Інший важливий сценарій — це постійне з'єднання між територіально розрізненими офісами, відоме як Site-to-Site (або схема «маршрутизатор-маршрутизатор»). Окрім внутрішніх потреб, технологія дозволяє створювати екстрамережі (Extranet) — захищені середовища для взаємодії з бізнес-партнерами або клієнтами, де доступ суворо регламентований.

Вагомою перевагою переходу на VPN є оптимізація витрат. Компанії можуть відмовитися від дорогих орендованих ліній міжміського зв'язку на користь значно дешевших локальних підключень до інтернет-провайдерів, зберігаючи при цьому високий рівень безпеки комунікацій [21].

Функціонування віртуальної мережі базується на трьох фундаментальних елементах: протоколах безпеки, механізмах шифрування та серверах.

Протоколи безпеки відповідають за встановлення та підтримку зашифрованого тунелю між клієнтом і сервером. Від обраного протоколу залежить баланс між швидкістю передачі даних та надійністю захисту. Хоча програмні методи не можуть гарантувати абсолютну невразливість на рівні фізично ізольованого кабелю, сучасні рішення, такі як OpenVPN, забезпечують надзвичайно високий рівень захисту і є стандартом де-факто в індустрії.

Другим критичним компонентом є шифрування — процес алгоритмічного перетворення інформації у вигляд, недоступний для розуміння без ключа дешифрування. Найчастіше в індустрії застосовується просунутий стандарт шифрування AES із довжиною ключа сто двадцять вісім або двісті п’ятдесят шість біт. Надійність таких алгоритмів базується на астрономічній кількості можливих комбінацій ключів, перебір яких зайняв би мільярди років навіть при використанні найпотужніших обчислювальних систем.

Третьою складовою є мережа серверів. Їх географічний розподіл дозволяє користувачам обирати оптимальну точку входу, що впливає на

швидкість та стабільність з'єднання. Принциповим моментом є те, що при використанні VPN весь трафік користувача спочатку потрапляє на VPN-сервер, який діє як посередник, перенаправляючи запити до кінцевих ресурсів. Завдяки цьому цільовий сайт бачить лише IP-адресу VPN-сервера, а реальна адреса та місцезнаходження користувача залишаються прихованими, що гарантує анонімність.

Цей тип підключення реалізується за допомогою спеціалізованого програмного забезпечення — VPN-клієнта, встановленого на пристрої користувача. Процес починається з того, що користувач підключається до Інтернету через свого локального провайдера, а потім ініціює тунель до шлюзу організації. Трафік формується і шифрується безпосередньо на пристрої клієнта. Важливим етапом є двостороння аутентифікація: сервер перевіряє права доступу користувача, а клієнт, у свою чергу, пересвідчується у справжності сервера. Після встановлення з'єднання віддалений працівник отримує доступ до корпоративних ресурсів так, ніби його робоче місце знаходиться в офісі. Схематичне зображення цього процесу представлено на рис. 1.2.

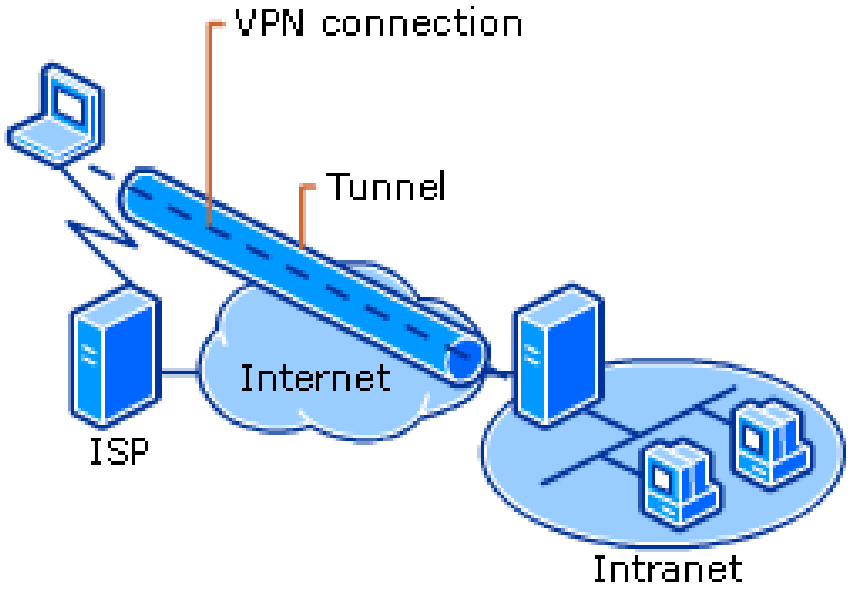


Рисунок 1.2. Алгоритм підключення віддаленого користувача до корпоративних ресурсів

На відміну від індивідуального доступу, технологія Site-to-site призначена для створення логічного мосту між цілими мережами, наприклад, між центральним офісом та філіями. У цьому сценарії VPN-сервери (зазвичай у ролі яких виступають маршрутизатори) забезпечують маршрутизацію трафіку між підмережами через Інтернет. Для кінцевих пристроїв у цих мережах процес є абсолютно прозорим. Аутентифікація відбувається на рівні обладнання: маршрутизатор-ініціатор підтверджує свої повноваження перед маршрутизатором-приймачем і навпаки. З точки зору мережевої архітектури, такий тунель функціонує як лінк канального рівня, об'єднуючи розрізнені локальні мережі в єдину логічну структуру [23]. Приклад такої архітектури наведено на рис. 1.3.

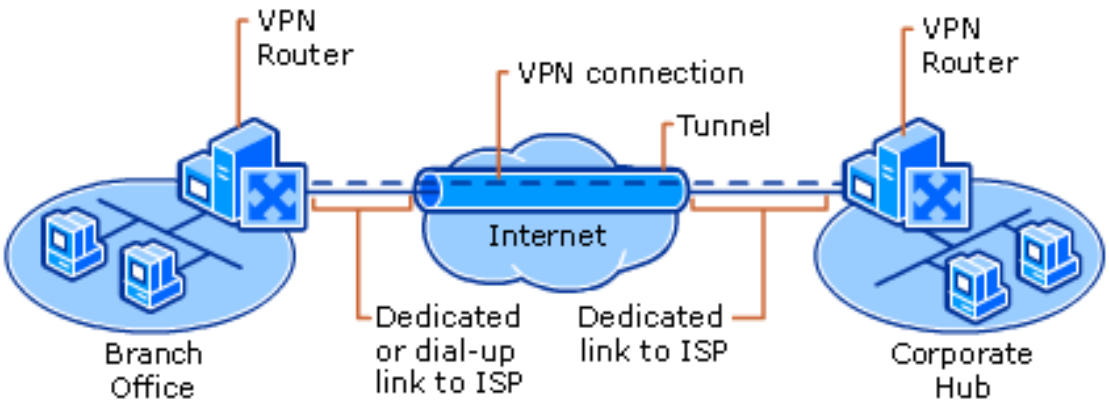


Рисунок 1.3. Організація захищеного каналу між локальними мережами

У сфері мережевих комунікацій під тунелюванням розуміють технологію, що дозволяє інкапсулювати (вкладати) пакети одного логічного протоколу всередину пакетів іншого. Цей метод є базовим для функціонування VPN-рішень у середовищі Windows та інших операційних систем. Наприклад, трафік внутрішньої мережі, такий як TCP/IP, може бути запакований у протоколи тунелювання на кшталт PPTP (Point-to-Point Tunneling Protocol) для безпечного транспортування через публічні канали зв'язку, зокрема Інтернет.

Функціонування тунелів на базі PPTP або L2TP можна порівняти з сеансом зв'язку, де критично важливим етапом є попереднє узгодження

параметрів між кінцевими точками. Сторони домовляються про схему IP-адресації, алгоритми шифрування та методи стиснення даних. Як правило, для безпосередньої передачі інформації всередині тунелю використовуються дейтаграмні протоколи, тоді як управління самим каналом — його створення, підтримка активності та коректне завершення — покладається на окремий керуючий протокол.

Процес передачі даних розпочинається лише після успішного встановлення тунелю. Клієнтська або серверна сторона формує пакет, додаючи до корисного навантаження спеціальний заголовок протоколу тунелювання. Цей інкапсульований об'єкт відправляється в мережу, яка доставляє його до кінцевої точки. Приймаюча сторона, в свою чергу, виконує зворотну операцію: знімає тунельний заголовок (декапсулює пакет) і передає оригінальні дані в цільову мережу. Цей алгоритм діє ідентично в обох напрямках обміну інформацією.

Залежно від ініціатора з'єднання, виділяють два ключові підходи до організації тунелів: добровільне та примусове (обов'язкове) тунелювання.

Сценарій добровільного тунелювання У цій моделі ініціатива створення захищеного каналу виходить безпосередньо від користувача або його клієнтського комп'ютера. Клієнт самостійно надсилає запит на встановлення VPN-з'єднання і виступає однією з кінцевих точок тунелю. Реалізація такого сценарію передбачає наявність на пристрої користувача спеціалізованого програмного забезпечення (VPN-клієнта) та попередньо налаштованих протоколів. Обов'язковою умовою для добровільного тунелювання є наявність активного IP-з'єднання, яке може забезпечуватися через локальну мережу (LAN) або комутований доступ.

Варто зазначити, що при використанні модемного з'єднання (dial-up) користувач спочатку встановлює зв'язок з інтернет-провайдером, і лише після виходу в глобальну мережу ініціює створення тунелю. Це класичний приклад віддаленої роботи. Якщо ж комп'ютер підключено до локальної мережі з постійним широкосмуговим доступом, тунелювання відбувається поверх

існуючого IP-каналу. Поширеною помилкою є ототожнення VPN виключно з комутованим доступом, хоча насправді комутація є лише транспортним рівнем для IP-пакетів, необхідним для подальшої побудови тунелю.

Сценарій примусового (обов'язкового) тунелювання При такій організації процесу тунель створюється автоматично сервером віддаленого доступу, без прямої участі користувача. Комп'ютер клієнта не є кінцевою точкою тунелю; цю роль виконує проміжний пристрій, розташований між користувачем і цільовим тунельним сервером. Такий пристрій функціонує як VPN-клієнт від імені користувача.

У термінології різних протоколів цей посередник має різні назви: FEP (Front-End Processor) для PPTP або LAC (L2TP Access Concentrator) для протоколу L2TP. Незалежно від назви, функція пристрою полягає в автоматичній ініціації тунелю при підключенні клієнта. Схема роботи виглядає так: клієнт через провайдера підключається до сервера мережевого доступу (NAS), який підтримує функції VPN (або FEP). Далі цей пристрій будує тунель до корпоративного сервера приватної мережі. Це дозволяє компаніям централізувати управління з'єднаннями та агрегувати трафік з різних регіонів на єдиному шлюзі.

Термін «примусове тунелювання» вказує на те, що весь трафік клієнта автоматично і безальтернативно спрямовується в тунель, створений FEP. Клієнт встановлює лише одне PPP-з'єднання, а всі подальші процеси маршрутизації відбуваються прозоро для нього. Важливою перевагою цього методу є можливість мультиплексування: один тунель між FEP і сервером може обслуговувати трафік багатьох користувачів одночасно. Новий тунель не створюється для кожного наступного підключення, якщо напрямок передачі співпадає, що значно економить ресурси мережі. Канал залишається активним до моменту відключення останнього користувача.

Протокол PPTP (Point-to-Point Tunneling Protocol) базується на інкапсуляції кадрів PPP у IP-датаграми для їх транспортування через IP-мережі, будь то Інтернет або корпоративна інтрамережа. Технічні специфікації

цього стандарту регламентовані документом RFC 2637 від IETF. Архітектура PPTP передбачає розділення функцій: для управління життєвим циклом тунелю використовується протокол TCP, а для передачі даних застосовується модифікована версія протоколу GRE (Generic Routing Encapsulation). Дані всередині тунелю можуть бути піддані шифруванню та стисненню [12]. Схематичне зображення архітектури підключення наведено на рис. 1.4.

