

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 підсистеми забезпечення гетерогенних віддалених підключень користувачів на базі технологій Remote Access VPN»

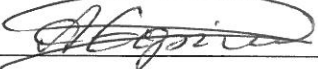
Виконав

студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

 Волинець Б. О.

Керівник,

завідувач кафедри КІ та КБ, к.т.н.

 Єфіменко А. А.

Рецензент

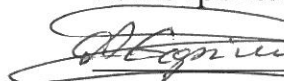
доцент кафедри КІ та КБ, к.т.н., доцент

 Пулеко І. В.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускнну кваліфікаційну роботу

Студента **Волинця Богуслава Олеговича**

Тема роботи: **Проект підсистеми забезпечення гетерогенних віддалених підключень користувачів на базі технологій Remote Access VPN**

затверджена Наказом по університету від «12» квітня 2021 р. № 134/С

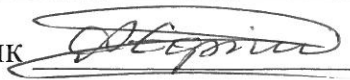
Термін здачі студентом закінченої роботи – «18» червня 2021р.

Вихідні дані для роботи:

1. Логічна топологія мережі
2. Маршрутизатори Cisco
3. Міжмережні екрани Cisco ASA
4. Операційні системи Cisco IOS, Windows 10, Windows 7, Windows 8 Lite,
5. Сервери AAA.
6. Графічний симулятор мереж GNS3

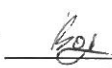
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

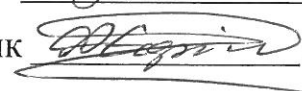
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	2.03.21	2.03.21
2	Єфіменко А.А.	6.04.21	6.04.21
3	Єфіменко А.А.	4.05.21	4.05.21

Керівник  Єфіменко А.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз протоколів та технологій віддаленого доступу.	12 квітня 2021 – 16 квітня 2021	Виконано
4	Аналіз можливостей міжмерережного екрану в налаштуванні технології Remote Access VPN	17 квітня 2021 – 19 квітня 2021	Виконано
5	Проектування мережної інфраструктури	20 квітня 2021 – 24 квітня 2021	Виконано
6	Проектування серверної інфраструктури	25 квітня 2021 – 30 квітня 2021	Виконано
7	Вибір компонентів серверної складової системи	1 травня 2021 – 4 травня 2021	Виконано
8	Проектування сценарію тестування мережі	5 травня 2021 – 9 травня 2021	Виконано
9	Базове налагодження пристроїв мережі	10 травня 2021 – 13 травня 2021	Виконано
10	Налагодження роботи підсистем віддаленого доступу	14 травня 2021 – 30 травня 2021	Виконано
11	Тестування роботи віддаленого доступу	31 травня 2021 – 3 червня 2021	Виконано
12	Аналіз результатів тестування	4 червня 2021 – 6 червня 2021	Виконано
13	Написання пояснювальної записки	7 червня 2021 – 12 червня 2021	Виконано
14	Підготовка презентації та виступу	13 червня 2021 – 14 червня 2021	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	15 червня 2021 – 16 червня 2021	Виконано
16	Захист	22 червня 2021	

Студент  Волинець Б.О.

Керівник  Єфіменко А.А.

РЕФЕРАТ

Випускна кваліфікаційна робота бакалавра містить проект підсистеми забезпечення гетерогених віддалених підключень користувачів на базі технологій Remote Access VPN, пояснювальну записку та ілюстративний матеріал до нього. Пояснювальна записка до випускної роботи містить 62 сторінки, 51 ілюстрацію та 5 таблиць.

Метою роботи є проектування мережної інфраструктури та налаштування серверної складової, які створюють захищений тунель до користувачів віддаленого доступу за допомогою технологій віддаленого доступу AnyConnect VPN.

В роботі проаналізовано теоретичні відомості та визначено завдання на розробку підсистеми забезпечення гетерогенних віддалених підключень. Також у роботі спроектовано мережну та серверну інфраструктуру систем віддаленого доступу. Окрім того, вибрано компоненти та обладнання для серверної складової системи. Також у роботі наведено сценарій налаштування роботи захищеного віддаленого доступу та результати тестування мережі.

КЛЮЧОВІ СЛОВА: REMOTE ACCESS VPN, СЕРВЕР, ВІДДАЛЕНІ КОРИСТУВАЧІ, МЕРЕЖА, ТУНЕЛЮВАННЯ.

					КІК.КР.Б-125-03-ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми забезпечення гетерогенних віддалених підключень користувачів на базі технологій Remote Access VPN	Літ.	Арк.	Аркушів
Розроб.		Волинець Б.О.		18.06.21				
Керівник		Єфіменко А.А.		18.06.21			4	75
Реценз.		Пудіко І.В.		18.06.21		ФІКТ, гр. КБ-1		
Н. Контр.								
Затверд.		Єфіменко А.А.		18.06.21				

ABSTRACT

The bachelor's thesis consists of subsystems for providing heterogeneous remote user connections based on Remote Access VPN technologies. Documentation for bachelor's graduate work contains 62 pages, 51 illustrations, and 5 tables.

The goal of the work is to design the network infrastructure and set up the server components that create a secure tunnel to remote access users using AnyConnect VPN remote access technologies.

In this paper analyzed theoretical information and defined tasks. The network and server infrastructure of remote access systems was designed. The components and equipment for the server components of the system were selected. The configuration of the protected remote access operation is given. The results of network testing are also being compiled.

KEYWORDS: REMOTE ACCESS VPN SERVER, REMOTE USER, NETWORK, TUNNELING.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

VPN – Virtual Private Network - віртуальна приватна мережа

ПК – Персональний комп'ютер

PPTP – Point to Point Tunneling Protocol

L2TP – Layer 2 Tunneling Protocol

NAT - Network Address Translation — перетворення мережевих адрес

PAT - Port Address Translation IP – Internet Protocol

IPsec - IP Security

MPLS - Multiprotocol Label Switching

IKE – Internet Key Exchange

NAT- Network address translation

SLA - Service Level Agreement

IGP- Interior Gateway Protocol

GRE - Generic Routing Encapsulation

DSL - Digital Subscriber Line

RDP - Remote Desktop Protocol

SHA - Secure Hash Algorithm

AES-CBC - Advanced Encryption Standard - Cipher Block Chaining

CPVPN - Customer Provisioned VPN

PPVPN - Provider Provisioned VPN

VNC- Virtual Network Computing

TCP-Transmission Control Protocol

IOT - Internet of things

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ЗМІСТ

ЗМІСТ.....	7
ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЙ ВІДДАЛЕНОЇ РОБОТИ КОРИСТУВАЧІВ В ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ.....	10
1.1 Організація віддаленого доступу до ресурсів інформаційної системи.	10
1.2 Технології та протоколи віддаленого досупу.....	11
1.3 Засоби організації віддаленого доступу.....	25
1.4 Технічне завдання.....	29
1.5 Висновки до розділу 1.....	30
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ	31
2.1 Проектування мережної інфраструктури.....	31
2.2 Проектування серверної інфраструктури.	37
2.3 Засоби віддаленого доступу кінця вузлів.....	38
2.4 Висновки до розділу 2.....	39
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ	40
3.1 Вибір компонентів серверної складової системи.....	40
3.2 Налагодження віддаленого доступу.....	44
3.2 Перевірка роботи та дослідження відаленого доступу.	56
3.4 Висновки до розділу 3.....	59
ВИСНОВКИ.....	61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	63
ДОДАТКИ.....	65

ВСТУП

Сьогодні майже кожна третя людина користувалася послугами VPN. Хтось використовував VPN клієнти для того щоб отримати доступ до закордонного контенту, послуг або привілеїв таких як недоступні каталог серіалів від Netflix, отримати скидку або більший термін безкоштовного періоду від послуг Amazon, перейти до іншого регіону в онлайн магазинах адже іноді ціни змінюються в залежності від регіона проживання або щоб обійти блокування до тих чи інших сервісів які заблокував за наказом держави або випадково ваш провайдер або особа турбується про свою безпеку в світовій павутині. Особливим скачком у користуванні послугами VPN стався під час світової пандемії COVID-19 де в усіх країнах люди потрапили на домашню самоізоляції. Під час цих не приятних умов весь світ втрапив у велику халепу, багато країн потрапили в економічний кризис або були близько тої прірви. Але як не дивно одним із ресурсів які допомогли стабілізувати ситуацію у світі це технології віддаленого доступу через VPN. Технології віддаленого дочтупу VPN стали розглядатися не тільки як технології, що дозволяють своїм користувачам залишитися анонімним в глобальній павутині, або забезпечити захищене підключення між декількома невеликих офісів підприємств які знаходяться на далекій відстані один від одного або в інших країнах але як фундамент в роботі всіх компанія вищої ліги. Раніше для компаній було нормою нормою розгортати свої віртуальні мережі для своїх офісів або філій з інших міст або країн для об'єднання їх в одну мережу але для цього аони використовували технології Site-to-Site VPN які використовувались для створення захищеного тунелю між філіями. Але вони зіткнулись із проблемою, як розгорнути VPN для всіх працівників з дому, адже найбільш популярні на той час в компаніях технології та рішення базувались на Site-to-Site VPN була зручною в об'єднанні кількох офісів компаній створюючи свою захищену WAN але була затратна в налаштуванні до кожного працівника. Предстате собі як до кожного працівника потрібно було б розгорнути захищений тунель та закупити для цього до кожної особи потрібне обладнання, було б добре якщо їх було б сотня або ж дві але коли

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

їх більше тисячі або десяти тисяч то важко представити якої б суми коштувала б така ідея.

Саме тому більшість компаній поглянули на дешеве та благорозумне рішення - розгорнути свої віртуальні мережі віддаленого доступу адже існують рішення для підключення до десяти тисяч користувачів одночасної почали розгортати як можна швидше, щоб помякшити збитки від довгого простою адже з кожною годиною вони втрачали масові капітали своїх фінансів та для того щоб працівники із дому не втратити цінну інформацію адже через самоізоляцію люди більше почали проводити часу в світовій пугині і звісно ж збільшились випадки хакерських атак, шахраїв та розповсюдження вірусів на незахищені підприємства або їх працівників.

Особливо хотіло виділити компанію Cisco яка як в воду дивилася і ще з початку 2000-чних років розпочала розвивати як технології VPN так і незабаром почали покращувати технології віддаленого доступу через VPN і на сьогодні має найкраще як по зручності роботи , розгортані так і по потужності рішення для віддаленого доступу.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЙ ВІДДАЛЕНОЇ РОБОТИ КОРИСТУВАЧІВ В ГЕТЕРОГЕННОМУ СЕРЕДОВИЩІ.

1.1 Організація віддаленого доступу до ресурсів інформаційної системи.

Віддалений доступ дозволяє своїм користувачам отримати доступ до файлів та інших системних ресурсів на будь-яких пристроях або серверах, які підключені до мережі та дозволяє підвищити продуктивність праці працівників адже вони можуть продовжувати працювати не маючи фізичного доступу до даних та дозволяє їм краще співпрацювати з колегами з усього світу.

Раніше для організація віддаленого доступу на підприємствах використовували модеми та комутовані технології для того щоб дозволити працівникам підключатися до офісних мереж через телефонні мережі, підключені до серверів віддаленого доступу. Пристрої, підключені до комутованих мереж, використовували аналогові модеми для виклику призначених їм телефонних номерів для встановлення з'єднань для надсилання або отримування повідомлень. Але дана технологія була слабою і мала ряд недоліків як із безпекою так і проблеми із швидкістю передачі даних вже не кажучи про вартість розгортання віддаленого доступу на велику відстань. Але час йде, технології змінюються на кращі, так само сталося і з нею, замінивши на технології широкосмугового доступу. Широкосмуговий доступ надає віддаленим користувачам можливості високошвидкісного підключення до корпоративних мереж та Інтернету. Сьогодні для організації віддаленого доступу доступні кілька типів широкосмугового зв'язку, включаючи такі:

- Кабельна широкосмугова мережа яка розподіляє пропускну здатність між багатьма користувачами і як результат, швидкість передачі даних у потоці може бути повільною під час роботи з високим рівнем використання в районах, де багато абонентів.

- Широкосмугова мережа DSL (Digital Subscriber Line) забезпечує високошвидкісну мережу через телефонну мережу, використовуючи широкосмуговий модем. Однак DSL працює лише на обмеженій фізичній відстані

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

і може бути недоступним у деяких регіонах, якщо місцева телефонна інфраструктура не підтримує технологію DSL.

- До мобільних пристроїв через мобільний пристрій можна отримати доступ до стільникового Інтернету з будь-якого місця, де доступна стільникова мережа.

- Служби супутникового Інтернету використовують телекомунікаційні супутники, щоб забезпечити користувачам доступ до Інтернету в районах, де наземний доступ до Інтернету недоступний, а також для тимчасових мобільних установок.

Сьогодні завдяки цим технологіям організації віддаленого доступу організації, корпорації та компанії мають можливість наймати найкращих спеціалістів з тої чи іншої галузі незважаючи на їх місцезнаходження, сприяти співпраці між командами та офісами чи філій, сприяє фахівцям служби технічної підтримки отримати доступ до комп'ютера із віддалених місць, щоб вирішити проблеми із своїми системами чи програмним забезпеченням. Дана технологія настільки розвинулась, що складно зрозуміти її складову і дуже легко заблудитися в ній. Але точно можна сформулювати визначення, що віддалений доступ – це будь яка технологія що дозволяє уповноваженій особі отримати доступ до комп'ютера або мережі з географічної відстані через мережеве з'єднання.

1.2 Технології та протоколи віддаленого досупу.

Незалежно від технологій, програмного забезпечення яке використовується, воно повинно базуватися на тих чи інших протоколів. Особливої уваги потрібно виділити даним протоколам які дають можливість розгорнути віддалений доступ:

- IPsec (Internet Protocol Security);
- Secure Sockets Layer (SSL)/ Transport Layer Security (TLS);
- L2TP (Layer Two Tunneling Protocol);
- PPTP (Point-to-Point Tunneling);
- RDP (Remote Desktop Protocol).

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Протокол IPsec забезпечує автентифікацію та шифрування для передачі пакетних IP-адрес за допомогою декількох протоколів безпеки. SSL та його наступник, TLS, - це протоколи безпеки на основі шифрування Інтернету, які забезпечують конфіденційність, автентифікацію та цілісність даних для Інтернет-комунікацій, захищаючи користувачів. L2TP являє собою протокол без автентифікації та шифрування і найчастіше його використовують в парі з іншим протоколом. Одним із найменш захищених протоколів можна назвати протокол RDP за допомогою якого також реалізують VPN. А протокол RDP використовується лише на ОС Windows та надає доступ до віддалених робочих столів за допомогою служб терміналів Windows. Далі розглянемо деякі із цих протоколів трохи детальніше.

IPsec (Internet Protocol Security) був розроблений, оскільки найпоширеніший протокол Інтернету, IPv4, не має багатьох положень безпеки. Дані, що передаються через IPv4, можуть бути легко перехоплені, змінені або зупинені. Він заповнив цю прогалину, виступаючи як фреймворк, який може автентифікувати з'єднання, а також довести цілісність даних і зробити їх конфіденційними. IPsec - це відкритий стандарт, який діє на рівні мережі. Протокол IPsec може використовуватися для безпечної передачі даних від хосту до хоста, мережі до мережі або між мережею та хостом. Даний протокол був визначений робочою групою IPSEC IETF (Internet Engineering Task Force) та на даний момент в його склад входять приблизно 20 пропозицій по стандартам і 18 документів RFC (Request for Comments).

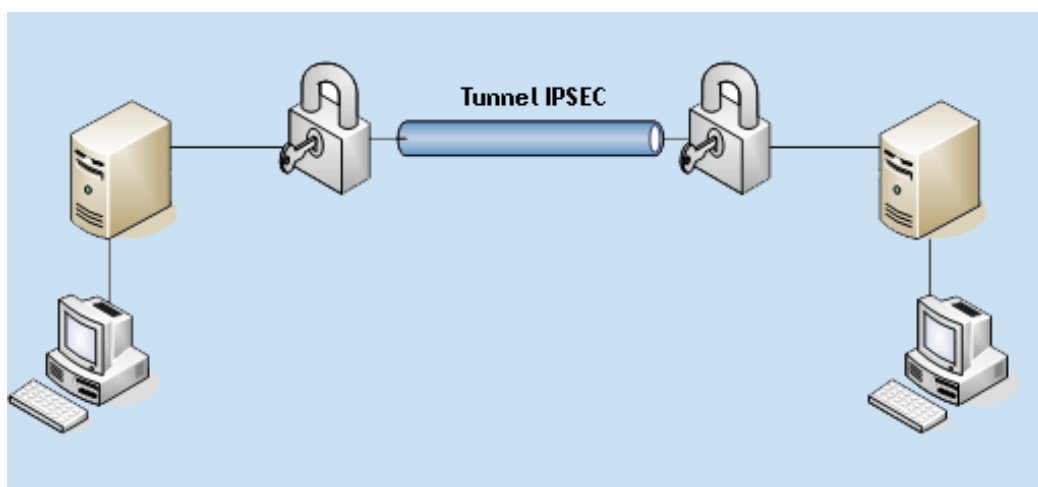


Рисунок 1.1 – приклад роботи IPsec

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

IPsec складається з трьох основних елементів. Перші два - це протоколи Encapsulating Security Payload (ESP) та Authentication Header (AH). Security Associations (SA) являються завершальним аспектом.

Authentication Header (AH) забезпечує аутентифікацію джерела даних, цілісність даних та захист від повторного відтворення. Використовує захищений алгоритм хешування однак протокол AH не забезпечує конфіденційності даних, а це означає, що всі ваші дані надсилаються у відкритому режимі.

Протокол Encapsulating Security Payload (ESP) забезпечує конфіденційність даних, а також додатково забезпечує аутентифікацію походження даних, перевірку цілісності даних та захист від відтворення. Він використовує симетричний алгоритм ключа (наприклад, 3DES-CBC або AES-CBC) для шифрування даних та захищений алгоритм хешування (наприклад, SHA1 або SHA2).

Security Associations (SA) - це набір специфікацій IPsec, які узгоджуються між пристроями, що встановлюють зв'язок IPsec. Ці специфікації включають налаштування типу автентифікації, шифрування та протоколу IPsec, які слід використовувати при встановленні з'єднання IPsec.

Протокол Ipsec надає можливість функціонувати як в транспортному так і тунельному режимі.

У транспортному режимі , як правило, шифрується або аутентифікується лише дані IP-пакету. Маршрутизація недоторкана, оскільки заголовок IP-адреси не модифікується і не шифрується; однак, коли використовується заголовок автентифікації , IP-адреси не можуть бути зміненими, оскільки це завжди призведе до недійсності хеш-значення. Транспортний та прикладний рівні завжди захищені хешем, тому їх неможливо будь-яким чином змінити (наприклад, перекладом номерів портів).

У тунельному режимі весь IP-пакет спочатку зашифровується та автентифікується. Потім він інкапсулюється в новий IP-пакет з новим IP-заголовком. Режим тунелю загалом використовується для створення мереж VPN для зв'язку між мережами (наприклад, між маршрутизаторами для зв'язку сайтів), та зв'язку між пристроями (наприклад, для віддаленого доступу користувача).

