МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«VPN технології для реалізації концепції високозахищеного віддаленого доступу»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Великодний Д.В.**

Студентки групи ІК.мз-91с — **Ховріна М.А.**

СУМИ 2020

Сумський Державний Університет

(назва вузу)

Факультет Електроніки та інформаційних технологій Кафедра Комп'ютерних наук

Спеціальність «Інформаційно-комунікаційні технології»

Затверджую:

зав.кафедрою _____

_____

"_____" _____ 20___р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Ховріна Марина Аркадіївна

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) VPN технології для реалізації концепції високозахищеного віддаленого доступу

затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проекту (роботи) _____

3. Вхідні данні до проекту (роботи)

_____

_____

_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1) Аналіз предметної області 2) Вибір технології побудови VPN мережі 3) Визначення способу підсилення захисту VPN мережі 4) Розробка схеми максимально захищеної VPN мережі для організації віддаленого доступу.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

_____

_____

_____

_____

6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання

_____

Керівник _____

Завдання прийняв до виконання _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
1	Аналіз предметної області	01.10.2020-13.10.2020	
2	Вибір технології побудови VPN мережі	14.10.2020-27.10.2020	
3	Визначення способу підсилення захисту VPN мережі	28.10.2020-05.11.2020	
4	Розробка схеми максимально захищеної VPN мережі для організації віддаленого доступу	06.11.2020-20.11.2020	
5	Оформлення пояснювальної записки	21.11.2020-01.12.2020	

Студент – дипломник _____

Керівник проекту _____

РЕФЕРАТ

Записка: 59 стор., 32 рис., 6 табл., 1 додаток, 67 джерел.

Мета роботи – розробка найбільш захищеного доступу віддалених співробітників до корпоративної мережі з розподіленими офісами за допомогою IPSec VPN та SSL VPN.

Об'єкт дослідження – комп'ютерні мережі на базі VPN.

Предмет дослідження – процесс забезпечення безпечної передачі даних у комп'ютерні мережах за допомогою технологій VPN.

Методи дослідження – теоретичний, аналізу та моделювання.

Результати – Для реалізації поставленої мети було обрано поєднання IPsec VPN та SSL VPN. Для побудови захищеної корпоративної мережі між віддаленими офісами було залучено технологію IPsec VPN, а для налаштування віддаленого доступу для співробітників – SSL VPN. Реалізація моделі була виконана в програмі Cisco Packet Tracer. Розроблена модель дозволе компаніям швидко налаштувати вискозахищений доступ до корпоративної мережі.

VPN, SSL, IPSEC, ВІДДАЛЕНИЙ ДОСТУП,
КОРПОРАТИВНА МЕРЕЖА, БЕЗПЕКА,
ШИФРУВАННЯ, АУТЕНТИФІКАЦІЯ

ЗМІСТ

ВСТУП

У зв’язку з непередбачуваними обставинами, які підготував 2020 рік та карантин, перед компаніями постало питання організації віддаленого режиму безпечної роботи для своїх співробітників. Оскільки багато організацій раніше не реалізовували такий перехід, то швидке впровадження даного режиму роботи призвело до проблем з інформаційною безпекою.

В умовах COVID-19 значно підвищилась активність шахраїв та зловмисників, які через комп’ютери віддалених співробітників можуть отримати доступ до ресурсів корпоративної мережі через те що, компанії не створили умов високозахищеного доступу до своїх систем. Великі компанії зі значною кількістю працівників та офісів повинні приділяти особливо велике значення захисту своїх серверів.

Найчастіше для дистанційної роботи використовується віддалене підключення, тому що у всіх нових версіях Windows є необхідне програмне забезпечення, яке використовує незахищений RDP протокол. Зазвичай такий спосіб підключення призводить до проблем безпеки мережі. Тому при організації дистанційної роботи користувачів компаніям рекомендується не використовувати такий варіант, а слід зупинитися на більш захищених технологіях та протоколах.