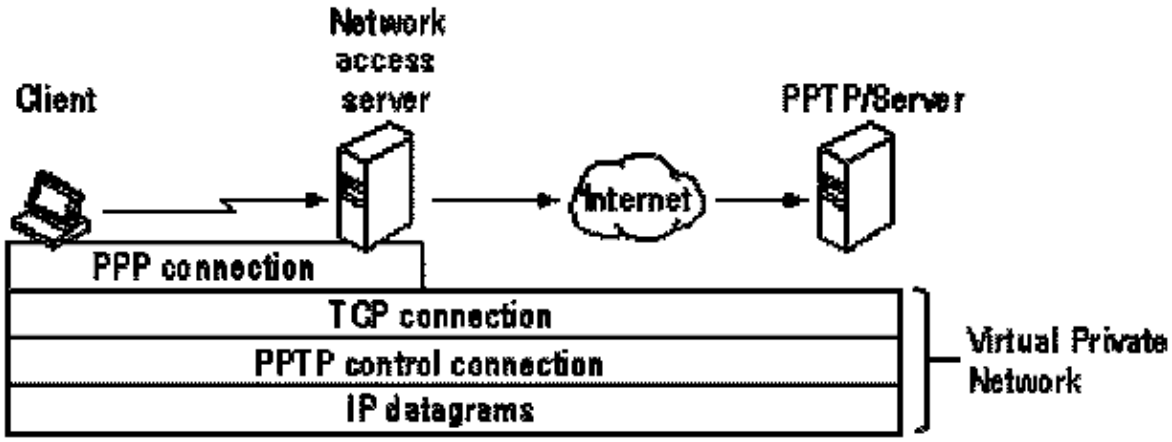


Рисунок 1.4. Архітектура взаємодії клієнта та сервера при використанні протоколу PPT

Для роботи PPTP необхідна наявність IP-маршрутизації між клієнтом та сервером. Аутентифікація користувачів здійснюється тими ж методами, що й у стандартному PPP: PAP, SPAP, CHAP, MS-CHAP (v1/v2) або EAP-TLS. Критично важливим аспектом є безпека: для шифрування даних використовується механізм MPPE (Microsoft Point-to-Point Encryption). Проте активація MPPE можлива лише за умови використання протоколів аутентифікації MS-CHAP, MS-CHAP v2 або EAP-TLS. Варто зауважити, що MPPE забезпечує шифрування лише на рівні каналу (від клієнта до VPN-сервера), а не наскрізне шифрування до кінцевого ресурсу. Для повного наскрізного захисту рекомендується додаткове використання IPSec після встановлення тунелю.

L2TP виник як результат компромісу та об'єднання технологій PPTP від Microsoft та L2F від Cisco Systems. Щоб уникнути фрагментації ринку

несумісними стандартами, організація IETF розробила уніфікований стандарт, описаний у RFC 2661. L2TP дозволяє передавати кадри PPP не лише через IP-мережі, але й через середовища X.25, Frame Relay або ATM. У випадку IP-мереж для транспортування використовується протокол UDP.

Особливістю L2TP є те, що він не має вбудованих механізмів шифрування на кшталт MPPE. Безпека даних у цьому протоколі повністю покладається на IPSec, який забезпечує конфіденційність, автентифікацію та цілісність за допомогою протоколу ESP (Encapsulating Security Payload). Хоча технічно можливо налаштувати L2TP без IPSec, таке з'єднання не вважається безпечним VPN і використовується виключно для діагностики та налагодження мережі. Структура пакетів L2TP подібна до PPTP, а методи аутентифікації ідентичні тим, що використовуються в PPP. L2TP-сервер зазвичай має два інтерфейси: один для зв'язку з публічною мережею (Інтернет), інший — для підключення до приватної інтрамережі [9].

OpenVPN представляє собою сучасне рішення з відкритим вихідним кодом, яке базується на криптографічних протоколах SSLv3/TLSv1. Головною перевагою технології є використання потужної бібліотеки OpenSSL, що забезпечує підтримку широкого спектра алгоритмів шифрування, таких як 3DES, Camellia, CAST-128, а також найбільш популярних — Blowfish та AES.

Протокол вирізняється високою гнучкістю налаштувань. Хоча він може працювати через TCP, рекомендованим транспортом є UDP, що забезпечує кращу продуктивність. Можливість використання будь-якого порту робить OpenVPN надзвичайно стійким до блокувань та фільтрації трафіку. Щодо шифрування, то за замовчуванням часто використовується 128-бітний Blowfish, проте золотим стандартом вважається алгоритм AES. Завдяки 128-бітному розміру блоку (проти 64-бітного у Blowfish), AES краще підходить для передачі великих обсягів даних і є стандартом, рекомендованим урядом США.

Попри те, що OpenVPN не інтегрований нативно у більшість операційних систем і потребує встановлення стороннього ПЗ, він залишається найпопулярнішим вибором серед VPN-провайдерів. Його налаштування може

бути дещо складнішим за PPTP чи L2TP через необхідність оперування конфігураційними файлами та ключами, проте це компенсується найвищим рівнем безпеки. Аналіз витоків інформації від спецслужб підтверджує, що OpenVPN, особливо при використанні ефемерних ключів та надійних шифрів, залишається стійким до злому та компрометації.

1.3 Комплексні рішення мережевої безпеки на базі Cisco ASA

У сучасному ландшафті інформаційних технологій платформа Cisco Adaptive Security Appliance (ASA) позиціонується як флагманське рішення для побудови захищеного мережевого периметра. Це сімейство пристроїв отримало широке визнання та впровадження у корпоративному секторі завдяки своїй здатності забезпечувати комплексний захист інфраструктури підприємства. Концептуально ASA є не просто апаратним брандмауером, а багатофункціональною екосистемою, що інтегрує широкий спектр інструментів кібербезпеки в межах єдиної платформи.

Архітектура пристрою спроєктована таким чином, щоб поєднувати можливості міжмережевого екрана з глибокою інспекцією пакетів, високопродуктивного концентратора віртуальних приватних мереж (VPN) та системи запобігання вторгненням (IPS). Така конвергенція технологій дозволяє адміністраторам мереж централізовано керувати політиками безпеки та моніторити трафік без необхідності розгортання безлічі окремих вузькоспеціалізованих пристроїв.

Функціонал Cisco ASA спрямований на нейтралізацію широкого спектра цифрових загроз. Система забезпечує проактивний захист від розповсюдження шкідливого програмного забезпечення, ефективно блокуючи активність троянських програм, мережевих хробаків та комп'ютерних вірусів ще на етапі їх спроби проникнення в корпоративну мережу. Завдяки високим показникам

відмовостійкості, масштабованості та універсальності, рішення на базі Cisco ASA стали своєрідним стандартом де-факто для організацій, які прагнуть побудувати надійний ешелонований захист своїх інформаційних активів [1].

Платформа Cisco ASA являє собою інтегрований комплекс безпеки, який консолідує в єдиному апаратному рішенні широкий спектр критично важливих сервісів для захисту корпоративної інфраструктури. Фундаментом цієї екосистеми є потужний міжмережевий екран, що виконує глибоку інспекцію трафіку. Пристрій здатен аналізувати дані на різних рівнях моделі OSI: від базової фільтрації пакетів на основі заголовків (Packet Filtering) до складного аналізу на рівні прикладних програм (Application Layer Filtering). Такий підхід дозволяє системі ефективно ідентифікувати та нейтралізувати загрози, що маскуються у легітимному трафіку додатків.

Механізми фільтрації та управління політиками безпеки Ключовою функцією пристрою є гнучке керування потоками даних. Адміністратори мають змогу формувати деталізовані політики безпеки, які регламентують проходження трафіку на основі IP-адрес джерел та призначень, номерів портів, типів протоколів та інших метаданих. Система оперує як статичними, так і динамічними списками контролю доступу (ACL). Використання динамічних ACL є особливо важливим для сучасних мереж, оскільки дозволяє фаєрволу автоматично адаптуватися до змінного ландшафту кіберзагроз, забезпечуючи надійний бар'єр проти несанкціонованого проникнення без необхідності постійного ручного втручання.

Організація захищених каналів зв’язку (VPN) У ролі VPN-концентратора Cisco ASA виступає гарантом безпечного віддаленого доступу до корпоративних активів. Пристрій підтримує сучасні криптографічні стандарти, зокрема протоколи IPsec та SSL VPN. Це дозволяє створювати зашифровані тунелі для працівників, що працюють дистанційно, забезпечуючи конфіденційність, цілісність даних та сувору аутентифікацію користувачів. Навіть при передачі критично важливої інформації через незахищене

середовище Інтернету, технології VPN нівелюють ризики перехоплення даних зловмисниками.

Виявлення та нейтралізація вторгнень Невід'ємною складовою комплексу є інтегрована система запобігання вторгненням (IPS), яка працює в режимі реального часу. Цей модуль здійснює безперервний моніторинг мережевого трафіку, порівнюючи його з базами сигнатур відомих загроз та аналізуючи поведінкові аномалії. IPS здатна ідентифікувати активність шкідливого програмного забезпечення, такого як віруси, трояни, мережеві хробаки, та блокувати їх розповсюдження ще до моменту проникнення в периметр мережі. Принцип функціонування цього модуля візуалізовано на рис. 1.5. У разі виявлення атаки система автоматично розриває з'єднання та блокує джерело загрози.

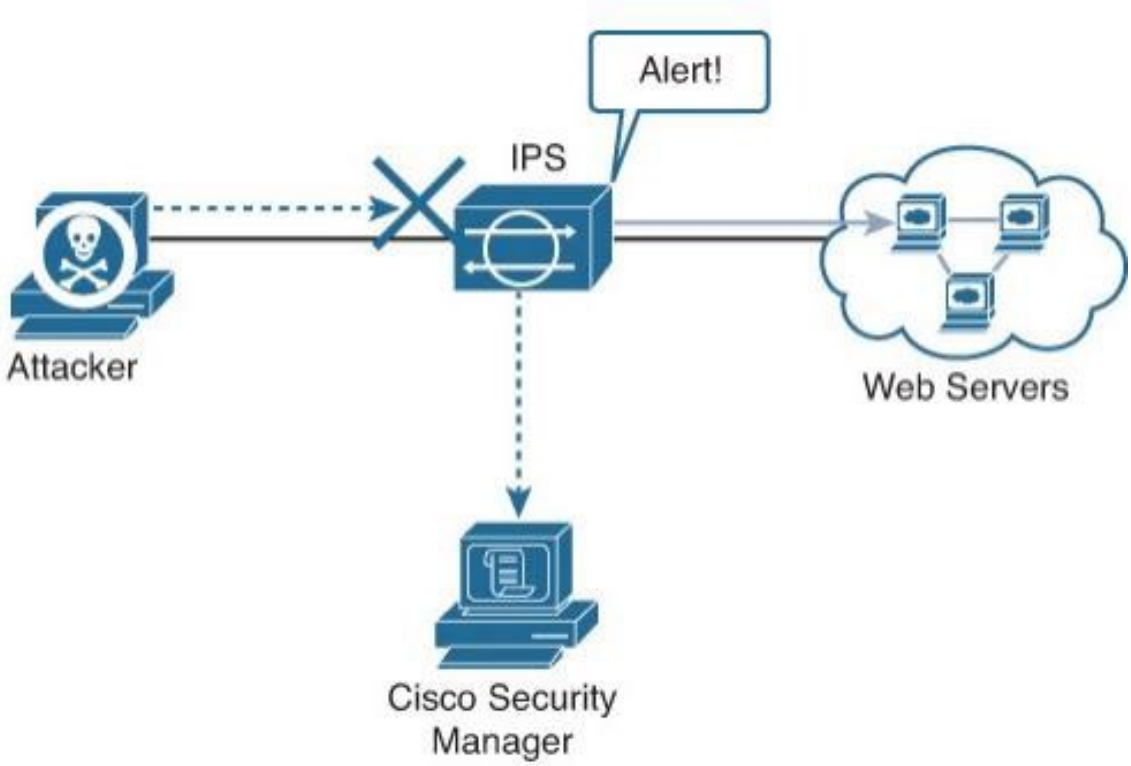


Рисунок 1.5. Схематичне зображення принципу дії системи запобігання вторгненням

Аудит подій та моніторинг стану мережі Для забезпечення прозорості мережевих процесів Cisco ASA оснащено розвиненими засобами логування та

діагностики. Система дозволяє адміністраторам налаштовувати деталізацію журналів подій, збирати статистику та аналізувати інциденти безпеки. Журнали можуть переглядатися як через вбудований інтерфейс управління, так і експортуватися на зовнішні сервери (наприклад, Syslog або SIEM-системи) для централізованого зберігання та глибинного аналізу. Це є критично важливим для проведення розслідувань інцидентів та своєчасного реагування на порушення політики безпеки.

Керування ідентифікацією та доступом Система підтримує широкий спектр механізмів аутентифікації, інтегруючись як із локальними базами даних користувачів, так і зі зовнішніми серверами аутентифікації, такими як LDAP, RADIUS та TACACS+. Це дозволяє реалізувати рольову модель доступу, де кожен користувач або група отримують права виключно на ті ресурси та сервіси, які необхідні їм для роботи. Така гранулярність значно підвищує загальний рівень захищеності мережі.

