

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеного мережного обміну на базі
протоколу SSL VPN»

Виконав студент 4-го курсу групи КІ-19-1
спеціальності 123 «Комп'ютерна інженерія»

 Галонза Дмитро

Керівник старший викладач кафедри КІ та КБ

 Руслан Петросян

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

 Юрій Бродський

Житомир – 2023

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Галонза Дмитро Володимирович

Тема роботи: «Проект захищеного мережного обміну на базі протоколу SSL VPN»

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 20 червня 2023 р.

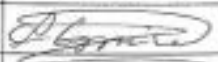
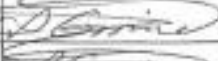
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Віртуальні приватні мережі, процес забезпечення безпечної передачі даних у комп'ютерних мережах на базі протоколу SSL VPN.

Обладнання та програмне забезпечення:

1. мережевий симулятор GNS3, VMWare
2. операційна система Windows 10
3. маршрутизатори Cisco c7200, 3725, мережевий екран ASA v 9.8.1

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 1.03.23	 1.03.23
2	Єфіменко А.А.	 1.03.23	 1.03.23
3	Єфіменко А.А.	 1.03.23	 1.03.23

Студент  Дмитро Галонза

Керівник  Руслан Петросян

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.03.2023 – 01.04.2023	
2	Написання вступної частини кваліфікаційної роботи	01.04.2023 – 03.04.2023	
3	Аналіз основних теоретичних відомостей SSL/TLS	03.04.2023 – 11.04.2023	
4	Проектування мережі	11.04.2023 – 18.04.2023	
5	Вибір обладнання та технологій	18.04.2023 – 24.04.2023	
6	Налаштування мережі в GNS3	24.04.2023 – 01.05.2023	
7	Налаштування SSL VPN на ASA	01.04.2023 – 08.05.2023	
8	Написання висновків	16.05.2023 – 20.05.2023	
9	Оформлення кваліфікаційної роботи	20.05.2023 – 25.05.2023	
10	Підготовка презентації до захисту	25.05.2023 – 02.06.2023	

Студент  Дмитро Галонза

Керівник  Руслан Петросян

		Галонза Д. В.		
		Петросян Р. В.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 123 – 02 – ПЗ

Арк.

6

АНОТАЦІЯ

Пояснювальна записка містить: 72 сторінки текстової частини, 34 рисунка, 2 таблиці та 31 джерело.

Метою роботи є проектування мережі на базі SSL VPN з використанням пристрою Cisco ASA.

В даній роботі було обґрунтовано вибір Cisco ASA для реалізації SSL VPN. Розглянуто різні підходи та технології для реалізації SSL VPN і визначено найкращий підхід для даного проекту. Наведено докладний огляд функціональності та можливостей пристрою Cisco ASA, зокрема функції мережевого брандмауера, підтримки VPN, IDS/IPS та інших функцій безпеки. В практичній частині презентовано реалізацію мережі на емуляторі GNS3 та наведено результати тестування Remote Access SSL VPN.

Ключові слова: ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, ТУНЕЛЮВАННЯ, SSL VPN, CISCO ASA, МЕРЕЖЕВИЙ БРАНДМАУЕР, БЕЗПЕКА МЕРЕЖІ, ТЕХНОЛОГІЯ ВІДДАЛЕНОГО ДОСТУПУ

					KIK.KP.B – 123 – 02 – ПЗ			
Зам. З	Арх. Ар	№ докум. №	Підпис/Підп	Дата	Проект захищеного мережного обміну на базі протоколу SSL VPN	Літ.	Арк.	Аркуші
Розроб.	Галонга Д. В.			20.06.23				
Керівник	Петроски Р. В.			20.06.23			4	72
Реценз.	Бродський Ю. Б.			20.06.23		ФІКТ, Гр. КІ-19-1		
Н. контр.	Петроски Р. В.							
Затверд.	Єфіменко А. А.			20.06.23				

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ANNOTATION

The explanatory note contains: 72 pages of text, 34 figures, 2 tables and 31 sources.

The purpose of the work is to design a network based on SSL VPN using a Cisco ASA device.

This paper justifies the choice of Cisco ASA for implementing SSL VPN. Different approaches and technologies for implementing SSL VPN are considered and the best approach for this project is determined. A detailed overview of the functionality and capabilities of the Cisco ASA device is provided, including network firewall, VPN support, IDS/IPS, and other security features. In the practical part, the article presents the implementation of the network on the GNS3 emulator and the results of testing Remote Access SSL VPN.

Keywords: VIRTUAL PRIVATE NETWORKS, TUNNELLING, SSL VPN, CISCO ASA, NETWORK FIREWALL, NETWORK SECURITY, REMOTE ACCESS TECHNOLOGY

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	12
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ.....	13
1.1 Особливості SSL VPN	13
1.2 Огляд стандартів безпеки і криптографічних алгоритмів	15
1.3 Інфраструктура відкритого ключа	20
1.4 Встановлення TLS Handshake.....	26
Висновки до першого розділу	32
РОЗДІЛ 2 ПРОЄКТУВАННЯ МЕРЕЖІ НА БАЗІ SSL VPN	33
2.1 Вибір засобів реалізації SSL VPN	33
2.2 Проєктування моделей та схем адресацій.....	37
2.3 Вибір обладнання.....	39
Висновки до другого розділу.....	42
РОЗДІЛ 3 НАЛАШТУВАННЯ SSL VPN У СИМУЛЯТОРІ GNS3	43
3.1 Базове налаштування пристроїв.....	43
3.2 Налаштування віддаленого доступу AnyConnect SSL VPN за допомогою ASDM	46
3.3 Підключення до AnyConnect SSL VPN	51
Висновки до третього розділу	55
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	58
ДОДАТКИ.....	61

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

ASA – Adaptive Security Appliance

ASDM – Adaptive Security Device Manager

ACL – Access Control List

OSI – Open System Interconnection

OSPF – Open Shortest Path First

PKI – Public Key Infrastructure

HMAC – Hash-based message authentication code

SSL – Secure Sockets Layer

TLS – Transport Layer Security

IPsec – Internet Protocol Security

CRL – Certificate Revocation List

CA – Certificate Authority

OCSP – Online Certificate Status Protocol

SHA – Secure Hash Algorithm

RSA – Rivest-Shamir-Adleman

DSA – Digital Signature Algorithm

AES – Advanced Encryption Standard

DH – Diffie-Hellman

MD5 – Message Digest Algorithm 5

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В сучасному світі, де інформаційні технології стають все більш важливими для бізнесу та громадян, захист інформації є однією з найважливіших задач. Під час передачі даних через мережу існує ризик їх зловживання, крадіжки або пошкодження. Щоб уникнути таких ситуацій, необхідно використовувати захищені технології передачі даних.

Однією з таких технологій є SSL VPN - технологія, що дозволяє створювати захищені тунелі для передачі даних через відкриті мережі. SSLVPN забезпечує високий рівень безпеки, дозволяє забезпечити доступ до корпоративних ресурсів з будь-якої точки світу та зменшує витрати на інформаційну інфраструктуру.

Метою кваліфікаційної роботи є дослідження можливостей використання SSLVPN для побудови захищеної мережі, а також практичне впровадження і налагодження SSLVPN в роботу корпоративної мережі. У процесі дослідження будуть розглянуті особливості технології SSLVPN, порівняння з іншими VPN-технологіями, вибір обладнання та налаштування сертифікатів SSL. Також будуть проведені тестування та оцінка ефективності захищеної мережі на базі SSLVPN.

Об'єктом дослідження є віртуальні приватні мережі.

Предметом дослідження є забезпечення безпечної передачі даних у мережі за допомогою технології SSLVPN.

Отже, тема "Побудова захищеної мережі на базі SSLVPN" є важливою та актуальною, оскільки захист інформації є однією з найважливіших задач для бізнесу та громадян. SSLVPN є ефективним та надійним інструментом для захисту даних під час їх передачі через відкриті мережі та забезпечує зручний доступ до корпоративних ресурсів.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Особливості SSL VPN

Два основні типи тунелів, які використовуються в VPN, це тунель віддаленого доступу (Remote Access) і тунель між мережами (Site-to-Site).

Remote Access VPN застосовується, за необхідності забезпечити створення захищеного каналу між співробітником та корпоративною мережею. Для цього користувачу потрібне інтернет-з'єднання та наявність відповідного програмного забезпечення, після чого комп'ютер самостійно побудує даний тунель до маршрутизатора компанії.

Site-to-Site VPN – тунель між віддаленими мережами, наприклад, філії з центральним офісом. Побудову тунелю виконує сам граничний маршрутизатор. Він будує віддалене з'єднання між маршрутизаторами, які об'єднуються в одну мережу, відтак, співробітник без спеціалізованого ПЗ працює у локальній мережі офісу.

SSL VPN належить до групи Remote Access VPN з'єднань, і дає змогу індивідуальним віддаленим співробітникам з будь-якої точки планети здійснювати під'єднання до корпоративної мережі, використовуючи персональний комп'ютер або смартфон. Однак, на відміну від IPSec, SSL VPN всередині працює за зовсім іншим принципом і крім повнотунельного режиму, має два додаткові - Clientless і Thin Client.

Clientless (безклієнтський) SSL VPN - безклієнтська VPN на основі браузера, яка дозволяє користувачам створювати безпечний віддалений доступ VPN-тунель до граничного пристрою і використовувати веб-браузер та вбудований SSL для захисту VPN-трафіку. Після автентифікації користувачі потрапляють на сторінку порталу і можуть отримати доступ до певних, заздалегідь визначених внутрішніх ресурсів з порталу[28].

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Thin Client SSL VPN - це технологія, яка дозволяє встановлювати безпечне з'єднання між клієнтським пристроєм і центральним VPN-сервером за допомогою SSL протоколу. У випадку Thin Client клієнтський пристрій використовується в якості "тонкого" клієнта, що означає, що на ньому не потрібно встановлювати спеціальне VPN-клієнтське програмне забезпечення.

Client-Based SSL VPN - це VPN, яка забезпечує повне тунельне SSL VPN-з'єднання, але вимагає встановлення клієнтської програми VPN на віддаленому хості. Після автентифікації користувачі можуть отримати доступ до будь-якого внутрішнього ресурсу так, ніби вони фізично знаходяться в локальній мережі.

Найбільшим переконливим аргументом на користь використання SSL є той факт, що він використовує, практично у всіх випадках, відкритий порт 443 для підключення, тоді як для використання IPSec необхідно використовувати порти 500 і 4500.

Деякі провайдери блокують підключення на 500 і 4500 порти з метою заборони використання VPN. Йдеться про блокування VPN трафіку саме на стороні провайдера, до якого підключений віддалений користувач. Таке може спостерігатися в публічних місцях, наприклад у Wi-Fi мережах інтернет-кафе або аеропортів.

На відміну від портів IPsec, 443-тий порт відкритий практично завжди. Ані провайдер, ані громадський заклад не можуть закрити цей порт, оскільки більшість сайтів в Інтернеті використовують саме його. Закрити 443 порт означало б заборонити доступ до перегляду веб-сторінок як до такого, і такий доступ в Інтернет не мав би сенсу. SSL VPN використовує 443 порт, що робить його більш універсальним порівняно з IPsec, адже обмеження деяких провайдерів на застосування IPsec більше не є проблемою для віддаленого співробітника, який використовує SSL VPN.

Для Clientless реалізації користувачеві не потрібно встановлювати VPN клієнт, і це є наступною перевагою SSL VPN. Користувач може отримувати

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

доступ до загальних папок, пошти, ftp-сервера та інших мережеслужб безпосередньо через браузер публічного комп'ютера з інтернет-кафе, або з гостьового комп'ютера, без необхідності встановлення VPN клієнта. Якщо у мережі дві тисячі користувачів, і більшій частині з них достатньо доступу до пошти, спільної папки або ftp-сервера, то не доведеться встановлювати VPN-клієнт на кожен з комп'ютерів, адже процес встановлення, оновлення, налаштування та керування всіма клієнтами може бути дуже тривалим і ресурсовитратним. Достатньо роздати логін/пароль і DNS ім'я VPN шлюзу, після чого користувачі використовуватимуть браузер для підключення до Clientless VPN.

Третя перевага SSL VPN - це підвищена безпека. Якщо користувачеві потрібно попрацювати тільки з поштою, загальною папкою, або тільки з конкретними застосунками, то зовсім необов'язково надавати повний доступ через Full Tunnel підключення. Ми можемо використовувати Clientless режим для загальної папки і пошти, а також Thin Client режим для роботи з портами конкретного застосунку.

У зв'язку зі значним зростанням роботи з дому, SSL-мережі VPN стали надзвичайно важливими в сучасному світі. Десятки мільйонів людей тепер працюють зі своїх домівок і користуються своїми особистими інтернет-з'єднаннями для забезпечення доступу до корпоративних ресурсів. Ця зміна вимагає надійних і безпечних засобів зв'язку, які забезпечують шифрування даних і захист мережевого трафіку від несанкціонованого доступу. Тому SSL-мережі VPN є життєво важливими для забезпечення безпеки та приватності в робочому середовищі, незалежно від місцезнаходження працівника.

1.2 Огляд стандартів безпеки і криптографічних алгоритмів

В сучасному цифровому світі безпека є одним з найважливіших аспектів, особливо в контексті обробки та передачі конфіденційної інформації. Захист даних від несанкціонованого доступу та зловживань стає все більш актуальним

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

завданням для організацій, користувачів та розробників програмного забезпечення. Один з основних інструментів, використовуваних для забезпечення безпеки, є стандарти безпеки та криптографічні алгоритми. Ці стандарти та алгоритми визначають набір правил, протоколів та методів, які дозволяють забезпечити конфіденційність, цілісність та доступність інформації.

Для забезпечення конфіденційності даних використовується шифрування, що захищає інформацію від перехоплення та прослуховування. Для забезпечення цілісності даних застосовується хешування, що перевіряє, чи були дані змінені під час передачі. Аутентифікація здійснюється за допомогою РКІ, що підтверджує автентичність сторін, які здійснюють обмін даними.

Хешування є процесом перетворення даних фіксованої довжини вхідного повідомлення на хеш-код. Хеш-функція виконує цю операцію шляхом застосування певного алгоритму, який обчислює унікальне значення для кожного вхідного повідомлення. Основна ідея хешування полягає в тому, що навіть незначні зміни вхідних даних повинні призводити до значних змін у хеш-значенні. Це робить його корисним інструментом для перевірки цілісності даних та виявлення змін або помилок в повідомленнях.

SSL/TLS не використовує хешування на пряму для захисту даних під час передачі, для цього використовується HMAC. HMAC використовує хеш-функцію та секретний ключ для обчислення аутентифікаційного коду для повідомлення. HMAC - це алгоритм аутентифікації повідомлення на основі хеш-функцій. Він використовується для перевірки цілісності та автентичності повідомлення, забезпечуючи механізм перевірки, що повідомлення не було змінено під час передачі.

Шифрування - це процес перетворення звичайного тексту (відомого як відкритий текст) у незрозумілий формат (шифротекст) за допомогою певних

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

алгоритмів та ключів. Шифрування забезпечує конфіденційність та захист від несанкціонованого доступу до інформації.

У криптографії використовуються два основних типи шифрування: симетричне і асиметричне.

1. У симетричному шифруванні використовується один і той самий ключ для шифрування, так і розшифрування повідомлення. Відправник та отримувач повинні мати однаковий секретний ключ. Симетричне шифрування є швидким та ефективним, але вимагає безпечного обміну ключем між сторонами.
2. У асиметричному шифруванні використовується пара ключів - приватний і публічний. Приватний ключ відомий тільки власнику, тоді як публічний ключ розповсюджується загальнодоступно. Повідомлення, зашифроване публічним ключем, може бути розшифроване тільки за допомогою відповідного приватного ключа, а повідомлення, підписане приватним ключем, може бути перевірене за допомогою публічного ключа. Розповсюдження публічного ключа відбувається безпечними каналами, а приватний ключ зберігається в таємниці.