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

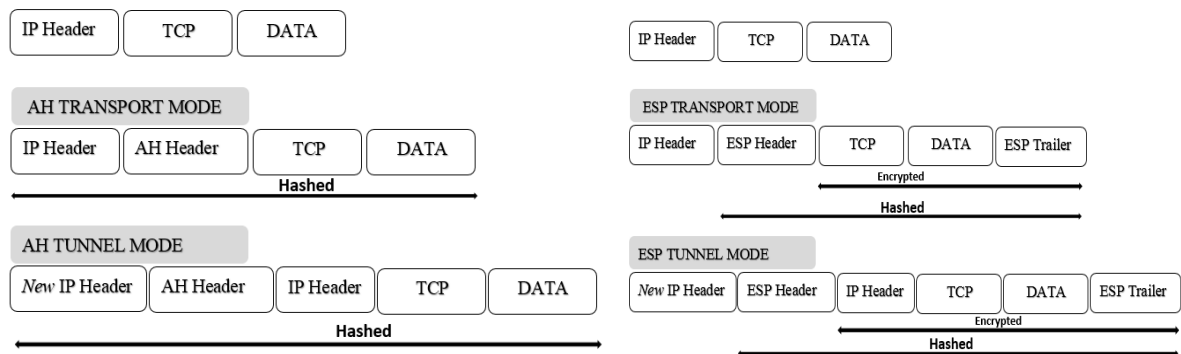


Рисунок 1.2 – приклад роботи протоколів ESP та AH у тунельному та транспортному режимі

SSL/TLS - це протоколи безпеки на основі шифрування Інтернету, які забезпечують конфіденційність, автентифікацію та цілісність даних для Інтернет-комунікацій, захищаючи користувачів від підслуховування або атак типу "man-in-the-middle". SSL та TLS являють собою розвиток одної технології. TLS розробили як наступника протокола SSL, після того як він став інтернет-стандартом. Така зміна зумовлена тим що протокол SSL з самого початку належала компанії Netscape. Сьогодні назви SSL та TLS продовжують використовувати як синоніми.

Принцип роботи SSL/TLS розділяють на два етапа: етап початкового з'єднання (Handshake) і етап передачі даних.

Під час початкового з'єднання дві сторони, які намагаються встановити зв'язок між собою, приймають рішення щодо версії протокола, алгоритму шифрування або набору шифрів, які будуть використані в процесі передачі даних. Виглядає даний етап таким чином:

- Клієнт просить сервер відкрити безпечну лінію, і він відповідає, відображаючи список версій TLS та наборів шифрів, з якими він сумісний. Після того, як вони домовились про загальні для використання параметри, вони починають так зване "рукошлякування".
- Сервер надсилає клієнту копію свого відкритого ключа, прикріпленого до цифрового сертифіката. Клієнт перевіряє цей сертифікат, щоб переконатися, що сервер є легітимним, і якщо все сходиться, продовжує транзакцію.
- Клієнт використовує відкритий ключ сервера та його приватний ключ для шифрування «ключа сеансу», який буде використовуватися двома сторонами для

шифрування та дешифрування інформації в цьому конкретному сеансі. Ключ сеансу стає недійсним, як тільки з'єднання припиняється.

– Обидві сторони перевіряють з'єднання, надсилаючи одне одному зашифровані повідомлення. Якщо інший може розшифрувати їх за допомогою сеансового ключа, з'єднання успішно захищено та починається передача даних.

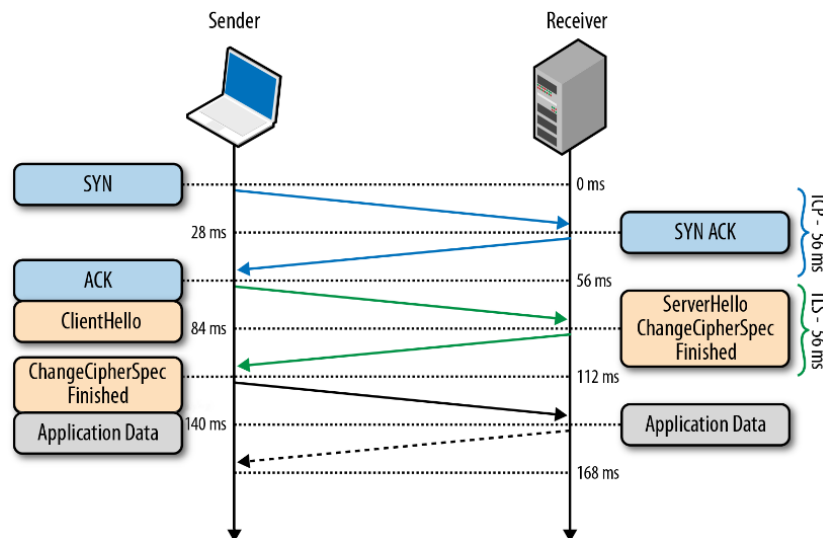


Рисунок 1.3 – етап початкового з'єднання в протоколі SSL

Важливим аспектом цього етапу являється цифрові сертифікати. Загалом, цифрові сертифікати - це цифрові документи, які «підписуються» довіреними органами та виступають як документи власності на відкритий ключ. Як розширення, вони служать для перевірки законності сервера або клієнта. Вони прикріплені до відкритих ключів і є доказом того, що власник відкритого ключа насправді є законним власником. Це пов'язано з тим, що цифрові сертифікати підписуються, продаються та видаються органами, які називаються «Органи сертифікації (Certificate Authorities)», які є довіреними органами, відповідальними за перевірку справжності кожного, хто вимагає сертифікат.

PPTP (Point-to-Point Tunneling) - це набір правил зв'язку, які регулюють безпечну реалізацію віртуальних приватних мереж, які дають організаціям метод розширення власних приватних мереж через загальнодоступний Інтернет за допомогою тунелювання. Даний протокол є наслідником протоколу PPP, та базується на його структурі автентифікації та шифрування. Як і всі технології тунелювання, PPTP інкапсулює пакети даних, створюючи тунель для передачі

даних через IP-мережу. Він використовує TCP-порт 1723 та IP-порт 47 та підтримує до 128-бітових ключів шифрування та стандартів Microsoft Point-to-Point Encryption. Переваги PPTP в тому що його легше налаштувати, він швидкий і вбудований на більшості платформ із-за чого для його використання не потрібно ніякого програмного забезпечення. Для підключення потрібні лише дані облікового запису та адресу сервера. Однак сьогодні замість PPTP рекомендується використовувати більш безпечніші протоколи.

Layer 2 Tunneling Protocol (L2TP) - це розширення протоколу тунельного тунелювання (PPTP), які використовуються постачальником послуг для забезпечення можливості роботи віртуальної приватної мережі (VPN) через Інтернет. Для отримання максимальних переваг його здебільшого поєднують із іншими протоколами. Найчастіше даний протокол використовують із протоколом IPSec, відкриваючи можливість використовувати кращі ключі шифрування(256-бітний AES та 3DES).

Зазвичай L2TP використовує порт TCP 1701 але якщо його використовують із IPSec, він використовує різні порти такі як UDP 500 для обміну ключами Інтернету (IKE) або 4500 для NAT і 1701 для трафіку L2TP.

Тунелювання L2TP починається з встановлення з'єднання між LAC (L2TP Access Concentrator) та LNS (L2TP Network Server) - двома кінцевими точками протоколу - в Інтернеті. Після досягнення цього рівня PPP-посилання підключаються та інкапсулюється, а потім передається. Після підключення PPP ініціює кінцевого користувача разом з провайдером. Як тільки LAC приймає з'єднання, зв'язок PPP встановлюється. Потім призначається вільний слот в мережевому тунелі, а запит передається в LNS. Нарешті, після повного підтвердження автентичності та прийняття зв'язку створюється віртуальний PPP-інтерфейс. На той момент фрейми посилань можуть вільно проходити через тунель. Кадри приймаються LNS, який потім видаляє інкапсуляцію L2TP і обробляє їх як звичайні кадри.

RDP (Remote Desktop Protocol) - це протокол або технічний стандарт для віддаленого використання персонального комп'ютера. Програмне забезпечення

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

для віддаленого робочого столу може використовувати декілька різних протоколів, включаючи RDP, незалежну обчислювальну архітектуру та обчислення віртуальної мережі (VNC), але RDP є найбільш часто використовуваним протоколом. RDP був спочатку випущений Microsoft і доступний для більшості операційних систем Windows, але його також можна використовувати з операційними системами Mac та Linux. Протокол RDP відкриває виділений мережевий канал для передачі даних між підключеними машинами (віддаленим робочим столом і комп'ютером, який зараз використовується). Для цього він завжди використовує мережевий порт 3389. Рухи миші, натискання клавіш, дисплей на робочому столі та всі інші необхідні дані надсилаються по цьому каналу через TCP / IP, що є транспортним протоколом, який використовується для більшості видів Інтернет-трафіку. RDP також шифрує всі дані, так щоб з'єднання через загальнодоступний Інтернет були більш менш безпечними.

RDP має кілька переваг. Однією із переваг є те, що для цього не потрібна VPN. Він також зберігає дані, які надійно зберігаються на робочому столі користувача, замість того, щоб зберігати їх на хмарних серверах або на незахищених персональних пристроях користувача. Крім того, RDP дозволяє компаніям зі застарілою локальною ІТ-установкою надавати можливість своїм співробітникам працювати вдома.

Після розгляду протоколів потрібно розглянути найбільш відомі технології віддаленого доступу. До таких можна віднести такі технології:

- Спільний доступ до робочого столу (Desktop sharing);
- PAM (Privileged Access Management);
- VPAM (Vendor Privileged Access Management);
- VPN.

Технології Desktop sharing складаються із різних програмних додатків або засобів які дозволяють обмінюватися файлами, відео трансляціями тощо. Чудове рішення для вебінарів, конференцій та презентацій і.т.д. Технології ж PAM являють собою альтернативу VPN та використовується як засіб контролю доступу до привілейованих облікових записів в інфраструктурах та використовують для

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

безпечної передачі даних та доступу до інформації із обмеженим доступом. Іншою альтернативою технологій VPN можна назвати VPAM, що являє із себе безпечний спільний доступ до мережі з постачальниками або підрядниками. Може надавати доступ лише до частин сервера. VPN є найпопулярнішою технологія яка надає доступ до віддалених підключень адже використовує захищену і зашифровану мережу створюючи тунель даних між пристроями або серверами. Якщо ж розглядати дані технології окремо то розрочнемо із найбільш відомої серед простих користувачів технологію віддалених робочих столів.

Спільний доступ до робочого столу (Desktop Sharing) – це загальна назва технологій які дозволяють обмінюватися змістом екрана або спільний доступ до файлів, презентацій або програм з іншими працівниками або пристроїв. Сьогодні існує багато додатків, що дають можливість спільного користування на робочому столі, включаючи віддалену підтримку, вебінари та он-лайн конференції з аудіо та візуальним вмістом (обмін презентаціями) та глобальну співпрацю над проектами в режимі реального часу. Так наприклад однією із програм спільного використання робочого столу є віддалений вхід для працівників, яким потрібен доступ до своїх робочих комп'ютерів із будь-якого підключеного до Інтернету пристрою (робочого столу, ноутбука, телефону або планшета). Це дає велику перевагу адже віддалений користувач може запускати програмне забезпечення, яке не встановлено на його комп'ютері, навіть програмне забезпечення, яке не сумісне з його операційною системою або яке вимагає набагато більшої обчислювальної потужності, ніж його комп'ютер зазвичай може обробити. Це тому, що віддалений користувач насправді не запускає програмне забезпечення на своєму комп'ютері, він просто переглядає та контролює робочий стіл (і, отже, програмне забезпечення) головного комп'ютера.

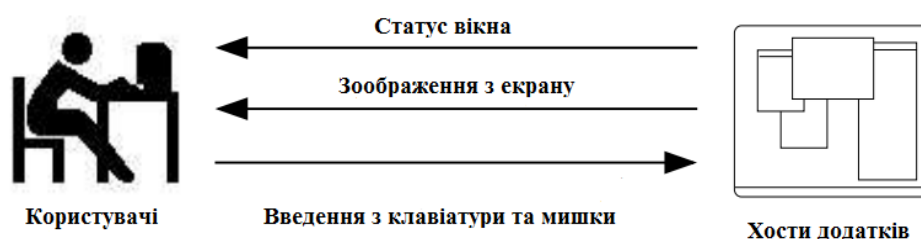


Рисунок 1.4 – приклад роботи спільного доступу до робочого столу

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Віртуальна приватна мережа (Virtual Private Network) являє вона собою одне або декілька мережних з'єднань поверх іншої (наприклад Інтернет) з'єднання якої здійснюються з використанням інформації з Інтернет-протоколів, наприклад IP-адреси, для встановлення зашифрованого тунелю між двома кінцевими точками. Пакети даних передаються через Інтернет за змінним набором маршрутів на основі доступних мережових шляхів до приймального кінця, який повторно збирає пакети у вихідний формат.

Технологія VPN виникла через те, що багато компаній розподілені по всій країні або по всьому світу. Де б не були їх офіси, співробітники, партнери або клієнти, існує потреба у безпечному, швидкому та надійному корпоративному обміні даними. Основна мета VPN - надати компаніям однакові можливості для всіх працівників. Залежно від обраного рішення, компанії виграють від VPN такими способами:

- Географічний зв'язок компаній розширюється при використанні VPN. Це дозволяє компаніям не відставати від національної та глобальної експансії. Неможливо досягти того самого глобального зв'язку при використанні придбаних або орендованих ліній, і навіть якщо зв'язок вдасться досягти, вартість буде величезною. VPN також забезпечують простішу та безпечнішу підтримку телекомунікаторів.

- Безпека не погіршується при використанні мереж VPN, оскільки передані дані зашифровуються або, якщо надсилаються незашифрованими, пересилаються через надійні мережі.

- VPN пропонують кращу масштабованість, більшу чи меншу залежно від обраного рішення. Масштабованість можна розглядати як ще одну форму економії коштів. Чому так? Компанія, що має лише два філії, може з'єднати два офіси лише однією лінією. Але по мірі зростання організації може знадобитися повний зв'язок між різними офісами. Це означає, що кількість орендованих ліній, а загальна вартість, пов'язана з їх розгортанням, зростає в геометричній прогресії. Крім того, якщо компанія хоче масштабуватися в глобальному масштабі, витрати, пов'язані з розгортанням орендованих ліній, будуть ще вищими, якщо можливо навіть досягти

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

того самого глобального зв'язку з орендованими лініями. VPN, що використовують Інтернет, уникають цієї проблеми, просто використовуючи вже наявну інфраструктуру. MPLS (див. Розділ 3.2.4) також вирішує цю проблему, оскільки пропонує будь-яке-будь-яке підключення за нижчою ціною.

- На додаток до економії витрат, VPN збільшують прибуток за рахунок підвищення продуктивності. Покращена продуктивність зумовлена можливістю доступу до ресурсів з будь-якого місця та в будь-який час (тобто можна вести більше бізнесу).

VPN-мережі можна класифікувати на дві великі категорії:

- VPN тунель забезпечує провайдер (Provider Provisioned VPN (PPVPN)) та відповідає за всі оперативні та управлінські завдання постачальника послуг, що надаються VPN.

- Клієнт несе відповідальність за функціонування та функції управління наданими клієнтом VPN (CPVPN). Отже, постачальник мережевих послуг не знає про схеми VPN клієнта, протоколи маршрутизації та адресні простори. VPN обмінюється інформацією лише між CE. Існує два загальновживаних протоколи тунелювання для реалізації CPVPN, а саме IPsec та GRE.

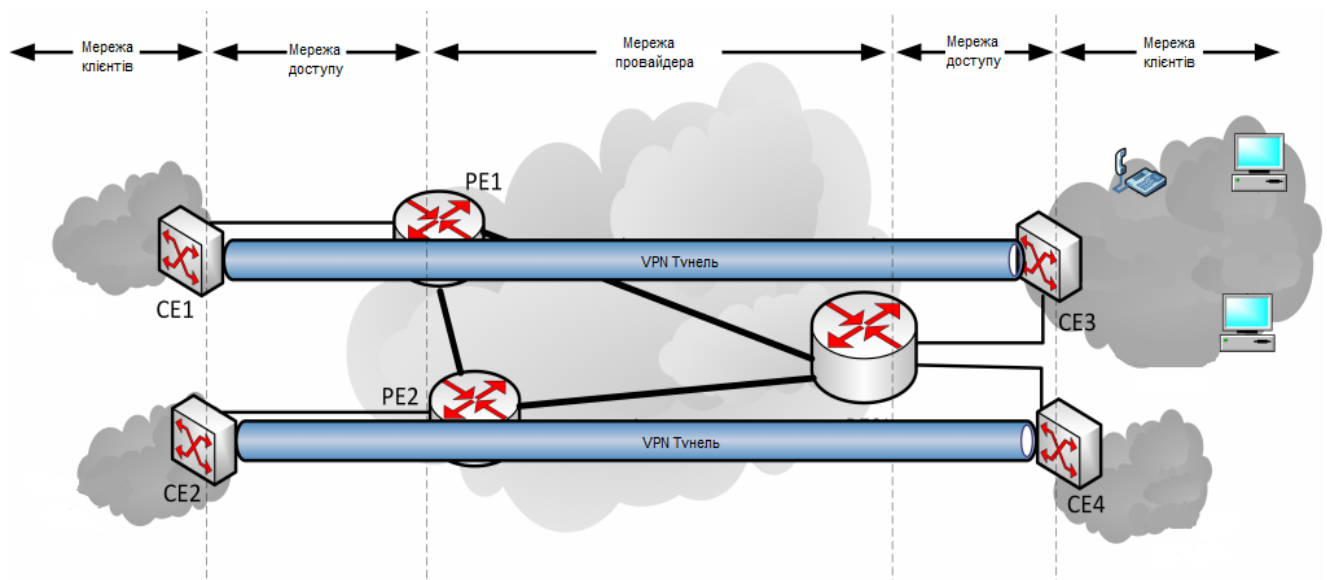


Рисунок 1.5 – приклад CPVPN

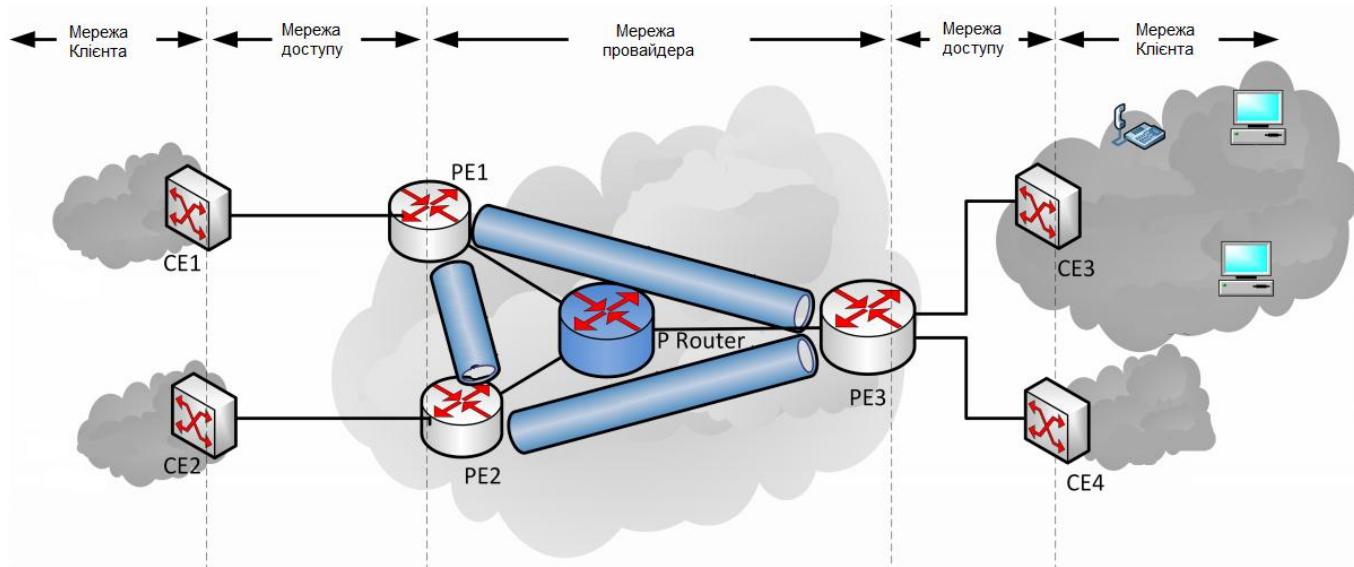


Рисунок 1.6 – приклад PPVPN

В той час як самі технології VPN поділяють на два типи:

- Віддалений доступ (Remote Access VPN)
- Сайт на сайт (Site-to-site)

VPN з віддаленим доступом - це з'єднання користувача з локальною мережею, що використовується компаніями, у яких є співробітники, яким потрібно під'єднатись до своєї приватної мережі з різних віддалених місць (наприклад, будинків, готельних номерів, аеропортів). Оскільки користувачі отримують доступ до мережі через Інтернет, VPN з віддаленим доступом є недорогим рішенням порівняно з комутованим рішенням.