Продуктивність та забезпечення безперервності бізнесу Архітектура Cisco ASA спроєктована з урахуванням вимог до високої доступності та відмовостійкості. Пристрій розрахований на роботу в умовах пікових навантажень, забезпечуючи високу пропускну здатність без деградації сервісів. Модульна структура дозволяє масштабувати функціональність шляхом встановлення додаткових плат розширення та оновлення програмного забезпечення. Крім того, підтримка технологій кластеризації та балансування навантаження гарантує безперервність бізнес-процесів навіть у разі виходу з ладу одного з вузлів системи.

У підсумку, поєднання функцій глибокої інспекції, криптографічного захисту, запобігання вторгненням та гнучкого управління робить Cisco ASA універсальним стандартом для побудови захищених корпоративних мереж будь-якого масштабу.

2 РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ПІДКЛЮЧЕННЯ

2.1 Системний аналіз вимог безпеки та функціональності

Фундаментальним етапом проєктування будь-якої системи захищеного віддаленого доступу на базі технології SSL VPN є детальне формування та аналіз вимог до безпеки. Це критично важливо для забезпечення надійної комунікації з кінцевими точками та мережевим обладнанням. Враховуючи динамічну природу кіберзагроз та постійну еволюцію методів атак, система повинна не лише відповідати сучасним стандартам, але й мати гнучкі механізми адаптації.

Першочерговим завданням при побудові системи є реалізація надійних процедур аутентифікації. Традиційні методи перевірки справжності користувача потребують посилення, оскільки стандартні парольні захисти часто виявляються недостатніми. Ефективним підходом є впровадження політик використання складних парольних комбінацій з обов'язковою періодичною зміною. Однак найвищий рівень безпеки досягається завдяки інтеграції двофакторної аутентифікації (2FA), яка поєднує знання пароля з володінням фізичним токеном, отриманням одноразових кодів або використанням криптографічної пари відкритого та закритого ключів.

Наступним критичним елементом є забезпечення конфіденційності даних шляхом шифрування. Весь трафік, що проходить через тунель SSL VPN, повинен бути захищений із використанням сучасних криптографічних алгоритмів. Адміністратори системи зобов'язані регулярно переглядати налаштування шифрування, відмовляючись від застарілих протоколів, що містять вразливості, та імплементувати новітні стандарти для нівелювання ризиків перехоплення інформації.

Не менш важливою складовою є процеси ідентифікації та авторизації. Необхідно забезпечити суворий контроль за тим, хто саме отримує доступ до мережі, та розмежувати права користувачів. Реалізація принципу найменших привілеїв, рольова модель доступу (RBAC) та використання цифрових сертифікатів дозволяють мінімізувати ризики внутрішніх загроз. Додатковим запобіжним заходом є автоматичне блокування облікових записів після серії невдалих спроб входу, що ускладнює проведення атак повного перебору (brute-force).

Четвертим стовпом безпеки є моніторинг та аудит. Система повинна забезпечувати безперервне протоколювання дій користувачів у межах VPN-сесій. Глибокий аналіз лог-файлів дозволяє виявляти аномальну поведінку, що може свідчити про компрометацію облікового запису або спробу зламу. Налаштування автоматизованих систем оповіщення та швидкого реагування на інциденти є необхідною умовою для підтримки цілісності мережевої інфраструктури.

Окрім базових принципів, архітектура системи повинна враховувати специфічні вектори атак. Зокрема, критичним є захист від атак типу «людина посередині» (MITM). Для цього система SSL VPN мусить використовувати сувору перевірку автентичності серверів та клієнтів за допомогою валідних цифрових сертифікатів, що унеможливлює непомітне втручання зловмисника в канал передачі даних.

Окрему увагу слід приділити запобіганню витокам інформації. Це досягається шляхом впровадження комплексних політик контролю, які регламентують обробку даних, обов'язкове шифрування інформації в русі (data-in-motion) та відповідність корпоративним стандартам безпеки. Також система повинна бути інтегрована з антивірусним програмним забезпеченням для захисту від шкідливого коду. Механізми перевірки кінцевих точок перед наданням доступу дозволяють переконатися, що пристрій користувача не інфікований вірусами чи шпигунським ПЗ, запобігаючи поширенню загроз всередину корпоративної мережі.

Технічна стійкість системи також включає захист від експлойтів, спрямованих на переповнення буфера. Це вимагає використання безпечного програмного коду та механізмів, що запобігають виконанню довільного коду зловмисниками. Важливим аспектом життєвого циклу системи є регулярне оновлення програмного забезпечення та встановлення патчів безпеки, що закривають відомі вразливості. Завершує контур безпеки налагоджена процедура реагування на інциденти, яка базується на інструментах SIEM для кореляції подій та автоматичної протидії загрозам.

Ефективність системи SSL VPN значною мірою залежить від якості та зручності клієнтського програмного забезпечення. Функціональні вимоги до клієнта спрямовані на забезпечення позитивного досвіду користувача (UX) та стабільності роботи.

Програмне забезпечення повинно характеризуватися простотою розгортання. Інсталяційний процес має бути максимально автоматизованим і зрозумілим навіть для непідготовлених співробітників, а початкова конфігурація — зводитися до імпорту профілю або вибору сервера зі списку. Інтерфейс програми має бути інтуїтивним, із можливістю збереження параметрів автентифікації та швидкого перемикання між різними шлюзами доступу.

Обов'язковою вимогою є кросплатформність. Клієнтський додаток повинен коректно функціонувати в усіх популярних операційних середовищах, включаючи настільні системи (Windows, macOS, Linux) та мобільні платформи (Android, iOS), забезпечуючи універсальний доступ з будь-якого пристрою. Критично важливою функцією є здатність до автоматичного відновлення з'єднання (reconnect). У разі короткочасних розривів зв'язку або зміни типу підключення (наприклад, перехід з Wi-Fi на LTE) VPN-тунель має відновлюватися прозоро для користувача.

Для спрощення технічної підтримки клієнт повинен мати вбудовані засоби діагностики та моніторингу. Користувач повинен мати змогу переглянути статус підключення та журнал подій, що дозволить швидко

локалізувати проблему. Розширений функціонал може включати опції приховування реальної IP-адреси, керування шириною каналу та нативну підтримку різних криптографічних протоколів, що робить рішення гнучким та адаптивним до різних сценаріїв використання.

2.2 Структурна організація та архітектурні принципи системи

Архітектура взаємодії між клієнтською частиною та серверним ядром VPN будується на фундаменті чітко визначених комунікаційних принципів. Ця система правил та обмежень регламентує всі аспекти обміну даними, гарантуючи стабільність та передбачуваність роботи мережевого шлюзу.

Першочерговим стовпом архітектури є принцип ефективності. Він передбачає реалізацію оптимізованих алгоритмів передачі пакетів, метою яких є мінімізація затримок (latency) та зменшення службового навантаження на канал. Це дозволяє підтримувати стійке з’єднання навіть за умов використання нестабільних або низькошвидкісних мереж доступу.

Другим критичним аспектом є прозорість процесів. Архітектура повинна бути побудована таким чином, щоб кожен етап обміну даними був зрозумілим і відкритим для інструментів контролю. Це забезпечує можливість наскрізного моніторингу, швидкої локалізації технічних збоїв та підтримки високої доступності сервісу.

Третій принцип — надійність — вимагає гарантованої доставки даних у повному обсязі, без спотворень чи втрат пакетів. Цілісність інформації є абсолютним пріоритетом, особливо коли йдеться про транзакції з критично важливими або конфіденційними даними.

Четвертим, і, безумовно, одним із найважливіших принципів, є безпека. Уся комунікація в межах тунелю між кінцевою точкою та сервером підлягає

обов'язковому шифруванню. Це нівелює ризики перехоплення трафіку або несанкціонованого доступу до інформаційних активів з боку третіх осіб.

Завершує цей перелік принцип сумісності, який гарантує універсальність системи. Вона повинна коректно функціонувати в гетерогенних середовищах, підтримуючи широкий спектр клієнтських пристроїв, операційних систем та версій мережевих протоколів, що забезпечує користувачам гнучкість у виборі платформи.

Регламентація обміну інформацією в системі SSL VPN покладається на набір комунікаційних протоколів, які відповідають за захист, сумісність та стабільність з'єднання. Центральне місце в цій ієрархії займають протоколи TLS (Transport Layer Security) та SSL (Secure Sockets Layer). Вони виступають базовою технологією, що забезпечує криптографічний захист каналу та взаємну аутентифікацію учасників з'єднання при передачі даних через відкриті мережі [1].

Для передачі гіпертекстової інформації застосовується протокол HTTP, який у поєднанні з криптографічними механізмами TLS/SSL трансформується в HTTPS. Така комбінація дозволяє забезпечити конфіденційність та цілісність веб-трафіку. На мережевому рівні захист забезпечується протоколом IPsec (Internet Protocol Security), який здійснює шифрування та аутентифікацію безпосередньо IP-пакетів і є стандартом для побудови багатьох VPN-рішень.

Окремої уваги заслуговує OpenVPN — популярне рішення з відкритим кодом, що реалізує технологію VPN на базі протоколів SSL/TLS. Завдяки підтримці надійних алгоритмів шифрування та надзвичайно гнучкій конфігурації, OpenVPN став одним із найбільш затребуваних інструментів для створення захищених тунелів [1]. Також поширеним є використання гібридного підходу L2TP/IPsec, де протокол L2TP відповідає за створення тунелю другого рівня, а IPsec забезпечує криптографічний захист та перевірку справжності пакетів. Комплексне застосування цих протоколів дозволяє побудувати масштабовану та захищену інфраструктуру обміну даними.

Технічна реалізація системи захищеного доступу базується на злагодженій роботі кількох ключових модулів. Ядром системи виступає VPN-сервер, який бере на себе основне навантаження з обслуговування підключень. Він відповідає за термінацію користувацьких сесій, управління процесами аутентифікації, а також за шифрування та дешифрування потоків даних.

На межі мережевого периметра функціонують VPN-шлюзи. Ці пристрої діють як посередники між незахищеною зовнішньою мережею та внутрішньою корпоративною інфраструктурою. Їхнє завдання полягає в первинній обробці вхідного трафіку, його фільтрації та маршрутизації до відповідних внутрішніх ресурсів.

Невід'ємною складовою безпеки є системи аутентифікації, що призначені для верифікації особистості користувачів. Вони можуть підтримувати різні методи перевірки, від класичних паролів до використання цифрових сертифікатів, апаратних токенів або біометричних даних. Безпосередній захист інформації покладається на модулі шифрування. Вони імплементують сучасні криптографічні алгоритми для забезпечення конфіденційності даних під час їх транзиту через публічні канали зв'язку.

Для забезпечення контролю та аудиту в систему інтегровано засоби моніторингу та логування. Ці компоненти фіксують усі події в мережі, включаючи успішні та невдалі спроби входу, параметри сесій передачі даних та системні повідомлення. Зібрана інформація використовується для аналізу безпеки, виявлення аномалій та розслідування інцидентів. Сукупність цих елементів формує надійну платформу для організації безпечного віддаленого доступу.

2.3 Конфігурація мережевого обладнання та інтеграція сервісів

Впровадження сервера TACACS (Terminal Access Controller Access-Control System) є стратегічним кроком для підвищення рівня керованості та безпеки корпоративної мережі. Цей протокол забезпечує відокремлення процесів аутентифікації, авторизації та обліку (AAA), що дозволяє реалізувати гранулярний контроль доступу адміністраторів до мережевого обладнання.

Процес аутентифікації через TACACS передбачає централізовану верифікацію особи користувача. Коли адміністратор намагається підключитися до маршрутизатора або комутатора, пристрій не перевіряє пароль локально, а надсилає запит на сервер TACACS. Останній звіряє отримані облікові дані зі своєю базою, що мінімізує ризики несанкціонованого проникнення та спрощує процедуру зміни паролів, оскільки це робиться в одному місці.

Після підтвердження особи настає етап авторизації. Сервер чітко регламентує перелік команд та операцій, доступних конкретному адміністратору. Це дозволяє реалізувати принцип найменших привілеїв, коли молодший персонал може лише переглядати конфігурацію, тоді як старші інженери мають право на внесення змін.

Ключовою перевагою є централізоване керування. Адміністратори безпеки отримують єдину точку входу для налаштування політик доступу для всієї інфраструктури, що гарантує їхню послідовність та усуває розбіжності в налаштуваннях окремих вузлів. Завдяки можливості інтеграції з каталогами користувачів, такими як Microsoft Active Directory або LDAP, зникає потреба в дублюванні облікових записів, а процеси надання та відкликання доступу стають автоматизованими.