Асиметричне шифрування відоме своїми обмеженнями в роботі з великими обсягами даних та вимогами до розміру ключів. Воно використовується для безпечного обміну ключами та забезпечення безпечних комунікацій, оскільки закритий ключ ніколи не надається у спільне користування, що забезпечує високий рівень безпеки. З іншого боку, симетричне шифрування є ефективним при роботі з великими обсягами даних, оскільки воно швидше та має нижчі витрати процесора. Однак, його слабкістю є потреба у спільному секретному ключі, що зменшує безпеку. У кінцевому рахунку, обидва підходи до шифрування мають свої переваги та обмеження, і вони використовуються в залежності від конкретних потреб та контексту безпеки системи.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Набори шифрів (cipher suites) в TLS використовуються для забезпечення безпеки під час з'єднання між клієнтом і сервером. Залежно від версії TLS, набір включає в себе декілька компонентів, серед яких:

1. Обмін ключами використовується для обміну секретними ключами між клієнтом і сервером. Наприклад, це може бути RSA, DH, DHE, ECDH, ECHE, PSK.
2. Шифрування використовується для захисту конфіденційності даних під час передачі. Це може бути наприклад CHACHA20, AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-128-CBC, 3DES-CBC, RC4-128, DES-CBC.
3. Аутентифікація використовується для перевірки справжності сервера перед початком з'єднання. Серед наявних існує наступний вибір: ECDSA, RSA, DSS, PSK.
4. Хешування використовується для забезпечення цілісності даних та перевірки цілісності повідомлень. Деякі приклади алгоритмів хешування, що можуть використовуватися, включають Poly1305, SHA384, SHA256, SHA та MD5.

Комбінація цих компонентів утворює шифровий набір, який використовується для встановлення захищеного з'єднання TLS між клієнтом і сервером. Під час встановлення з'єднання TLS, клієнт і сервер обмінюються підтримуваними наборами шифрів і вибирають найбільш придатний спосіб забезпечення безпеки для їх з'єднання.



Рисунок 1.1 – Набір шифрування для версії TLS 1.2 та менше[7]

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

TLS 1.3 розділяє ці функції на 3 ортогональні варіанти:



Рисунок 1.2 – Набір шифрування для версії TLS 1.3[7]

В цілому, розділення цих функцій на ортогональні варіанти у TLS 1.3 покращує безпеку, забезпечує надійну конфіденційність, цілісність та аутентифікацію даних, що робить його більш ефективним і захищеним протоколом для забезпечення безпеки з'єднання. Крім того, це дозволяє використовувати меншу кількість шифрувальних наборів, оскільки вибір здійснюється окремо для кожної функції. TLS 1.3 використовує сучасні алгоритми шифрування. У TLS 1.3 доступно всього лише п'ять наборів шифрування: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_CCM_SHA256, TLS_AES_128_CCM_8_SHA256.

Всі шифри, що підтримуються в TLS 1.3, є AEAD. AEAD (Authenticated Encryption with Associated Data) шифри - це криптографічні алгоритми, які надають одночасну аутентифікацію та шифрування даних, включаючи додаткові дані. У традиційних шифрах аутентифікація та шифрування можуть бути виконані окремо, що може створювати потенційні ризики безпеки. AEAD шифри вирішують цю проблему, забезпечуючи цілісність, конфіденційність та аутентичність даних в одному процесі.

TLS 1.3 включає лише шифри, які підтримують "forward secrecy". Forward secrecy (пряма секретність) - це властивість криптографічної системи, що забезпечує захист раніше переданих повідомлень, навіть якщо в довгостроковому ключі або секреті станеться компрометація у майбутньому. У контексті протоколів забезпечення безпеки, таких як TLS, forward secrecy

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

означає, що при компрометації приватного ключа сервера в майбутньому, зловмисник не зможе розшифрувати раніше зашифровану комунікацію.

У контексті алгоритму DHE "ephemeral" вказує на використання тимчасових або короткочасних ключів для процесу обміну ключами. Неефемерний означає, що параметри DH є статичними - записані у файлах та не рекомендується використовувати. DHE - це варіант, в якому як клієнт, так і сервер генерують новий набір публічних та приватних ключів для кожного сеансу або з'єднання. Використання ефемерних ключів в алгоритмі DH забезпечує forward secrecy. TLS 1.3 використовує протокол обміну ключами на основі ECDHE, що дозволяє створювати унікальний ключ для кожного з'єднання.

Було розглянуто актуальні криптографічні алгоритми, що забезпечують захист трафіку та конфіденційність даних. Розуміння цих стандартів і алгоритмів є ключовим для ефективної реалізації безпечного SSL VPN з високим рівнем захисту.

1.3 Інфраструктура відкритого ключа

Public Key Infrastructure (PKI) - це система, що складається з трьох основних компонентів: клієнта, сервера та центра сертифікації (CA)[15].

- Клієнт - це сутність або особа, яка використовує криптографічні послуги PKI. Клієнти можуть бути користувачами, комп'ютерами, пристроями або програмами, що здійснюють доступ до ресурсів мережі. Клієнти використовують криптографічні ключі для шифрування, розшифрування, цифрового підпису та інших операцій забезпечення безпеки.
- Сервер - це сутність, яка надає ресурси або послуги в мережі. Вони можуть бути веб-серверами, файловими серверами, поштовими серверами тощо. Сервери також використовують криптографічні ключі для захисту комунікації з клієнтами та інших безпечних операцій.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

- Центр сертифікації є довіреною стороною в PKI, яка видає цифрові сертифікати. Він підтверджує автентичність суб'єктів мережі і надає гарантію щодо використання правильних публічних ключів. СА видає сертифікати, які містять публічний ключ клієнта або сервера та іншу інформацію, таку як ім'я суб'єкта, дату видачі, термін дії тощо. СА також виконує функції управління ключами, відкликання сертифікатів та забезпечення довіреності системи.

PKI є потужним інструментом для забезпечення безпеки та аутентифікації в різних доменах, де необхідно перевірити ідентичність сторін та забезпечити захист від несанкціонованого доступу.

Центр сертифікації є наріжним каменем процесу TLS/SSL. Процес отримання сертифіката від СА включає кілька кроків:

1. СА володіє як відкритими, так і закритими ключами. Крім того, СА володіє власним сертифікатом, який може бути самопідписаним або підписаним іншим СА.
2. Сервер генерує відкритий і закритий ключі
3. Сервер генерує запит на підписання сертифіката (CSR). CSR містить відкритий ключ сервера та підписується приватним ключем сервера.
4. Сервер надсилає підписаний CSR до СА
5. СА перевіряє та підтверджує інформацію в CSR
6. СА створює сертифікат, використовуючи інформацію з CSR
7. СА підписує сертифікат, використовуючи особистий приватний ключ
8. СА надає сертифікат серверу
9. Після цього сервер може надати сертифікат для підтвердження своєї ідентичності клієнту.

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Загалом, CSR є файлом, який містить важливі дані про суб'єкта та його публічний ключ, і використовується для запиту на підпис сертифіката до СА. CSR або запит на підпис сертифіката складається з наступних елементів:

- Ім'я суб'єкта (Subject) - це інформація про особу або сутність, для якої ви хочете отримати сертифікат. Включає такі дані, як повне ім'я (Common Name), організацію (Organization), відділ (Organizational Unit), місцезнаходження (Locality), штат або провінцію (State/Province), країну (Country) тощо.
- CSR містить публічний ключ, який буде використовуватися для шифрування даних або підпису. Це ключ, який був згенерований разом із приватним ключем.
- CSR може також містити додаткові дані, такі як електронна пошта контактної особи, інформація про сервер або мережу, альтернативні імена (Subject Alternative Names), якщо це необхідно.
- Останнім елементом CSR є цифровий підпис, створений за допомогою приватного ключа. Це підтверджує, що дані в CSR не були змінені після їх підписання ідентифікатором.

Сертифікат складається з трьох розділів: дані сертифіката, алгоритм підпису та сам підпис.

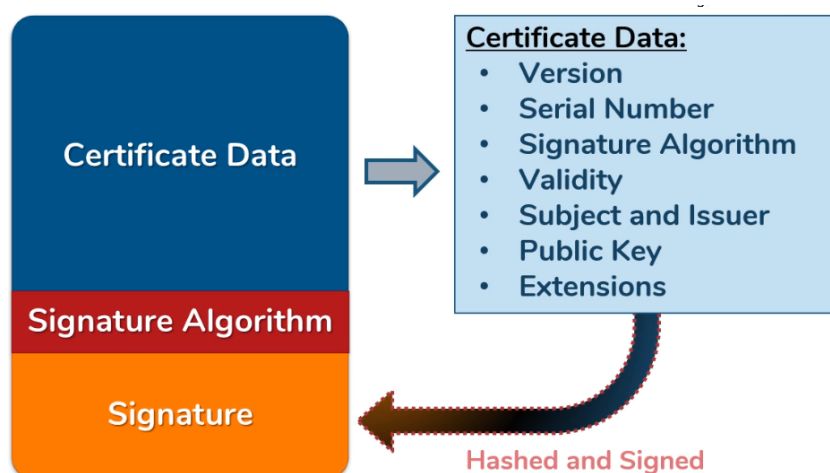


Рисунок 1.3 – Структура сертифіката x509[2]

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Версія специфікації x509[18]:

- Version: визначає версію специфікації x509, де версія 3 є типовою для сучасних сертифікатів та додає розширення сертифікатів.
- Serial Number: довжиною 20 байт, що унікально ідентифікує сертифікат та використовується для перевірки терміну дії сертифіката. Серійні номери можуть бути однаковими для різних центрів сертифікації. Використовується для перевірки валідності сертифіката.
- Signature Algorithm: алгоритм, який використовується для генерації підпису сертифіката та асиметричного шифрування за допомогою якого було згенеровано підпис.
- Validity: період часу, протягом якого сертифікат є дійсним, вказується двома значеннями: Not Before та Not After.
- Subject and Issuer: Subject, те що намагається ідентифікувати сертифікат. Issuer - центр сертифікації, який видав та підписав сертифікат. Центри сертифікації також мають сертифікати. Центри сертифікації випускають власні сертифікати, також відомі як само підписані сертифікати - поля subject та issuer ідентичні. Обидва поля вказані у форматі Distinguished Name. Атрибути, що використовуються в кожному DN, не визначені явно. Не обов'язково використовувати кожен атрибут. Найважливіша загальна назва (CN). CN може містити символ підстановки: * .
- Public Key: відкритий ключ
- Extensions: необов'язкові поля, які додають функції та обмеження до сертифікатів. Додано в x509 v3.

Кожного разу, коли клієнт отримує сертифікат від сервера, є два питання на які він повинен відповісти, щоб підтвердити дійсність сертифіката: Чи дійсний сертифікат? Чи є сервер справжнім власником сертифіката?

Перевірка дійсності сертифіката включає наступні кроки:

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

1. Центр сертифікації створює хеш даних сертифіката і шифрує його за допомогою свого приватного ключа. Цей підпис відомий як цифровий підпис СА.
2. Клієнт, перед тим як підключитися до сервера, вже має встановлений сертифікат СА. Він використовує відкритий ключ СА для розшифрування цифрового підпису.
3. Після розшифрування клієнт обчислює хеш даних сертифіката.
4. Якщо обчислений хеш збігається з отриманим розшифрованим підписом, це означає, що сертифікат не був змінений з моменту його створення СА. Це підтверджує дійсність сертифіката.
5. Після перевірки дійсності сертифіката, клієнт може також перевірити додаткові атрибути, такі як чи не закінчився термін дії сертифіката, чи не відкликано сертифікат.

Перевірка справжності сервера здійснюється за допомогою наступних методів, які гарантують, що клієнт спілкується зі справжнім власником сертифіката:

Перший спосіб - Клієнт-ініціатор:

1. Клієнт генерує випадкове значення.
2. Клієнт шифрує значення за допомогою відкритого ключа сервера
3. Сервер розшифровує за допомогою приватного ключа сервера, щоб отримати оригінальне значення.
4. Значення використовується для генерації сеансових ключів.

Другий спосіб - Сервер-ініціатор:

1. Під час рукописного сервер повинен відправити значення клієнту.
Це значення є відкритим ключем Діффі-Хеллмана.
2. Сервер підписує значення за допомогою приватного ключа сервера.
3. Клієнт перевіряє підпис за допомогою відкритого ключа сервера.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Значення використовуються для генерації сеансових ключів. У поєднанні з іншими значеннями, відомими лише клієнту та серверу.

Ці методи забезпечують взаємну перевірку та підтвердження справжності сертифіката сервера, що дозволяє клієнту впевнитись, що він спілкується з правильним сервером із запропонованого домену.

Відкликання сертифіката (Certificate Revocation) є важливим аспектом PKI, оскільки дозволяє відкликати дійсність сертифікату в разі виявлення проблем або загрози безпеці. Відкликання сертифіката означає, що сертифікат більше не вважається дійсним і не повинен використовуватися для автентифікації та шифрування комунікації.

Існує кілька причин, з яких сертифікат може бути відкликаним. Одна з найпоширеніших причин - це втрата приватного ключа, який використовується для підписування сертифіката. Якщо приватний ключ стає доступним несанкціонованим особам, це може призвести до зловживання іншою стороною, яка може використовувати сертифікат для підробки або підробленої комунікації. Інші причини відкликання сертифіката включають компрометацію приватного ключа, порушення політики безпеки, випадок, коли власник сертифіката більше не має право використовувати цей сертифікат (наприклад, після закінчення співробітництва або зміни ролі в організації), або зміна відомостей, що містяться в сертифікаті (наприклад, зміна даних про власника)[12].

Існує декілька способів перевірити, чи відкликано сертифікат: CRL та OSCP:

- CRL - це метод, який використовує список відкликаних сертифікатів (CRL), що публікується Центром сертифікації. CRL містить перелік сертифікатів, які втратили свою дійсність перед закінченням терміну дії. Клієнти можуть періодично завантажувати актуальну версію CRL і перевіряти, чи не знаходиться сертифікат в списку відкликаних.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

- OCSP - це протокол, який дозволяє клієнтам запитувати статус відкликання сертифікату без необхідності завантажувати весь CRL. Клієнт може відправити запит OCSP серверу, який відповість, чи є сертифікат відкликаним або дійсним.
- OCSP Stapling передбачає, що сервер самостійно запитує OCSP сервер про статус свого сертифіката і додає цю інформацію до відповіді сервера. Клієнт отримує статус сертифіката безпосередньо від сервера, що спрощує процес перевірки.

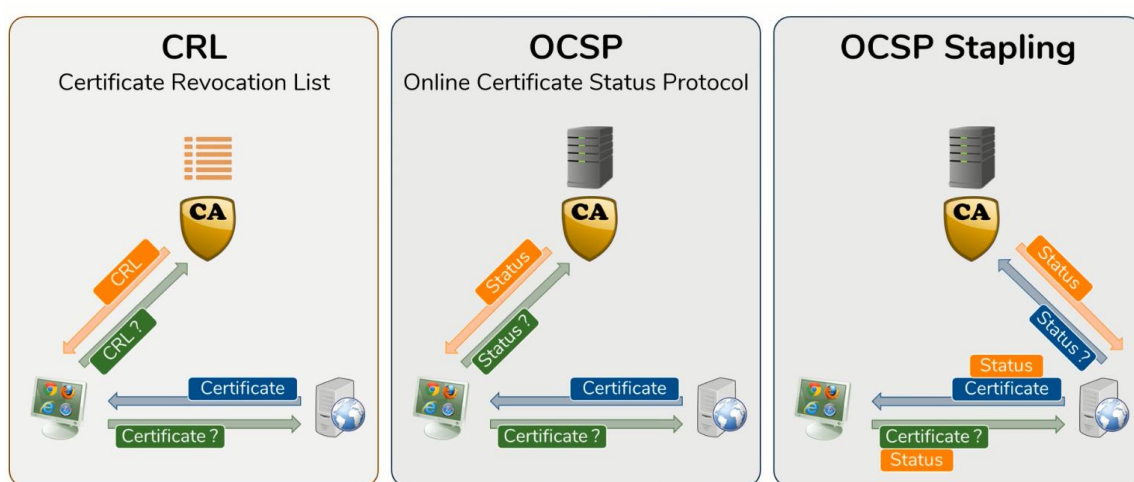


Рисунок 1.4 – Методи відкликання сертифікатів[4]

Кожен з цих методів має свої переваги і може бути використаний для відкликання сертифікатів залежно від потреб системи та доступних ресурсів.