Загалом існує два основних метода реалізації віддаленого доступу до VPN, а саме на основі Secure Sockets Layer (SSL) і на IP Security (IPsec). Тип впровадженого методу VPN базується на вимогах доступу користувачів та ІТ-процесах організації. І технологія VPN з SSL, і технологія VPN з IPsec пропонують доступ практично до будь-яких додатків або мережевих ресурсів.

VPN з SSL пропонують такі функції, як просте підключення до настільних комп'ютерів до мережі, якими не керує компанія, низький рівень обслуговування або відсутність технічного обслуговування настільного програмного забезпечення та веб-порталів, налаштованих користувачем під час входу в систему. Протокол SSL підтримує різні криптографічні алгоритми для таких операцій, як автентифікація сервера та клієнта між собою, передача сертифіката та

налаштування ключа сеансу. Найчастіше дане рішення використовують у Cisco IOS VPN в яких можливо надати віддалений доступ за допомогою програмного забезпечення Cisco AnyConnect та Secure Mobility Client.

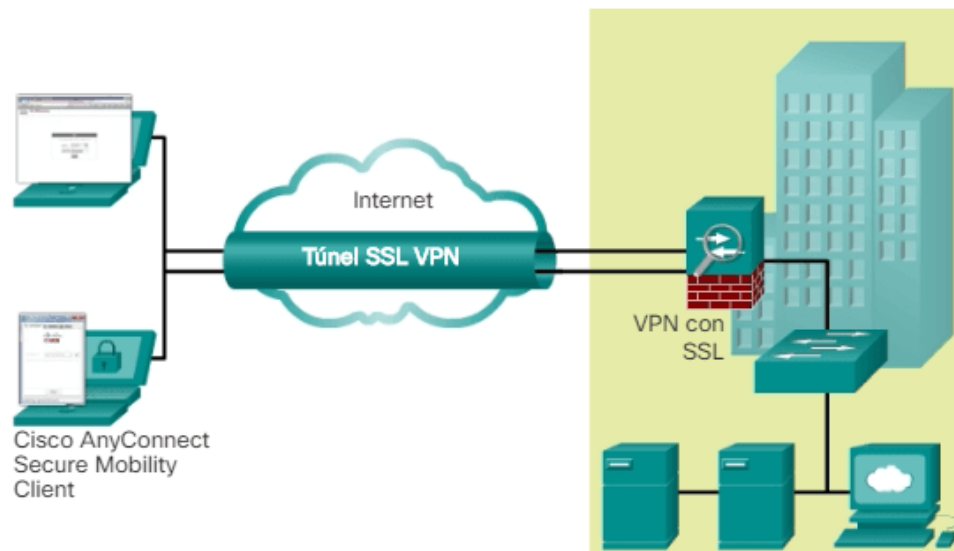


Рисунок 1.7 – метод реалізації SSL VPN

Коли ж VPN реалізуються для віддалених працівників та невеликих філій, простота впровадження є критично важливою, особливо якщо технічні ресурси недоступні для налаштування VPN на віддаленому веб-маршрутизаторі. Використовують рішення VPN-з'єднання віддаленого доступу з IPsec для автентифікації та шифрування даних. Гарним прикладом даного рішення будуть на рішеннях Cisco Easy VPN які пропонує гнучкість, масштабованість та простоту використання для VPN з IPsec віддаленого доступу.



Рисунок 1.8 – метод реалізації Easy VPN

Використовуючи спеціальне обладнання, компанії можуть підключати декілька локальних мереж через загальнодоступну мережу Інтернета, створюючи таким чином VPN від сайту до сайту. Site-to-Site VPN використовуються в

глобальних мережах для підключення локальних мереж окремих філій або офісів без необхідності використання окремого програмного забезпечення VPN на кожному пристрої, створюючи з декількох мереж офісів мережу WAN. Використання VPN від сайту до сайту може мати багато переваг порівняно з традиційним клієнтом VPN.

– Безпека Site-to-Site VPN є найважливішою перевагою, оскільки протоколи IPsec забезпечують шифрування всього трафіку під час транзиту через тунель VPN. VPN-тунель від сайту до сайту дозволяє пропускати трафік лише з одного кінця до іншого, блокуючи будь-які спроби перехопити трафік ззовні. Весь трафік повинен бути підписаний цифровим сертифікатом, а для автентифікації повинна бути розгорнута інфраструктура відкритого ключа (PKI). Обмін ключами Інтернета, який зазвичай асоціюється з протоколом IPsec, не такий сильний, як PKI.

– У порівнянні з Remote Access VPN, основною перевагою Site-to-Site VPN є її масштабованість. Замість того, щоб вимагати, щоб кожна система співробітників працювала на клієнтському програмному забезпеченні VPN, вимагає лише шлюз VPN у кожному місці. Це полегшує додавання нового веб-сайту чи іншого відділення офісу до мережі або переміщення віддаленого офісу чи сайту.

– Якщо організація потребує поліпшення продуктивності, VPN від сайту до сайту можна налаштувати на зниження затримки за допомогою MPLS для маршрутизації трафіку через інфраструктуру постачальника VPN, а не через загальнодоступний Інтернет. Використання MPLS через провайдера VPN також означає меншу роботу IT-співробітників організації, оскільки постачальник буде виконувати більшу частину налаштування та обслуговування. Однак це буде дорожче.

– VPN від сайту до сайту може бути запущений як повністю керована служба провайдером керованих служб безпеки. Таке рішення може бути менш затратним варіантом для менших компаній, які не мають бюджету, щоб інвестувати в продукти безпеки, а персонал управляти ними.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

– Потенційною альтернативою MPLS або IPsec VPN за нижчою ціною є програмно визначена глобальна мережа, хоча SD-WAN може бути більш складною для налаштування без допомоги провайдера.

Перед усім потрібно зауважити, що використання Site-to-Site VPN передбачає використання центральних фізичних місць, де співробітники збираються, оскільки тунель VPN може бути лише між двома статичними місцями. І потрібно розуміти, що для невеликих організацій із відносно невеликою кількістю співробітників, яким потрібен доступ до локальної мережі, традиційні клієнти VPN можуть бути більш економічно вигідним варіантом.

Щоб вийти за межі VPN та спільного використання робочого столу, вам потрібна альтернатива, яка може керувати ідентифікаціями краще та ближче, ніж просто технології IAM, такі як Active Directory. Це особливо стосується привілейованих або адміністраторських облікових записів, які використовуються для багатьох завдань підтримки на рівні підприємства. Для досягнення надійного управління обліковими даними для привілейованих облікових записів було розроблено краще рішення: управління привілейованим доступом РАМ. РАМ - це набір інструментів та технологій, які можна використовувати для захисту, контролю та контролю доступу через привілейовані облікові записи до ресурсів організації. Найефективніші рішення РАМ стосуються кількох областей захисту інформаційної безпеки, таких як вдосконалена безпека облікових даних, системи та контроль доступу до даних, моніторинг активності користувачів. Забезпечення постійного нагляду за цими цільовими областями допомагає зменшити загрозу несанкціонованого доступу до мережі та полегшує ІТ-менеджерам розкриття підозрілої діяльності в мережі. Найкращі практики в РАМ вказують на те, що слід застосовувати протоколи найменших привілеїв, коли користувачі мають доступ лише до певних обмежених ресурсів, які їм потрібні, а не вільне правління, щоб блукати по всій мережі. Крім того, менеджери мереж повинні мати можливість обмежувати або розширювати доступ користувачів за потреби в режимі реального часу. Багато організацій повинні надавати привілейовані облікові записи для двох

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

типів користувачів: внутрішнім користувачам (співробітникам) та зовнішнім користувачам (постачальникам технологій та підрядникам).

Однак організації, які використовують постачальників або підрядників, повинні захищатися від потенційних загроз із цих джерел. Зовнішні користувачі представляють унікальну загрозу, оскільки менеджери мереж не можуть контролювати налаштування безпеки своїх партнерів та постачальників; вони можуть захистити лише від ризикованої поведінки користувачів. Управління привілейованим доступом постачальника (VRAM) відноситься до рішень, що стосуються ризиків, пов'язаних із зовнішніми постачальниками та підрядниками, які є унікальними для сторонніх користувачів віддаленого доступу. Як впливає з назви, VRAM має відношення до RAM, але є ключові відмінності. Традиційні рішення RAM розроблені для управління внутрішніми привілейованими рахунками на основі обґрунтованого припущення, що адміністратори знають особу та статус зайнятості кожної людини, яка отримує доступ до мережі. Однак це не стосується сторонніх користувачів, і тому рішення VRAM використовують багатофакторну автентифікацію, щоб забезпечити додатковий рівень захисту. Загалом, менеджери мереж та адміністратори повинні мати можливість ідентифікувати та аутентифікувати зовнішніх користувачів за допомогою більш досконалих методів VRAM, які можуть підтвердити, що ці користувачі підключені до активних облікових записів співробітників постачальників. Потужне, ефективне рішення VRAM зможе постійно контролювати діяльність користувачів постачальника, використовуючи детальне відстеження, щоб забезпечити оптимальний захист від несанкціонованого використання.

1.3 Засоби організації віддаленого доступу.

Після того як було розглянуто найбільш вживанні протоколи та технології, які базуються навколо них, тепер потрібно розглянути приклади засобів організації віддаленого доступу. Так наприклад одними із самих популярних клієнтів серед технологій спільного доступу до робочого столу можна назвати такі програмні додатки:

- TeamViewer;

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

- Chrome Remote Desktop;
- AnyDesk;
- Remote Utilities;
- UltraVNC;
- AeroAdmin.

Розглянемо дану технологію на прикладі TeamViewer. Головною перевагою даного програмного клієнта є підтримка не тільки платформ Windows, Linux, MacOS, Android але й для деяких IOT платформ. Існують Chrome app плагін та існувала веб версія хоча дана версія потребувала Flash із-за чого на даний момент не є актуальною. Також TeamViewer може працювати без остаточного встановлення, хоча потрібно щоб клієнт працював на двох робочих машинах.

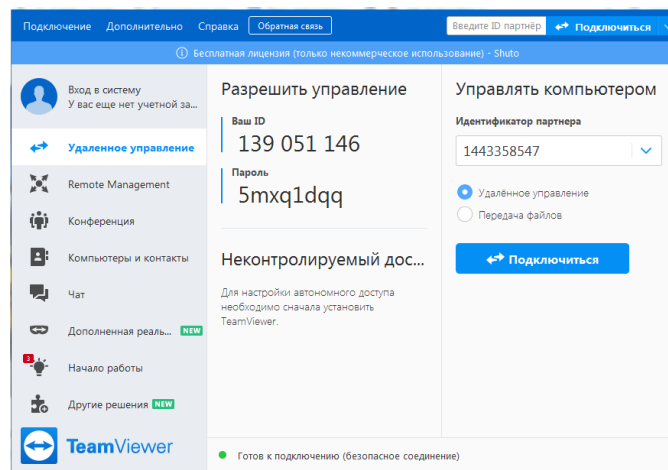


Рисунок 1.9 – головне меню TeamViewer

Хоча даний проєкт рідко використовується в компаніях, загалом якщо і використовують то в компаніях та сервісах тех. Підтримки. Однак даний клієнт отримав підтримку та одобрення від звичайних користувачів для отримання доступу до свого робочого ПК.

В той же час якщо вибрати серед рішень віддаленого підключення через VPN найкращими рішеннями стануть рішення Cisco AnyConnect та OpenVPN.

OpenVPN - реалізація VPN, що використовує протокол SSL/TLS для захисту з'єднань. OpenVPN – рішення VPN з відкритим кодом. Всі хто зацікавлений у використанні OpenVPN можуть використовувати не платячи ні копійки. Окрім офіційної команди , інші розробники можуть запропонувати різні досконалення

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

даного протоколу. Безпеку ж забезпечує 256-бітне шифрування та шифри високого класу (AES, Camellia, 3DES, CAST-128 або Blowfish), а це означає що ваші дані неможливо розшифрувати. Також підтримує безпечний метод шифрування Perfect Forward Secrecy, який допомагає боротися з небезпеками в Інтернеті. Також працює на всіх типах пристроїв і платформ, чим саме OpenVPN підходить як для досвідчених так і для нових користувачів. Оскільки OpenVPN можна використовувати на будь-якому порту, який працює на TCP або UDP, він може пройти через основні обмеження безпеки. Навіть якщо в мережі накладені брандмауери, вона не зможуть заблокувати з'єднання з OpenVPN. Але дане рішення має свої недоліки. Найбільш помітний недолік для адміністраторів серверів адже налаштування є складним і тривалим процесом і якщо не набратися терпіння та зробити все належним чином, результат може стати руйнівною лавиною. Іншим недоліком являється швидкість роботи OpenVPN. Як зазначалось раніше, дане рішення фокусує велику кількість ресурсів на шифруванні та передові методи інкапсуляції даних із-за чого швидкість передачі даних різко падає. Останім же виявленим мною недоліком можна зазначити, що хоч OpenVPN і сумісний з багатьма операційними системами але він не поставляється попередньо встановленим або налаштованим.

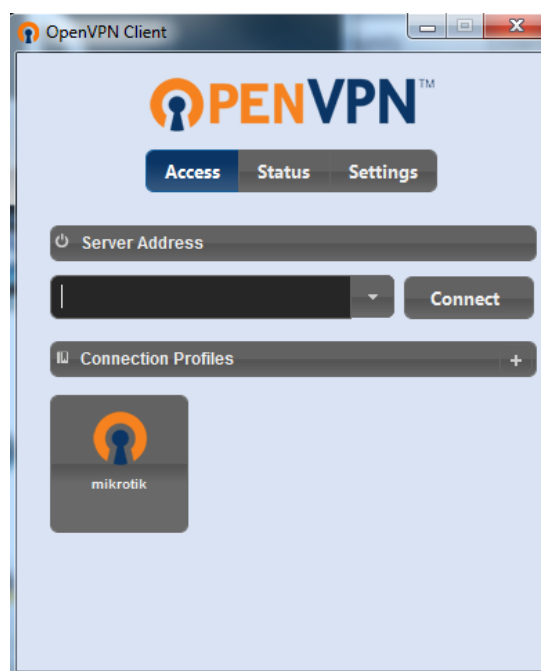


Рисунок 1.10 – клієнт OpenVPN

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Рішення від компанії Cisco Anyconnect VPN пропонує з'єднання не тільки через рівень захищених сокетів SSL та IPsec IKEv2, але й забезпечує покращений захист за допомогою різних унікальних модулів. Так наприклад менеджер доступу Cisco AnyConnect Network Access забезпечує сильні можливості підключення. Він надає суплікант IEEE 802.1X, який може бути наданий як частина можливостей автентифікації, авторизації та обліку (AAA), а також деякі унікальні технології шифрування, такі як MACsec IEEE 802.1AE. Вбудований модуль VPN реалізує веб-безпеку за допомогою локальної мережі Cisco Secure Web Appliance або хмарної мережі Cisco Secure Web. Поєднуючи веб-безпеку з доступом до VPN, адміністратори можуть забезпечити всебічну, безпечну мобільність для всіх кінцевих користувачів, що життєво важливо для розгортання власного пристрою (BYOD). Підприємства мають вибір розгортань для захисту мережі від веб-зловмисного програмного забезпечення та контролю та захисту використання Інтернету. Інша особливість Cisco Umbrella Roaming являє собою хмарну службу безпеки, яка захищає пристрої, коли вони виходять за межі корпоративної мережі. Незалежно від того, вимикають користувачі VPN чи забувають його вмикати, Umbrella Roaming забезпечує захист на рівні DNS для захисту від шкідливого програмного забезпечення, фішингу та зворотних викликів команд і контролю через будь-який порт або протокол. Хоча сервер можна налаштувати лише на пристроях від компанії Cisco таких як: мережні екрани Cisco ASA 5500 та Cisco ASA 5500-X, багатофункціональних захисних пристроях Cisco Firepower, віртуальних мережних екранів Cisco ASAv і Cisco ASAv на AWS та Azure тощо, але підтримує на всіх можливих операційних платформах (Windows, macOS, Linux та мобільних платформ). Також одною із версій ліцензії надає можливість налаштувати безклієнтську SSL VPN яка надає можливість підключати користувачів через веб-інтерфейс.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

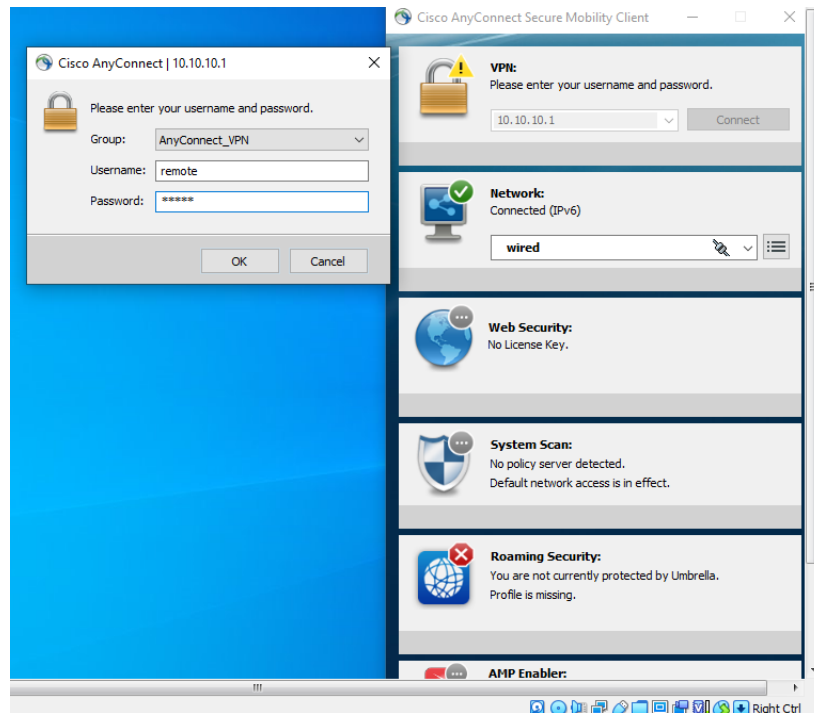


Рисунок 1.11 – клієнт AnyConnect VPN

1.4 Технічне завдання.

Після розгляду теорії можемо зробити певні висновки, а саме те що віддалений доступ дуже широкий термін який включає в себе безліч технологій. Узагальнюючи можна їх охарактеризувати як будь яка технологія що дозволяє уповноваженій особі отримати доступ до комп'ютера або мережі з географічної відстані через мережеве з'єднання та дозволяє користувачам підключатися до необхідних їм систем, коли вони перебувають фізично далеко.

Але найбільш мене зацікавила технологія віддаленого доступу за допомогою віртуальних приватних мереж яка дозволяє захищено підключитися до мережі з будь якої географічної відстані та бути впевненим що ваш трафік не буде розшифрований.

Саме тому головним завданням на цю дипломну роботу буде спроектувати мережу та налаштувати сервер за допомогою технології Remote Access VPN.