Оскільки зазначена проблема є актуальною, в даній роботі планується розглянути основні аспекти роботи VPN, визначити відмінності між проколами і технологіями та розробити власну модель найбільш захищеного доступу до корпоративної мережі.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальні положення VPN

Історія виникнення VPN почалася з середини 60-х років 20 століття, коли була запроваджена система автоматичного з'єднання абонентів АТС – Centrex. Це був спосіб надання послуг зв'язку абонентам декількох компаній на основі спільного обладнання однієї станції. Можна сказати, що це була віртуальна приватна телефонна мережа, тому що орендувалися раніше створені канали, завдяки чому створювалися віртуальні канали для передачі інформації. [20,22] Основна перевага Centrex полягала в тому, що фірми могли заощадити кошти на покупку власних станцій, їх монтаж, а також експлуатацію. Абоненти Centrex створювали замкнуті групи користувачів, у яких був обмежений зовнішній доступ, і для них в станціях мережі використовувались віртуальні станції. [20,22]

Виникнення віддалених робочих місць почалося у 1996 році, коли Microsoft розробила VPN мережу для доступу віддалених працівників до своїх ресурсів. [38]

У 1999 році була розроблена модель аутентифікації та додаткові засоби для конфігурації клієнтів. А у 2000 році відбулося включення VPN до Windows. [20]

Існує велике різноманіття визначень VPN, але всі вони засновані на тому, що їх основною відмінною рисою є передача пакетів за допомогою Інтернет.

Наприклад, найбільш вузьке та загальне визначення виглядає наступним чином: «VPN (англ. Virtual Private Network – віртуальна приватна мережа) – узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет).» [9] Дане визначення жодним чином не вказує на особливості технології.

У наступних визначеннях вже вказуються певні важливі характеристики технології: «VPN – це безпечне, зашифроване підключення між двома мережами або між окремим користувачем і мережею» [38] або «VPN – це мережева технологія, яка створює захищене мережеве з’єднання через загальнодоступну мережу, таку як

Інтернет, або приватну мережу, що належить постачальнику послуг». [33] Проте, і такі визначення не можна вважати досконалими.

Натомість, Оліфер дає більш розгорнуте визначення VPN як «досить широкого кола технологій, що забезпечують безпечний та якісний зв'язок у межах контрольованої групи користувачів по відкритій (публічній) глобальної мережі. Термін «віртуальна приватна мережа» використовується також для позначення стійких інформаційних потоків одного підприємства, які існують в публічній мережі з комутацією пакетів і які в достатній мірі захищені від впливу потоків даних інших користувачів цієї публічної мережі.» [23]

А на думку Платунової С.М., «VPN є об'єднанням окремих машин або локальних мереж у віртуальну мережу, яка забезпечує цілісність і безпеку переданих даних. Вона має властивості виділеної приватної мережі і дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад Internet.» [25]

Отже, головною метою VPN є організація доступу до мережі компанії за допомогою мереж загального користування.

Оліфер зазначає загальнопогоджену думку, що VPN використовується для вирішення наступних завдань:

- «для організації глобального зв'язку між філіями однієї компанії (intranet)
- для з'єднання приватної мережі компанії з її діловими партнерами і клієнтами (extranet)
- для взаємодії окремих мобільних користувачів або співробітників, які працюють вдома, з корпоративною мережею (віддалений доступ).» [23]

VPN забезпечує конфіденційність, цілісність та доступність інформації. Тобто гарантує те, що інформація не буде доступна небажаним особам, буде збережена та доступна лише визначеним користувачам.[8] Дані характеристики забезпечується за допомогою основних компонентів VPN, які наведені на рис. 1.1