Важливим елементом безпеки є також аудит та журналювання. Сервер фіксує кожну команду, введену користувачем під час сесії управління. Деталізовані логи дозволяють відтворити хронологію подій у разі інцидентів,

виявити підозрілу активність та забезпечити відповідність вимогам регуляторних стандартів (compliance).

Для забезпечення стабільності комутованих мереж критично важливим є використання протоколу Spanning Tree Protocol (STP). Цей стандарт другого рівня моделі OSI, розроблений Радьєю Перлман, вирішує проблему широкомовних штормів, які виникають через надлишкові фізичні з'єднання між комутаторами. Алгоритм STP логічно блокує певні порти, перетворюючи граф мережі з циклами на деревоподібну топологію без петель.

Функціонування протоколу базується на обміні спеціальними кадрами — BPDU (Bridge Protocol Data Units). На основі інформації з цих кадрів (пріоритет, MAC-адреса, вартість лінків) комутатори обирають кореневий міст (Root Bridge), який стає точкою відліку для побудови дерева. У разі змін у топології генеруються повідомлення TCN (Topology Change Notification).

Порти комутаторів у класичному STP проходять через послідовність станів: блокування (Blocking), прослуховування (Listening), навчання (Learning) та пересилання (Forwarding). Кожен перехід займає певний час, що в сумі може призводити до значних затримок у збіжності мережі (до 50 секунд) при зміні топології. Кореневий комутатор періодично (за замовчуванням кожні 2 секунди) розсилає Hello BPDU для підтвердження своєї працездатності.

Сучаснішою альтернативою є протокол RSTP (Rapid Spanning Tree Protocol). Він значно прискорює процес збіжності мережі завдяки відмові від пасивних таймерів на користь активного механізму рукостискання (Proposal/Agreement). RSTP дозволяє портам переходити в стан пересилання майже миттєво, що є критичним для чутливих до затримок сервісів. При цьому протокол зберігає зворотну сумісність із застарілим STP обладнанням.

Впровадження технології SSL VPN на рівні маршрутизаторів та комутаторів є важливим етапом побудови захищеного периметра. Використання сучасних платформ (включно з віртуальними середовищами типу GNS3) дозволяє активувати функції VPN безпосередньо на мережевих вузлах. Це забезпечує створення захищених тунелів для віддалених

співробітників, гарантуючи конфіденційність трафіку через шифрування та сувору аутентифікацію. Такий підхід робить мережу більш масштабованою, оскільки потужні маршрутизатори здатні термінувати тисячі одночасних сесій [13].

Ще більш ефективним є поєднання SSL VPN із міжмережевими екранами (фаєрволами) наступного покоління (NGFW), такими як Cisco ASA або рішення від Palo Alto. Інтеграція на цьому рівні дозволяє застосовувати глибоку інспекцію трафіку всередині тунелю. Адміністратори можуть створювати гранулярні правила доступу, обмежуючи користувачів лише певними сервісами або сегментами мережі в залежності від їхньої ролі. Це мінімізує поверхню атаки та запобігає горизонтальному переміщенню зловмисників у разі компрометації облікового запису віддаленого працівника.

Для максимальної безпеки система SSL VPN повинна бути інтегрована з сервером TACACS+. Це дозволяє централізувати управління доступом не лише для адміністраторів, а й для кінцевих користувачів VPN (або використовувати RADIUS для останніх, а TACACS+ для адміністрування). Шлюз VPN звертається до сервера AAA для перевірки облікових даних та отримання атрибутів авторизації (наприклад, ACL, які динамічно застосовуються до сесії користувача). Така архітектура забезпечує єдину точку керування політиками безпеки для всієї організації.

Практична реалізація описаних технологій демонструє їхню ефективність у різних сценаріях. На рис. 2.1 представлено типову схему розгортання Cisco ASA для забезпечення захищеного зв'язку з невеликими філіями, де пристрій виконує роль шлюзу безпеки.

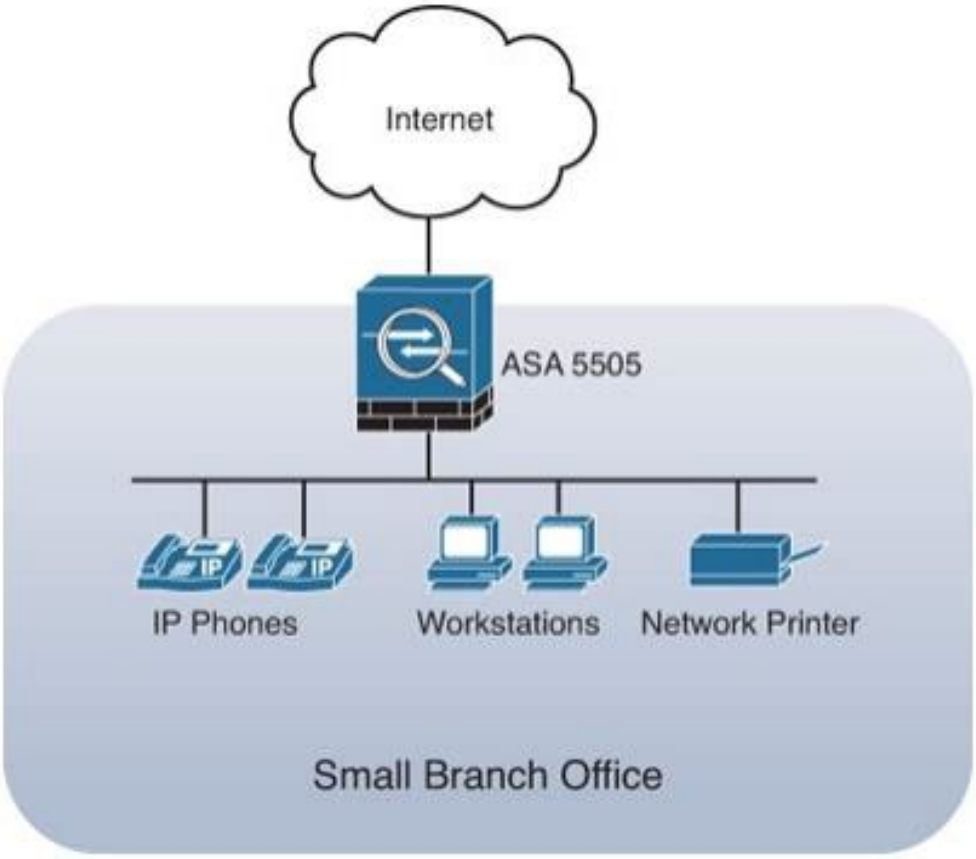


Рисунок 2.1. Архітектура підключення віддалених філій з використанням шлюзу безпеки Cisco ASA

На рис. 2.2 зображено архітектуру для сегмента малого та середнього бізнесу, де реалізовано поділ на ізольовані зони безпеки (DMZ, внутрішня мережа, гостьова мережа) з використанням функцій SSL VPN для віддаленого доступу.

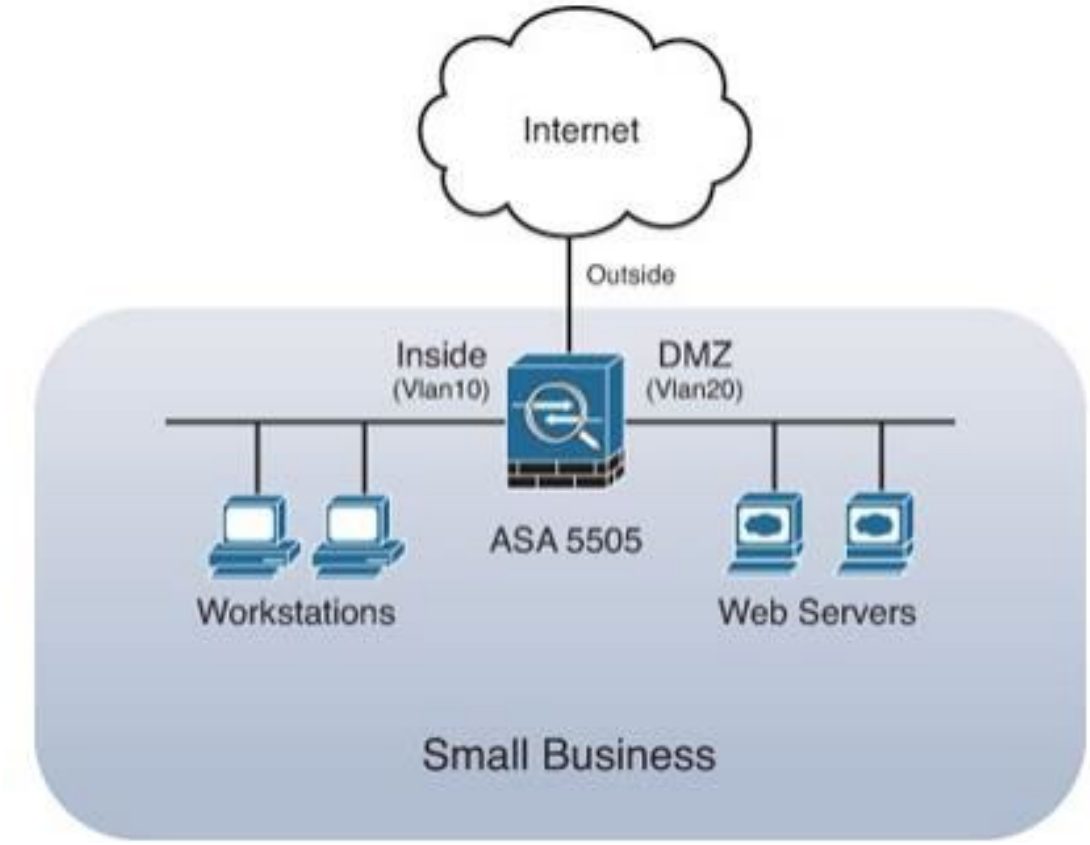


Рисунок 2.2. Схема організації захищених сегментів мережі для підприємств малого бізнесу на базі Cisco ASA.

В табл.2.1 зазначено аналіз практичних прикладів інтеграції захищених мережевих рішень, що дає змогу побудувати якісну інфраструктуру.

Таблиця 2.1 – Аналіз практичних прикладів інтеграції захищених мережевих рішень

Галузь застосування	**Проблематика та ключові виклики**	**Реалізоване технічне рішення**	**Отриманий ефект та переваги**
Банківський та фінансовий сектор	Установи даного сектору функціонують в умовах підвищених	Розгортання комплексу мережевого захисту на базі платформи Cisco	Мінімізація ризиків, пов'язаних із фінансовим шахрайством та

	ризиків, що вимагає безкомпромісного захисту транзакційних даних та конфіденційної інформації клієнтів. Критичним завданням є забезпечення цілісності фінансових операцій та відповідність жорстким регуляторним вимогам щодо кібербезпеки.	ASA з інтеграцією протоколів SSL VPN. Це дозволяє створити ізольовані, криптографічно захищені тунелі для безпечного віддаленого доступу співробітників до внутрішніх банківських систем та баз даних.	витоком чутливих даних. Як наслідок, відбувається зміцнення репутації установи, зростання рівня довіри з боку клієнтів та партнерів, а також гарантується стабільність бізнес-процесів.
Транснаціональні IT-корпорації та сервісні провайдери	Великі технологічні компанії стикаються з проблемою управління розгалуженою інфраструктурою та необхідністю консолідації	Побудова єдиного захищеного корпоративного периметра з використанням шлюзів Cisco ASA та технології SSL VPN. Рішення	Суттєве підвищення ефективності роботи технічних команд завдяки стабільному доступу до ресурсів. Скорочення

	різнорідних мережевих ресурсів. Головний виклик полягає в організації безпечних комунікаційних каналів для глобальних команд, що працюють у різних часових поясах.	забезпечує надійну маршрутизацію трафіку та захист даних при обміні інформацією між географічно віддаленими офісами та центрами обробки даних.	часу реакції на інциденти, оптимізація витрат на адміністрування мережі та забезпечення глобальної доступності сервісів для персоналу.
Освітні заклади та університетські мережі	Перед академічними установами стоїть завдання захисту інтелектуальної власності та персональних даних при одночасному забезпеченні відкритого доступу до електронних бібліотек та лабораторних	Впровадження системи безпечного віддаленого доступу на основі Cisco ASA та SSL VPN. Це рішення дозволяє розмежувати права доступу та створити віртуальні захищені канали для	Створення безпечного та гнучкого середовища для електронного навчання (E-learning). Забезпечення зручності користування цифровими ресурсами з будь-якої точки світу, що сприяє безперервності освітнього

	ресурсів для тисяч студентів та викладачів, часто з використанням власних пристроїв.	авторизованих учасників освітнього процесу без загрози для ядра університетської мережі.	процесу та захисту наукових напрацювань.