Для виконання випускної роботи бакалавра було використано обладнання від компанії Cisco адже на сьогоднішній час вона тримає лідерство на ринку послуг по розгортанню віддаленого доступу за допомогою VPN. Звісно мережна інфраструктура буде спрощена для зручності у використанні та економії ресурсів.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк. 29
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

1.5 Висновки до розділу 1.

Під час написання першого розділу було проведено аналіз теоретичних відомостей які надали характеристики організації віддаленого доступу та зрозуміли на чому в наш час організовується віддалений доступ. Проаналізували основні переваги протоколів на яких на даному моменті працюють технології віддаленого доступу. Також було розглянуто сучасні технології віддаленого доступу та відокремили технології VPN, а саме технології віддаленого доступу через приватні віртуальні мережі Remote Access VPN. Під кінець було розглянуто декілька прикладів засобів віддаленого доступу та було сформовано технічне завдання.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

2.1 Проектування мережної інфраструктури

В комп'ютерних мережах в загалом існує два типи топологій: Фізична та логічна топологія.

Фізична топологія описує спосіб з'єднання комп'ютерів або вузлів між собою в комп'ютерній мережі. Це може бути розташування різних елементів (наприклад вузлів), включаючи розташування пристрою. Іншими словами, ми можемо сказати, що фізична топологія включає в собі розташування вузлів, робочих станцій та кабелів у мережі. Фізична топологія складається із шести типів а саме із:

- топологія шини;
- топологія кільця;
- топологія зірок;
- топологія сітки;
- топологія дерева;
- гібридна топологія.

Логічна топологія описує шлях та потік даних від одного комп'ютера до іншого. Він прив'язаний до мережевого протоколу та визначає, як дані переміщуються по мережі та який шлях вони проходять. Іншими словами, логічна топологія спосіб внутрішнього спілкування пристроїв.

Так як при проектуванні мережі нас не цікавить фізична топологія тому було використано гібридну топологію мережі. Спроектовану мережу можна поділити на дві складові.

- мережа клієнта.
- мережа провайдера.

Мережу клієнтів для зручності розділимо на офіс компанії та віддалених користувачів. Офіс складається із брандмауера, сервера AAA, 3 маршрутизаторів та 5 комутаторів із кінцевим обладнанням (більшість мереж будуть використовувати VPCS для зменшення навантаження на сервер та образ Windows

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

7 для підключення та налаштування брандмауера). А віддалені користувачі складаються із 2 маршрутизаторів та комутаторів із віддаленими обладнанням.

Мережа провайдера складає із себе один маршрутизатор так як тунелювання йде між мережею офіса та віддаленими користувачами і провайдер не знає про схеми VPN їх клієнтів, протоколи маршрутизації і т.д.

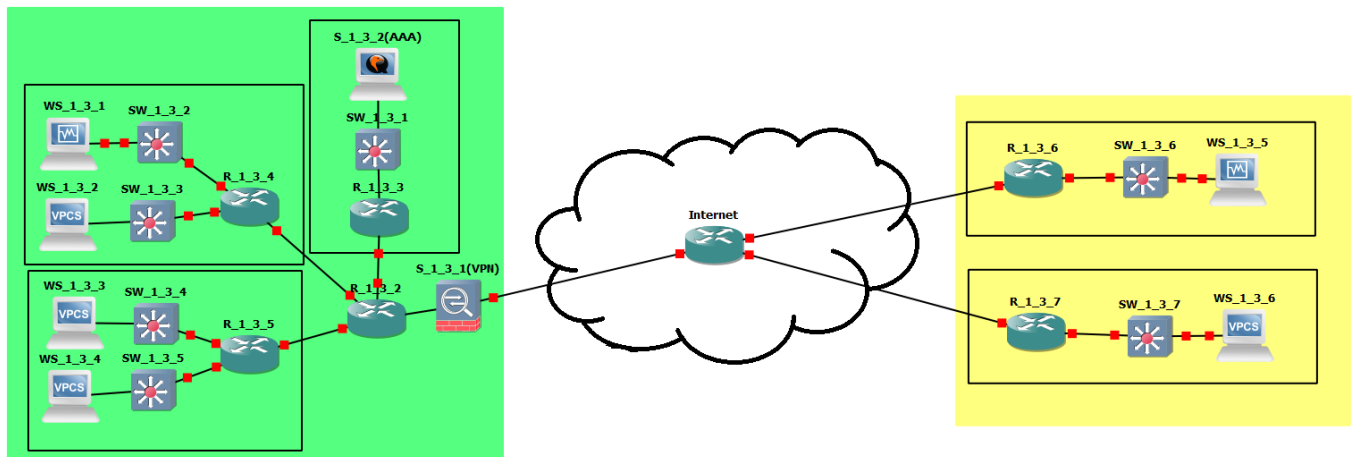


Рисунок 2.1 – топологія мережі.

Загалом використовують маршрутизаторів 4 комутаторів на 16 портів, брандмауера та сервера AAA. Проект складаються із 9 підмереж.

Розглянемо кожну підмережу. Підмережа А та В складається із двох комутаторів SW_1_3_2 та SW_1_3_3 по 16 портів які підключені до маршрутизатора R_1_3_4 та по 10 ПК.

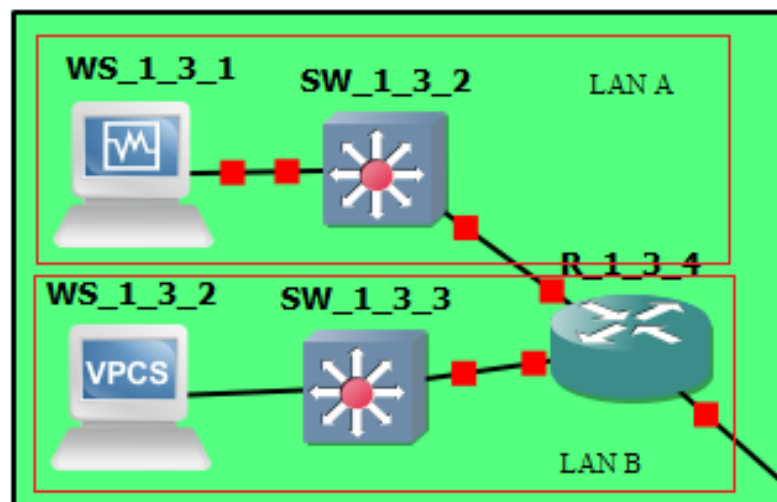


Рисунок 2.2 – підмережа А та В.

Наступні підмережі C та D ідентичні минулих підмереж але комутатори SW_1_3_4 та SW_1_3_5 мають 24 порта кожний та підключені до маршрутизатора R_1_3_5. Підмережі мають 18 та 20 ПК.

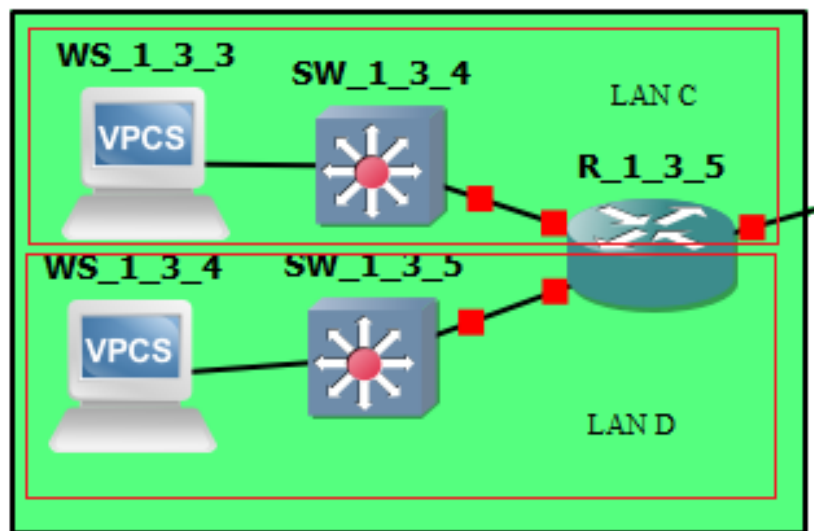


Рисунок 2.3 – підмережа C та D.

Підмережа E складається із комутатора SW_1_3_1 який підключений до маршрутизатора R_1_3_3 на 12 портів та сервер S_1_3_2(AAA). Така кількість портів зумовлена майбутнім розширенням серверної інфраструктури у майбутньому.

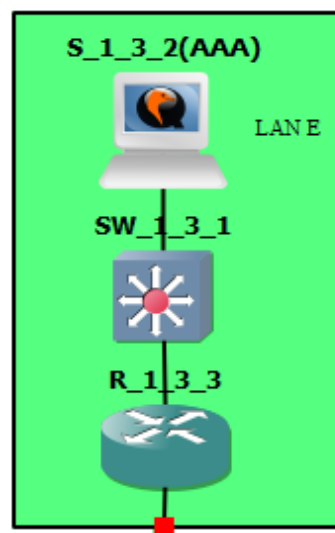


Рисунок 2.4 – підмережа E.

Підмережа L та G мають по 2 комутатора на 24 порта порта та маршрутизатору та кінцеве обладнання із 40 ПК.

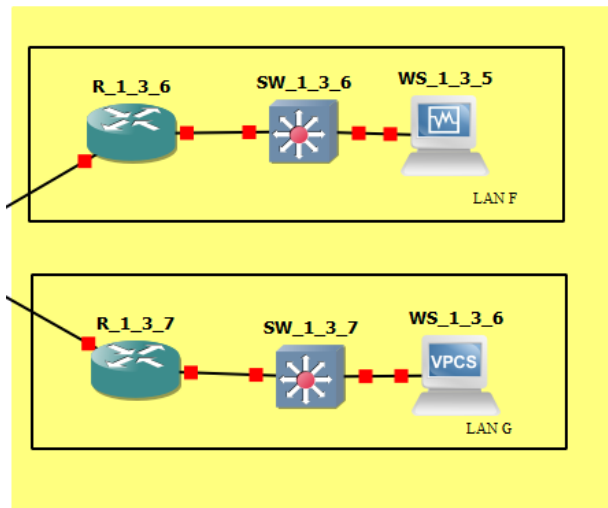


Рисунок 2.5 – підмережа F та G.

Для мережі провайдера та між підключенням брандмауера та маршрутизаторами IP адреси були розподілені таким чином щоб використати мінімальну кількість адрес.

S_1_4_1(VPN) – Internet – 10.132.16.0 /30

S_1_4_1(VPN) – R_1_3_2 – 10.132.17.0 /30

R_1_3_2 – R_1_3_4 – 10.133.17.0 /30

R_1_3_2 – R_1_3_5 – 10.134.17.0 /30

R_1_3_2 – R_1_3_3 – 10.135.17.0 /30

Internet – R_1_3_6 – 11.134.16.0 /30

Internet – R_1_3_7 – 12.133.16.0 /30

Розрахунок IP адрес для підмереж наведені у наступній таблиці

Таблиця 2.1 – Адресація підмереж

Підмережа	IP-адреса	Маска мережі	Шлюз по замовчуванню	Діапазон адрес комутаторів	Діапазон адрес ПК	Діапазон вільних адрес
Підмережа А	192.162.13.0	255.255.255.224	192.162.13.1	192.162.13.2	192.162.13.3-192.162.13.14	192.162.13.15-192.162.13.30
Підмережа В	192.162.14.0	255.255.255.224	192.162.14.1	192.162.14.2	192.162.14.3-192.162.14.14	192.162.14.15-192.162.14.30
Підмережа С	192.162.15.0	255.255.255.224	192.162.15.1	192.162.15.2	192.162.15.3-192.162.15.14	192.162.15.15-192.162.15.30
Підмережа D	192.162.16.0	255.255.255.224	192.162.16.1	192.162.16.2	192.162.16.3-192.162.16.14	192.162.16.15-192.162.16.30
Підмережа Е	192.162.17.0	255.255.255.224	192.162.17.1	192.162.17.2	192.162.17.3-192.162.17.14	192.162.17.15-192.162.17.30
Підмережа F	192.162.18.0	255.255.255.224	192.162.18.1	192.162.18.2	192.162.18.3-192.162.18.14	192.162.18.15-192.162.18.30
Підмережа G	192.162.19.0	255.255.255.224	192.162.19.1	192.162.19.2	192.162.19.3-192.162.19.14	192.162.19.15-192.162.19.30

Таблиця 2.2 - Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Маршрутизатор Internet	Fa 0/0	10.132.16.2	255.255.255.252	/30
	Fa 1/0	10.134.16.1	255.255.255.252	/30
	Fa 2/0	10.133.16.1	255.255.255.252	/30
Брандмауер S_1_3_1(ServVPN)	Gi 0/0	10.132.16.1	255.255.255.252	/30
	Gi 0/1	10.132.17.1	255.255.255.252	/30
Маршрутизатор R_1_3_2	Fa 0/0	10.132.17.2	255.255.255.252	/30
	Fa 0/1	10.135.17.1	255.255.255.252	/30
	Fa 1/0	10.133.17.1	255.255.255.252	/30
	Fa 2/0	10.134.17.1	255.255.255.252	/30
Маршрутизатор R_1_3_3	Fa 0/0	10.135.17.2	255.255.255.252	/30
	Fa 0/1	192.162.17.1	255.255.255.224	/27
Маршрутизатор R_1_3_4	Fa 0/0	10.133.17.2	255.255.255.252	/30
	Fa 1/0	192.162.13.1	255.255.255.224	/27
	Fa 2/0	192.162.14.1	255.255.255.224	/27
Маршрутизатор R_1_3_5	Fa 0/0	10.135.17.2	255.255.255.252	/30
	Fa 1/0	192.162.15.1	255.255.255.224	/27
	Fa 2/0	192.162.16.1	255.255.255.224	/27
Маршрутизатор R_1_3_6	Fa 0/0	10.134.16.2	255.255.255.252	/30
	Fa 1/0	192.162.18.1	255.255.255.224	/27
Маршрутизатор R_1_3_7	Fa 0/0	10.133.16.2	255.255.255.252	/30
	Fa 0/1	192.162.15.1	255.255.255.224	/27
Комутатор SW_1_3_1	Мережний адаптер	192.162.17.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.17.1	-	
Комутатор SW_1_3_2	Мережний адаптер	192.162.13.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.13.1	-	
Комутатор SW_1_3_3	Мережний адаптер	192.162.14.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.14.1	-	
Комутатор SW_1_3_4	Мережний адаптер	192.162.15.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.15.1	-	

Продовження до таблиці 2.2

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Комутатор SW_1_3_5	Мережний адаптер	192.162.16.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.16.1	-	
Комутатор SW_1_3_6	Мережний адаптер	192.162.18.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.18.1	-	
Комутатор SW_1_3_7	Мережний адаптер	192.162.19.2	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.19.1	-	
Сервер S_1_3_2(AAA)	Мережний адаптер	192.162.17.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.17.1	-	
Робоча станція WS_1_3_1	Мережний адаптер	192.162.13.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.13.1	-	
Робоча станція WS_1_3_2	Мережний адаптер	192.162.14.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.14.1	-	
Робоча станція WS_1_3_3	Мережний адаптер	192.162.15.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.15.1	-	
Робоча станція WS_1_3_4	Мережний адаптер	192.162.16.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.16.1	-	
Робоча станція WS_1_3_5	Мережний адаптер	192.162.18.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.18.1	-	
Робоча станція WS_1_3_6	Мережний адаптер	192.162.19.3	255.255.255.224	/27
	Шлюз за замовчуванням	192.162.19.1	-	

2.2 Проектування серверної інфраструктури.

Після того як було продумано та спроектовано мережну інфраструктуру потрібно розглянути важливу складову проекту, а саме VPN сервер. Так як сервер VPN буде розташований на міємережному екрані від компанії Cisco, то вибір буде на технології яку ця компанія розробила, а саме Anyconnect VPN. Дане рішення має можливість розгорнути VPN сервер на базі протоколу SSL (TLS та DTLS) або IPsec IKEv2. Нажаль працездатність Anyconnect VPN буде урізаною із за того що образ використаний не має ліцензію, але дає можливість розглянути основи налаштування Remote Access VPN.

Для того щоб полегшити налаштування сервера було вирішено встановити на образ сервера диспетчер пристроїв адаптивного захисту (Adaptive Security Device Manager (ASDM)), який дозволить керувати брандмауером з допомогою локального веб-інтерфейсу. ASDM надає можливість налаштовувати та керувати обладнання, переглядати журнали та панелі моніторингу в реальному часі, що дозволить оглядати стан та роботи пристрою брандмауера, функції усунення несправності. В більшості нових версіях образів брандмауерів від Cisco диспетчер вже встановлений.

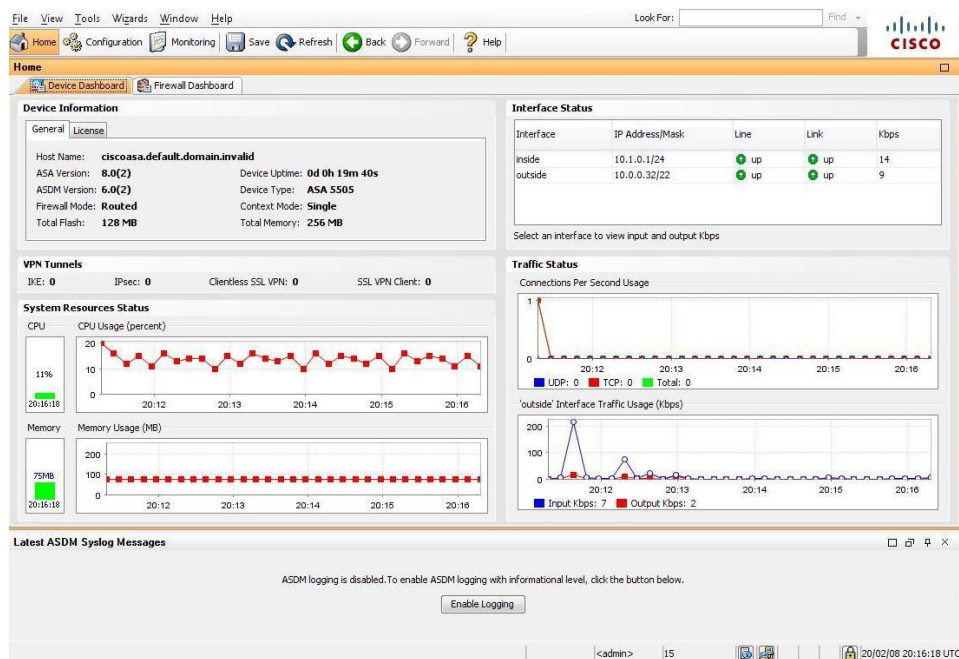


Рисунок 2.6 – Голоане меню ASDM.

Також для того щоб зменшити навантаження на сервер VPN, та для зручності в роботі вирішено використати сервер для обробки запитів користувачів на доступ

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк. 37
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

до комп'ютерних ресурсів і до підприємства забезпечуючи послуги автентифікації, авторизації та обліку користувачів (authentication, authorization, and accounting (AAA)). Серед наявних серверів AAA можна вибрати TACACS+ або RADIUS. Порівняння між службами наведена в таблиці. Система контролю доступу термінального контролера доступу (Terminal Access Controller Access Control System) TACACS+ - власний протокол Cisco, а служба віддаленого доступу RADIUS (Remote Authentication in Dial-In User Service) – відкритий стандартний протокол. Більш детальні порівняння наведені в таблиці.