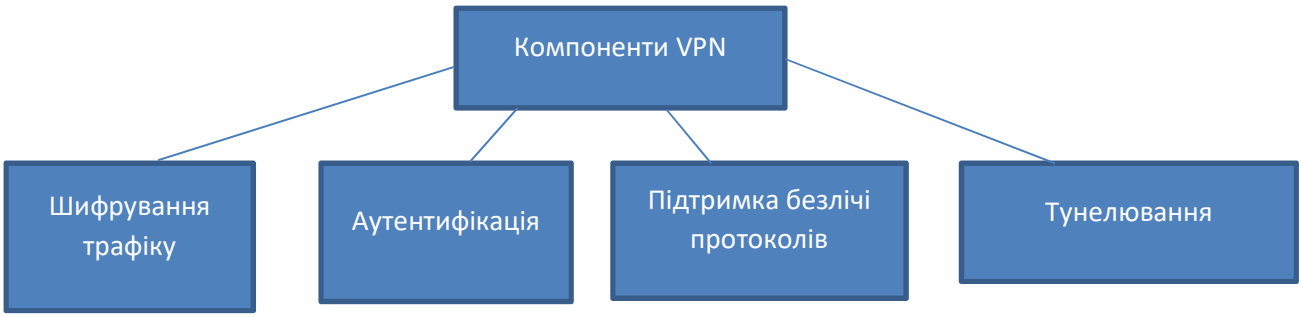


Рисунок 1.1 – Компоненти VPN

Розглянемо більш детально наведені вище компоненти VPN.

Шифрування трафіку включає в себе кодування інформації для запобігання отримання даних третіми особами. Доступ до такої інформації будуть мати лише ті користувачі, яким для дешифрування було надано відповідний ключ. Шифрування має бути складним для забезпечення конфіденційності інформації, що передається в межах періоду, до якого вона буде актуальна. Алгоритм шифрування повинен протидіяти протизаконному дешифруванню трафіку на довгий період. [4,63]

Щодо аутентифікації, то мається на увазі, що на центральному сервері відбувається аутентифікація користувачів. Також може відбуватися взаємна аутентифікація з’єднаних вузлів. Для більшої безпеки рекомендується використовувати двофакторну аутентифікацію. [4]

Протоколи VPN визначають рівень захищеності трафіку та те як VPN взаємодіє з іншими системами в Інтернеті. VPN забезпечує підтримку великої кількості протоколів, що буде розглянуто більш детально в розділі 1.3.

Остання характеристика вказує на те, що VPN створює відокремлений канал між з’єднаними пристроями. При цьому кожен кінцевий вузол VPN здатен забезпечувати кілька одночасних з'єднань з іншими вузлами. Водночас за допомогою шифрування трафік розділяється, і всі вузли є відокремленими один від одного. [4]

1.2 Класифікація VPN

В літературі існують різні варіанти класифікації VPN за різноманітними параметрами. Консолідована класифікація наведена на рис. 1.2.

Розглянемо кожний вид VPN більш детально:

1. За рівнем захисту:

– Довірительні. Використовуються для налаштування віртуальної нової мережі під основною мережею. При цьому не приділяється увага проблемам забезпечення безпеки, оскільки середа для передачі даних є довірчою.

– Захищені. Використовуються для налаштування надійних і високозахищених мереж на основі існуючих незахищених мереж. [3,6,19,28]