2.4 Проєктування топології та стратегія ір-адресації

Розробка логічної структури мережі та планування IP-адресації є фундаментальним етапом проєктування, від якого безпосередньо залежить коректність обміну даними між усіма вузлами системи. Цей процес вимагає системного підходу та врахування низки технічних нюансів для забезпечення стабільності та масштабованості інфраструктури.

На початковому етапі здійснюється вибір IP-адресного простору. Інженерам необхідно визначити оптимальний діапазон адрес, який би відповідав масштабу проєкту та гарантував повну сумісність із поточною мережевою інфраструктурою, уникаючи конфліктів адрес. При цьому вибір повинен базуватися на аналізі технічної документації використовуваного обладнання, а також враховувати галузеві рекомендації та стандарти щодо інформаційної безпеки мереж.

Наступним критично важливим кроком є логічна сегментація мережі, тобто розподіл загального обраного адресного простору на окремі підмережі. Така структуризація повинна базуватися на реальній кількості підключених пристроїв, а також враховувати функціональне призначення та специфіку окремих сегментів мережі (наприклад, виділення окремих підмереж для серверів, користувачів та управління). Цей підхід значно спрощує процеси системного адміністрування, підвищує загальний рівень захищеності шляхом

ізоляції широкомовного трафіку та забезпечує необхідну гнучкість для майбутнього розширення системи. Візуалізацію загальної структури та логічних зв'язків у мережі наведено на рис. 2.3.

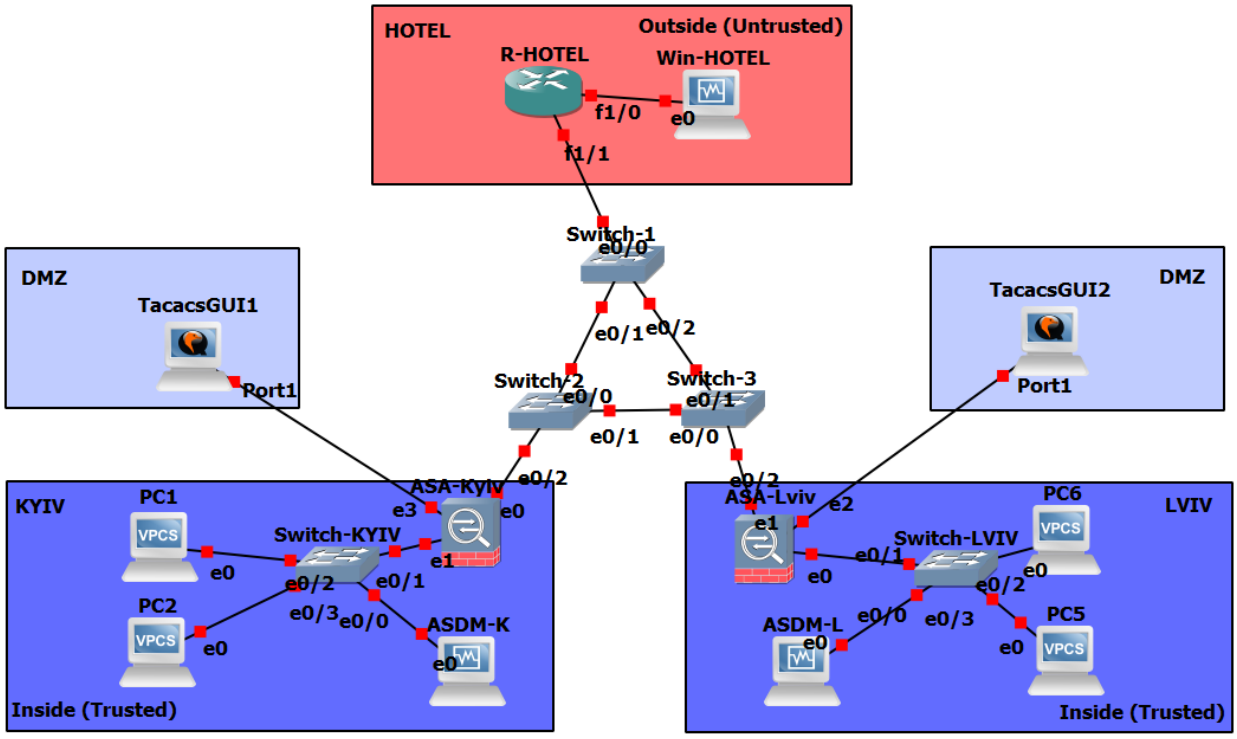


Рисунок 2.3. Загальна схема спроєктованої мережевої інфраструктури.

Після завершення теоретичного планування розпочинається етап безпосередньої конфігурації обладнання. Визначені IP-адреси та маски підмереж прописуються на інтерфейсах активних мережевих пристроїв — маршрутизаторів, комутаторів рівня розподілу та доступу, а також на серверах. Коректне налаштування адресації на цьому етапі є запорукою правильної маршрутизації пакетів та забезпечення безперебійної взаємодії між усіма елементами архітектури.

Завершальною фазою є комплексна верифікація налаштувань. Вона передбачає проведення низки діагностичних тестів (наприклад, перевірка доступності вузлів за допомогою утиліт ping та traceroute) для підтвердження надійності каналів зв'язку. Таке тестування дозволяє переконатися у відсутності помилок конфігурації або конфліктів IP-адрес та виявити

потенційні проблеми ще до моменту введення системи в промислову експлуатацію.

Сегмент мережі / Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Префікс
Зовнішні підключення (wan/hotel)				
Підмережа wan (зовнішня)	-	200.50.50.0	255.255.255.0	/24
Підмережа HOTEL	-	192.168.50.0	255.255.255.0	/24
R-hotel	Fa0/0 (wan)	200.50.50.2	255.255.255.0	/24
	Fa1/0 (LAN)	192.168.50.1	255.255.255.0	/24
Win-HOTEL	E0	192.168.50.2	255.255.255.0	/24
Філія київ (kyiv)				
Підмережа KYIV (LAN)	-	172.16.10.0	255.255.255.0	/24
Підмережа DMZ-KYIV	-	172.16.20.0	255.255.255.0	/24
Asa-kyiv	Gig0/2 (wan)	200.50.50.3	255.255.255.0	/24
	Gig0/0 (LAN)	172.16.10.1	255.255.255.0	/24
	Gig0/1 (DMZ)	172.16.20.1	255.255.255.0	/24
Tacacs-1	Port1	172.16.20.2	255.255.255.0	/24
	Шлюз	172.16.20.1	-	-

Asdm-k (mgmt)	E0	172.16.10.2	255.255.255.0	/24
	Шлюз	172.16.10.1	-	-
Vpcs-k-1	Fa0/0	172.16.10.3	255.255.255.0	/24
Vpcs-k-2	Fa0/0	172.16.10.4	255.255.255.0	/24
Філія львів (lviv)				
Підмережа LVIV (LAN)	-	10.20.10.0	255.255.255.0	/24
Підмережа DMZ-LVIV	-	10.20.20.0	255.255.255.0	/24
Asa-lviv	Gig0/1 (wan)	200.50.50.1	255.255.255.0	/24
	Gig0/0 (LAN)	10.20.10.1	255.255.255.0	/24
	Gig0/2 (DMZ)	10.20.20.1	255.255.255.0	/24
Tacacs-2	Port1	10.20.20.2	255.255.255.0	/24
	Шлюз	10.20.20.1	-	-
Asdm-l (mgmt)	E0	10.20.10.2	255.255.255.0	/24
	Шлюз	10.20.10.1	-	-
Vpcs-l-1	Fa0/0	10.20.10.3	255.255.255.0	/24
Vpcs-l-2	Fa0/0	10.20.10.4	255.255.255.0	/24

Ефективне проєктування системи мережевої безпеки неможливе без детального планування адресації та вибору відповідної апаратної платформи. Коректна конфігурація підмереж та IP-адрес виступає фундаментом для стабільної комунікації між вузлами, тоді як правильно підібране обладнання гарантує продуктивність та захищеність цих каналів зв'язку. Компанія Cisco Systems, проаналізувавши динаміку ринкових потреб, представила лінійку адаптивних пристроїв безпеки серії ASA 5500. Ця серія розроблена з акцентом

на гнучке масштабування та можливість модернізації, що дозволяє організаціям зберігати ефективність інвестицій у довгостроковій перспективі.

Найбільш популярним рішенням для невеликих офісів є модель Cisco ASA 5505. Її передня панель, зовнішній вигляд якої представлено на рис. 2.4, містить набір індикаторів для діагностики стану пристрою.

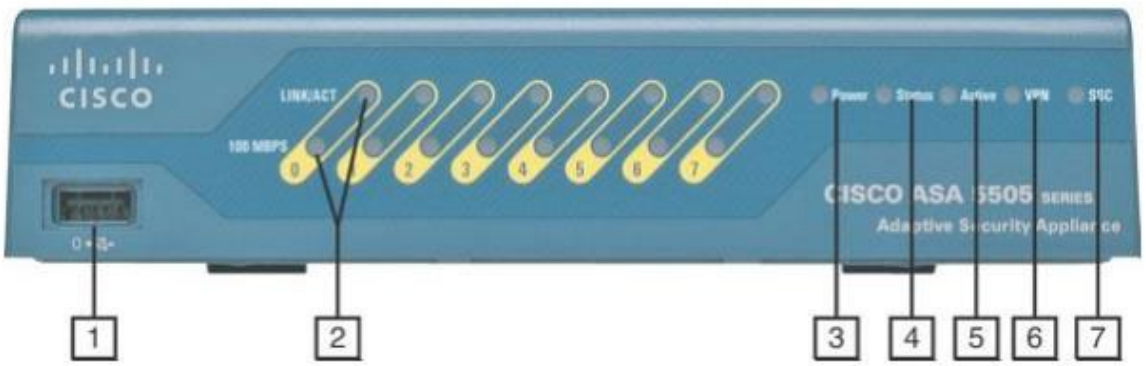


Рисунок 2.4. Фронтальна панель шлюзу безпеки Cisco ASA 5505

Крім зарезервованого для майбутніх розширень USB-порту, тут розташована панель світлодіодної індикації портів. Кожен із восьми інтерфейсів оснащений індикаторами швидкості та активності. Логіка їх роботи наступна: відсутність світіння індикатора швидкості свідчить про роботу в режимі 10 Мбіт/с, тоді як зелене світло сигналізує про з’єднання на швидкості 100 Мбіт/с. Індикатор активності (Link/Act) при постійному зеленому світінні підтверджує наявність фізичного лінку, а миготіння вказує на процес передачі даних.

Окрім мережевих інтерфейсів, на передню панель виведено системні індикатори. Індикатор Power сигналізує про наявність живлення, а індикатор Status відображає етапи завантаження: миготіння означає проходження самодіагностики, постійне зелене світло — штатну роботу, а янтарний колір — апаратну помилку. Індикатор Active підтверджує, що пристрій є активним вузлом у кластері відмовостійкості або працює в автономному режимі. Також присутній спеціалізований індикатор VPN, який активується при встановленні

захищених тунелів, та індикатор SSC, що вказує на наявність додаткової карти безпеки.

Комутаційні та управлінські роз'єми винесено на тильну сторону корпусу, яку зображено на рис. 2.5.

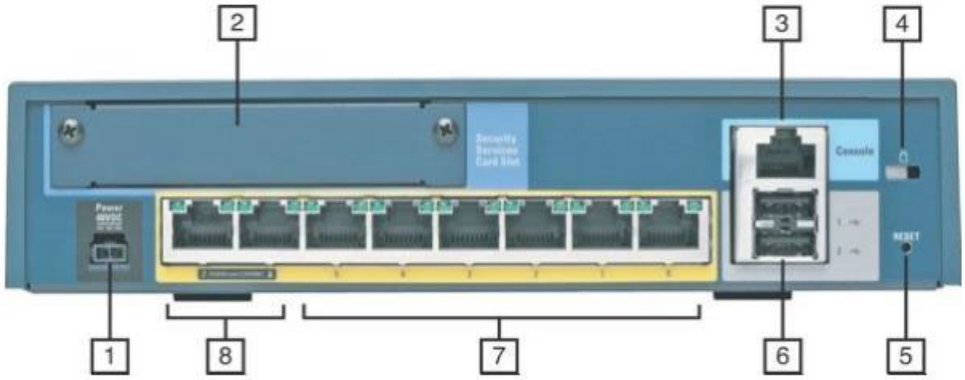


Рисунок 2.5. Інтерфейсна панель та роз'єми Cisco ASA 5505

Тут розміщено вхід для джерела живлення, замок Kensington для фізичного захисту від крадіжки, кнопку скидання (Reset) та два USB-порти версії 2.0, функціонал яких зарезервовано. Для первинної конфігурації через інтерфейс командного рядка (CLI) передбачено консольний порт стандарту RJ-45. Мережева частина представлена восьмипортовим комутатором Fast Ethernet (10/100 Мбіт/с), причому порти з номерами 6 та 7 підтримують технологію живлення через Ethernet (PoE), що дозволяє підключати IP-телефони або точки доступу безпосередньо до шлюзу безпеки. Також на задній панелі знаходиться слот розширення для модуля SSC, хоча старі моделі карт, такі як Cisco AIP-SSC-5, вже виведені з експлуатації.