1.4 Встановлення TLS Handshake

Кожна розмова в TLS/SSL складається з записів (records). Існує чотири типи записів: Handshake, Alert, Change Cipher Spec та Application Data. Записи типу Handshake і Alert поділяються на підтипи: Handshake - Client Hello, Handshake - Server Hello, Alert - Handshake failure та багато інших.

Кожен запис складається з Record Header, який включає в себе: Record Type, Version, Record Length. Після заголовку йде Record Payload.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

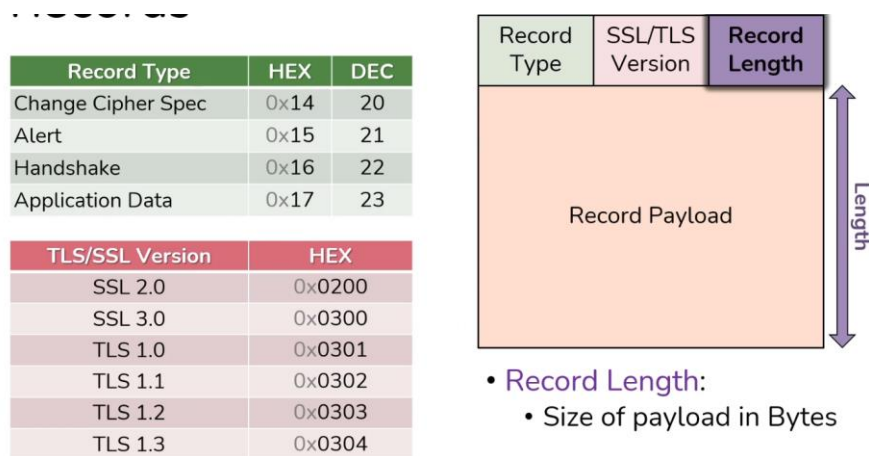


Рисунок 1.5 – Структура запису[4]

Change Cipher Spec вказує на те, що відправник має все необхідне для безпечного спілкування, тобто він знає, які набори шифрів будуть використовуватися, і вже розрахував сеансові ключі. Відправляється незалежно як клієнтом, так і сервером.

Alert використовується для надсилання повідомлень про помилки між клієнтом і сервером під час встановлення та забезпечення безпечного з'єднання. Повідомлення "alert" може бути надіслане в будь-який момент під час TLS-сесії і містить інформацію про певну помилку, яка сталася. Це можуть бути такі помилки, як недійсний сертифікат, непідтримуваний алгоритм шифрування, проблеми з аутентифікацією або інші помилки, які виникли під час обміну даними між сторонами.

Handshake використовується для встановлення безпечного з'єднання між клієнтом і сервером, а також для взаємної аутентифікації сторін і вирішення параметрів шифрування та ключів. Протокол рукостискання включає кілька етапів, які відбуваються між клієнтом і сервером для встановлення безпечного з'єднання. Класифікується на підтипи. Надсилаються незашифрованими, за винятком файлів сертифікатів певних підтипів.

Handshake Sub-Type	HEX	DEC	22	SSL/TLS Version	Record Length
Client Hello	0x01	1		Handshake Sub-Type	Sub-Type Length
Server Hello	0x02	2			
Certificate	0x0B	11	Handshake Sub-Type Payload		
Server Key Exchange	0x0C	12			
Server Hello Done	0x0E	14			
Client Key Exchange	0x10	16			
Finished	0x14	20			
(and many others)					

Рисунок 1.6 – Структура Handshake Record[4]

Після успішного виконання рукостискання і встановлення безпечного з'єднання, сторони можуть починати обмінюватися даними за допомогою записів "application data". Цей тип запису містить фактичні дані, які передаються між сторонами. В даному випадку на рис вказано AEAD шифр. AEAD надають як конфіденційність, так і цілісність даних. Вони шифрують дані, щоб забезпечити їх конфіденційність, і додатково додають аутентифікаційний тег, який дозволяє перевірити цілісність даних. Це дозволяє захистити дані від несанкціонованого доступу та змін.

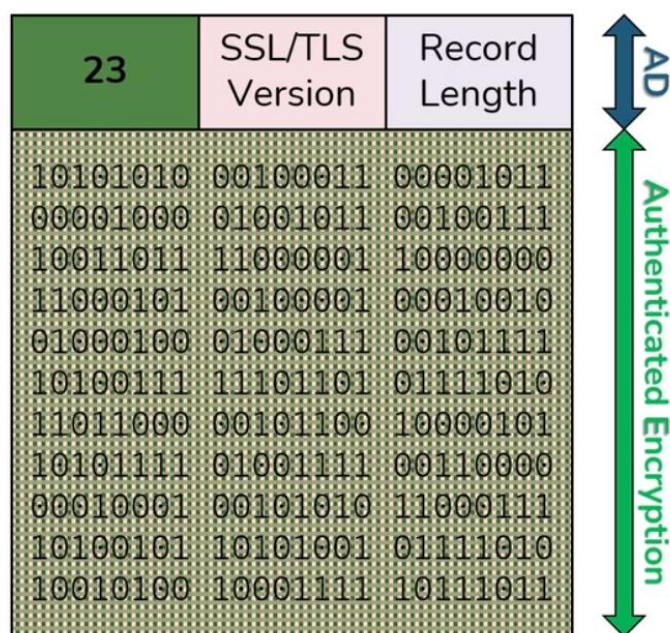


Рисунок 1.7 – Структура Application Data Record[4]

Побудова SSL/TLS тунелю в TLS 1.2 складається з наступних кроків[5]:

1. Клієнт ініціює з'єднання, надсилаючи серверу повідомлення "Client Hello". Воно містить версію TLS, список підтримуваних шифрів, випадкове число і параметри.
2. Сервер обирає найбільш підходящий шифр зі списку, надісланого клієнтом, і відправляє повідомлення "Server Hello" разом із своїм сертифікатом, випадковим числом і обраними параметрами.
3. Сервер надсилає свій цифровий сертифікат, який містить публічний ключ RSA. Цей сертифікат використовується клієнтом для перевірки автентичності сервера.
4. Сервер надсилає повідомлення "Server Hello Done", щоб підтвердити завершення своєї частини обміну.
5. Client Key Exchange: Клієнт генерує Pre Master Secret, зашифровує його за допомогою публічного ключа сервера і надсилає його серверу. Сервер розшифровує його за допомогою свого приватного ключа. Обидві сторони мають однаковий Pre Master Secret, який використовується для генерації Master Secret і сеансових ключів.
6. Обидві сторони надсилають повідомлення "Change Cipher Spec", щоб показати, що вони переходять до використання нових шифрів і ключів для захищеної комунікації.
7. Обидві сторони обчислюють і надсилають повідомлення "Finished", яке містить хеш (згортку) попередніх повідомлень. Це повідомлення використовується для перевірки цілісності та підтвердження, що обидві сторони правильно отримали та розшифрували дані.
8. Після обміну повідомленнями "Finished" обидві сторони вважають, що TLS Handshake завершено успішно. Захищений тунель встановлено і вони готові передавати дані один одному через нього.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

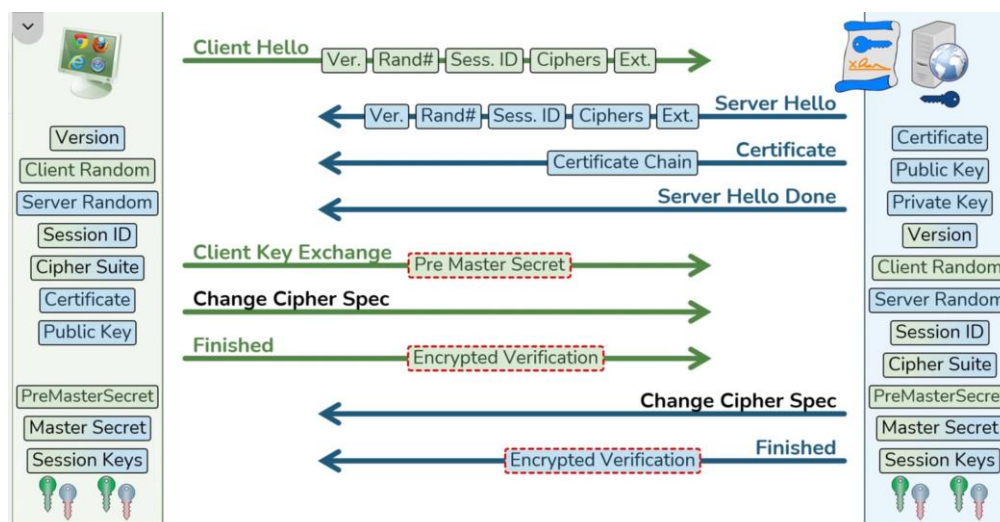


Рисунок 1.8 – Побудова SSL/TLS тунелю в TLS 1.2 (RSA Key Exchange)[6]

У процесі обміну ключами RSA тільки клієнт генерує SEED, що використовується для створення спільного секретного ключа. У випадку DHE обидві сторони, клієнт і сервер, приносять свій внесок у створення SEED значення. Обидві сторони також обмінюються публічними ключами DH. Сервер підписує своє публічне значення DH власним приватним ключем для підтвердження його автентичності. Клієнт перевіряє цей підпис за допомогою публічного ключа сервера. Після цього обидві сторони генерують Pre Master Secret, який використовується для подальшого створення спільного сеансового ключа.

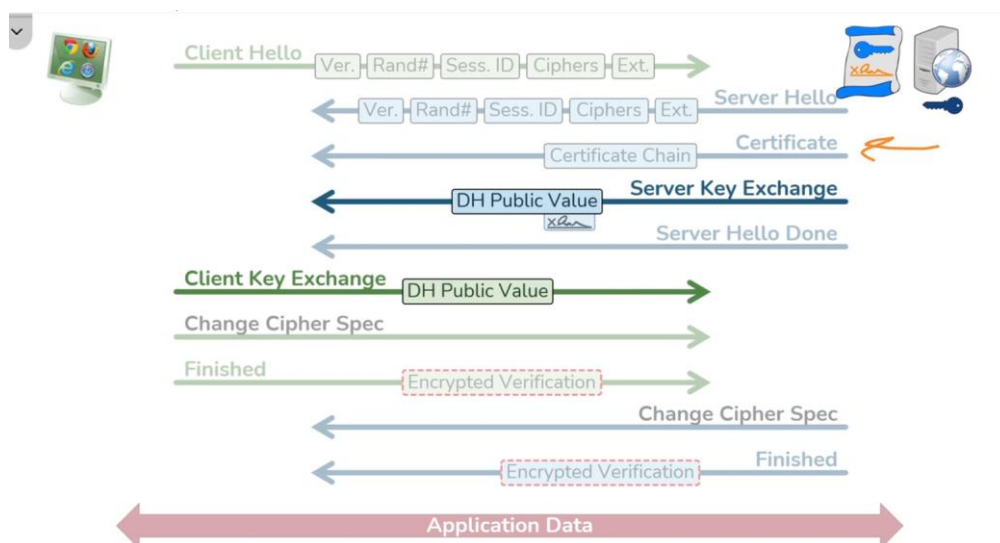


Рисунок 1.9 – Побудова SSL/TLS тунелю в TLS 1.2 (DH Key Exchange)[6]

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

У типовому TLS/SSL аутентифікується тільки сервер, тобто тільки сервер надає сертифікат для підтвердження своєї ідентичності. HTTPS-сайти автентифікують клієнта за допомогою імені користувача та пароля (щось зовнішнє для SSL/TLS). TLS/SSL забезпечує спосіб автентифікації як клієнта, так і сервера, відомий як mutual TLS (взаємна аутентифікація), коли і клієнт, і сервер надають сертифікат для підтвердження. Для веб-сайтів/HTTPS це рідкіний випадок, але більш поширений у SSL VPN.

Ось як буде виглядати TLS рукоштовування з використання mTLS:

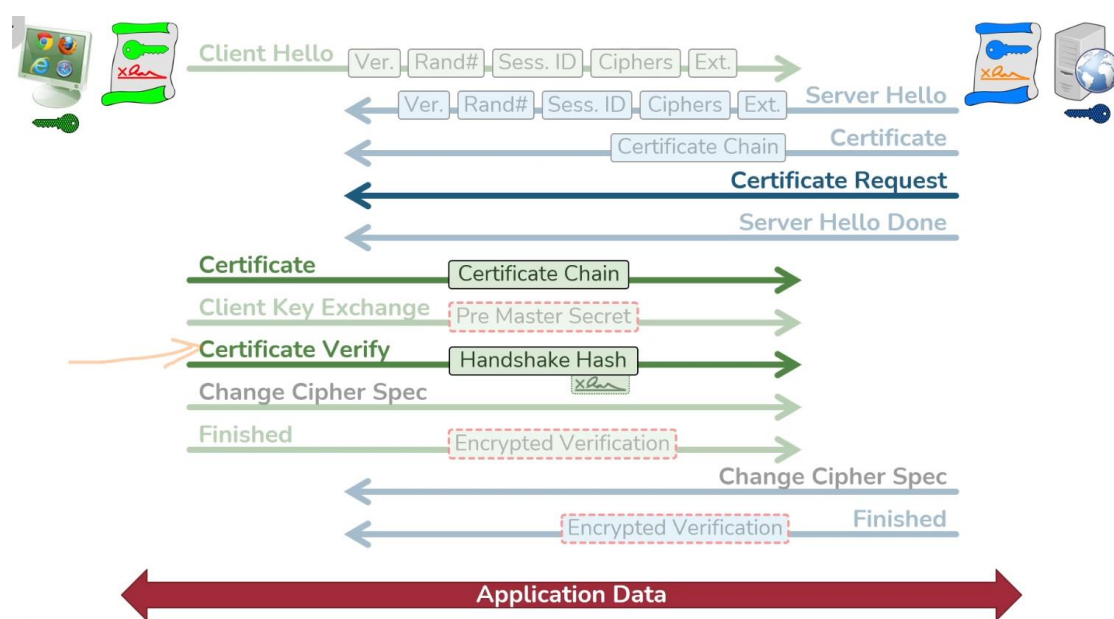


Рисунок 1.10 – Побудова SSL/TLS тунелю в TLS 1.2 (mutual TLS)[6]

Згідно рисунку, з'явилися три нові записи[8]:

1. Handshake: Certificate Request. Відправляється сервером для отримання запиту на сертифікат від клієнта. За бажанням може містити тип сертифікату, список довірених центрів сертифікації.
2. Handshake: Certificate. Включає повний сертифікат клієнта та ланцюжок сертифікатів.
3. Handshake: Certificate Verify. Підтвердження серверу, що клієнт є справжнім власником сертифіката. Клієнт обчислює хеш всіх записів типу Handshake та підписує цей хеш своїм приватним ключем.

Висновки до першого розділу

У першому розділі досліджено теоретичні відомості, пов'язані з SSL VPN технологією для віддаленого доступу. Було розглянуто особливості SSL VPN і його переваги, зокрема забезпечення безпеки та зручності для користувачів. Було проведено огляд стандартів безпеки і криптографічних алгоритмів, які використовуються у SSL VPN. Це включало огляд TLS протоколу і криптографічних алгоритмів, які забезпечують конфіденційність, цілісність та автентичність даних.

Також було розглянуто інфраструктуру відкритого ключа, яка використовується у SSL VPN для керування ключами та сертифікатами. Це важливий компонент, що дозволяє забезпечити безпеку комунікації та перевірку автентичності сторін.

Нарешті, було детально розглянуто процес встановлення TLS Handshake, який відбувається між клієнтом і сервером у SSL VPN з'єднанні. Ці відомості будуть надалі використовуватися для практичної реалізації та налаштування SSL VPN у наступних розділах.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ МЕРЕЖІ НА БАЗІ SSL VPN

2.1 Вибір засобів реалізації SSL VPN

При впровадженні SSL VPN в організації, важливо правильно вибрати засоби реалізації, які найкраще відповідатимуть потребам та вимогам компанії. При виборі засобів реалізації SSL VPN слід звернути увагу на кілька ключових аспектів.