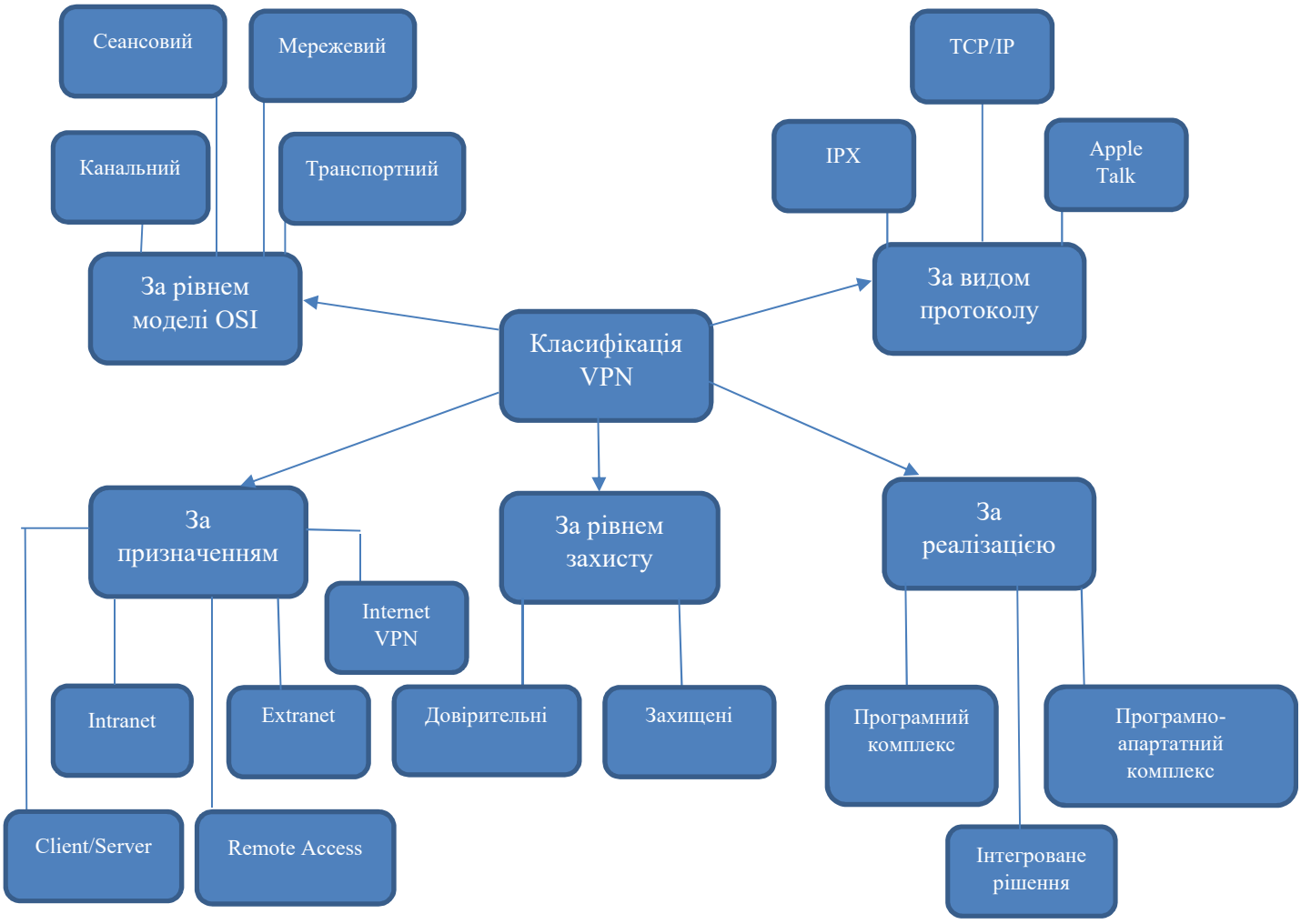


Рисунок 1.2 – Класифікація VPN

2. За реалізацією:

– Інтегроване рішення. Використовується програмно-апаратний комплекс, який налаштовує мережевий екран та фільтрує трафік.
– Програмно-апаратний комплекс. Реалізується за рахунок спеціалізованих програмно-апаратних засобів.
– Програмний комплекс. Використовується комп'ютер клієнта зі спеціальним програмним забезпеченням. [3,6,19,28]

3. За призначенням:

– Intranet. Об'єднує філії організації у високозахищену мережу для обміну інформацією за рахунок створення відкритих каналів.
– Extranet. Об'єднує кілька різних компаній в єдину мережу, але для небажаних користувачів обмежується доступ до конфіденційної інформації.
– Remote Access. Створюється захищений канал між віддаленим співробітником та мережею компанії.
– Client/Server. Поділяє фізичну мережу на декілька логічних підмереж.
– Internet. Забезпечує доступ по спільному фізичному каналу для декількох користувачів у мережі провайдера. [3,6,19,28]

4. За рівнем моделі OSI

– Канальний (протоколи SLIP, PPP, PPTP, L2TP). Здійснює інкапсуляцію декількох типів трафіку, а також створює віртуальні тунелі за принципом точка-точка.
– Мережевий (протоколи IPsec, MPLS). Забезпечує інкапсуляцію одного IP пакету в інший.
– Транспортний (протоколи SSL/TLS). Забезпечує цілісність і конфіденційність даних, управляє ключами в процесі передачі даних, а також здійснює аутентифікацію відправника та отримувача.