Лінійка Cisco ASA пропонує рішення для різних сегментів бізнесу, що дозволяє обрати оптимальний баланс між вартістю та продуктивністю. Модель Cisco ASA 5510 позиціюється як оптимальний вибір для малого та середнього бізнесу з обмеженим бюджетом, забезпечуючи необхідний базовий рівень захисту на етапі становлення інфраструктури.

Для організацій, що активно розвиваються та потребують вищої пропускної здатності, розроблено модель Cisco ASA 5520. Вона вирізняється

підтримкою інтерфейсів Gigabit Ethernet та здатністю обробляти значно більші обсяги трафіку, що робить її стандартом для корпоративних мереж середнього масштабу. Найпотужнішою у розглянутому сегменті є платформа Cisco ASA 5540, орієнтована на великі підприємства з підвищеними вимогами до безпеки та відмовостійкості. Взаємозв'язок між вартістю пристроїв та їх функціональними можливостями проілюстровано на рис. 2.6.

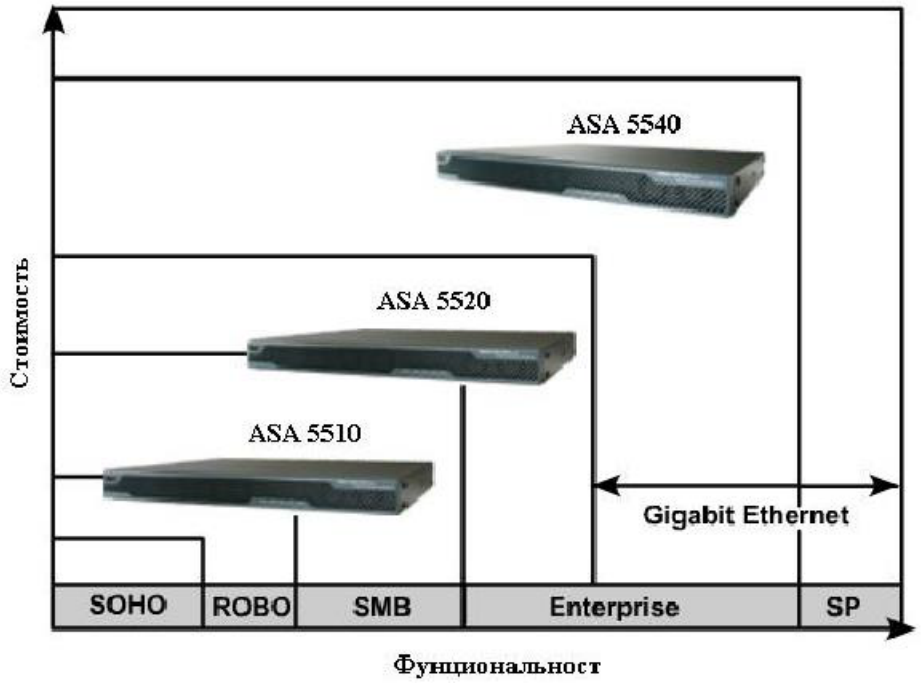


Рисунок 2.6. Графік співвідношення цінової політики та функціональності моделей ASA

Ключовою перевагою платформи ASA є її модульна архітектура. Усі моделі підтримують інтеграцію спеціалізованих сервісних модулів (SSM), які значно розширюють можливості базового фаєрвола. До таких компонентів, приклад яких наведено на рис. 2.7, належать модулі адаптивного запобігання вторгненням (AIP-SSM) та модулі контролю безпеки контенту (CSC-SSM).



Рисунок 2.7. Зовнішній вигляд модуля розширення адаптивної перевірки

Завдяки такій гнучкості, адміністратори можуть адаптувати систему захисту до поточного ландшафту кіберзагроз, додаючи нові функції без повної заміни обладнання.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ВЕРИФІКАЦІЯ КОМПЛЕКСУ ЗАХИСТУ МЕРЕЖІ

3.1 Алгоритм розгортання та конфігурації підсистеми віддаленого доступу

Для організації захищеного каналу зв'язку, що дозволяє віддаленим користувачам отримувати доступ до корпоративних інформаційних активів за допомогою технології SSL VPN, було обрано метод налаштування через спеціалізоване програмне забезпечення Cisco Adaptive Security Device Manager (ASDM). Цей інструмент надає адміністраторам зручний графічний інтерфейс для керування політиками безпеки без необхідності використання командного рядка.

Першим етапом впровадження стала авторизація в системі управління. Після запуску клієнта ASDM необхідно пройти процедуру аутентифікації, ввівши облікові дані адміністратора та IP-адресу пристрою, як показано на рис. 3.1.

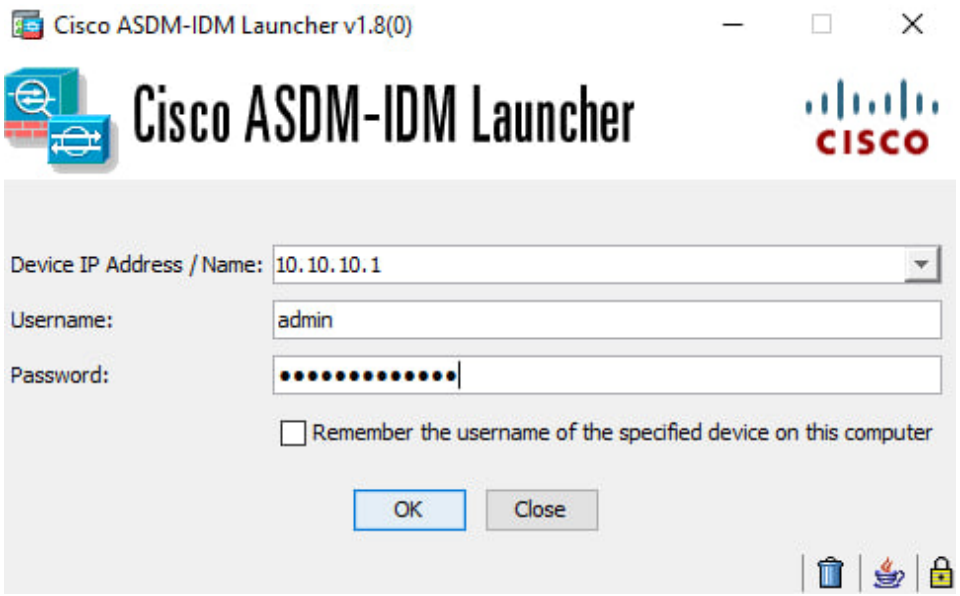


Рисунок 3.1. Вікно авторизації в панелі керування Cisco ASDM

Успішний вхід відкриває доступ до головної інформаційної панелі (Dashboard), яка відображає поточний статус апаратної платформи, статистику завантаження інтерфейсів та загальний стан системи безпеки. Інтерфейс моніторингу наведено на рис. 3.2.

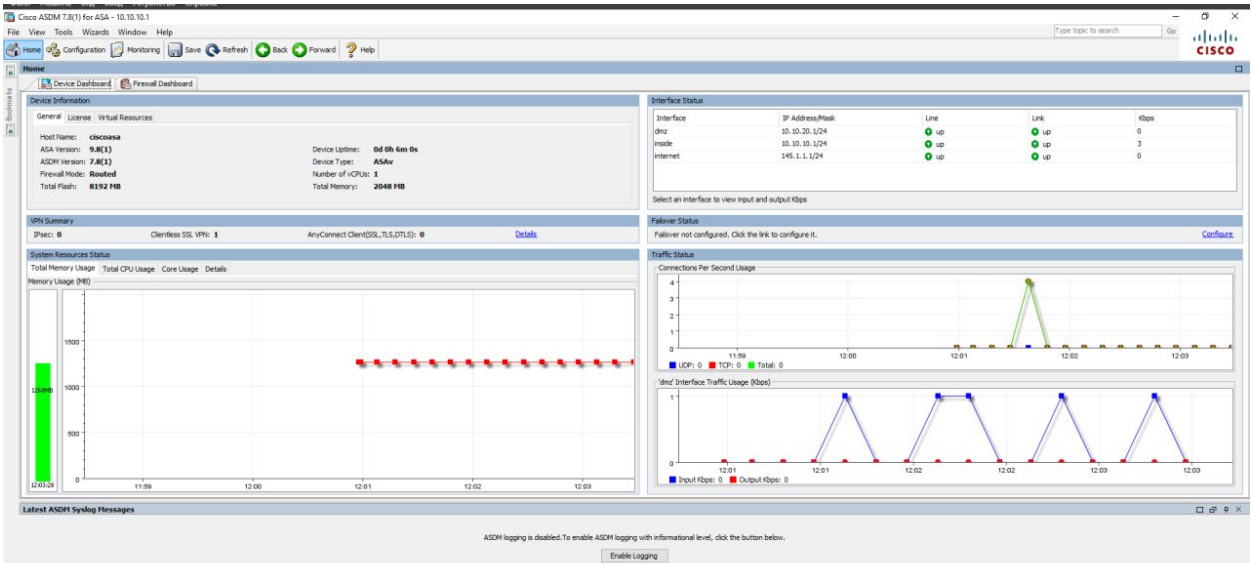


Рисунок 3.2. Головна інформаційна панель стану системи ASDM

Безпосереднє налаштування VPN-сервісу здійснювалося за допомогою інтегрованого майстра конфігурації Clientless SSL VPN Wizard. Цей інструмент дозволяє крок за кроком сформувати новий профіль підключення, мінімізуючи ймовірність помилок. У параметрах профілю було задано унікальне ім'я для ідентифікації групи тунелювання, визначено пул IP-адрес, які будуть динамічно призначатися віддаленим клієнтам, а також окреслено перелік мережевих ресурсів, доступних для цієї групи користувачів. Деталі налаштування профілю візуалізовано на рис. 3.3.

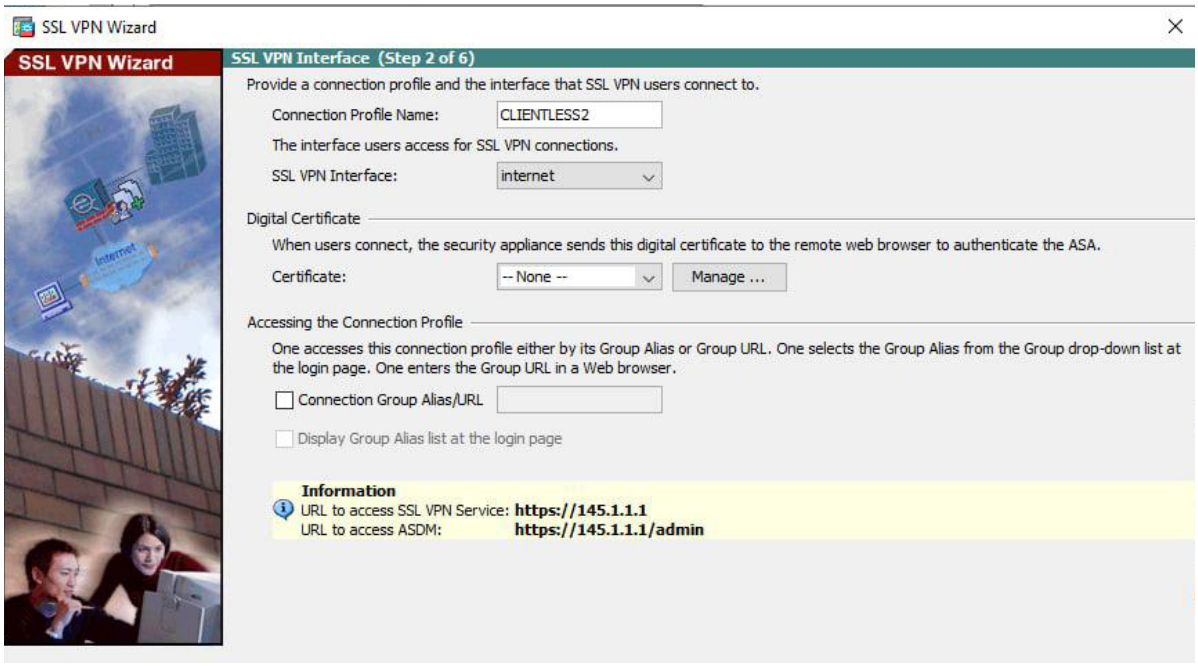


Рисунок 3.3. Меню конфігурації параметрів профілю SSL VPN

Наступним кроком стала реєстрація облікових записів для суб'єктів доступу. Було створено нові записи користувачів із визначеними правами, що дозволяють їм проходити аутентифікацію на веб-порталі сервісу SSL VPN. Процес додавання користувача та налаштування його параметрів входу відображено на рис. 3.4.