Одним з головних факторів, які потрібно враховувати, є рівень безпеки, який надає SSL VPN. Переконайтесь, що обране рішення підтримує сильні криптографічні алгоритми. Додатково, зверніть увагу на наявність механізмів аутентифікації, контролю доступу та захисту від атак, таких як DDoS.

Потрібно враховувати потреби організації та визначати, які функції SSL VPN є необхідними. Наприклад, деякі рішення можуть підтримувати доступ до веб-додатків, файлових ресурсів, електронної пошти, а також забезпечувати віртуальні робочі столи. Важливо, щоб обраний SSL VPN відповідав конкретним потребам компанії.

Наступним кроком треба переконатись, що SSL VPN рішення сумісне з існуючими мережевими пристроями та операційними системами, які використовуються в організації. Наприклад, деякі рішення можуть бути більш оптимальними для роботи зі засобами від певних виробників.

Потрібно розглядати потенційну масштабованість організації та переконатись, що обраний SSL VPN може впоратися зі зростанням навантаження та кількості користувачів. Потрібно обирати таке рішення, яке може легко розширюватися та забезпечувати високу продуктивність.

Необхідно, приділяти увагу інтерфейсу управління SSL VPN та можливостям моніторингу, налаштування та адміністрування. Переконайтесь, що виробник надає відповідну технічну підтримку та регулярно оновлює програмне забезпечення, щоб запобігти вразливостям безпеки.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Існує кілька популярних марок SSL VPN, які відомі своєю надійністю та функціональністю. Деякі з них включають:

1. Cisco AnyConnect є одним з провідних рішень SSL VPN на ринку. Він надає широкі можливості для безпечного віддаленого доступу до мережі та ресурсів, включаючи розширені можливості аутентифікації та контролю доступу.
2. Pulse Secure є іншим популярним вибором для реалізації SSL VPN. Він надає безпеку та зручність використання, а також підтримку широкого спектра платформ і пристроїв.
3. FortiGate від Fortinet є інтегрованим засобом безпеки, який також пропонує розширені можливості SSL VPN. Він забезпечує захист мережі, а також дозволяє забезпечити безпечний віддалений доступ.
4. Check Point є відомою маркою в галузі безпеки, і їх рішення Remote Access VPN надає безпечний та зручний доступ до мережі через SSL VPN. Воно підтримує широкий спектр платформ і функціональні можливості.

Це лише деякі з популярних марок SSL VPN, проте на ринку існує багато інших варіантів, включаючи комерційні та відкриті рішення. Вибір конкретної марки залежить від ваших потреб, бюджету та вимог до безпеки та функціональності.

Враховуючи вимоги проекту та функціональні можливості Cisco ASA, будуть розглянуті основні складові системи SSL VPN та обґрунтовані аргументи щодо їх вибору.

Cisco ASA надає вбудований VPN-клієнт, який може бути використаний для забезпечення безпечного з'єднання між клієнтськими пристроями та Cisco ASA. Використання вбудованого клієнта спрощує конфігурацію та управління SSL VPN.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Cisco ASA підтримує різні методи аутентифікації користувачів для SSL VPN, такі як локальна база даних користувачів, інтеграція з Active Directory або використання зовнішніх серверів аутентифікації, таких як RADIUS або TACACS+. Вибір методу аутентифікації залежить від потреб проекту та наявних ресурсів[29].

Cisco ASA надає можливості контролю доступу до ресурсів мережі на основі різних параметрів, таких як ідентифікатор користувача, IP-адреса, група або роль. Це дозволяє задавати політики доступу до різних ресурсів мережі залежно від потреб проекту та рівня привілеїв користувачів.

Cisco ASA підтримує різні шифрувальні алгоритми та протоколи безпеки, такі як SSL/TLS. Важливо вибрати надійні шифрувальні алгоритми та протоколи, які відповідають сучасним стандартам безпеки і забезпечують захист передачі даних по SSL VPN.

Cisco ASA є одним з провідних рішень для мережевої безпеки та забезпечує широкий набір функцій для захисту мережі та ресурсів. Cisco ASA працює на власному фірмовому програмному забезпеченні, яке надає надійну та безпечну роботу пристрою. Функціональність програмного забезпечення може бути розширена за допомогою модулів та додаткових пакетів, які надають додаткові можливості безпеки та мережевого управління.

Cisco ASA виконує роль firewall, дозволяючи аналізувати мережевий трафік та встановлювати правила для фільтрації пакетів на основі IP-адрес, портів, протоколів та інших параметрів. За допомогою firewall Cisco ASA можна контролювати доступ до мережі, блокувати небажаний трафік, захищати мережу від атак та недозволених з'єднань.

Cisco ASA підтримує різні види VPN, включаючи IPsec VPN, SSL VPN та AnyConnect VPN. IPsec VPN дозволяє створювати зашифровані тунелі між різними мережами, забезпечуючи безпечний обмін даними. SSL VPN надає

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

безпечний доступ до ресурсів мережі через веб-браузер, не потребуючи додаткового клієнтського програмного забезпечення. AnyConnect VPN є розширеним рішенням, що дозволяє забезпечити безпечний доступ для віддалених користувачів, підтримуючи різні пристрої та платформи.

Cisco ASA може виступати в ролі IDS/IPS, що дозволяє виявляти та запобігати вторгненням в мережу. Він аналізує мережевий трафік, виявляє потенційні загрози та вживає заходів для їх запобігання.

Cisco ASA надає можливості фільтрації веб-трафіку, що дозволяє контролювати доступ до веб-сайтів та блокувати небажану або шкідливу активність. Він також має вбудовані механізми захисту від загроз, такі як антивірусний сканер та захист від шкідливих URL-адрес.

Cisco ASA надає різні можливості управління мережею, включаючи централізоване керування та моніторинг пристроєм. Інтерфейс командного рядка (CLI) та графічний інтерфейс (ASDM) дозволяють адміністраторам налаштовувати та керувати пристроєм.

Cisco ASA підтримує режим високої доступності, що дозволяє налаштувати збереження пристрою та автоматичне переключення на резервний пристрій у разі відмови. Це забезпечує неперервну роботу мережі та уникнення відключень.

Cisco ASA є комплексним рішенням для мережевої безпеки, яке надає широкий спектр функціональності та можливостей. Він працює як firewall, забезпечує різні види VPN, IDS/IPS, виконує фільтрацію трафіку, надає захист від загроз та має можливості управління мережею. Також він підтримує режим високої доступності для забезпечення неперервності роботи. Cisco ASA є надійним та потужним рішенням для захисту мережі та забезпечення мережевої безпеки.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

2.2 Проектування моделей та схем адресацій

Для налаштування Remote Access SSL VPN було побудовано наступну топологію мережі:

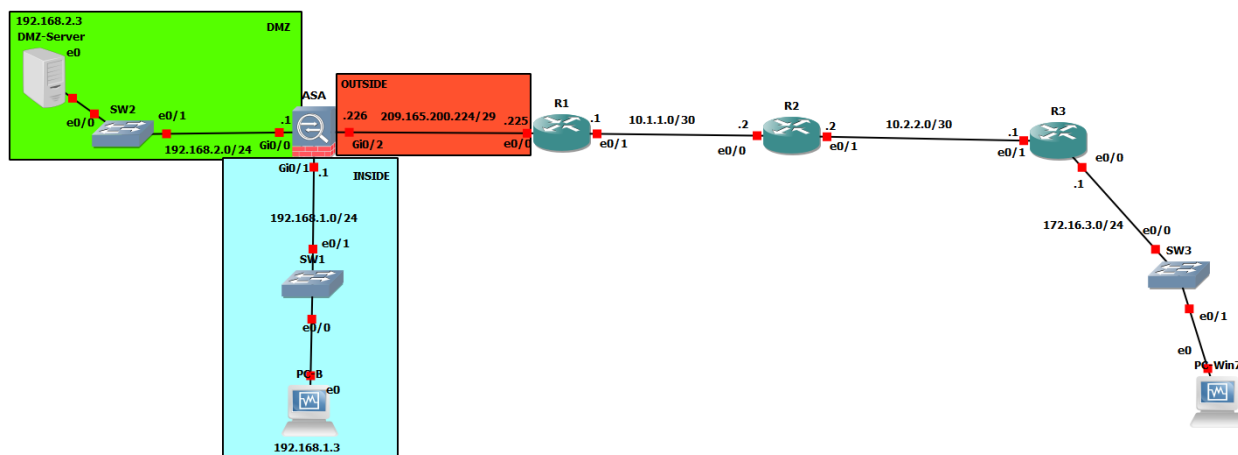


Рисунок 2.1 – Топологія мережі

Компанія має дві локації, підключені до інтернет-провайдера. R1 - це пристрій CPE (Customer Premises Equipment), яким керує провайдер. R2 являє собою проміжний інтернет-маршрутизатор. R3 з'єднує користувачів у віддаленому філіалі з провайдером. ASA - це пограничний пристрій безпеки, який з'єднує внутрішню корпоративну мережу і демілітаризовану зону з провайдером, забезпечуючи при цьому надаючи послуги NAT внутрішнім хостам.

DMZ (Demilitarized) Zone — це зона або сегмент мережі, який розташований між внутрішньою мережею (наприклад, локальною мережею) і зовнішньою мережею (наприклад, Інтернетом). DMZ зона служить для розміщення серверів, які повинні бути доступними для зовнішніх користувачів, але потребують певного рівня захисту. У DMZ зоні зазвичай розміщуються публічно доступні сервери, такі як веб-сервери, поштові сервери, FTP-сервери або сервери VPN. Ці сервери мають зовнішній IP-адреси і призначені для обробки запитів від користувачів з Інтернету.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

У пристрої Cisco ASA (Adaptive Security Appliance) існує поняття "inside" та "outside" інтерфейсів, які використовуються для налаштування мережевих з'єднань та контролю доступу між внутрішньою та зовнішньою мережами.

Інтерфейс "inside" вказує на внутрішню мережу або локальну мережу, яка знаходиться за пристроєм Cisco ASA. Внутрішня мережа може бути приватною мережею, до якої підключаються комп'ютери, сервери та інші пристрої. Inside інтерфейс зазвичай має приватну IP-адресу та використовується для маршрутизації трафіку між внутрішніми пристроями та зовнішніми мережами.

Outside інтерфейс вказує на зовнішню мережу або мережу, що знаходиться поза пристроєм Cisco ASA. Зовнішня мережа може бути публічною мережею, такою як Інтернет, або іншою зовнішньою мережею, до якої підключається пристрій ASA. Outside інтерфейс зазвичай має публічну IP-адресу, яка використовується для зв'язку зі зовнішніми мережами та отримання доступу до Інтернету.

Inside та outside інтерфейси використовуються для налаштування правил мережевої безпеки, контролю доступу та маршрутизації трафіку між внутрішньою та зовнішньою мережами. Налаштування правил фільтрації, налаштування VPN, налаштування NAT (Network Address Translation) та інші настройки безпеки мережі виконуються з використанням inside та outside інтерфейсів для визначення джерел та призначень трафіку.

Для керування Cisco ASA існує можливість використання ASDM (Adaptive Security Device Manager) - графічного інтерфейсу користувача, який надає зручний спосіб налаштування та управління пристроєм ASA. Для підключення до Cisco ASA за допомогою ASDM необхідно мати комп'ютер (PC-B), на якому встановлено програмне забезпечення ASDM. Це спрощує процес управління мережевою безпекою та дозволяє зосередитися на потрібних налаштуваннях, забезпечуючи безпеку мережі на основі Cisco ASA.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Для підключення до Cisco ASA з використанням клієнта AnyConnect будемо використовувати PC-C. Клієнт AnyConnect є програмним забезпеченням VPN, розробленим Cisco, яке надає безпечний доступ до мережі через SSL VPN.

На основі схеми зображеною на рис. 2.1 була створена наступна схема адресації.

Таблиця 2.1 – Схема адресації мережі

Пристрій	Інтерф ейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Порт підключення
Маршрутизатор R1	E0/0	209.165.200.225	/30	N/A	ASA Gi0/2
	E0/1	10.0.1.1	/30	N/A	N/A
Маршрутизатор R2	E0/0	10.0.1.2	/30	N/A	N/A
	E0/1	10.0.3.1	/30	N/A	N/A
Маршрутизатор R3	E0/0	172.16.3.1	/24	N/A	S3 E0/1
	E0/1	10.2.2.1	/30	N/A	N/A
ASA	Gi0/1	192.168.1.1	/24	N/A	S2 E0/1
	Gi0/2	209.165.200.226	/29	N/A	R1 E0/0
	Gi0/0	192.168.2.1	/24	N/A	S3 E0/1
PC-A	NIC	192.168.2.3	/24	192.168.2.1	S1 E0/0
PC-B	NIC	192.168.1.3	/24	192.168.1.1	S2 E0/0
PC-C	NIC	172.16.3.3	/24	172.16.3.1	S3 E0/1

2.3 Вибір обладнання

Для побудови мережі необхідно вибрати обладнання, яке відповідає вимогам проекту. У даному випадку, вибір обладнання буде здійснюватися з асортименту компанії Cisco, яка є провідним виробником телекомунікаційного обладнання. Важливо зазначити, що Cisco відома своєю надійністю обладнання, підтримкою спільнотою Інтернету та надає можливість для навчання з

використанням програмних симуляторів або емуляторів, таких як Cisco Packet Tracer або GNS3.

Cisco ASA 5500-X Series та Cisco ASA 5500 Series є популярними моделями мережевих пристроїв від компанії Cisco, які надають можливості SSL VPN разом з іншими функціями мережевої безпеки.

Cisco ASA 5500-X Series має розширені можливості мережевої безпеки, включаючи функції SSL VPN. Пропонує високу продуктивність та масштабованість для обробки великих обсягів трафіку та підключень. Підтримує сучасні криптографічні алгоритми та протоколи, що забезпечують безпечну передачу даних. Має різні моделі, які можуть відповідати різним потребам організацій різного розміру. Наприклад, Cisco ASA 5506-X, 5512-X, 5525-X та інші.



Рисунок 2.2 – Cisco ASA 5500-X серії

Cisco ASA 5500 Series також надає можливості SSL VPN та інші функції мережевої безпеки, але це попередня модель, яка була оновлена до серії ASA 5500-X. Має меншу продуктивність порівняно з серією ASA 5500-X, але все ще забезпечує надійну безпеку мережі. Популярні моделі включають Cisco ASA 5510, 5520 та 5540.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Cisco ASA має різні типи ліцензій, які надають доступ до різних функцій та можливостей пристрою. Основні типи ліцензій Cisco ASA включають:

Таблиця 2.2 – Ліцензії Cisco ASA

Ліцензія	Опис
Base License	Базова ліцензія, яка включає основні можливості мережевої безпеки, включаючи брандмауер та базові функції VPN.
Security Plus	Розширена ліцензія, яка надає додаткові функції, такі як Clustering, Active/Active Failover та підтримка до 50 VPN-тунелів.
AnyConnect Plus	Ліцензія, яка надає розширені можливості SSL VPN, включаючи доступ до веб-програм, файлових ресурсів та електронної пошти через AnyConnect.
AnyConnect Apex	Розширена ліцензія AnyConnect, яка додає функціональність передачі голосу та відео, динамічне налаштування політик безпеки та інтеграцію з системами мультифакторної аутентифікації.
VPN Only	Ліцензія, яка надає тільки функціональність VPN без додаткових можливостей мережевої безпеки.

Різні моделі ASA можуть мати відмінності у доступних ліцензіях та їх можливостях. Рекомендується перевірити офіційну документацію Cisco або звернутися до представника Cisco для отримання конкретної інформації про ліцензії для моделі ASA.