Таблиця 2.3 – Порівняння TACACS+ та RADIUS

TACACS+	RADIUS
Використовує TCP як протокол передачі	Використовує UDP для передачі даних.
Використовує TCP-порт номер 49.	використовує UDP-порт номер 1812 для автентифікації та авторизації та 1813 для обліку.
Усі пакети AAA зашифровані.	Лише пароль шифрується, тоді як інша інформація, така як ім'я користувача, облікова інформація тощо, не шифрується.
Надає більше налаштування, які можна виконувати на сервері доступу.	Ускладнює розмежування понять аутентифікації і авторизації.
TACACS + пропонує підтримку мультипротоколів	Немає підтримки мультипротоколів.
Використовується для адміністрування пристрою.	використовується для доступу до мережі
Усі пакети AAA зашифровані.	Лише пароль шифрується, тоді як інша інформація, така як ім'я користувача, облікова інформація тощо, не шифрується.

Звідси можна зрозуміти, що TACACS + кращий вибір для нашого проекту.

2.3 Засоби віддаленого доступу кінця вузлів.

Оскільки VPN сервером ми використовуємо Anyconnect VPN клієнт та будемо використовувати для даного рішення. Клієнт Anyconnect VPN являє собою

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

нащадком Cisco VPN Client. AnyConnect пропонує для своїх користувачів не тратити лишній час на пошук клієнта для його встановлення або для оновлення бо при підключення до VPN- шлюза автоматично скачується та оновлюється до потрібної версії як Windows, Linux так і на macOS, що надає можливість розгорнути VPN-мережу на особистих пристроях працівників що працюють віддалено від офісу компанії. Мобільні користувачі також мають можливість скачати Cisco AnyConnect із Apple AppStore або Google Play.

Також однією із цікавих функцій в AnyConnect є Always-On VPN, яка запобігає прямий доступ до Інтернету, якщо користувач знаходиться в довірєній мережі (інфраструктура компанії). Якщо користувач знаходиться в корпоративній мережі, VPN автоматично відключається, а коли користувач працює з дому (покидає довірєну мережу) VPN знову підключає вас до захищеного тунелю. До речі дана функція працює прозоро і непомітно для користувача. Іншою зручною функцією можна назвати split tunneling, яка надає можливість шифрувати трафік до інфраструктури офісу і робочих хмар, а трафік до інших ресурсів (соц. мережі) будуть йти без захисту з боку AnyConnect. Дана функція надає можливість розділити особисте та службове життя, адже не всі компанії мають змогу забезпечити своїх працівників службовою технікою коли вони працюють віддалено.

2.4 Висновки до розділу 2.

В другому розділі було спроектовано мережну інфраструктуру де ми розробили топологію мережі та розглянули кожен з підмереж та розробили загальну адресацію мережі. Також було спроектовано серверну інфраструктуру віддаленого доступу в якій вибрали рішення для розгортання сервера Remote Access VPN а саме рішення від компанії Cisco AnyConnect VPN. Також розглянули та вибрали протокол на якому буде розгорнутий сервер AAA. Вибраний протокол був TACACS+. І в останньому підрозділі вибрали клієнт віддаленого доступу Cisco AnyConnect Secure Mobility Client розглянули його особливості.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

3.1 Вибір компонентів серверної складової системи.

Як і розбиралось раніше VPN сервер має бути розташованим на продукції від компанії Cisco адже AnyConnect VPN являється їхнією продукцією та може розгортатися тільки на їх продукції.

Компанія Cisco пропонує безліч рішень VPN з віддаленим доступом на маршрутизаторах серії Cisco ASA 5500, маршрутизаторах інтегрованих служб Cisco та маршрутизатори служб агрегування Cisco ASR 1000. Нажаль більшість цих рішень не включають клієнтського доступу через Інтернет та повний доступ до мережі без попередньо встановленого програмного забезпечення для настільних мереж VPN, але забезпечують захищений від загроз VPN для захисту від зловмисного програмного забезпечення та хакерів, а також рішення VPN на основі SSL та IPsec. Крім того, інноваційні можливості автоматичного оновлення Cisco AnyConnect та AnyConnect Secure Mobility Client, що містяться у рішеннях VPN з віддаленим доступом та забезпечують унікальну масштабованість, економічну ефективність та простоту в управлінні архітектури віддаленого доступу VPN. Завдяки фундаменту динамічного розподілу політик та невимушеного забезпечення, функції автоматичного оновлення Cisco AnyConnect та AnyConnect Secure Mobility Client дозволяють легко підтримувати конфігурації віддалених пристроїв та клієнтів VPN, як правило, необхідні для рішень VPN з віддаленим доступом SSL або IPsec.

Таблиця 3.1 - Порівняння обладнання від компанії Cisco

	Site-to-Site VPN	IPsec Remote-Access VPN	SSL Remote -Access VPN
Маршрутизатори Cisco\ Комутатори Cisco Catalyst	Найбільш функціональний	Підтримує	Підтримує(лише на маршрутизаторах)
Серія Cisco ASR 1000	Найбільш функціональний	Підтримує	Не підтримує
Серія Cisco ASA 5500	Підтримує	Найбільш функціональний	Найбільш функціональний

За даними табл. 3.1 видно що обладнання серії Cisco ASA 5500 найкраще зарекомендувало для розгортання VPN з відаленим доступом. Саме тому розглянемо особливості цієї серії та виберемо найкращу модель.

Універсальні адаптивні пристрої захисту Cisco ASA серії 5500 забезпечують захист корпоративного класу та надають можливість підключити VPN для малого, середнього бізнесу та великих корпоративних мереж у модульному спеціальному пристрої. Серія Cisco ASA 5500 поєднує в собі широкий спектр інтегрованих служб безпеки, включаючи міжмережний екран, систему запобігання вторгненню (IPS) та послуги Anti-X із службами SSL та IPsec VPN та є простою в розгортанні високопродуктивних рішень. Завдяки інтеграції VPN та служб безпеки, серія Cisco ASA 5500 захищає розгортання VPN від того, щоб стати каналом для мережових атак, таких як хробаки, віруси, шкідливе програмне забезпечення. Детальна політика застосування та контролю доступу застосовується до трафіку VPN, тому законні користувачі мають доступ до послуг та ресурсів.



Рисунок 3.1 – Каталог адаптивних пристроїв захисту Cisco ASA серії 5500.

Серія Cisco ASA 5500 - це найкраще рішення Cisco для віддаленого доступу на основі SSL та IPsec, що підтримує надійне зв'язок. Серія забезпечує вищу масштабованість і більші можливості пропускну здатності, ніж широко розгорнуті концентратори серії Cisco VPN 3000, завдяки чому дане рішення на сьогоднішній день було замінено на рішення від серії ASA 5500.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Таблиця 3.2 - Порівняння обладнання від компанії Cisco

Модель	Масштабованість SSL / IPsec	Максимальна пропускна здатність VPN
Cisco ASA 5505	25 одночасних з'єднань VPN	100 Mbps
Cisco ASA 5510	250 одночасних з'єднань VPN	170 Mbps
Cisco ASA 5520	750 одночасних з'єднань VPN	225 Mbps
Cisco ASA 5540	2500/5000 одночасних з'єднань VPN	325 Mbps
Cisco ASA 5550	5000 одночасних з'єднань VPN	425 Mbps
Cisco ASA 5580-20 and 5580-40	10,000 одночасних з'єднань VPN	1 Gbps

Перевагами серії Cisco ASA 5500 включають:

- Гнучка платформа яка надає IPsec та SSL VPN на одній платформі та виключає неефективність на додаткові витрати на розгортання окремих платформах.
- Покращений безклієнтський мережевий доступ. Безклієнтський віддалений доступ на основі SSL VPN не вимагає програмного забезпечення для настільних клієнтів. Покращені можливості допомагають забезпечити надійну візуалізацію складних програм або веб-сторінок із вмістом Java, JavaScript та ActiveX.
- Розширений повний доступ до мережі на основі клієнта. Налаштоване з'єднання забезпечується за допомогою динамічно завантажуваного клієнта Cisco SSL VPN або клієнта AnyConnect Secure Mobility Client. Для розгортання IPsec та SSL AnyConnect VPN динамічно передає найновіші політики безпеки VPN до віддалених пристроїв та клієнтів VPN, забезпечуючи гнучкість, масштабованість та простоту використання.
- Еластична кластеризація яка надає можливість у розгортанні віддаленого доступу масштабуватись економічно та рівномірно розподіляючи сесії VPN між усіма пристроями Cisco ASA 5500 без втручання користувача або зовнішнього обладнання для балансування навантаження. Ця надзвичайно еластична можливість усуває будь-яку точку відмови і допомагає захистити мережні інвестиції.

– Не захищений VPN є основним джерелом доступу шкідливих програм, таких як хробаки, віруси, шпигунське програмне забезпечення, кейлоггери, троянські коні та руткіти, до мереж організацій. Функції глибокого запобігання вторгненню Cisco ASA 5500, антивірусні програми, брандмауер, що захищає додатки, та має можливість захисту кінцевих точок VPN допомагають гарантувати, що з'єднання VPN не стануть каналом для загроз безпеці.

Після розгляду обладнання зрозуміло, що найкращим рішенням буде модель Cisco ASA5580, а точніше ASA5580-20-4GE-K9 яку можна назвати титаном по розгортанню VPN з відаленим підключенням. Детальні характеристики даної моделі будуть наведені у додатках.



Рисунок 3.2 – Cisco ASA5580-20-4GE-K9.

Далі розберемо з вибором сервера автентифікації, авторизації та обліку користувачів. Так як ми вибрали щосервера AAA буде працювати на протоколі TACACS+ тому найкращим вибором стане проект TacsacsGUI. Даний проект розповсюджується із відкритим кодом та створений для підтримки AAA, для різних типів та пристроїв. Він включає різні бібліотеки, плагіни які розповсюджуються відкрито та ядро проекту демон TACACS+ який створений Марком Хубеном . Загалом TacsacsGUI молодий проект, який швидко набрав популярності із за потужного інструменталу для управління різними типами пристроїв. Ось кілька функцій які вже були реалізовані:

– Підтримка LDAP (Windows AD та OpenLDAP). Це потужна функція, яка може допомогти компаніям використовувати локальну базу даних користувачів,

яка зберігається в Active Directory. Більше того, дана функція надає можливість використовувати групу Active Directory для фільтрації доступу користувачів до пристроїв.

- Підтримка автентифікації одноразового пароля (ОТР) яка являє собою заміну дорогого способу аутентифікації користувачів за допомогою маркера. Тепер користувач може використовувати власний мобільний пристрій для генерації ОТР. Перевага цього рішення полягає в тому, що пароль не зберігається, і він змінюється кожні хвилини або менше. Рішення на основане на стандарті RFC 4226.

- Підтримує список контролю доступу яка допомагає легко обмежити доступ до пристрою для користувача чи групи.

- Повна реєстрація AAA, що являє собою базу даних усіх подій, які користувач надіслав на сервер. Коли користувач аутентифікувався або налаштовував то записує та зберігає, яку команду виконував користувач тощо.

Так як TascacsGUI розроблений під операційну систему Ubuntu та не підтримує інші ОС Linux то використаємо образ Ubuntu 18.04. Також було вирішено використати даний проект як сервер AAA із за того що дає змогу легко налаштовуватися за допомогою веб-браузера і не потрібно гратися із конфігураціями файлів адже всі налаштування із веб-браузера переносяться до файлів конфігурацій що дає змогу менше тратити час на налаштування та запобігає зменшення помилок під час налаштуванні.

3.2 Налагодження віддаленого доступу.

Перетим як розпочати проектування мережної інфраструктури потрібно розібратися на чому буде розроблятися наша мережа. Так як довілі важко отримати доступ до реального обладнання через всім відому ситуацію у світі, через це логічним вибором стане вибір програмного забезпечення яке надасть можливість симулювати роботу мережної інфраструктури.

Одним із таких рішень є програмний додаток GNS3. Graphical Network Simulator - графічний емулятор мережі який дозволяє створювати різноманітні мережні топології прямо на робочій станції. Найчастіше його використовують як

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

лабораторний стенд на якому можна перевірити технології та схеми конфігурування для подальшого перенесення його на реальну топологію. Хоча варто зазначити що GNS3 скоріше не симулятор, емулятор. Адже емулятор дозволяє створити модель обладнання і запускати в середині програмного забезпечення. Емолюється все починаючи від процесора, пам'ятті та пристроями вводу виводу інформації. Наприкладі Cisco, емулятор створює модель маршрутизатора та запускає всередині операційну систему Cisci IOS. Таким чином ми отримуємо повноцінний образ обладнання. В той час як симулятор імітує поведінку системи і її інтерфейса як це робиться в Cisco Packet Tracer.

Якщо мова йде про переваги GNS3 то ось кілька переваг які я отримав під час використання даного продукту.

- Перша і напевно найголовніша перевага так це повний функціонал емульованого пристроїв. Тобто запустивши даний маршрутизатор, нам будуть доступні всі функції, які працюють на реальному маршрутизаторі. В той час якщо говорити про Cisco Packet Tracer, то там більшість функціоналу банально недоступна, тому що це всього лише симулятор і не більше.

- Можливість побудови гетерогенних мереж. Мається на увазі, що ми можемо зібрати схему де будуть не тільки пристрої Cisco, а й Juniper, Mikrotik, CheckPoint тощо. Адже рідко зустрінеш організацію, де вся мережа побудована на обладнанні одного виробника.

- Можливість додавати до мережі повноцінні робочі станції і серверів. В Cisco Packet Tracer, в якості кінцевих пристроїв були доступні клієнтські комп'ютери або сервери з дуже обмеженим функціоналом. У GNS3 ми можемо додати повноцінний ПК з Windows 10 або Ubuntu. Чи можемо використовувати в схемі Windows Server або RedHat. Робиться це за допомогою технологій віртуалізації (VirtualBox або VMWare) або підключивши GNS3 до реальної мережі. Таким чином ми можемо перевірити в лабораторній роботі установку VPN клієнта на робочу станцію, аутентифікацію користувачів через сервер AAA, використовувати справжній браузер при підключенні до цього Інтернету і так далі.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Але якщо говорити про недоліки то їх також хватає особливо зверну увагу на такі недоліки:

– Один із важливий недоліків так це дуже високі вимоги до системних ресурсів. Хоча це не проблема GNS3, а проблема в тому , що запускаються в ньому пристроїв, які використовують дуже багато ресурсів. GNS3 на відміну від Cisco Packet Tracer працює з реальними прошивками пристроїв. Для прикладу, щоб запустити Cisco ASA вам потрібно мінімум 2Гб оперативної пам'яті. А якщо ви хочете зібрати кластер? А якщо в схемі ще присутній Cisco IPS, який теж використовує близько 1Гб? А якщо потрібно додати в топологію ще пару серверів. Обіцяю що з використанням цих образів в своїй топології ви не обійдетеся однією чашкою чаю або кави. На сьогоднішній день, мінімальні системні вимоги для GNS3 це 8Гб оперативної пам'яті. Але краще мати хоча б 16, якщо ви плануєте збирати більш менш масштабні схеми.

– Іншим недолік який добавить вам пару сивих волос так це безліч багів або глюків. У GNS3 їх досить багато. Причому зараз почастишали релізи нових версій GNS3 і, якщо чесно, це навіть трохи дратує. Так ось майже кожен реліз несе новий баг. Старі баги звичайно теж виправляють але всі ми знаємо що один виправлений баг додає десяток нових.

Далі перейдемо до налаштування мережної інфраструктури. Налаштуємо адресацію та веб-інтерфейс для доступу до Cisco ASA. Адресація буде аналогічної по всій мережі тому немає сенсу показувати налаштування на кожному обладнанні. Після того як було налаштовано мережна інфраструктура розпочнемо конфігурувати серверну складову проекту. Для початку нам буде потрібно завантажити на наш брандмауер образ VPN клієнта для цього підключаємося до однієї із робочих станцій із запущеним програмним додатком TFTPd32.exe та виконуємо наступні налаштування.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```

ServerVPN(config)# int g0/0
ServerVPN(config-if)# ip add 10.132.16.1 255.255.255.252
ServerVPN(config-if)# nameif outside
ServerVPN(config-if)# no shut
ServerVPN(config-if)# int g0/1
ServerVPN(config-if)# ip add 10.132.17.1 255.255.255.252
ServerVPN(config-if)# nameif inside
ServerVPN(config-if)# no shut
ServerVPN(config-if)# ex
ServerVPN(config)# router eigrp 1
ServerVPN(config-router)# network 10.132.17.0
ServerVPN(config-router)# network 10.132.16.0
ServerVPN(config-router)# ex
ServerVPN(config)# object network INSIDE-NET
ServerVPN(config-network-object)# subnet 10.132.17.0 255.255.255.252
ServerVPN(config-network-object)# nat (inside,outside) dynamic interface
ServerVPN(config-network-object)# ex
ServerVPN(config)# policy-map global_policy
ServerVPN(config-pmap)# class inspection_default
ServerVPN(config-pmap-c)# inspect icmp
ServerVPN(config-pmap-c)# username admin password cisco privilege 15
ServerVPN(config)# http server enable
ServerVPN(config)# http 192.162.13.0 255.255.255.224 inside

```

Рисунок 3.3 – Приклад налаштування адресації та веб-інтерфейса