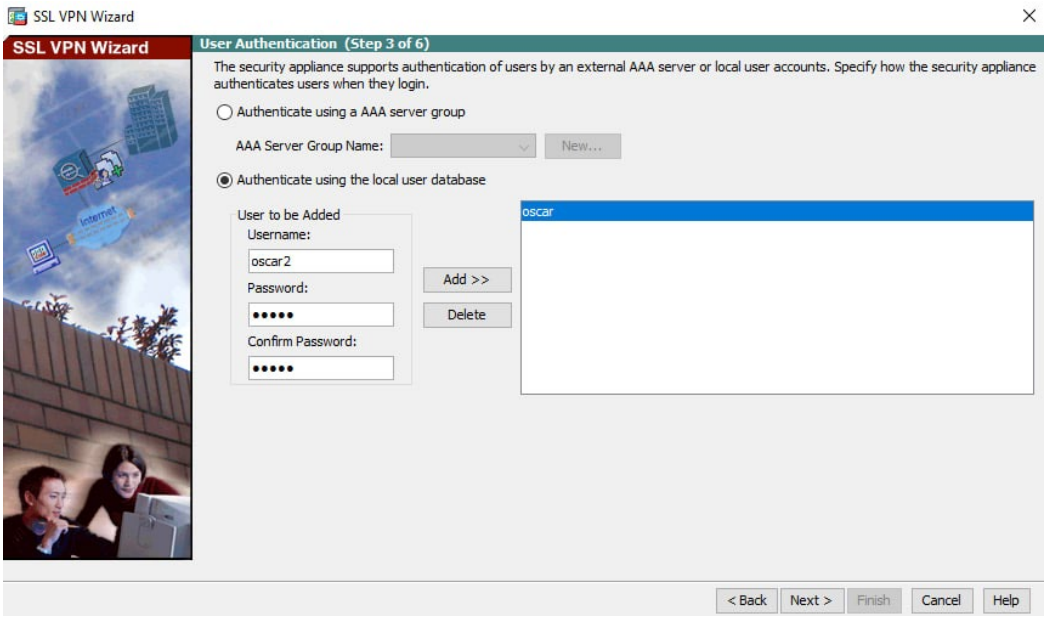


Рисунок 3.4. Процедура реєстрації нового користувача для доступу до порталу

Для забезпечення зручної навігації та швидкого доступу до необхідних сервісів, у розділі керування закладками (Bookmarks) було сформовано каталог посилань. Це дозволяє користувачам переходити до внутрішніх веб-сайтів, файлових сховищ та додатків безпосередньо з інтерфейсу браузера, без необхідності запам'ятовувати IP-адреси. Приклад додавання закладки для ресурсу TACGUI-KYIV продемонстровано на рис. 3.5.

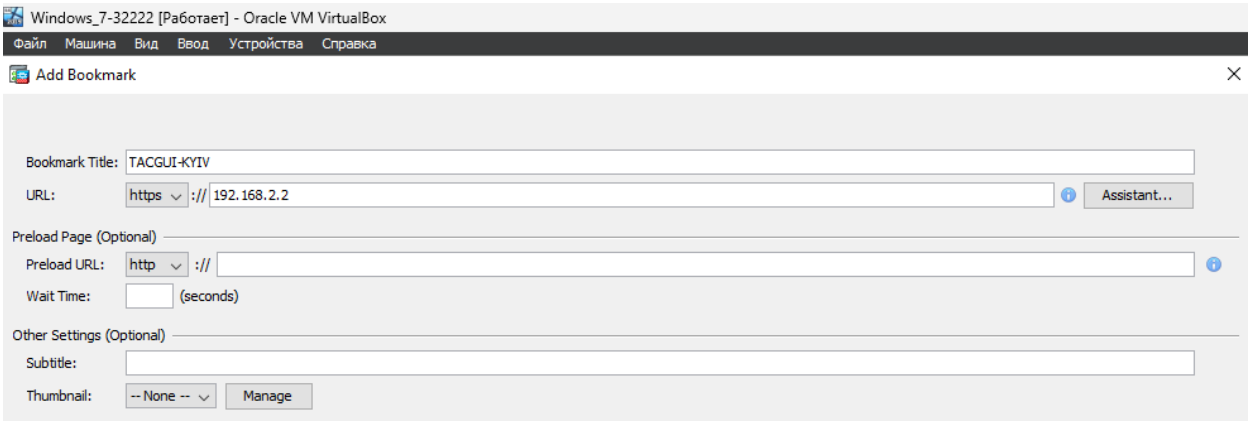


Рисунок 3.5. Налаштування швидкого доступу до внутрішнього ресурсу TACGUI-KYIV

Окрему увагу було приділено параметрам безпеки каналу передачі даних. Для захисту трафіку, що проходить через публічну мережу Інтернет, було активовано протоколи шифрування SSL/TLS та налаштовано механізми перевірки цифрових сертифікатів. Це гарантує конфіденційність сесії та захист від атак типу «людина посередині». Конфігурацію криптографічних параметрів наведено на рис. 3.6.

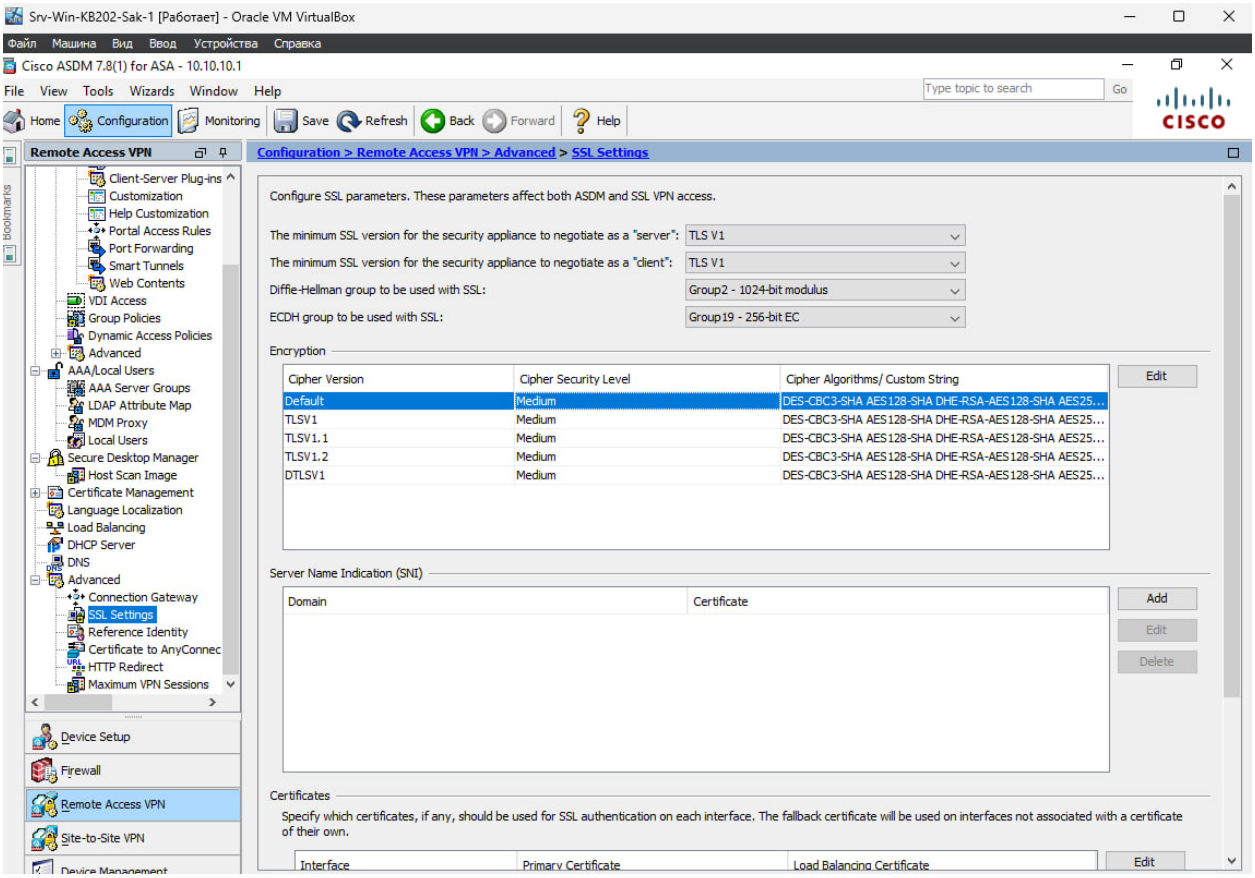


Рисунок 3.6. Параметри криптографічного захисту з'єднання SSL VPN

Завершальним етапом стала комплексна перевірка всіх внесених налаштувань на предмет коректності та відсутності конфліктів. Після верифікації параметрів зміни було активовано в поточній сесії функцією «Apply» та записано в енергонезалежну пам'ять пристрою командою «Save Configuration» для збереження після перезавантаження. У результаті проведених робіт було успішно розгорнуто функціональну систему SSL VPN, що забезпечує надійний та зручний доступ до корпоративної мережі через веб-інтерфейс.

3.2 Комплексне тестування та діагностика налаштованих сервісів

У рамках даного етапу роботи було проведено всебічну перевірку працездатності сконфігурованого протоколу Clientless SSL VPN на базі платформи Cisco ASA, а також протестовано функціональність сервера реєстрації подій Kiwi Syslog Server. Основною метою впровадженого VPN-рішення є надання користувачам, що знаходяться за межами захищеного корпоративного периметра, можливості безпечно взаємодіяти з внутрішніми інформаційними ресурсами, використовуючи для цього стандартний веб-браузер без необхідності встановлення спеціалізованого клієнтського програмного забезпечення.

Процедура верифікації охоплювала широкий спектр параметрів. Зокрема, було перевірено валідність та коректність роботи цифрових сертифікатів, що є критичним для встановлення довірених з'єднань. Також детально проаналізовано застосовані політики доступу (ACL) та налаштування криптографічних алгоритмів шифрування трафіку. Окремим пунктом тестування стала перевірка стабільності та безперервності сесій при підключенні з різнорідних клієнтських пристроїв та через різні типи зовнішніх мереж.

Особливий акцент під час тестування було зроблено на ергономіці та функціональності веб-інтерфейсу порталу Cisco ASA. Для оптимізації роботи користувачів було створено та перевірено систему закладок (bookmarks), які забезпечують швидку навігацію до внутрішніх веб-сервісів, зокрема до адміністративної панелі сервера TACACS. Такий підхід значно спрощує взаємодію персоналу з інфраструктурою.

Результати проведених випробувань підтвердили, що конфігурація Clientless SSL VPN функціонує коректно та стабільно, гарантуючи високий рівень захищеності каналу. Успішну ініціалізацію сесії та вхід до сервісу

львівської філії продемонстровано на рис. 3.7, а аналогічний процес для київського сегмента мережі наведено на рис. 3.8.