Однією з рекомендованих моделей Cisco ASA є Cisco ASA 5506-X. Ця модель є компактною та потужною, і надає широкий спектр функцій мережевої безпеки. Основні характеристики Cisco ASA 5506-X включають:

- Забезпечує пропускну здатність до 750 Mbps для пропуску трафіку мережі, що дозволяє обробляти великі обсяги даних.
- Пристрій має вбудовані 8 портів Fast Ethernet (10/100 Mbps) для підключення до внутрішньої мережі, зовнішньої мережі та інших пристроїв.
- Модель підтримує SSL VPN, що дозволяє встановлювати безпечні з'єднання з віддаленими користувачами та дозволяє доступ до

важливих ресурсів організації з будь-якого місця з Інтернет-підключенням.

- Модель підтримує можливість додавання додаткових модулів та розширень, що дозволяє пристосувати пристрій до зростаючих потреб вашої мережі.
- ASA 5506-X має функцію керування трафіком, яка дозволяє регулювати пропускну здатність мережі та забезпечувати пріоритети для різних видів трафіку.

Це лише загальний огляд основних характеристик Cisco ASA 5506-X. Рекомендується проконсультуватися з представником Cisco або переглянути офіційну документацію для отримання детальнішої інформації та визначення, чи відповідає ця модель конкретним потребам у мережевій безпеці.

Висновки до другого розділу

У даному розділі було розглянуто кілька важливих аспектів, пов'язаних з проектуванням мережі на базі SSL VPN. Спочатку було проаналізовано вибір засобів реалізації SSL VPN. Розглянуто різні альтернативи, їх переваги та можливості. Вибір конкретного рішення повинен ґрунтуватися на специфічних потребах та вимогах конкретної організації. Було спроектовано моделі та схеми адресацій для мережі на базі SSL VPN.

Детально розглянули моделі Cisco ASA 5500-X Series та Cisco ASA 5500 Series і навели їх основні характеристики. Обладнання Cisco ASA відоме своєю надійністю та розширеними можливостями мережевої безпеки, що робить його привабливим вибором для реалізації SSL VPN. Ці кроки допомагають забезпечити безпеку, надійність та ефективність мережевого середовища на основі SSL VPN. З цими відомостями можна переходити до наступного розділу, де буде детальніше розглядатися конфігурація та реалізація SSL VPN в обраній мережі.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

РОЗДІЛ 3 НАЛАШТУВАННЯ SSL VPN У СИМУЛЯТОРІ GNS3

3.1 Базове налаштування пристроїв

Крок 1: Підключення мережі, як показано в топології (рис. 2.1).

Крок 2: Налаштування основних параметрів для кожного пристрою (табл. 2.2).

Налаштування маршрутизатора R1:

```
R1(config)#hostname R1
R1(config)#security passwords min-length 10
R1(config)#enable algorithm-type scrypt secret cisco12345
R1(config)#username admin01 algorithm-type scrypt secret admin01pass
R1(config)#ip domain name ccnasecurity.com
R1(config)#line con 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
R1(config-line)#exit
R1(config)#int ethernet 0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.248
R1(config-if)# no shut
R1(config-if)#exit
R1(config)#int ethernet 0/1
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 e0/1
```

Налаштування R2:

```
R2(config)#interface e0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface e0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#ip route 209.165.200.224 255.255.255.248 e0/0
R2(config)#ip route 172.16.3.0 255.255.255.0 e0/1
```

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Налаштування маршрутизатора R3:

```
R3(config)#hostname R3
R3(config)#security passwords min-length 10
R3(config)#enable algorithm-type scrypt secret cisco12345
R3(config)#username admin01 algorithm-type scrypt secret admin01pass
R3(config)#interface e0/0
R3(config-if)#ip address 172.16.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#int e0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 e0/1
```

Налаштування інтерфейсів та встановлення security level:

```
ciscoasa(config)# hostname ASA
ASA(config)# domain-name security.com
ASA(config)# enable password cisco12345
ASA(config)# int Gi0/1
ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA(config-if)# ip add 192.168.1.1 255.255.255.0
ASA(config-if)# no sh
ASA(config-if)# int Gi0/2
ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA(config-if)# ip add 209.165.200.226 255.255.255.248
ASA(config-if)# no sh
ASA(config-if)# int Gi0/0
ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA(config-if)# security-level 70
ASA(config-if)# ip add 192.168.2.1 255.255.255.0
ASA(config-if)# no sh
```

Налаштування маршрутизація, NAT та аутентифікації на Cisco ASA:

```
ASA(config)# object network inside-net
ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)# object network dmz-server
ASA(config-network-object)# host 192.168.2.3
ASA(config-network-object)# access-list OUTSIDE-DMZ extended permit ip any hos$
ASA(config)# object network inside-net
ASA(config-network-object)# nat (inside,outside) dynamic interface
ERROR: % Invalid input detected at '^' marker.
ASA(config-network-object)# nat (inside,outside) dynamic interface
ASA(config-network-object)# object network dmz-server
ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
ASA(config-network-object)# access-group OUTSIDE-DMZ in interface outside
ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
ASA(config)# username admin01 password admin01pass
ASA(config)# aaa authentication telnet console LOCAL
ASA(config)# aaa authentication ssh console LoCAL
ERROR: aaa-server group LoCAL does not exist
ASA(config)# aaa authentication ssh console LOCAL
ASA(config)# aaa authentication http cnsle LOCAL
ERROR: % Invalid input detected at '^' marker.
ASA(config)# aaa authentication http console LOCAL
```

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Налаштування HTTPS сервера на Cisco ASA:

```
ASA(config)# http server enable
ASA(config)# http 192.168.1.0 255.255.255.0 inside
ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
ASA(config)# telnet 192.168.1.0 255.255.255.0 inside
ASA(config)# telnet timeout 10
ASA(config)# ssh timeout 10
ASA(config)# class-map inspection_default
ASA(config-cmap)# match default-inspection-traffic
ASA(config-cmap)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# inspect icmp
ASA(config-pmap-c)# crypto key generate rsa modulus 1024
```

Підключення через HTTPS до ASA:

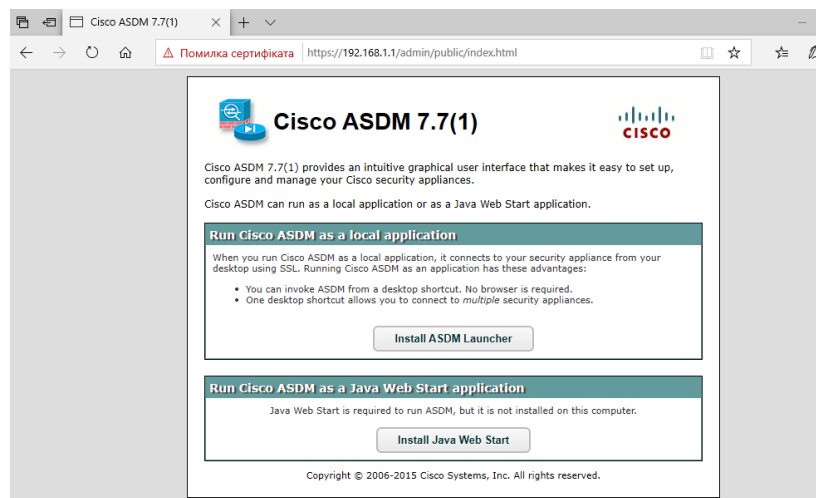


Рисунок 3.1 – Підключення до ASA через HTTPS

Після встановлення Cisco ASDM-IDM Launcher, було виконано вхід за допомогою користувача admin01:

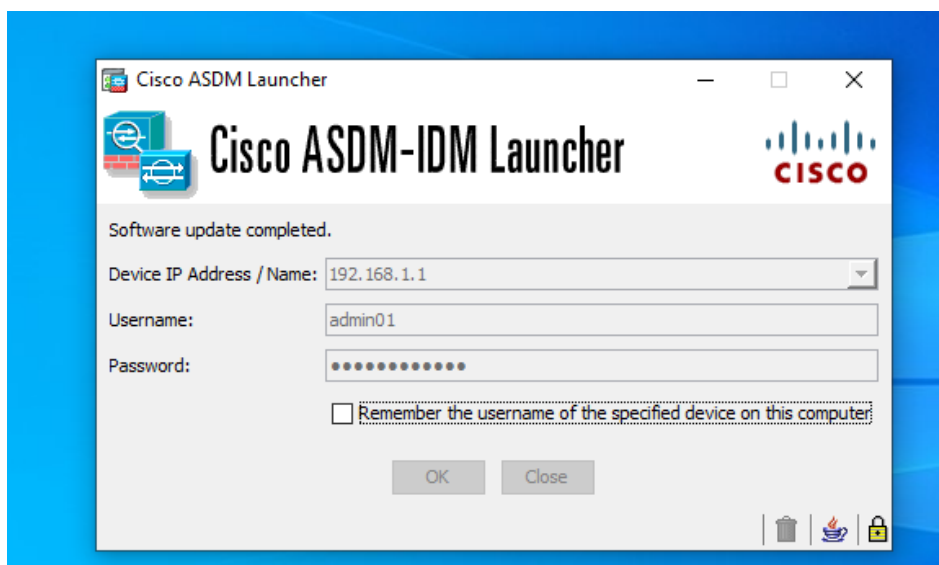


Рисунок 3.2 – Вхід до Cisco ASDM-IDM Launcher

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Налаштування віддаленого доступу AnyConnect SSL VPN за допомогою ASDM

Запуск майстра VPN. У головному меню ASDM потрібно обрати Wizards > VPN Wizard > AnyConnect VPN Wizard:

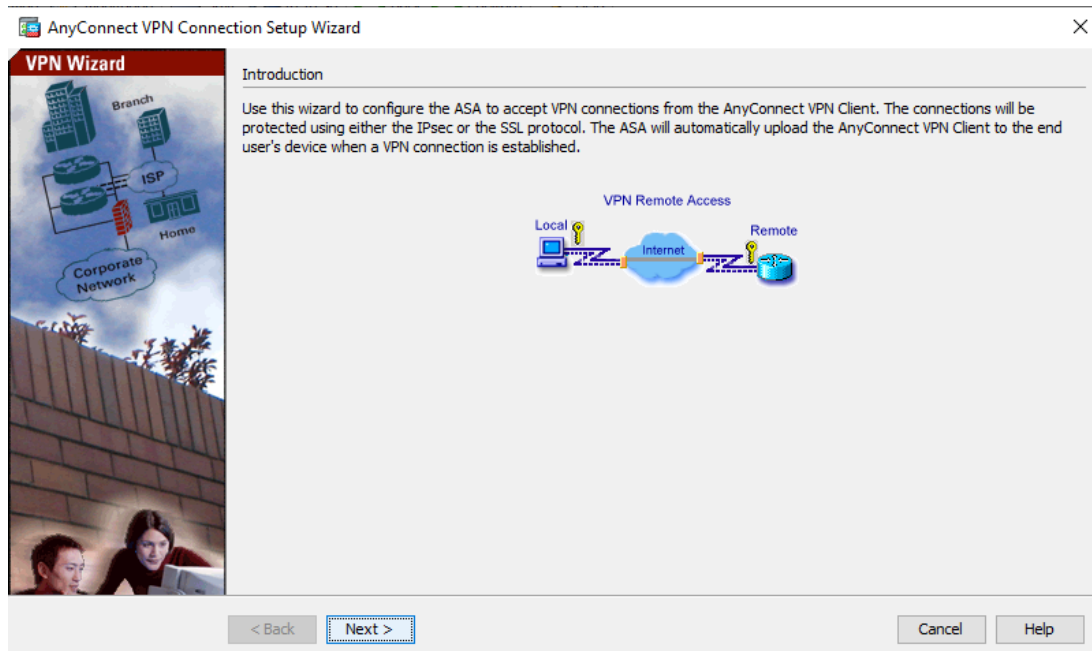


Рисунок 3.3 – AnyConnect VPN Connection Setup Wizard

Налаштування профілю підключення інтерфейсу SSL VPN:

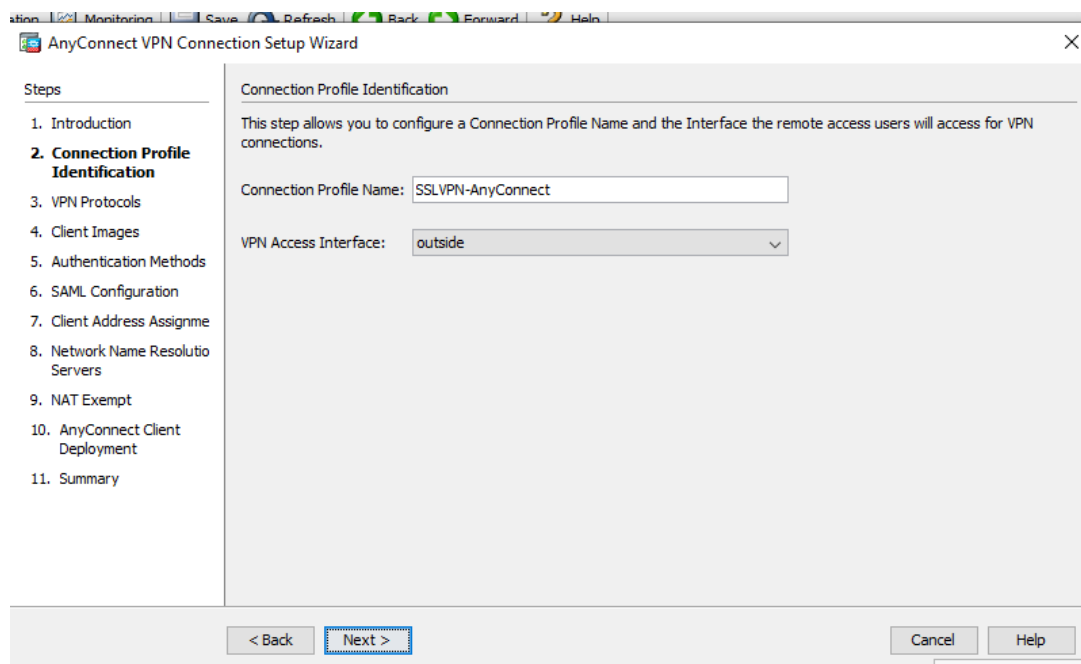


Рисунок 3.4 – Створення профілю

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

Вибір протоколу шифрування VPN.