```

ciscoasa# copy tftp: disk0

Address or name of remote host []? 192.162.13.3

Source filename []? anyconnect-win-4.9.06037-webdeploy-k9.pkg

Destination filename [disk0]? anyconnect-win-4.9.06037-webdeploy-k9.pkg

Accessing tftp://192.162.13.3/anyconnect-win-4.9.06037-webdeploy-k9.pkg...!

```

Рисунок 3.4 – Скачування образу за допомогою команди copy tftp

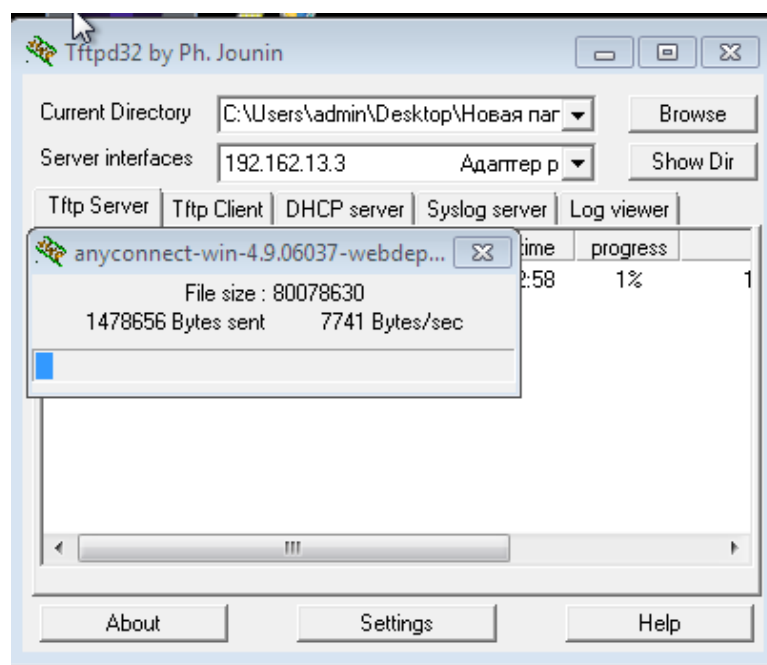


Рисунок 3.5 – Скачування образу через програмний додаток який використовується як tftp сервер

Після того як образ встановився потрібно підключитися через веб-браузер до сервера Tacacsgui та створити та налаштувати на ньому групи, користувачів для подальшої роботи.

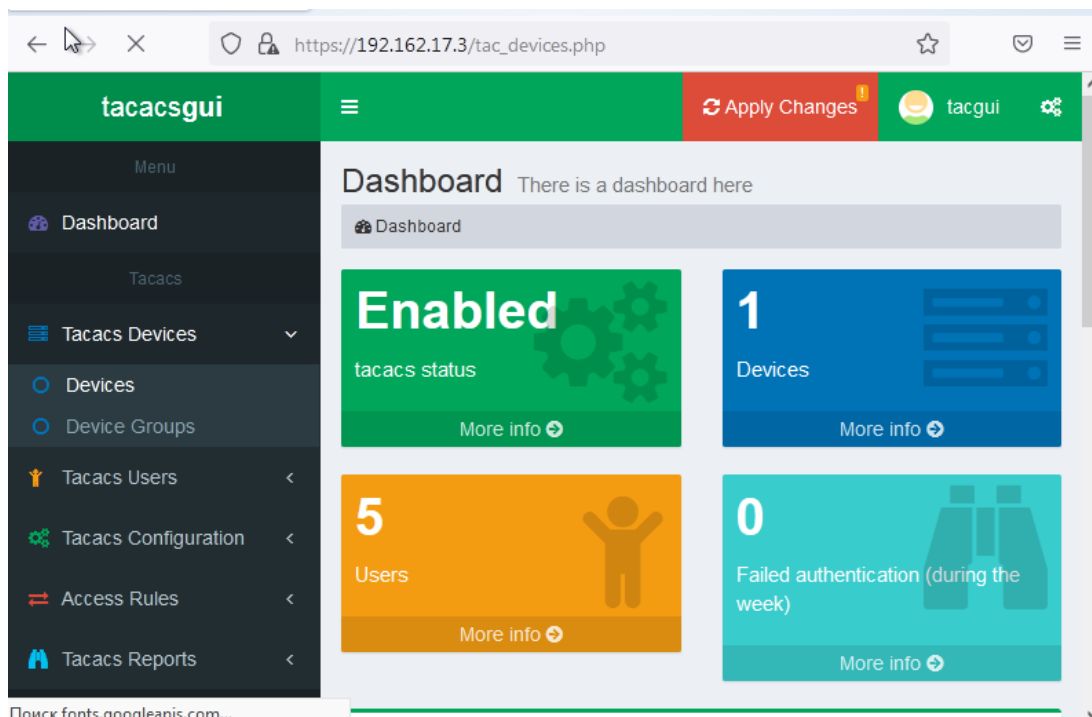


Рисунок 3.6 – Веб-інтефейс TacacsGUI

Для початку створимо дві групи користувачів RemoteUser та Admin. Група користувачів RemoteUser для віддалених користувачів та група Admin яка створена для адміністраторів заради зручного доступу до підключення.

Рисунок 3.7 – Створення групи користувачів.

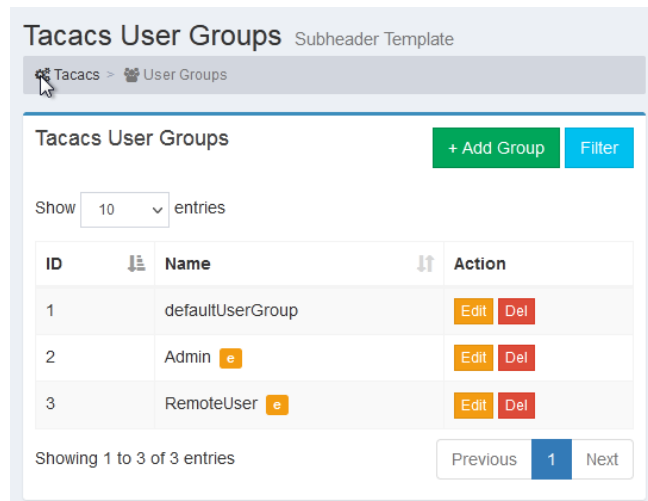


Рисунок 3.8 – Налаштовані групи користувачів

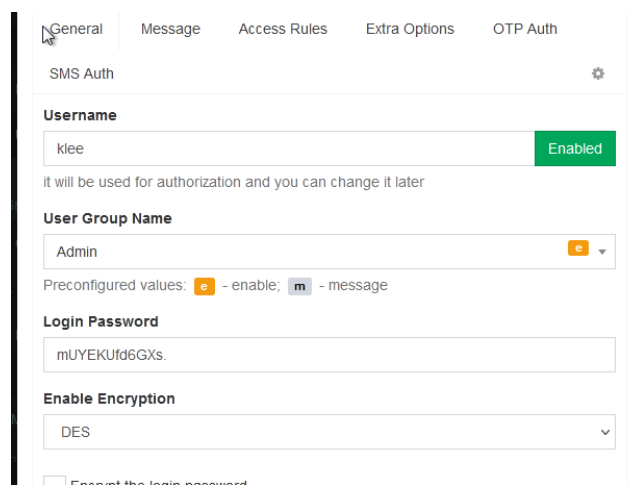


Рисунок 3.9 – Створення облікового запису користувача

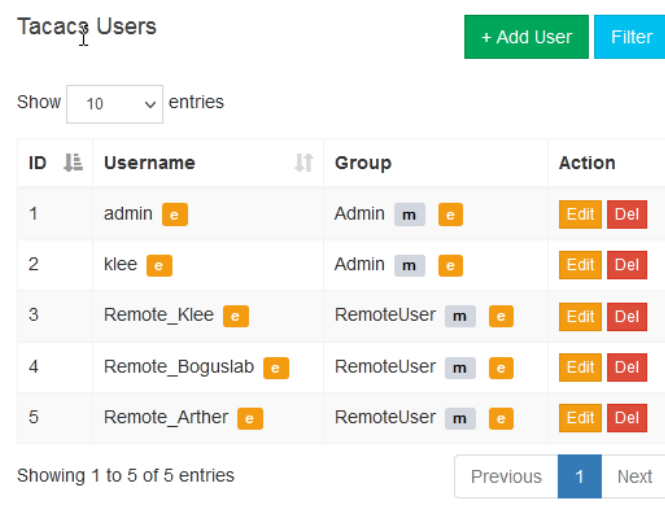


Рисунок 3.10 – Створені облікові записи користувачів.

Також для того щоб Cisco ASA змогла підключитися до сервера AAA потрібно налаштувати групи девайсів та самі девайси які будуть віднесені до цієї групи.

Add New Device Group

General Messages

Device Group Name
VPN_serv
it should be unique, but you can change it later

Set as Default
☒ Set Group As Default
if you check it, that group will be as a default group

Tacacs Key
cisco

Enable Password
cisco

Рисунок 3.11 – Створення групи пристроїв.

Device's Name
S_1_3_1(VPN) Enabled
it should be unique, but you can change it later

Device Group Name
VPN_serv
Preconfigured values: **k** - key; **e** - enable; **d** - default

Device's IP Address
10.132.17.1 Ping

Prefix /32
32

Tacacs Key
cisco

Enable Password
cisco

Рисунок 3.12 – Створення пристрою для підключення.

Після налаштування сервера TacacsGui передемо за IP-адресою брандмауера та скачуєм диспечер ASDM. Після встановлення підключаємося до брандмауера через диспечер.

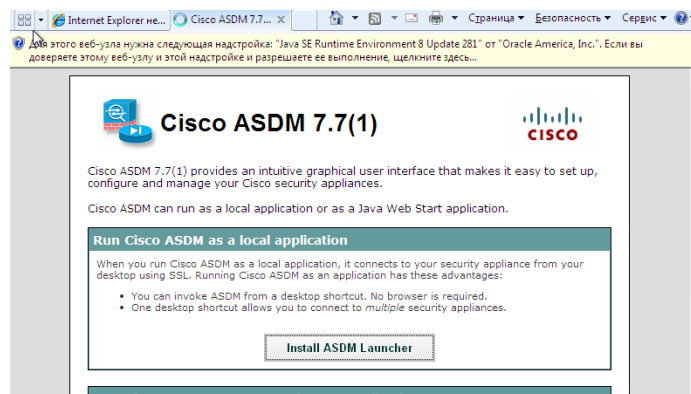


Рисунок 3.13 – Скачування Cisco ASDM

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

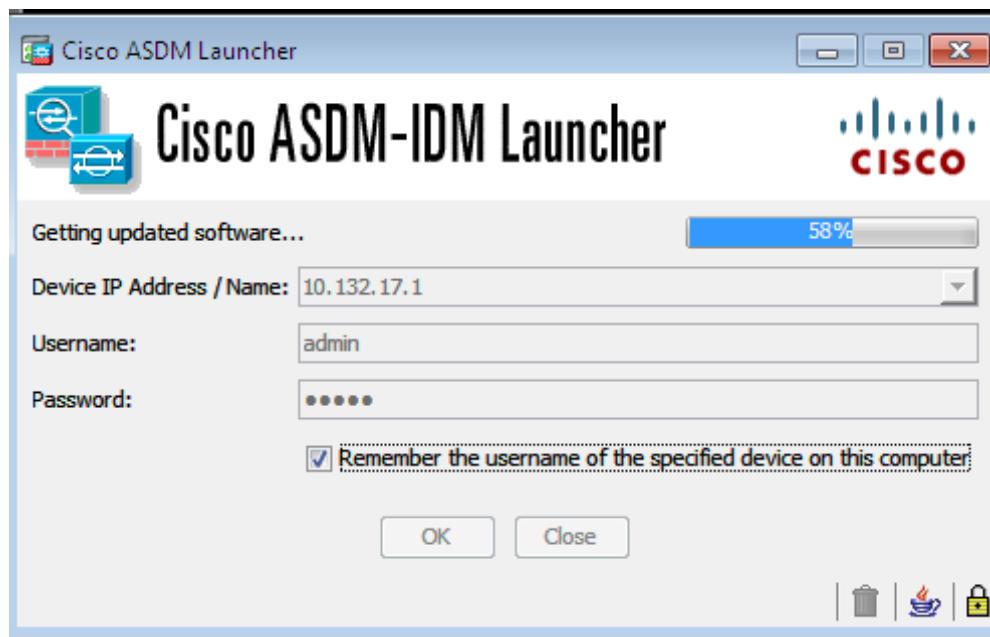


Рисунок 3.14 – вхід до S_1_3_1(VPN) через ASDM.

Для подальших налаштувань переходимо через меню “Wizards” до “VPN Wizards” та серед всіх можливих рішень вибираємо “AnyConnect VPN Wizard”. Після чого запуститься майстер, який допоможе нам швидко та зручно налаштувати необхідні служби.

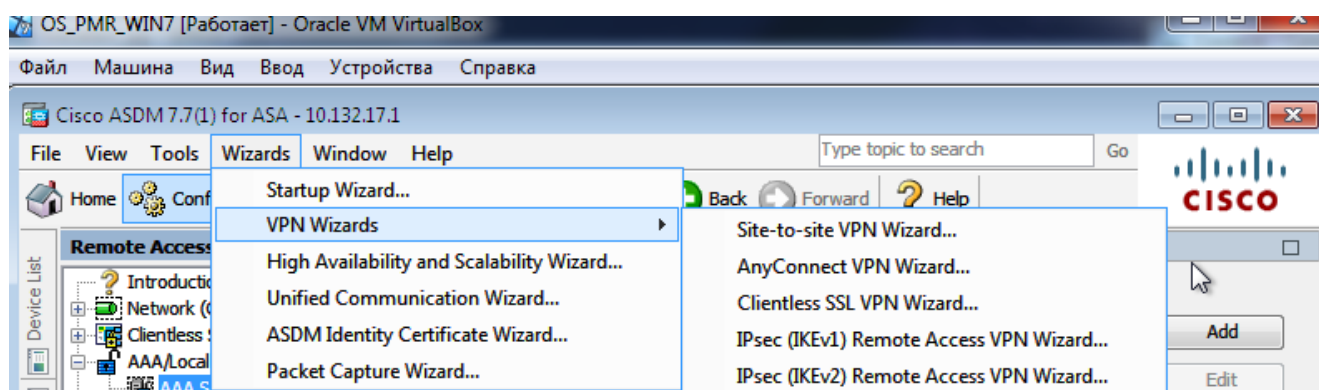


Рисунок 3.15 – Виклик майстра конфігурування AnyConnect VPN Wizard.

Після того як відкриється майстер налаштувань першим кроком який ми побачимо так це вступ яка коротко пояснить про дане рішення та його переваги. Ознайомлюємося із вступом та переходимо до наступного кроку яких надає нам можливість налаштувати назву профіля підключення та вибрати назву інтерфейсу на якому будуть розгортуватися VPN тунелі. Переходимо на наступний етап налаштування.

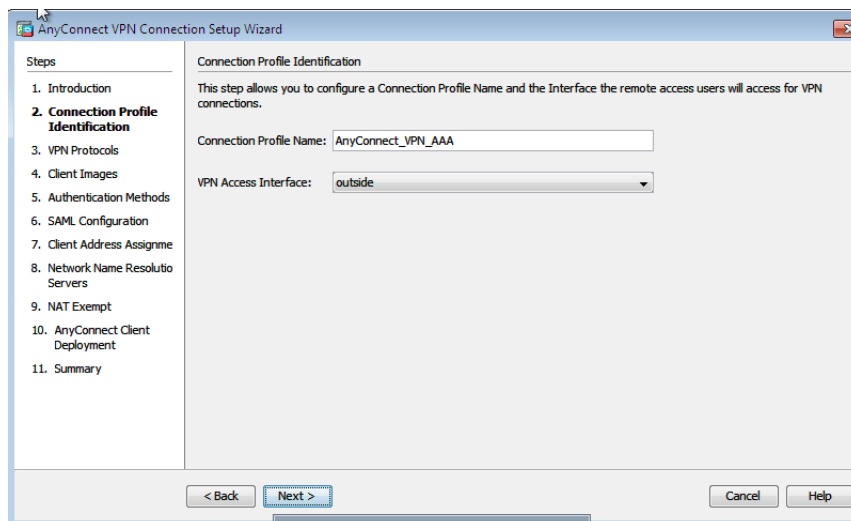


Рисунок 3.16 – Перший етап налаштування AnyConnect VPN

На даному етапі налаштовуємо протоколи для захисту трафіку. Вибираємо між протоколом SSL та IPsec та маємо можливість вибрати сертифікат або його створити але нажалі даний образ Cisco ASA не має ліцензію із за чого ми не можемо створювати сертифікати. Вибираємо потрібний нам протокол та переходимо на наступний етап.

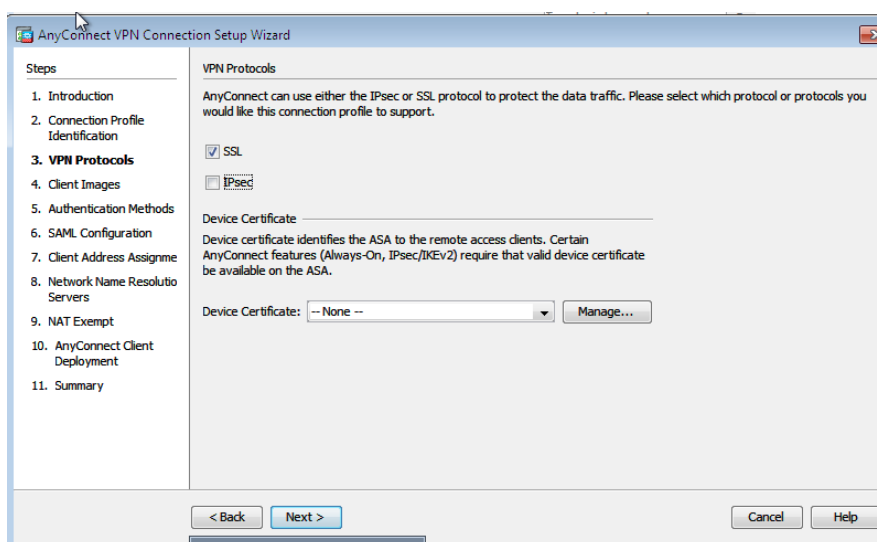


Рисунок 3.17 – Вибір протоколів для захисту трафіку.

На третьому етапі вибираємо образ VPN клієнта який ми недавно завантажували. Ми можемо завантажити образ на пристрій із нашої робочої станції але іноді можливі збої із завантаженням через що краще завантажити потрібні образи зазделегіть. Також можемо вибрати його із диску нашого брандмауера. Так як ми зазделегіть завантажили образ то вибираємо потрібний образ та переходимо далі.

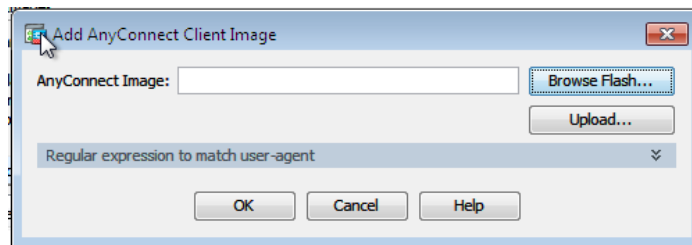


Рисунок 3.18 – Меню вибору образу клієнта.

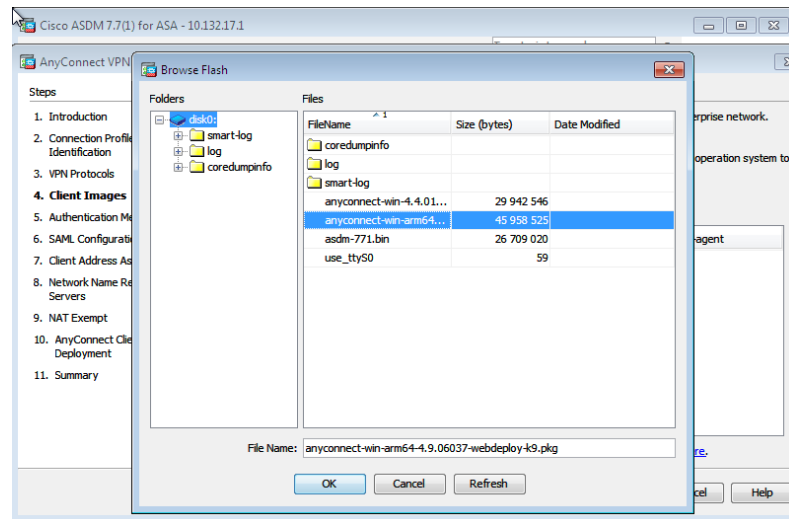


Рисунок 3.19 – Вибір образ клієнта із диска нашого брандмауера.

На подальшому етапі ми налаштовуємо методи аутентифікації. Ми можемо виконувати AAA без використання зовнішніх баз даних або використовувати сервер AAA такі як RADIUS або TACACS. У першому варіанті ми можемо створити користувачів на нашому девайсі а на другому варіанті ми вказуємо адресу сервера AAA та на назву на якому інтерфейсі він розгорнутий для того щоб перевірка віддалених користувачів йшла через сервер.

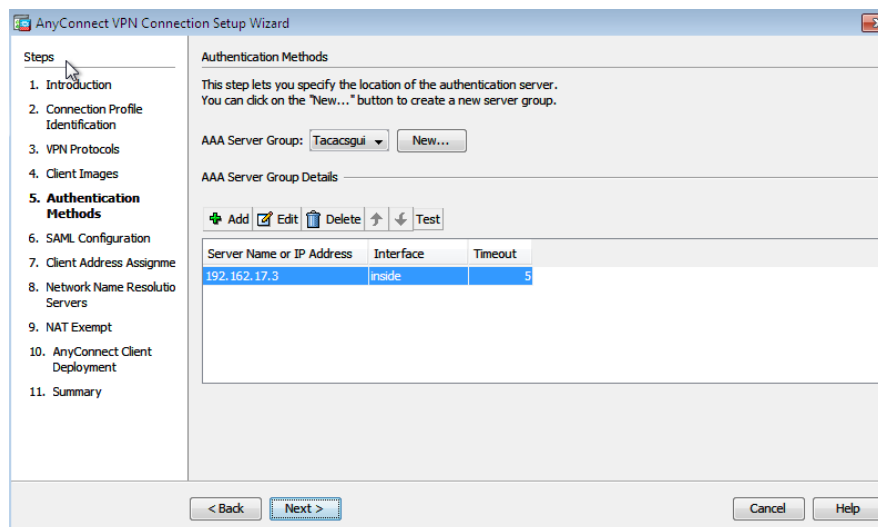


Рисунок 3.20 - Налаштування метода AAA

Наступний етап дозволяє нам налаштувати стандарт обміну даних між провайдером, що надає облікові записи (Identity provider, або IdP) та провайдера сервісу (Service provider, або SP). Також можемо налаштувати метод AAA таким чином, якщо сервере AAA вийде з ладу то аутентифікація буде проводитися через локальну базу даних. На даному етапі вибираємо маркер на випадок якщо сервере AAA впаде та переходимо до наступних налаштувань.

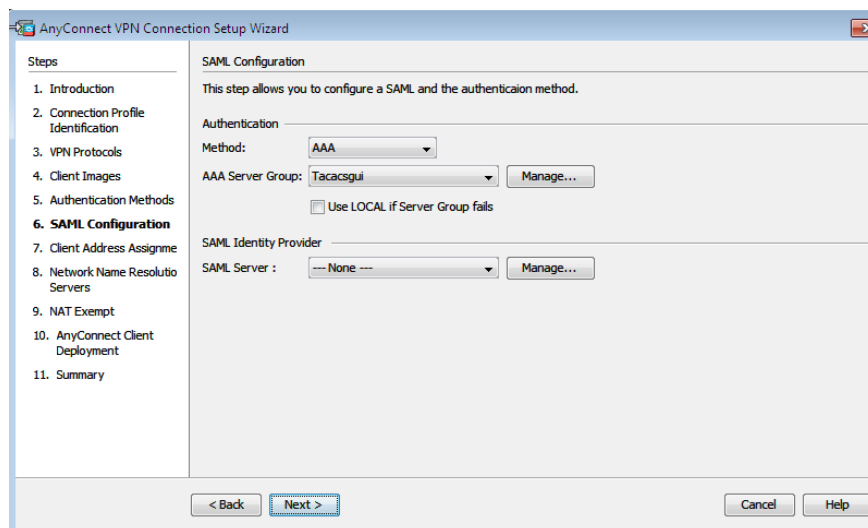


Рисунок 3.21 – Налаштування SAML

Сьомий етап складається із налаштувань IP-адрес які отримають наші віддалені користувачі при підключенні до нашого VPN тунелю. Налаштовуємо та переходимо далі.

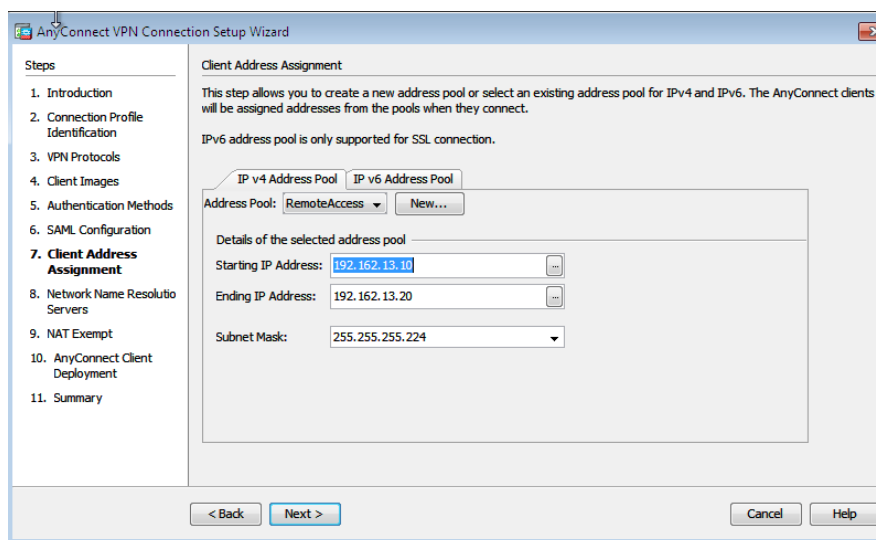


Рисунок 3.22 – Налаштування пулу адрес віддалених користувачів

На наступному етапі налаштовуємо адресу DNS сервера та ім'я домену до яких будуть підключатися віддалені користувачі. Заповнюємо дані та переходимо далі.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

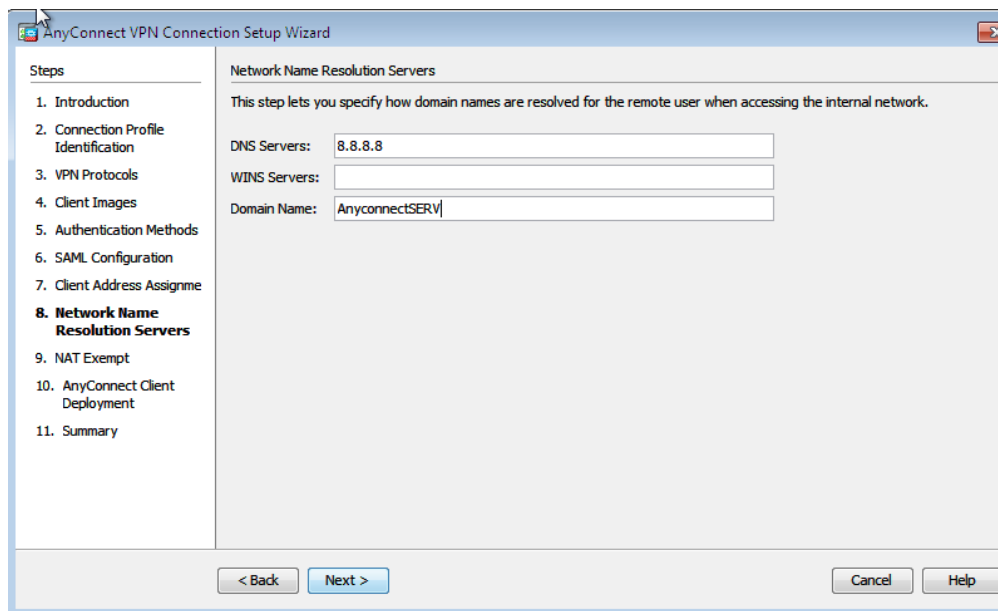


Рисунок 3.23 – Налаштування DNS та назву домену

Дев'ятий етап дає можливість налаштувати нам видимість та можливість підключитися віддаленим користувачам до мереж офісу. Ми можемо налаштувати до якого інтерфейсу та підмережі будуть мати доступ користувачі що підключаються до них через VPN клієнти. Дана функція перекочувала ще з EasyVPN адже ще там ми мали можливість налаштовувати видимість внутрішньої інфраструктури. Даний етап можна назвати останіми адже наступні етапи являють собою коротку інструкцію для клієнтів та видимість загальних налаштувань.

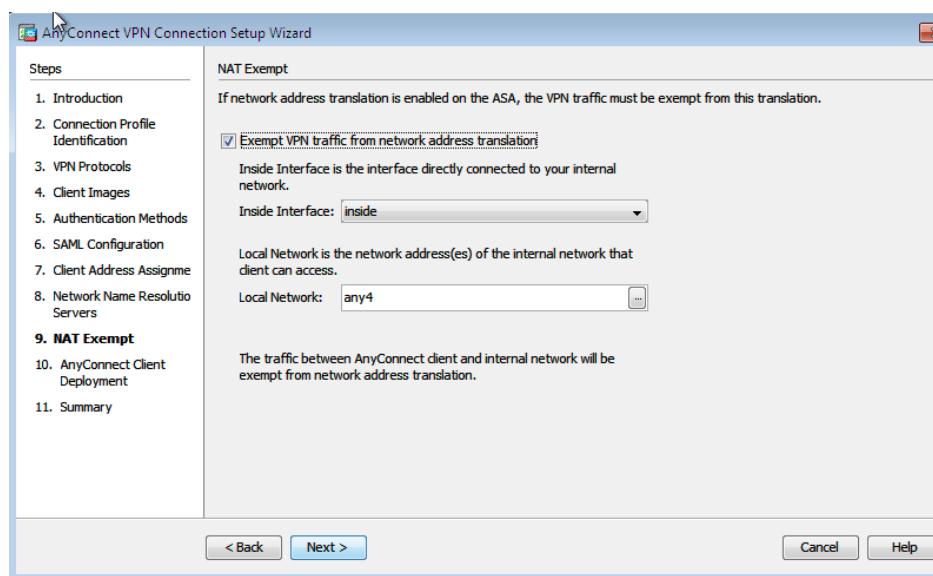


Рисунок 3.24 – Налаштування доступу віддалених користувачів до підмереж офісу

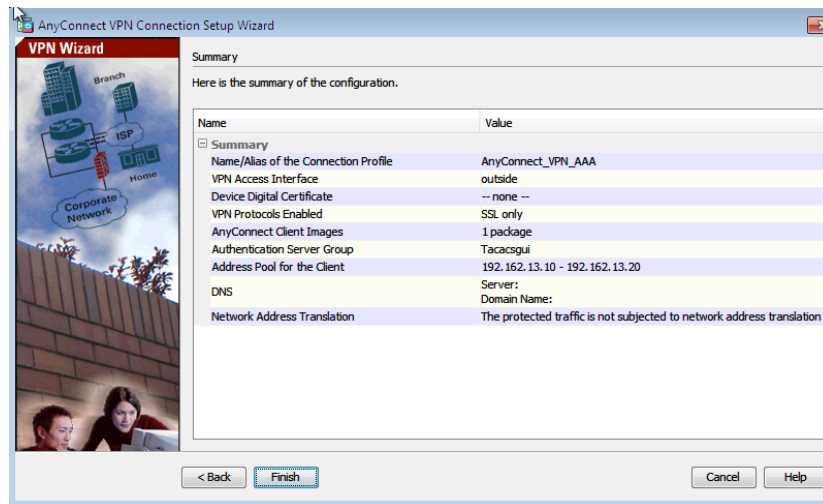


Рисунок 3.25 – Загальні конфігурації

3.2 Перевірка роботи та дослідження віддаленого доступу.

Після налаштування Anyconnect VPN сервера потрібно перевірити роботу на віддалених клієнтах. Для початку після запуску робочої станції віддаленого користувача потрібно підключитися до сервера через веб-браузер для того щоб завантажити AnyConnect Secure Mobility Client. Після входу сервер автоматично перевірить вашу операційну систему та запропонує потрібний для вас образ в випадку якщо на сервері не має образу клієнта під вашу операційну систему або якщо ПК не підтримує даний клієнт то отримаємо повідомлення про помилку.

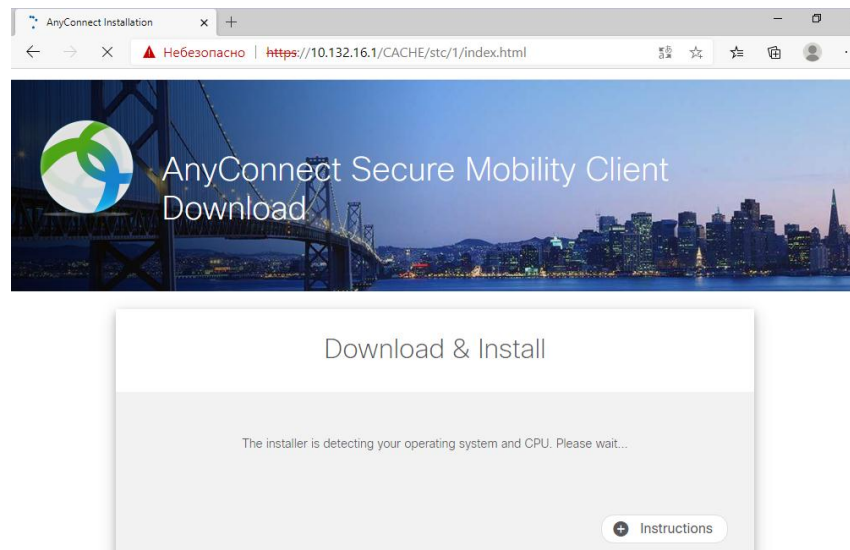


Рисунок 3.26 – Підключення клієнта до веб-інтерфейса сервера VPN

Після того як ми завантижили та встановили VPN клієнт спробуємо підключитися до сервера та створити з ним захищений тунель. Водимо IP-адресу

нашого сервера та якщо все налаштовано правильно то отримаємо вікно якому водимо дані облікового запису користувача після чого підключаємося.

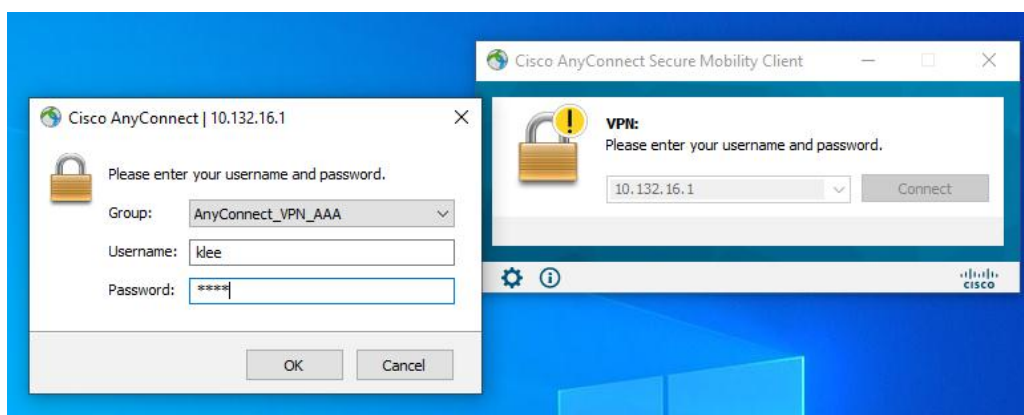


Рисунок 3.27 – Підключення до VPN сервера

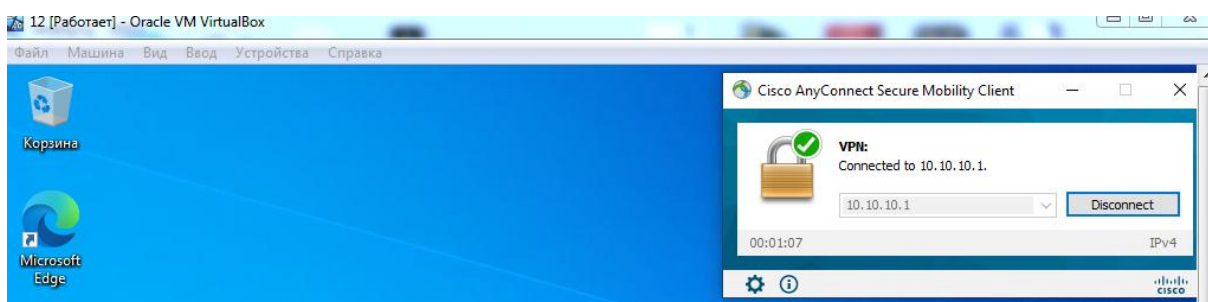


Рисунок 3.28 – Вдале підключення

Після вдалого підключення можемо переглянути інформацію про підключення наприклад історія повідомлень між сервером загальну інформацію.

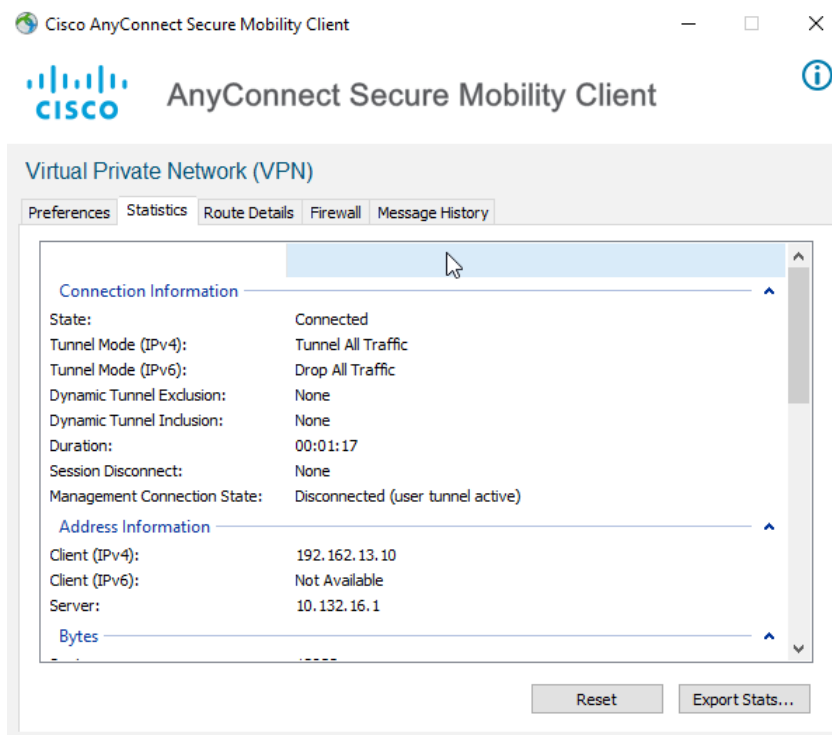


Рисунок 3.29 – Інформація про підключення

Також для впевненості перевіримо підключення між пристроями кінців вузлів.