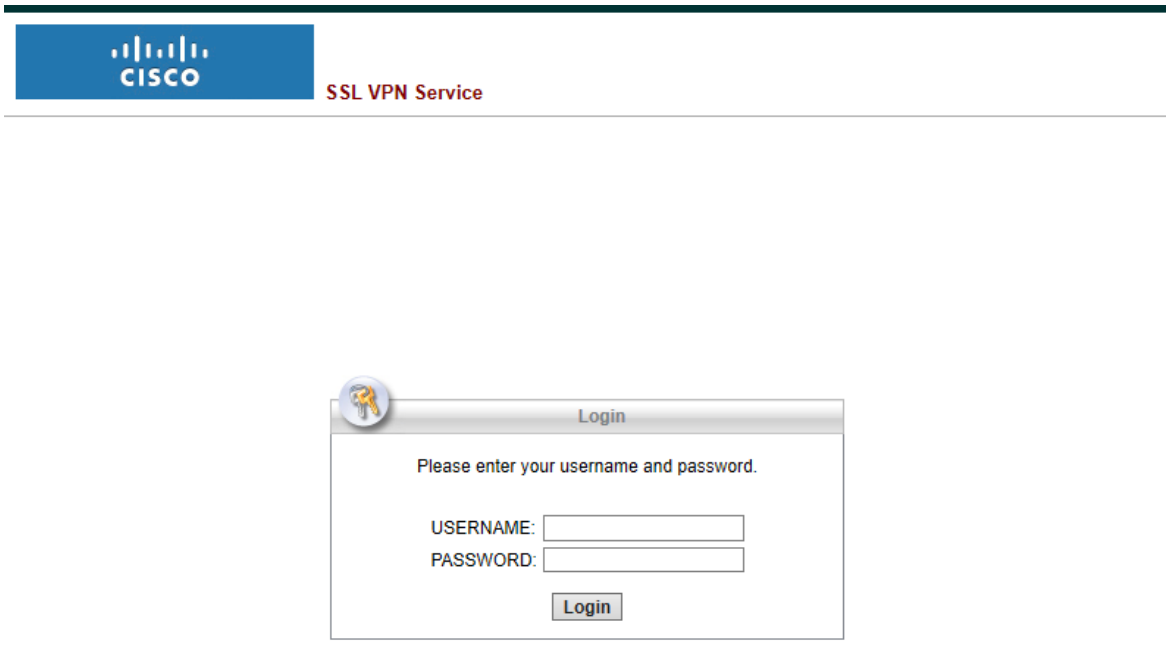


Рисунок 3.7. Візуалізація успішного встановлення з’єднання з сервісом SSL VPN (філія Львів).

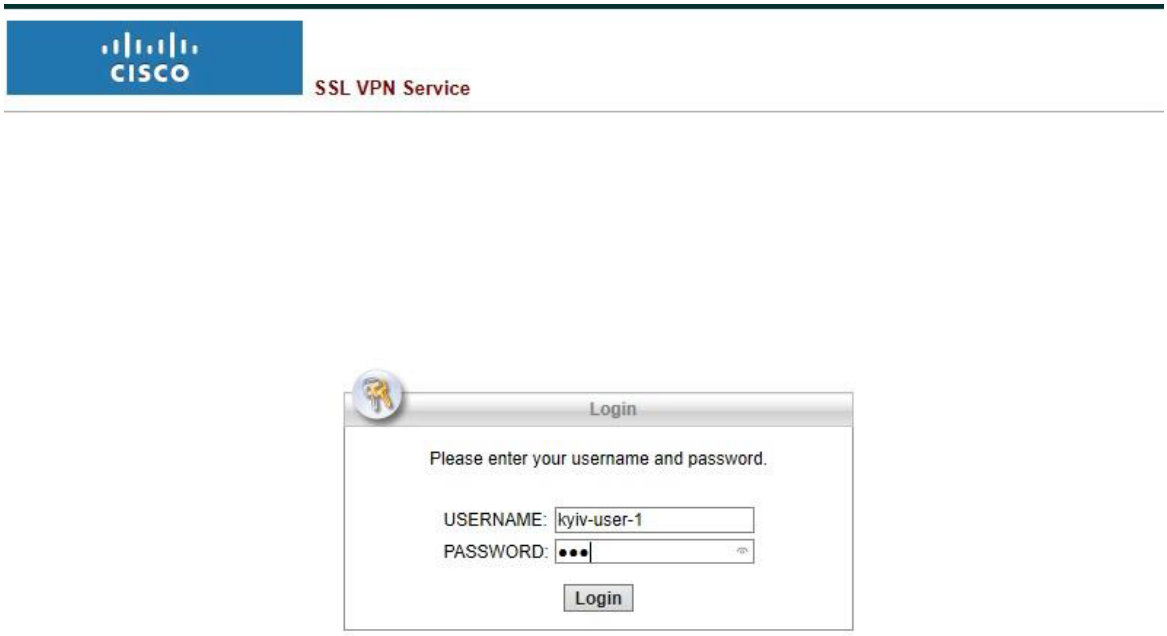


Рисунок 3.8. Візуалізація успішного встановлення з’єднання з сервісом SSL VPN (філія Київ).

Вигляд користувацького веб-інтерфейсу з активним посиланням для доступу до ресурсів сервера TACACS у львівській філії показано на рис. 3.9, тоді як інтерфейс для київського підрозділу відображено на рис. 3.10.

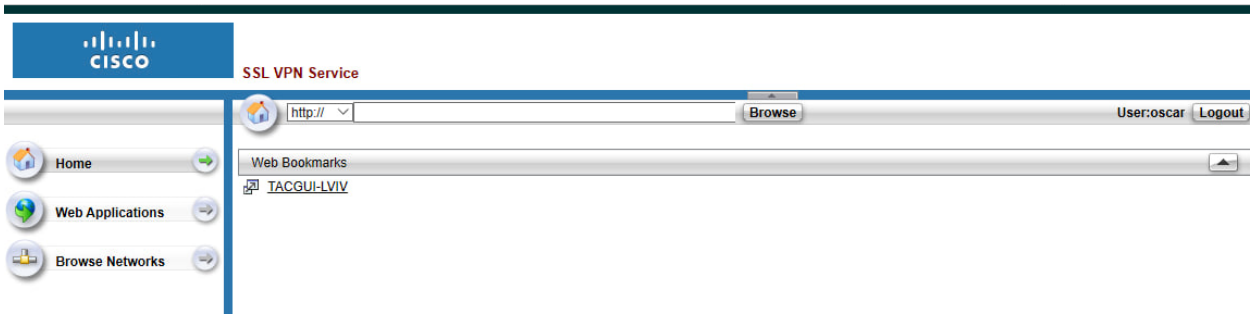


Рисунок. 3.9. Інтерфейс користувача SSL VPN порталу з інтегрованим посиланням на сервер TACACS (Львів).

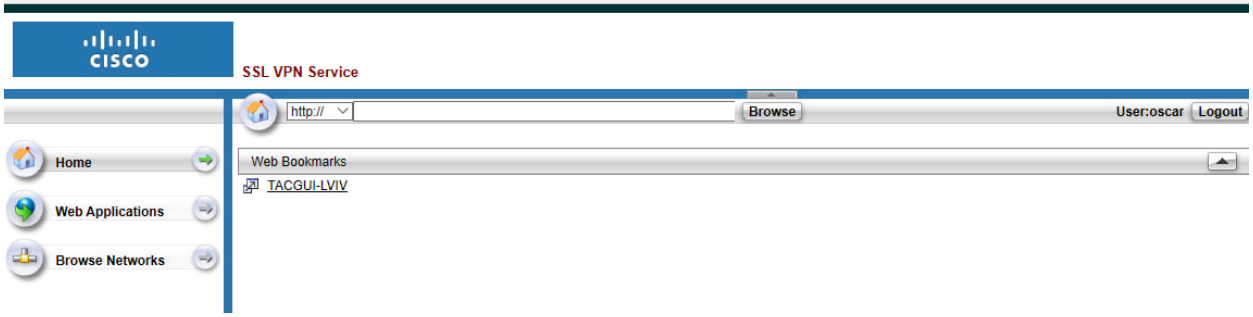


Рисунок 3.10. Інтерфейс користувача SSL VPN порталу з інтегрованим посиланням на сервер TACACS (Київ).

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне науково-прикладне завдання щодо розробки комплексної системи мережевої безпеки, яка базується на використанні міжмережевого екрана Cisco ASA для організації захищеного віддаленого доступу за технологією SSL VPN.

Основні результати роботи полягають у наступному:

1. Проведено глибокий аналіз еволюції протоколів безпеки від SSL 1.0 до сучасного стандарту TLS 1.3 . Визначено, що використання застарілих версій створює критичні вразливості, тому система була спроєктована з урахуванням сучасних криптографічних вимог.

2. Досліджено концептуальні засади функціонування VPN та механізми тунелювання. Обґрунтовано переваги SSL VPN для забезпечення легкого доступу через веб-браузер без попереднього встановлення клієнтського ПЗ.

3. Розроблено архітектуру комплексної системи захисту на базі Cisco ASA, яка поєднує функції міжмережевого екрана, VPN-концентратора та системи запобігання вторгненням. Це дозволило створити ешелонований захист периметра мережі.

4. Спроєктовано та впроваджено логічну структуру мережі з поділом на зони безпеки для філій у Києві та Львові . Розроблена схема IP-адресації забезпечила коректну маршрутизацію та уникнення конфліктів адрес.

5. Реалізовано практичне налаштування сервісу SSL VPN за допомогою інструменту Cisco ASDM . Створено профілі підключення, налаштовано портал користувача, систему закладок для швидкого доступу до внутрішніх ресурсів та визначено політики групового доступу.

6. Забезпечено інтеграцію системи з сервером TACACS+ для централізованої аутентифікації адміністраторів та користувачів, що дозволило

реалізувати гранулярний контроль доступу та підвищити рівень керованості інфраструктури .

7. Проведено фінальну верифікацію та тестування системи . Результати перевірки підтвердили стабільність встановлених SSL-тунелів, коректність роботи сертифікатів та успішний доступ до захищених ресурсів через веб-портал, що свідчить про повну готовність системи до промислової експлуатації.

Розроблена система створює надійну основу для безпечної віддаленої роботи персоналу, забезпечуючи конфіденційність корпоративних даних та відповідність сучасним стандартам кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Internet Engineering Task Force, RFC 8446, pp. 1-160, Aug. 2018. https://doi.org/10.17487/RFC8446.
2. T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force, RFC 5246, pp. 1-104, Aug. 2008. https://doi.org/10.17487/RFC5246.
3. T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1," Internet Engineering Task Force, RFC 4346, pp. 1-87, Apr. 2006. https://doi.org/10.17487/RFC4346.
4. K. Hamzeh et al., "Point-to-Point Tunneling Protocol (PPTP)," Internet Engineering Task Force, RFC 2637, pp. 1-57, Jul. 1999. https://doi.org/10.17487/RFC2637.
5. W. Townsley et al., "Layer Two Tunneling Protocol 'L2TP'," Internet Engineering Task Force, RFC 2661, pp. 1-80, Aug. 1999. https://doi.org/10.17487/RFC2661.
6. O. Santos, "Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services," Cisco Press, 3rd ed., pp. 50-120, 2014.
7. J. Snader, "VPNs Illustrated: Tunnels, VPNs, and IPsec," Addison-Wesley Professional, vol. 1, no. 1, pp. 15-45, 2005.
8. W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson, 7th ed., pp. 450-490, 2016.
9. D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Engineering Task Force, RFC 5280, pp. 1-151, May 2008. https://doi.org/10.17487/RFC5280.
10. S. Kent and K. Seo, "Security Architecture for the Internet Protocol," Internet Engineering Task Force, RFC 4301, pp. 1-101, Dec. 2005. https://doi.org/10.17487/RFC4301.

11. I. Ristic, "Bulletproof SSL and TLS," Feisty Duck, vol. 1, pp. 20-55, 2017.

12. T. Dahm, A. Ota, and D. Medway Gash, "The TACACS+ Protocol," Internet Engineering Task Force, RFC 8907, pp. 1-45, Sep. 2020. https://doi.org/10.17487/RFC8907.

13. H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Internet Engineering Task Force, RFC 2104, pp. 1-11, Feb. 1997. https://doi.org/10.17487/RFC2104.

14. N. Ferguson, B. Schneier, and T. Kohno, "Cryptography Engineering: Design Principles and Practical Applications," Wiley, vol. 1, pp. 67-85, 2010.

15. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978. https://doi.org/10.1145/359340.359342.

16. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976. https://doi.org/10.1109/TIT.1976.1055638.

17. "IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges," IEEE Std 802.1D-2004, pp. 1-281, 2004. https://doi.org/10.1109/IEEESTD.2004.94575.

18. B. Moller, T. Duong, and K. Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback," Google Security Team, Whitepaper, pp. 1-8, 2014.

19. R. Stewart, "Cisco ASA Security Appliance Hands-On Training for Accidental Administrators," Soundtraining.net, pp. 30-65, 2016.

20. M. Feilner, "OpenVPN: Building and Integrating Virtual Private Networks," Packt Publishing, pp. 10-40, 2006.

21. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," *FIPS PUB 197*, pp. 1-51, 2001

22. C. Allen and T. Dierks, "The TLS Protocol Version 1.0," *Internet Engineering Task Force*, RFC 2246, pp. 1-80, Jan. 1999. https://doi.org/10.17487/RFC2246.

23. Electronic Frontier Foundation, "Encrypted Web Traffic: The Case for Transport Layer Security," *EFF Whitepaper*, 2019. https://www.eff.org/encrypt-the-web.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)