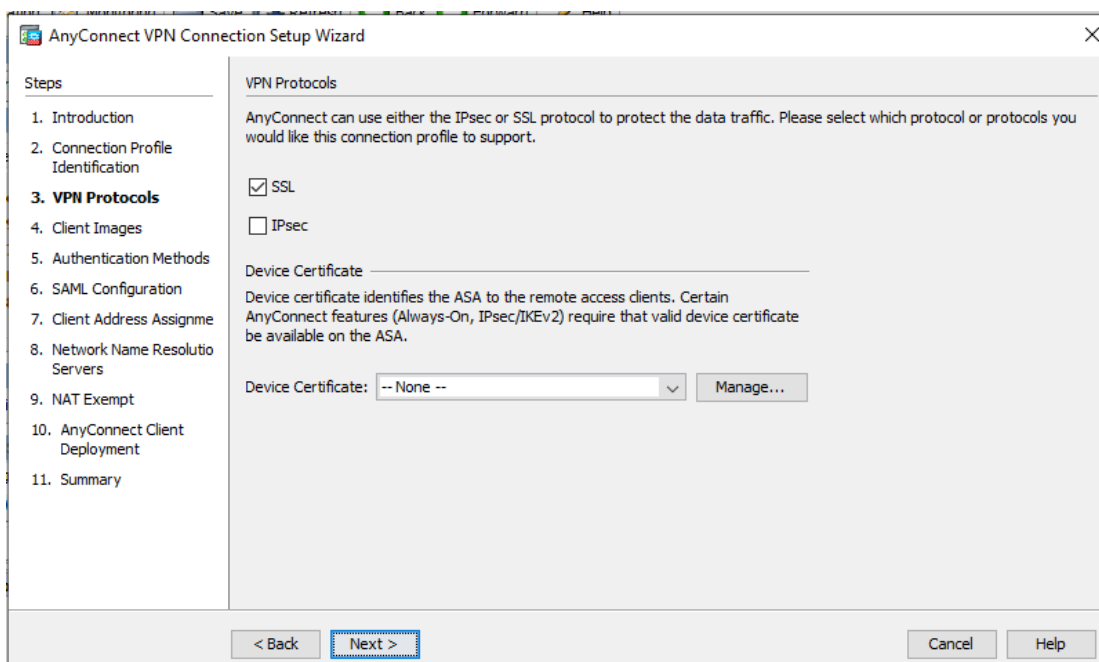


Рисунок 3.5 – Вибір протоколу

Потрібно налаштувати образ клієнта для завантаження користувачам AnyConnect, якщо образа немає, його потрібно завантажити на flash пам'ять пристрою Cisco ASA:

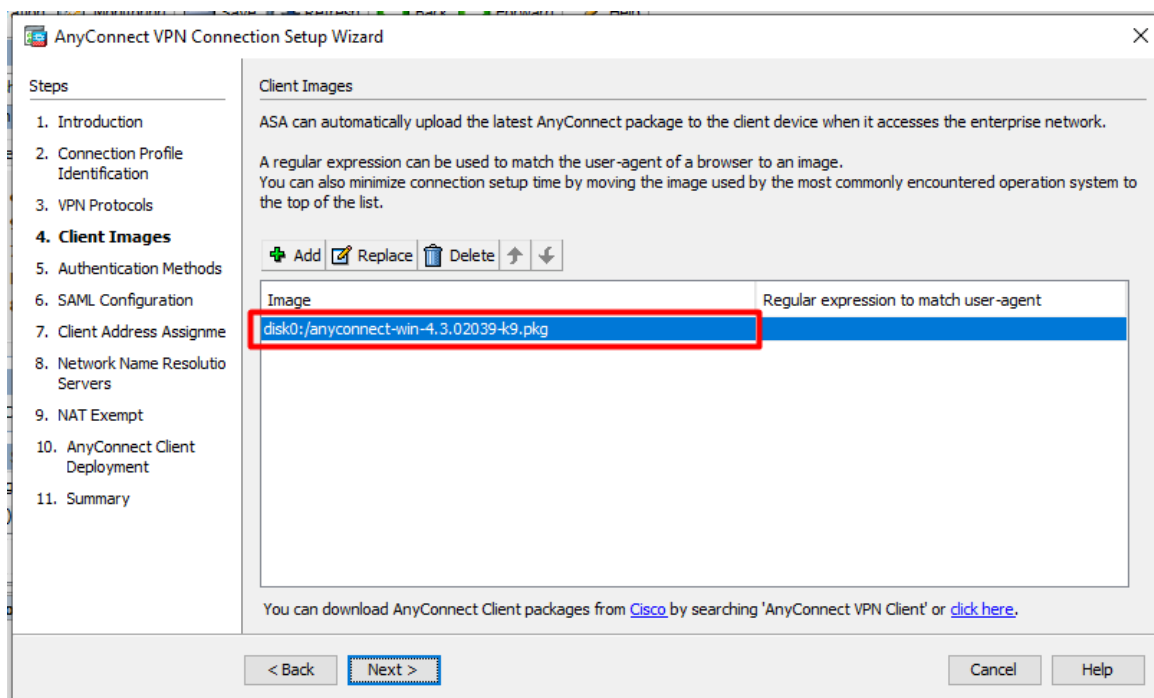


Рисунок 3.6 – Вибір образу Anyconnect додатку

Налаштування локальної автентифікації AAA:

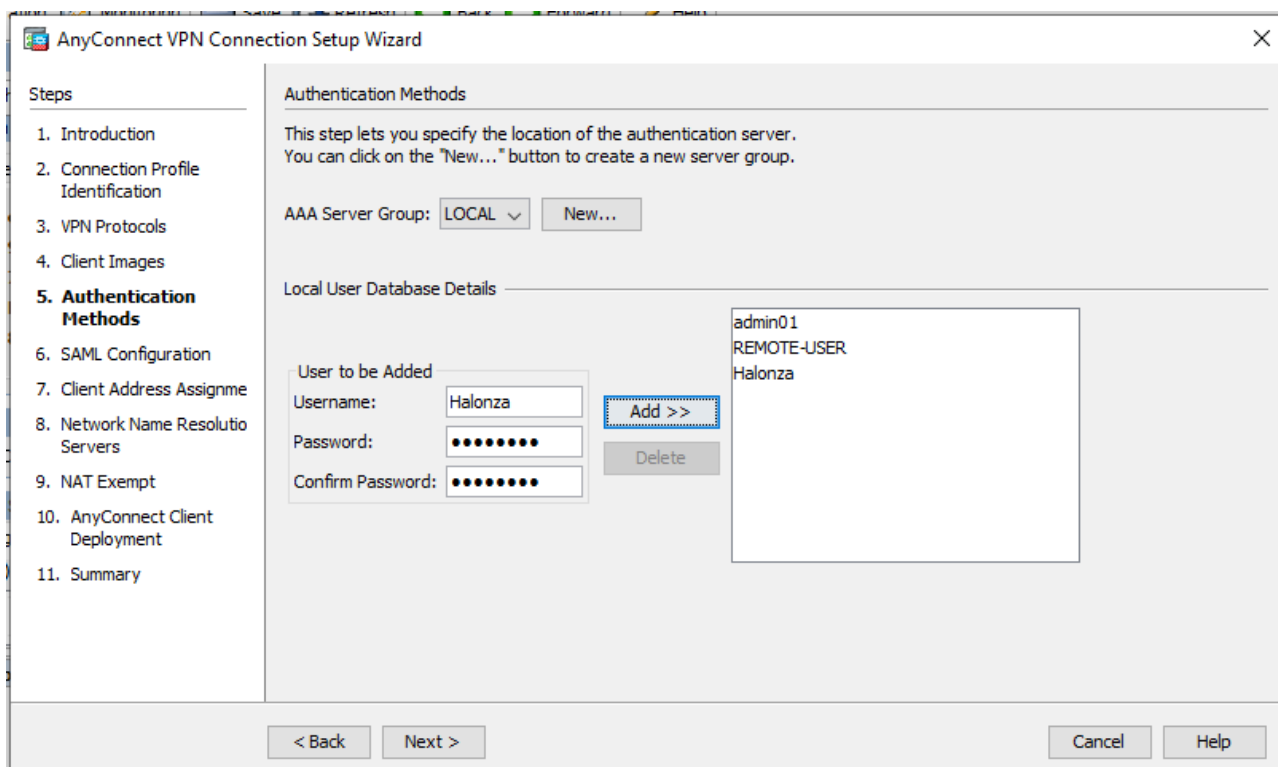


Рисунок 3.7 – Налаштування локальної автентифікації

Налаштування діапазону клієнтських адрес:

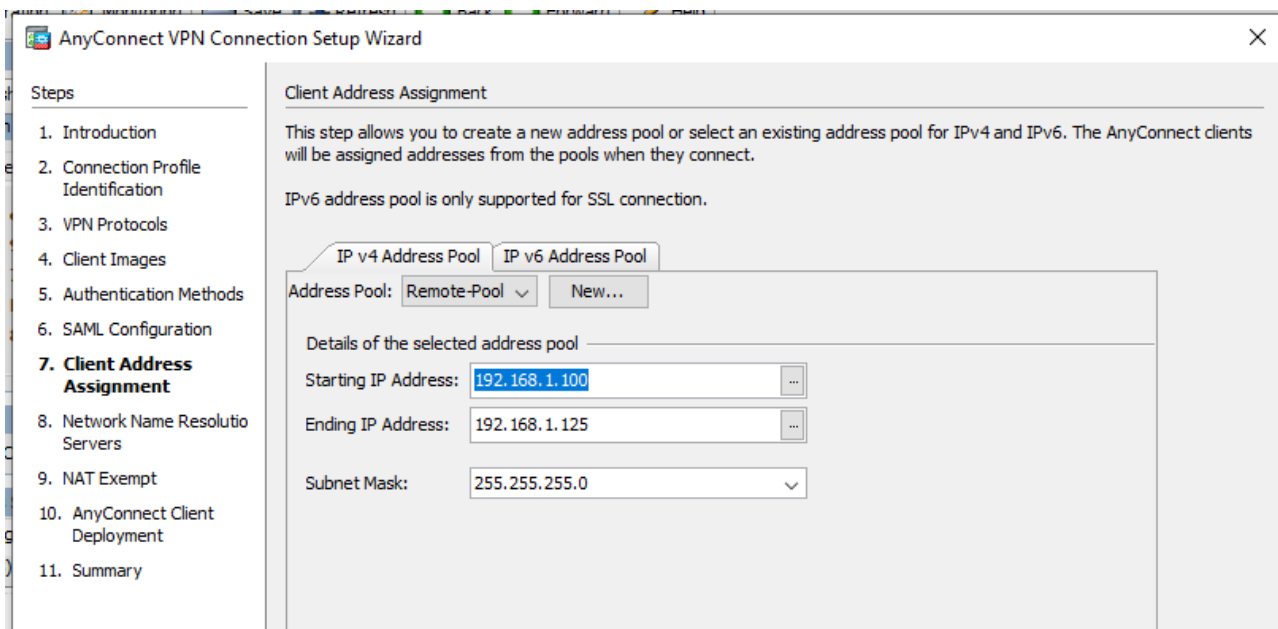


Рисунок 3.8 – Вибір пулу клієнтських адрес

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування розпізнавання адрес мережевих імен:

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. On the left, a 'Steps' list includes: 1. Introduction, 2. Connection Profile Identification, 3. VPN Protocols, 4. Client Images, 5. Authentication Methods, 6. SAML Configuration, 7. Client Address Assignme, **8. Network Name Resolution Servers**, 9. NAT Exempt, 10. AnyConnect Client Deployment, and 11. Summary. The main area is titled 'Network Name Resolution Servers' and contains the text: 'This step lets you specify how domain names are resolved for the remote user when accessing the internal network.' Below this text are three input fields: 'DNS Servers:' with the value '192.168.2.3', 'WINS Servers:' which is empty, and 'Domain Name:' with the value 'security.com'. At the bottom of the window are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Рисунок 3.9 – Налаштування DNS

Вимкнення трансляції адрес для VPN-трафіку.

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window at Step 9, 'NAT Exempt'. The 'Steps' list on the left is identical to the previous screenshot, with '9. NAT Exempt' highlighted. The main area is titled 'NAT Exempt' and contains the text: 'If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.' Below this text is a checkbox labeled 'Exempt VPN traffic from network address translation', which is checked. Underneath the checkbox is a description: 'Inside Interface is the interface directly connected to your internal network.' followed by an 'Inside Interface:' dropdown menu showing 'inside'. Below that is another description: 'Local Network is the network address(es) of the internal network that client can access.' followed by a 'Local Network:' input field containing 'any4'. At the bottom of the window are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

Рисунок 3.10 – Вимкнення NAT для VPN трафіку

Огляд вікна Summary та застосування конфігурації до ASA:

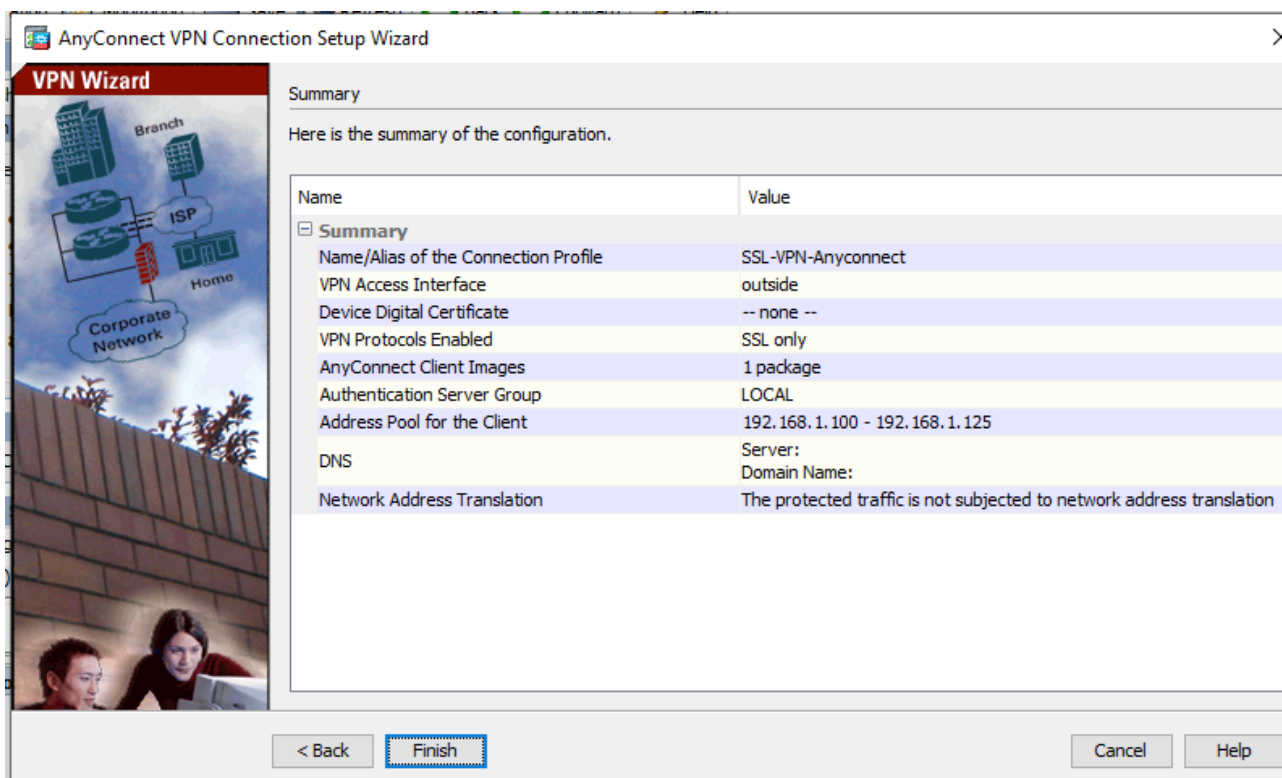


Рисунок 3.11 – Вікно Summary

Перевірка профілю клієнта AnyConnect:

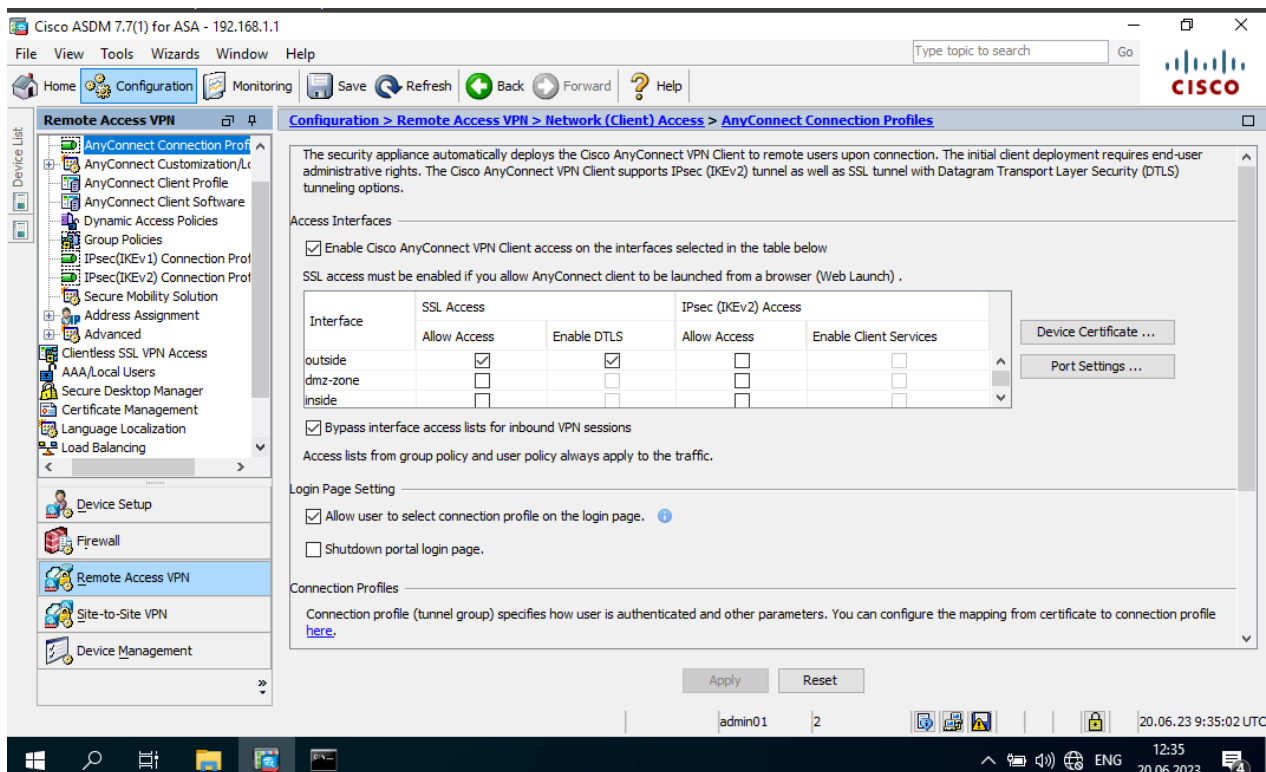


Рисунок 3.12 – Профіль AnyConnect

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк. 50
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Редагування профілю клієнта AnyConnect для увімкнення функції split-tunnel профілю, щоб тільки специфічний трафік відправлявся через тунель:

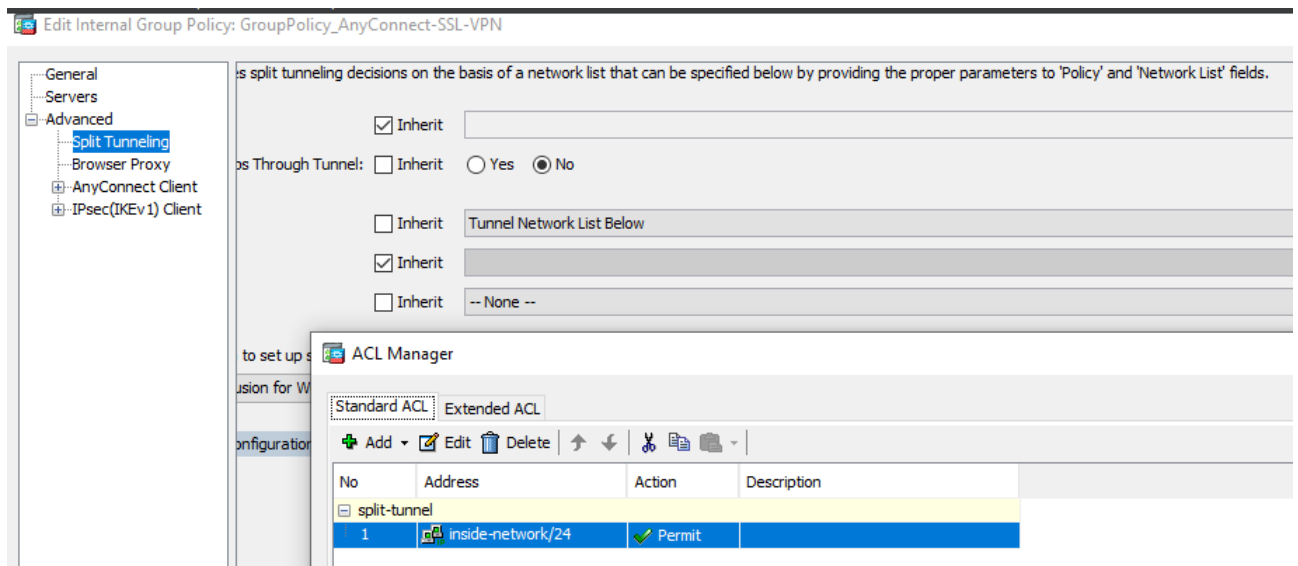


Рисунок 3.13 – Додавання функції split-tunnel

3.3 Підключення до AnyConnect SSL VPN

Потрібно здійснити перехід за посиланням <https://209.165.200.226> для SSL VPN. Вхід було виконано за допомогою створеного користувача Halonza:

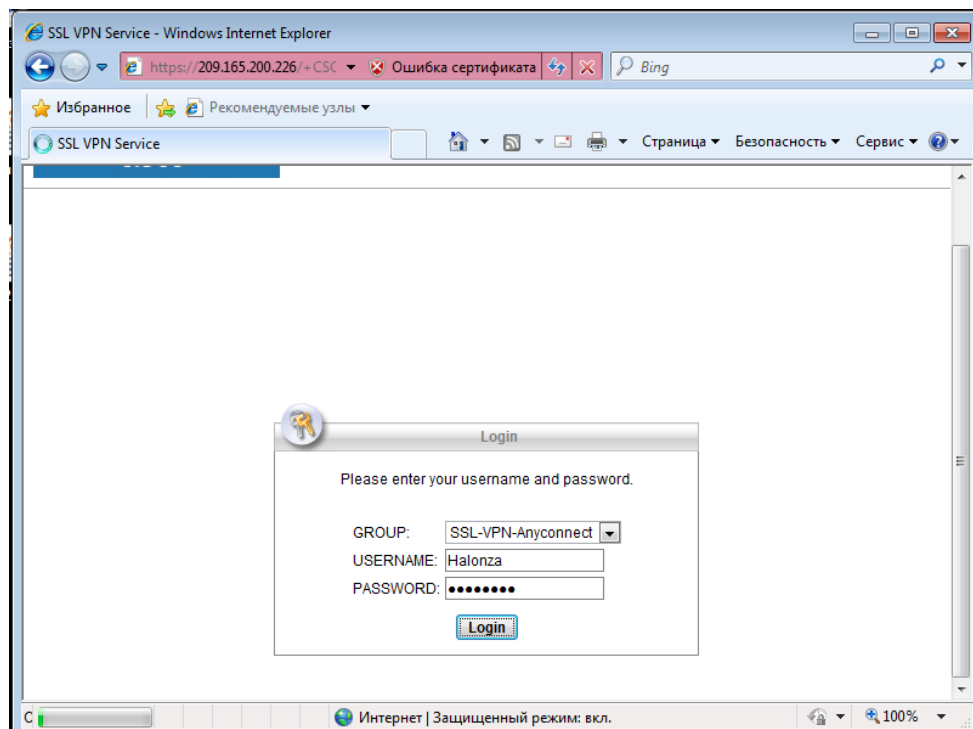


Рисунок 3.14 – Вхід до SSL VPN

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

ASA почне процес автоматичного завантаження програмного забезпечення, що складається з серії перевірок на відповідність для цільової системи. ASA виконує виявлення платформи, запитуючи клієнтську систему, намагаючись визначити тип клієнта, який підключається до пристрою безпеки. На основі ідентифікованої платформи може бути автоматично завантажений відповідний програмний пакет:

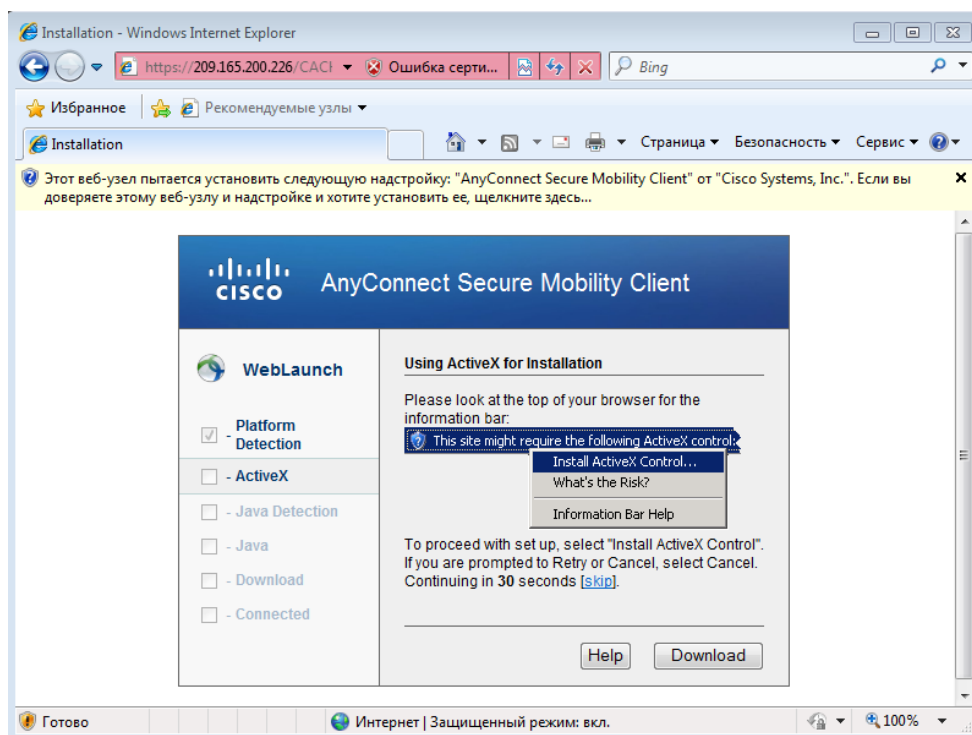


Рисунок 3.15 – Виконується виявлення платформи

У вікні AnyConnect Secure Mobility Client Downloader розпочнеться відлік часу завантаження:

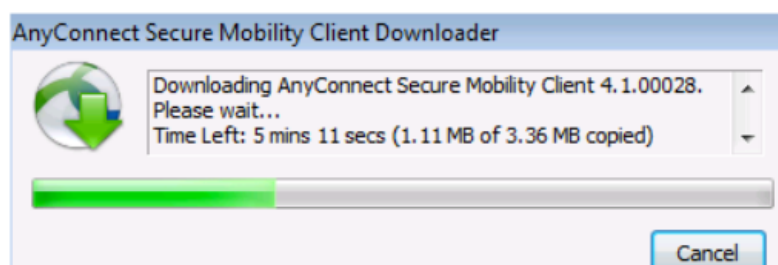


Рисунок 3.16 – Завантаження AnyConnect Secure Mobility Client Downloader

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Після встановлення AnyConnect VPN потрібно запустити програму Cisco AnyConnect VPN Client та увійти за допомогою створеного користувача:



Рисунок 3.17 – Успішне встановлення з'єднання

Виведення статистики з'єднань та інформацію про них:

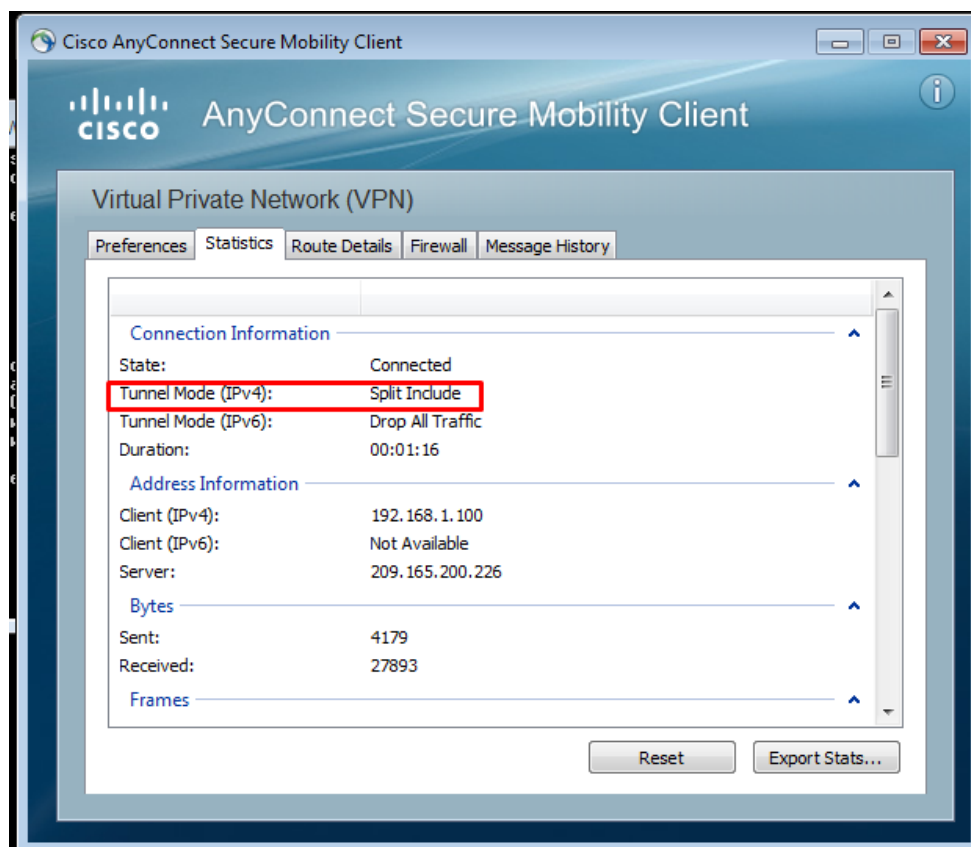


Рисунок 3.18 – Системна інформація

У командному рядку на віддаленому хості було перевірено IP-адресу за допомогою команди `ipconfig`. З наступного виводу видно, що там вказано дві IP-адреси. Одна з них - це локальна IP-адреса віддаленого хоста PC-C (172.16.3.3), а інша - це IP-адреса, призначена для тунелю SSL VPN (192.168.1.100).

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

```

C:\Windows\system32\cmd.exe
C:\Users\NetAcad>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : ccnasecurity.com
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::70f5:f35c:59de:53a7%11
    IPv4 Address. . . . . : 172.16.3.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.3.1

C:\Users\NetAcad>

```

Рисунок 3.19 – Вивід команди ifconfig

З віддаленого хост-комп'ютера PC-C було виконано за допомогою командної утиліти ping PC-B (192.168.1.3), щоб перевірити наявність зв'язку:

```

C:\Users\admin>ping 192.168.1.3

Обмен пакетами с 192.168.1.3 по 32 байтами данных:
Ответ от 192.168.1.3: число байт=32 время=70мс TTL=128
Ответ от 192.168.1.3: число байт=32 время=18мс TTL=128
Ответ от 192.168.1.3: число байт=32 время=5мс TTL=128
Ответ от 192.168.1.3: число байт=32 время=6мс TTL=128

Статистика Ping для 192.168.1.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
    Минимальное = 5мсек, Максимальное = 70 мсек, Среднее = 24 мсек

```

Рисунок 3.20 – Результат утиліти ping

Перевірка чи шифрується трафік за допомогою програми Wireshark:

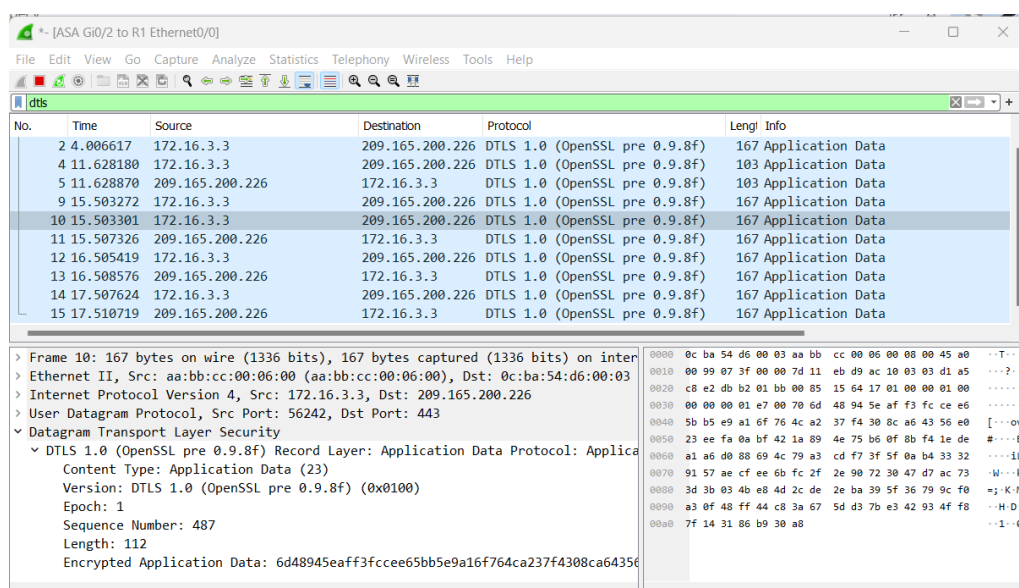


Рисунок 3.21 – Wireshark

За допомогою ASDM Monitor було виконано перегляд AnyConnect віддалених користувацьких сесій:

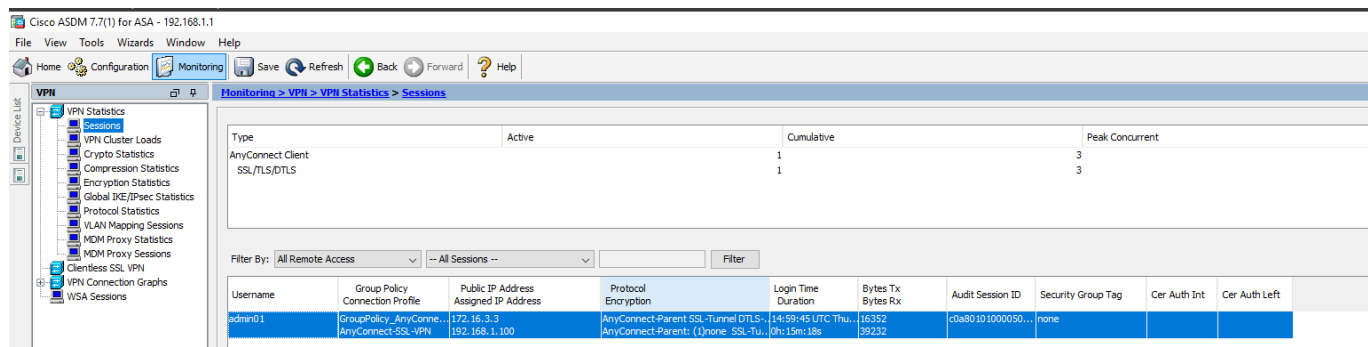


Рисунок 3.22 – Перегляд віддалених сесій

Висновки до третього розділу

У цьому розділі було детально розглянуто процес налаштування SSL VPN за допомогою симулятора GNS3. Спочатку було акцентовано увагу на початковому налаштуванні пристроїв. Було розглянуто процес додавання пристроїв ASA та маршрутизаторів, а також налаштування основних параметрів, таких як IP-адреси, інтерфейси та маршрутизація. Це дозволило створити необхідне середовище для SSL VPN.

Далі, було перейдено до налаштування віддаленого доступу AnyConnect SSL VPN за допомогою ASDM. Був розглянутий процес імпорту сертифікату, створення груп користувачів, налаштування політик безпеки та розподілу IP-адрес для підключених клієнтів. Це забезпечило налаштування безпечного доступу до ресурсів мережі через SSL VPN.

Нарешті, розглянутий був процес підключення до AnyConnect SSL VPN з боку клієнта. Описано процес завантаження та налаштування AnyConnect VPN-клієнта, а також показано, як встановити з'єднання з сервером SSL VPN і отримати доступ до ресурсів мережі.

В результаті даного розділу отримано практичні навички налаштування SSL VPN у симуляторі GNS3, з ключовими кроками налаштування пристроїв, створення VPN-підключень та забезпечення безпеки з'єднання. Ці знання будуть

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

корисними для подальшої роботи з SSL VPN та його впровадження в реальних мережових середовищах.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У першому розділі було представлено теоретичні відомості про SSL VPN, включаючи його особливості, переваги та безпекові стандарти. Була оглянута інфраструктура відкритого ключа, яка використовується для керування ключами та сертифікатами в SSL VPN.

У другому розділі було проаналізовано проектування мережі на базі SSL VPN, включаючи вибір засобів реалізації та моделі адресацій. Були розглянуті моделі обладнання Cisco ASA 5500-X Series та Cisco ASA 5500 Series, які відомі своєю надійністю та розширеними можливостями мережевої безпеки.

Третій розділ детально описує процес налаштування SSL VPN з використанням симулятора GNS3. Були описані кроки налаштування пристроїв ASA та маршрутизаторів, а також налаштування параметрів безпеки та віддаленого доступу AnyConnect SSL VPN з використанням ASDM. Також було представлено процес підключення до SSL VPN з боку клієнта.

В результаті цього дослідження отримано практичні навички налаштування SSL VPN у симуляторі GNS3, які будуть корисними для роботи з цією технологією в реальних мережових середовищах.

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchsecurity/definition/SSL-VPN>
2. Rolf Oppliger. SSL and TLS: Theory and Practice, 2009. – 304 с.
3. [Електронний ресурс] – Режим доступу: <https://ostec.blog/en/general/ssl-vpn-benefits/>
4. [Електронний ресурс] – Режим доступу: <https://www.f5.com/glossary/ssl-vpn>
5. [Електронний ресурс] – Режим доступу: <https://www.practicalnetworking.net/classes/tls/>
6. Paul Baka, Jeremy Schatten. SSL/TLS Under Lock and Key: A Guide to Understanding SSL/TLS Cryptography, 2021. – 132 с.
7. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html>
8. [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html>
9. Ivan Ristic. Bulletproof SSL and TLS, 2014. – 538 с.
10. Alasdair Gilchrist. A Concise Guide to SSL/TLS for DevOps: 2nd Edition 2015. – 224 с.
11. [Електронний ресурс] – Режим доступу: <https://networklessons.com/cisco/asa-firewall/cisco-asa-anyconnect-remote-access-vpn>
12. [Електронний ресурс] – Режим доступу: <https://support.eset.com/en/kb3481-how-do-i-configure-my-cisco-asa-ssl-vpn-device-for-use-with-eset-secure-authentication>
13. [Електронний ресурс] – Режим доступу: <https://support.eset.com/en/kb3481-how-do-i-configure-my-cisco-asa-ssl-vpn-device-for-use-with-eset-secure-authentication>

		Галонза Д. В.			<i>KIK.KP.B – 123 – 02 – ПЗ</i>	Арк.
		Петросян Р. В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

14. [Электронный ресурс] – Режим доступа:
<https://www.udemy.com/course/cisco-asa-firewall-fundamentals/>
15. [Электронный ресурс] – Режим доступа:
<https://www.udemy.com/course/virtualprivatenetwork/>
16. [Электронный ресурс] – Режим доступа:
<https://support.huawei.com/enterprise/en/doc/EDOC1100086057>
17. Joshua Davies. Implementing SSL / TLS Using Cryptography and PKI, 2011.
– 1235 с.
18. Jeff Stapleton, W. Clay Epstein. Security without Obscurity: A Guide to PKI Operations
19. [Электронный ресурс] – Режим доступа:
https://www.youtube.com/watch?v=Er5toSsbM8I&ab_channel=KatherineMcNamara
20. [Электронный ресурс] – Режим доступа:
https://www.youtube.com/watch?v=G8Fk9d_Wt84&t=20s&ab_channel=KevinWallaceTraining%2CLLC
21. [Электронный ресурс] – Режим доступа:
https://www.youtube.com/watch?v=kANFvl6yj3w&ab_channel=soundtraining.net
22. The Art of Service - Public Key Infrastructure Publishing. Public Key Infrastructure A Complete Guide, 2021. – 315 с.
23. [Электронный ресурс] – Режим доступа:
https://www.youtube.com/watch?v=vj_VGganQfs&ab_channel=TechHelpingHands
24. Jazib Frahim, Omar Santos, Andrew Ossipov. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services, 2014. – 1248 с.
25. Richard Deal. Cisco ASA Configuration (Network Professional's Library), 2009. – 752 с.
26. Kevin Wallace, Brad Edgeworth, Ramiro Garza Rios, Jason Gooley, David Hucaby, Raymond Lacoste. CCNP Enterprise Core ENCOR 350-401 and

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Advanced Routing ENARSI 300-410 Official Cert Guide Library, 2020. - 850с.

27. [Электронный ресурс] – Режим доступа: <https://nordvpn.com/uk/blog/ssl-vpn-explained/>
28. [Электронный ресурс] – Режим доступа: <https://www.vpnunlimited.com/help/more-about-vpn/ssl-vs-ipsec>
29. [Электронный ресурс] – Режим доступа: <https://www.techtarget.com/searchsecurity/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks>
30. [Электронный ресурс] – Режим доступа: <https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/>
31. [Электронный ресурс] – Режим доступа: <https://openvpn.net/faq/why-ssl-vpn/>

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Конфігураційний файл міжмережевого екрану Cisco ASA

ASA Version 9.7(1)

hostname ciscoasa

enable password \$sha512\$5000\$ dhUTZ

JODkdBCbqMDKQGcPQ==\$/yxqb90Qr7UHRsspEHx9Qg==\$ pbkdf2

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

names

ip local pool Remote-Pool 192.168.1.100-192.168.1.125 mask 255.255.255.0

?

interface GigabitEthernet0/0

name if dmz-zone

security-level 70

ip address 192.168.2.1 255.255.255.0

interface GigabitEthernet0/1

name if inside

security-level 100

ip address 192.168.1.1 255.255.255.0

ginterface GigabitEthernet0/2

name if outside

security-level 0

ip address 209.165.200.226 255.255.255.0

		Галонза Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

```

object network dmz-server
host 192.168.2.3
object network NETWORK_OBJ_192.168.1.96_27
subnet 192.168.1.96 255.255.255.224
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
access-list split-tunnel standard permit 192.168.1.0 255.255.255.0
pager lines 23
mtu dmz-zone 1500
mtu inside 1500
mtu outside 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (inside, outside) source static any any destination static NETWORK_OBJ_192.16
8.1.96_27 NETWORK_OBJ_192.168.1.96_27 no-proxy-arp route-lookup
!
object network inside-net
nat (inside, outside) dynamic interface
object network dmz-server
mat (dmz-zone, outside) static 209.165.200.227
access-group OUTSIDE-DMZ in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30

```

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
 at imeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
 timeout tcp-proxy-reassembly 0:01:00
 timeout floating-conn 0:00:00
 timeout conn-holddown 0:00:15
 timeout igp stale-route 0:01:10
 user-identity default-domain in LOCAL
 aaa authentication telnet console LOCAL
 aaa authentication ssh console LOCAL
 aaa authentication http console LOCAL
 http server enable
 http 192.168.1.0 255.255.255.0 inside
 no snmp-server location
 no snmp-server contact
 crypto ipsec security-association mtu-aging infinite
 crypto ca trustpoint _SmartCallHome Server CA
 no validation-usage
 telnet 192.168.1.0 255.255.255.0 inside
 telnet timeout 5
 ssh stricthostkeycheck
 ssh 192.168.1.0 255.255.255.0 inside
 ssh timeout 5
 ssh key-exchange group dh-group1-sha1
 console timeout
 threat-detection basic-threat
 threat-detection statistics access-list

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no threat-detection statistics tcp-intercept
webcpn
enable outside
anyconnect image disk0: /anyconnect-win-4.3.02039-k9.pkg 1
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
group-policy GroupPolicy AnyConnect-SSL-UPN internal
group-policy GroupPolicy AnyConnect-SSL-UPN attributes
wins-server none
dns-server value 192.168.2.3
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
dynamic-access-policy-record DfltAccessPolicy
username admin01 password $sha512$5000$M/K3a712DsPTyb1idc jg
IA==$0/gaqC7189wwt/9
fJKAyQ== pbkdf2
username REMOTE-USER password
S9TJYDLmJA== pbkdf2
tunnel-group AnyConnect-SSL-UPN type remote-access
tunnel-group AnyConnect-SSL-VPN general-attributes
address-pool Remote-Pool
default-group-policy GroupPolicy AnyConnect-SSL-VPN
tunnel-group AnyConnect-SSL-VPN webvpn-attributes
group-alias AnyConnect-SSL-UPN enable
!
$sha512$5000$WgSJEesN3xtNzqcXCPOEHA==$UUpoGJmSsn

```

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

```

class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
policy-map type inspect dns migrated_dns_map_2
parameters
message-length maximum client auto

```

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

message-length maximum 512

no tcp-inspection

service-policy global policy global

prompt hostname context

no call-home reporting anonymous

call-home

profile Cisco TAC-1

no active

destination address http <https://tools.cisco.com/its/service/oddce/services/DDCEService>

destination address email callhome@cisco.com

destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group

subscribe-to-alert-group

subscribe-to-alert-group telemetry periodic daily

profile License

destination address http <https://tools.cisco.com/its/service/oddce/services/DDCEService>

destination transport-method http

Cryptochecksum:2bd4b7d0464350b9eb22080041383b39

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток В – Конфігураційний файл маршрутизатора R1

Current configuration : 2180 bytes

!

! Last configuration change at 08:56:42 UTC Fri Jun 23 2023

!

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

security passwords min-length 10

enable secret 9

\$9\$CqnRKUOsCg0bgn\$g1qkN3Z9HW62plN0vw/PnnT/Hwh17B88Mtsi1QPsXo6

!

no aaa new-model

!

--More--

*Jun 23 08:56:42.673: %SYS-5-CONFIG_I: Configured from console by console

bsd-client server url https://cloudsso.cisco.com/as/token.oauth2

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

no ip icmp rate-limit unreachable

no ip domain lookup

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

cts logging verbose

!

!

username halonza secret 9

\$9\$x.Guoqr7VQecZ1\$xUaVmsgQ74wjyszsvk7bq0nkV0/DCOH0gYbYy9V7DyEE

!

redundancy

!

!

ip tcp synwait-time 5

!

interface Ethernet0/0

ip address 209.165.200.225 255.255.255.248

!

interface Ethernet0/1

ip address 10.1.1.1 255.255.255.252

!

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 10.1.1.2

!

!

!

!

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
  transport input none
!
!
end

```

Додаток С – Конфігураційний файл маршрутизатора R2

Building configuration...

Current configuration : 2232 bytes

```

!
! Last configuration change at 08:59:02 UTC Fri Jun 23 2023
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

hostname R2

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 9

\$9\$FONCGnkub1Uk91\$lG7GGeAZAhfR1zSQrWqRwiNAuiRqgQzk5HqDLG4ulZ

I

!

no aaa new-model

!

!

!

bsd-client server url https://cloudsso.cisco.com/as/token.oauth2

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

!

!

!

!

no ip icmp rate-limit unreachable

!

!

!

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

!

no ip domain lookup

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

username halonza secret 9

\$9\$4QwgSm/EU/qg7X\$3v./HuaZ2J6gseHzEMzpodWYVxCeRxDEff2zHfnPAcI

!

redundancy

!

!

ip tcp synwait-time 5

!!

interface Ethernet0/0

ip address 10.1.1.2 255.255.255.252

!

interface Ethernet0/1

ip address 10.2.2.2 255.255.255.252

!

!

!

no ip http server

no ip http secure-server

ip route 172.16.3.0 255.255.255.0 10.2.2.1

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 209.165.200.224 255.255.255.248 10.1.1.1
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
  transport input none
!
end

```

Додаток D – Конфігураційний файл маршрутизатора R3

```

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!

```

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

!

security passwords min-length 10

enable secret 9

\$9\$Qt/6rUo8yfB1cX\$siHVNANOp.B3ooyYphXWaMilNrSOs/wpY5lOVtIjYgM

!

no aaa new-model

!

!

!

bsd-client server url https://cloudsso.cisco.com/as/token.oauth2

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

!

no ip icmp rate-limit unreachable

!

!

no ip domain lookup

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

cts logging verbose

!

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
username halonza secret 9
$9$vOaTyhvt3aITQX$RXkP3lLgK9VmgB.l1l4uv7zoYEcuCqAhax0c
QWRXIfs
!
redundancy
!
ip tcp synwait-time 5
!interface Ethernet0/0
ip address 172.16.3.1 255.255.255.0
!
interface Ethernet0/1
ip address 10.2.2.1 255.255.255.252
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.2.2.2
!
!
!
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15

```

		Галонза Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
transport input none
!
!
end

		Галонза Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Петросян Р. В.				76
Змн.	Арк.	№ докум.	Підпис	Дата		