```
C:\Windows\system32>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet 2:

    DNS-суффикс подключения . . . . . : AnyconnectSERV
    Локальный IPv6-адрес канала . . . . : fe80::91e:d442:8d58:5ef7%11
    Локальный IPv6-адрес канала . . . . : fe80::5270:3ece:b2af:51c9%11
    IPv4-адрес. . . . . : 192.162.13.10
    Маска подсети . . . . . : 255.255.255.224
    Основной шлюз. . . . . : ::
                                192.162.13.1

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . . : fe80::e847:d014:5203:548b%14
    IPv4-адрес. . . . . : 192.162.18.3
    Маска подсети . . . . . : 255.255.255.224
    Основной шлюз. . . . . : 192.162.18.1

C:\Windows\system32>
```

Рисунок 3.30 – Перевірка інтерфейсі на WS_1_3_5

```
C:\Windows\system32>ping 192.162.13.1

Обмен пакетами с 192.162.13.1 по с 32 байтами данных:
Ответ от 192.162.13.1: число байт=32 время=100мс TTL=254
Ответ от 192.162.13.1: число байт=32 время=233мс TTL=254
Ответ от 192.162.13.1: число байт=32 время=161мс TTL=254
Ответ от 192.162.13.1: число байт=32 время=124мс TTL=254

Статистика Ping для 192.162.13.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 100мсек, Максимальное = 233 мсек, Среднее = 154 мсек

C:\Windows\system32>ping 192.162.13.3

Обмен пакетами с 192.162.13.3 по с 32 байтами данных:
Ответ от 192.162.13.3: число байт=32 время=666мс TTL=126
Ответ от 192.162.13.3: число байт=32 время=1165мс TTL=126
Ответ от 192.162.13.3: число байт=32 время=219мс TTL=126
Ответ от 192.162.13.3: число байт=32 время=164мс TTL=126

Статистика Ping для 192.162.13.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 164мсек, Максимальное = 1165 мсек, Среднее = 553 мсек

C:\Windows\system32>
```

Рисунок 3.31 – Пінгування з WS_1_3_5 до WS_1_3_1

```
C:\Users\admin>ping 192.162.13.10

Обмен пакетами с 192.162.13.10 по с 32 байтами данных:
Ответ от 192.162.13.10: число байт=32 время=288мс TTL=126
Ответ от 192.162.13.10: число байт=32 время=299мс TTL=126
Ответ от 192.162.13.10: число байт=32 время=239мс TTL=126
Ответ от 192.162.13.10: число байт=32 время=174мс TTL=126

Статистика Ping для 192.162.13.10:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 174мсек, Максимальное = 299 мсек, Среднее = 250 мсек

C:\Users\admin>
```

Рисунок 3.32 – Перевірка підключення з WS_1_3_1 до WS_1_3_6

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```
C:\Windows\system32>tracert 192.162.13.1

Трассировка маршрута к 192.162.13.1 с максимальным числом прыжков 30

 1      56 ms    67 ms    91 ms   192.162.13.1
 2     113 ms    82 ms    98 ms   192.162.13.1

Трассировка завершена.
```

Рисунок 3.33 – Перевірка тунелювання з WS_1_3_5

Також можна перевірити підключення через диспетчер ASDM, для цього потрібно перейти до вкладки Monitoring. Тут ми бачимо наш сеанс та можемо дізнатися трохи детальніше вибавши у фільтрі технологію AnyConnect та побачимо детальну інформацію про сеанси підключення всіх користувачів (в даному випадку тільки один сеанс).

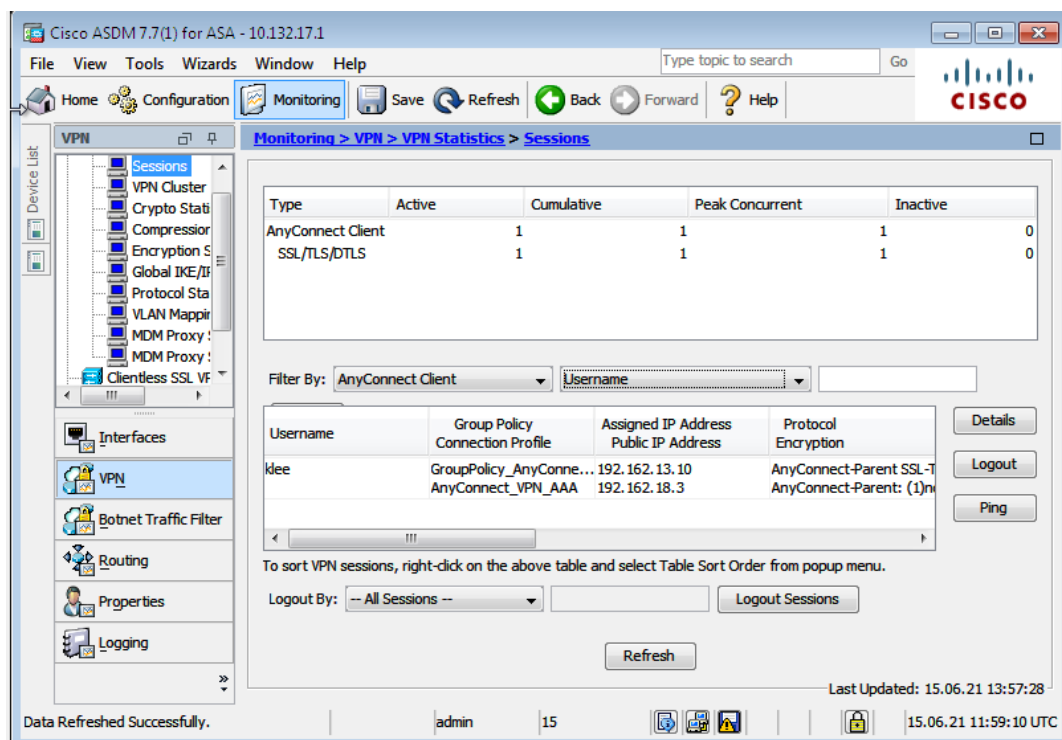


Рисунок 3.34 – Перевірка підключення через ASDM за допомогою функції моніторингу

3.4 Висновки до розділу 3.

В останньому розділі було розглянуто та вибрано обладнання серверної складової мережі. Проаналізували обладнання які підтримують налаштування сервера віддаленого доступу VPN, а саме обладнання серії Cisco ASA 5500.

Розглянули відомості про дану серію обладнання та їх особливості та порівняли моделі між собою. Також було вибрано проект TacsGUI як складова сервера аутентифікації, авторизації та обліку користувачів. Розглянули особливості даного проекту та його переваги. Після чого було налаштовано адресацію мережі та серверна складова. Розглянули особливості налаштування та створення груп користувачів та самих користувачів. Також створили групу девайсів для підключення до бази даних сервера AAA до сервера VPN. Налаштували сервер AnyConnect VPN на брандмауері за допомогою диспетчера ASDM та завантажили образи клієнтів на сервер. І нарешті перевірили підключення до мережі VPN.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

ВИСНОВКИ

Під час виконання випускної роботи бакалавра було спроектовано та реалізовано мережу на базі технологій Remote Access VPN та було виконано наступні завдання:

В першому розділі був проведений аналіз теоретичних відомостей які надали характеристики організації віддаленого доступу та зрозуміли на чому в наш час організовується віддалений доступ. Проаналізували основні переваги протоколів на яких на даному моменті працюють технології віддаленого доступу. Також було розглянуто сучасні технології віддаленого досутпу та відокремили технології VPN, а саме технології віддаленого доступу через приватні віртуальні мережі Remote Access VPN. Під кінець було розглянуто декілька прикладів засобів віддаленого доступу та було сформовано технічне завдання.

В другому розділі було проаналізовано середовище графічного симулятора GNS3 в якому буде виконуватися дипломна робота. Було спроектовано мережну інфраструктуру де ми розробили топологію мережі та розглянули кожну з підмереж та розробили загальну адресацію мережі. Також було спроектувано серверну інфраструктуру віддаленого доступу в якій вибрали рішення для розгортання сервера Remote Access VPN а саме рішення від компанії Cisco AnyConnect VPN. Також розглянули та вибрали протокол на якому буде розгорнутий сервер AAA. Вибраний протокол був TACACS+. І в останньому підрозділі вибрали клієнт віддаленого доступу Cisco AnyConnect Secure Mobility Client розглянули його особливості.

В останньому розділі було розглянуто та вибрано обладнання серверної складової мережі. Проаналізували обладнання які підтримують налаштування сервера віддаленого доступу VPN, а саме обладнання серії Cisco ASA 5500. Розглянули відомості про дану серію обладнання та їх особливості та порівняли моделі між собою. Також було вибрано проект TacsacsGUI як складова сервера аутентифікації, авторизації та обліку користувачів. Розглянули особливості даного проекту та його переваги. Після чого було налаштовано адресацію мережі та серверна складова. Розглянули особливості налаштування та створення груп

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

користувачів та самих користувачів. Також створили групу девайсів для підключення до бази даних сервера AAA до сервера VPN. Налаштували сервер AnyConnect VPN на брандмауері за допомогою диспечера ASDM та завантажили образи клієнтів на сервер. І нарешті перевірили підключення до мережі VPN.

Реалізована мережа та налаштування сервера може швидко перенестись на реальну топологію мережі завдяки зручному симулятору GNS3 та із-за використання емульованих реальних образів.

В майбутньому можливо розширити серверну структуру та налаштувати додаткові функції на сервері аунтикації та VPN.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.8 [Електронний ресурс], - Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8.pdf
2. J. Steinberg - SSL VPN: Understanding, Evaluating And Planning Secure, Web-based Remote Access/J. Steinberg T. Speed – М.: Computers – Networking, 2005 - 214стр.
3. J. Steinberg - SSL VPN: Understanding, evaluating and planning secure, web-based remote access: A comprehensive overview of SSL VPN technologies and design strategies/J. Steinberg T. Speed – М.: Computers – Networking, 2005 - 203стр.
4. ENHANCING SECURITY AND SCALABILITY OF VIRTUAL PRIVATE LAN SERVICES [Електронний ресурс], - Режим доступу: <http://jultika.oulu.fi/files/isbn9789526213767.pdf>
5. IPsec and IKE Administration Guide [Електронний ресурс], - Режим доступу: <https://docs.oracle.com/cd/E19683-01/816-7264/index.html>
6. Richard Deal- The Complete Cisco VPN Configuration Guide/ Richard Deal– М.: Cisco Press, 2005 - 1032стр.
7. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap) [Електронний ресурс], - Режим доступу: <https://datatracker.ietf.org/doc/html/rfc607>
8. Jazib Frahimс- Книги в Google Play Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance/Jazib Frahim, Omar Santos - М.:Pearson Education, 2009 р. - 1152 стор.
9. Cisco IPsec and SSL VPN Solutions Portfolio [Електронний ресурс], - Режим доступу: <http://www.ccsleeds.co.uk/kb/routers/cisco-vpn-throughput-comparison-doc.pdf>
10. SSL (Secure Sockets Layer) [Електронний ресурс], - Режим доступу: <https://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL>

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

11. IPsec vs. SSL VPN: Comparing speed, security risks and technology [Електронний ресурс], - Режим доступу: <https://searchsecurity.techtarget.com/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks>
12. Types of remote access: Pros and cons [Електронний ресурс], - Режим доступу: <https://securityboulevard.com/2019/08/types-of-remote-access-pros-and-cons/>
13. What is the OpenVPN protocol, and what are its 5 hype advantages? [Електронний ресурс], - Режим доступу: <https://vladtalks.tech/vpn/what-is-openvpn-protocol>
14. Cisco AnyConnect Secure Mobility Solution [Електронний ресурс], - Режим доступу: <https://federalnewsnetwork.com/wpcontent/uploads/pdfs/WhitePaper3CiscoAnyConnectSecureMobilitySolution.pdf>
15. Bob Vachon - CCNA Security (640-554) Portable Command Guide/ Bob Vachon- M.:Cisco Press,2012 p. - 368 стор
16. Cisco AnyConnect Secure Mobility Client At-a-Glance [Електронний ресурс],- Режим доступу: <https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/at-a-glance-c45-578609.html>
17. Ключи, шифры, сообщения: как работает TLS [Електронний ресурс], - Режим доступу <https://tls.dxdt.ru/tls.html>
18. Порівняння TACACS + і RADIUS [Електронний ресурс], - Режим доступу: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html
19. Настройка cisco aaa + tac_plus (tacacs+) [Електронний ресурс], - Режим доступу: <https://m.habr.com/ru/post/131113/>
20. Sheila Frankel - Guide to Ssl Vpns/ Sheila Frankel, Paul Hoffman, Angela Orebaugh- M.:Createspace Independent Pub, 2008 p. - 92 стор.

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Технічні характеристики пристроїв спроектованої мережі

Таблиця А.1 – Системні характеристики Cisco ASA5580-20-4GE-K9

Бренд	Cisco
Артикул	Cisco ASA5580-20-4GE-K9
Тип пристрою	маршрутизатор (router)
Можливість установки в стійку	має
Об'єм оперативної пам'яті	8192 Мб
Обсяг флеш-пам'яті	1024 Мб
консольний порт	має
Кількість портів комутатора	2 x Ethernet 10/100/1000 Мбіт / сек
Внутрішня пропускна здатність	6,5 Гбіт / сек
Підтримка VPN pass through	Має
Брандмауер (Firewall)	Має
Підтримка VPN-тунелів	має
Кількість VPN-тунелів	5000
Габарити	48,3 x 67,3 x 17,6 см
вага	29,9 кг

Таблиця А.2 – Системні характеристики Маршрутизатора Cisco 2801

Виробник	Cisco
Ідентифікатор товару	CISCO2801
Опис продукту	2801 w / AC PWR, 2FE, 4slots (2HWIC), 2PVDM, 2AIM, IP BASE, 64F / 128D
Тип продукту	маршрутизатор
Інтерфейси / порти	
Загальна кількість портів	2
USB	Має
Порт управління	має
Кількість мережевих портів (RJ-45)	2
Розширення вводу-виводу	
Кількість загальних слотів розширення	8
Тип слота розширення	AIM \ PVDM
Network & Communication	
Мережеві технології	10 / 100Base-TX
Технологія Ethernet	Fast Ethernet
Пам'ять	
Стандартна пам'ять	128 MB
Максимум пам'яті	384 MB
Технологія пам'яті	DRAM
Флеш-пам'ять	64 MB
Опис живлення	
Вхідна напруга	110 V AC \ 220 V AC
Фізичні характеристики	
Сумісний блок стійки	1U
Форм-фактор	Монтаж в стійку
Висота	1.7
Ширина	17.5
Глибина	16.5

Конфігураційні файли пристроїв мережі

Конфігураційний файл міжмереженого екрану Cisco ASA

```

ServerVPN# show run
: Saved
: Serial Number: 9A8LX5DWT85
: Hardware:  ASAv, 2048 MB RAM, CPU
Pentium II 2194 MHz
ASA Version 9.7(1)
hostname ciscoasa
enable password
$sha512$5000$krVaOasANfdkv8Hw+ySViA==$N
NcemfNSS+58bUvTne/JkA== 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 RemoteAcces 192.162.13.10-
192.162.13.20 mask 255.255.255.224
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.132.16.1 255.255.255.252
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.132.17.1 255.255.255.252
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!

```

```

interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif MGMT
security-level 100
ip address 192.168.56.2 255.255.255.0
!
ftp mode passive
object network INSIDE-NET
subnet 10.132.17.0 255.255.255.252
object network
NETWORK_OBJ_192.162.13.0_27
subnet 192.162.13.0 255.255.255.224
pager lines 23
mtu outside 1500
mtu inside 1500
mtu MGMT 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_192.162.13.0_27
NETWORK_OBJ_192.162.13.0_27 no-proxy-arp
route-lookup
!
object network INSIDE-NET
nat (inside,outside) dynamic interface
router eigrp 1
network 10.0.0.0 255.0.0.0
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-
invite 0:03:00 sip-disconnect 0:02:00

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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
aaa-server Tacacsgui protocol tacacs+
aaa-server Tacacsgui (inside) host 192.162.17.3
timeout 5
key *****
user-identity default-domain LOCAL
http server enable
http 192.162.13.0 255.255.255.224 inside
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging
infinite
crypto ca trustpoint
_SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain
_SmartCallHome_ServerCA
certificate ca
18dad19e267de8bb4a2158cdcc6b3b4a
308204d3 308203bb a0030201 02021018
dad19e26 7de8bb4a 2158cdcc 6b3b4a30
0d06092a 864886f7 0d010105 05003081
ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967
6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374
204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269
5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520
6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320
5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574
686f7269 7479202d 20473530 1e170d30
36313130 38303030 3030305a 170d3336
30373136 32333539 35395a30 81ca310b
30090603 55040613 02555331 17301506
0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656
65726953 69676e20 54727573 74204e65
74776f72 6b313a30 38060355 040b1331
28632920 32303036 20566572 69536967
6e2c2049 6e632e20 2d20466f 72206175
74686f72 697a6564 20757365 206f6e6c
79314530 43060355 0403133c 56657269
5369676e 20436c61 73732033 20507562
6c696320 5072696d 61727920 43657274
69666963 6174696f 6e204175 74686f72
69747920 2d204735 30820122 300d0609
2a864886 f70d0101 01050003 82010f00
3082010a 02820101 00af2408 08297a35
9e600caa e74b3b4e dc7cbc3c 451cbb2b
e0fe2902 f95708a3 64851527 f5f1adc8
31895d22 e82aaaa6 42b38ff8 b955b7b1

```

```

b74bb3fe 8f7e0757 ecef43db 66621561
cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9feb5f a191c233
49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf
1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c
eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe
ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0
6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381
b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04
04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516
09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d
8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572
69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f
d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105
05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4
a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9
f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620
c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a
584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc
defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51
5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d
86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2
ac11d6a8 ed636a
quit
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-arm64-4.9.06037-webdeploy-k9.pkg 1
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable
group-policy
GroupPolicy_AnyConnect_VPN_AAA internal

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

```

group-policy
GroupPolicy_AnyConnect_VPN_AAA attributes
wins-server none
dns-server value 8.8.8.8
vpn-tunnel-protocol ssl-client
default-domain value AnyconnectSERV
dynamic-access-policy-record DfltAccessPolicy
username admin password
$sha512$5000$/kZ7r6yji4Dpu9+DmkLffA==$vUrr
UtP8PrzeBb6BjYxBfA==$pbkdf2 privilege 15
username klee password
$sha512$5000$8/hsCzR/juMUslwgpHX5CA==$yZ
g2dLuSTgWWXtyEiy3/1A==$pbkdf2 privilege 15
tunnel-group AnyConnect_VPN_AAA type
remote-access
tunnel-group AnyConnect_VPN_AAA general-
attributes
address-pool RemoteAcces
authentication-server-group TacacsGuiLOCAL
default-group-policy
GroupPolicy_AnyConnect_VPN_AAA
tunnel-group AnyConnect_VPN_AAA
webvpn-attributes
group-alias AnyConnect_VPN_AAA enable
!
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
message-length maximum 512
no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
destination address email
callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic
monthly
subscribe-to-alert-group configuration periodic
monthly
subscribe-to-alert-group telemetry periodic
daily
profile License
destination address http
https://tools.cisco.com/its/service/oddce/services/DD
CEService
destination transport-method http
Cryptochecksum:a29e29f25b1f248e5699b5589
8669ff4
: end

```

Конфігураційні файли маршрутизаторів Cisco 3700

```

R_1_3_3#show run
Building configuration...

```

```

Current configuration : 1230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_3
!
boot-start-marker
boot-end-marker
!

```

```

no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

```

ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 10.135.17.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.162.17.1 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 1

```

R_1_3_2#show run
Building configuration...

Current configuration : 1237 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_2
!
boot-start-marker
boot-end-marker
!
no aaa new-model

```

interface FastEthernet0/0
ip address 10.132.17.2 255.255.255.252
duplex auto
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 10.133.17.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.134.17.1 255.255.255.252
duplex auto
speed auto
!
router eigrp 1
network 10.0.0.0
auto-summary
!

```

```

network 10.0.0.0
network 192.162.17.0
auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
speed auto
!
interface FastEthernet0/1
ip address 10.135.17.1 255.255.255.252
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
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

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

line vty 0 4
login
!
End

```

```

R_1_3_4#show run
Building configuration...

```

```

Current configuration : 1268 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
--More--
*Mar 1 00:01:03.179: %DUAL-5-
NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.133.17.1 (FastEthernet0/0) is down: holding time
expired

```

```

ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 10.133.17.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.162.13.1 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 192.162.14.1 255.255.255.224
duplex auto
speed auto

```

```

!
router eigrp 1
network 10.0.0.0
network 192.162.13.0
network 192.162.14.0
auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

```

R_1_3_5#show run
Building configuration...

```

```

Current configuration : 1268 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_5
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5

```

```

!
interface FastEthernet0/0
ip address 10.134.17.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.162.15.1 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 192.162.16.1 255.255.255.224
duplex auto
speed auto
!
router eigrp 1
network 10.0.0.0
network 192.162.15.0
network 192.162.16.0
auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
Internet#show run
Building configuration...

Current configuration : 1208 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker

```

```

boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated

!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 10.132.16.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 10.134.16.1 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 1
network 10.0.0.0
auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

```

logging synchronous
line vty 0 4
login
!
!
End

```

```

R_1_3_6#show running-config
Building configuration...

```

```

Current configuration : 1031 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_6
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 10.134.16.2 255.255.255.252
duplex half
!
interface FastEthernet1/0
ip address 192.162.18.1 255.255.255.224
duplex half
!
router eigrp 1
network 10.0.0.0
network 192.162.18.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
shutdown
!

```

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
--More--
*Jun 16 03:28:49.399: %DUAL-5-
NBRCHANGE: EIGRP-IPv4 1: Neighbor
10.134.16.1 (FastEthernet0/0) is down: holding time
expired

```

```

stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
transport input all
!
!
end

```

```

R_1_3_7#show run
Building configuration...

```

```

Current configuration : 1230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_3_7
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 10.133.16.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.162.19.1 255.255.255.224

```

		Волинець Б.О.			КІК.КР.Б-125-03-ПЗ	Арк.
		Сфіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 1
network 10.0.0.0
network 192.162.19.0
auto-summary
!
ip forward-protocol nd
!

```

```

!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```