– Сеансовий (протокол SOCKS). Забезпечує підтримку необхідних програм, для яких потрібно встановити умови доступу для користувачів та спрямувати інформаційний потік. [6,19,28]

5. За видом протоколу

Можна виділити VPN під IPX, AppleTalk і TCP/IP. Найбільш популярним є TCP / IP. [3,6]

1.3 Основні протоколи VPN

Розглянемо основні способи організації VPN в корпоративній мережі. Основою створення VPN є побудова тунелю, тобто каналу між двома пристроями для передачі даних. [27]

Найбільш поширеними підключеннями є:

– підключення віддаленого користувача до мережі компанії (remote-access VPN)

– з'єднання двох офісів за типом точка - точка (site-to-site VPN).

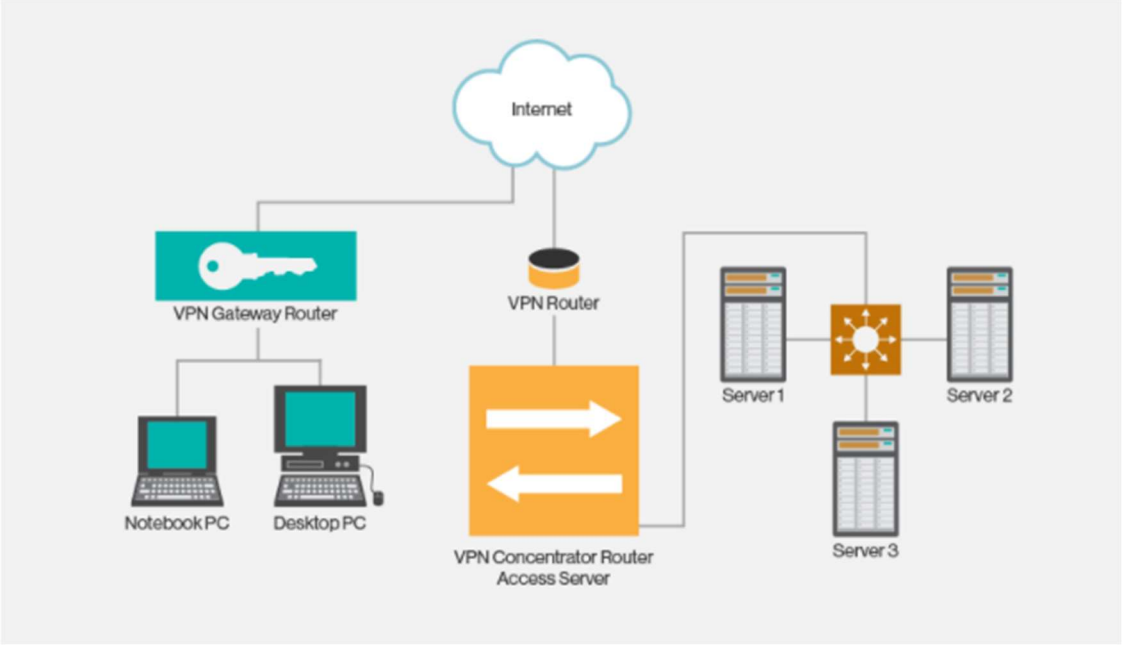


Рисунок 1.3 – Схема Remote access VPN

1. Remote access VPN (рис.1.3). При цьому створюється тунель між комп'ютером клієнта та сервером компанії. Клієнтський VPN на віддаленому пристрої підключається до VPN-шлюзу корпоративної мережі, за допомогою якого аутентифікуються користувачі. Після успішної аутентифікації надається доступ до ресурсів в мережі компанії (сервери даних, бази знань, адміністративні пристрої та інші) [8]

2. Site-to-site VPN (рис.1.4). Налаштовується за рахунок побудови стабільного тунелю між двома пристроями (роутерами), завдяки цьому немає необхідності в додатковому ПЗ на ПК користувачів в офісах. [27]

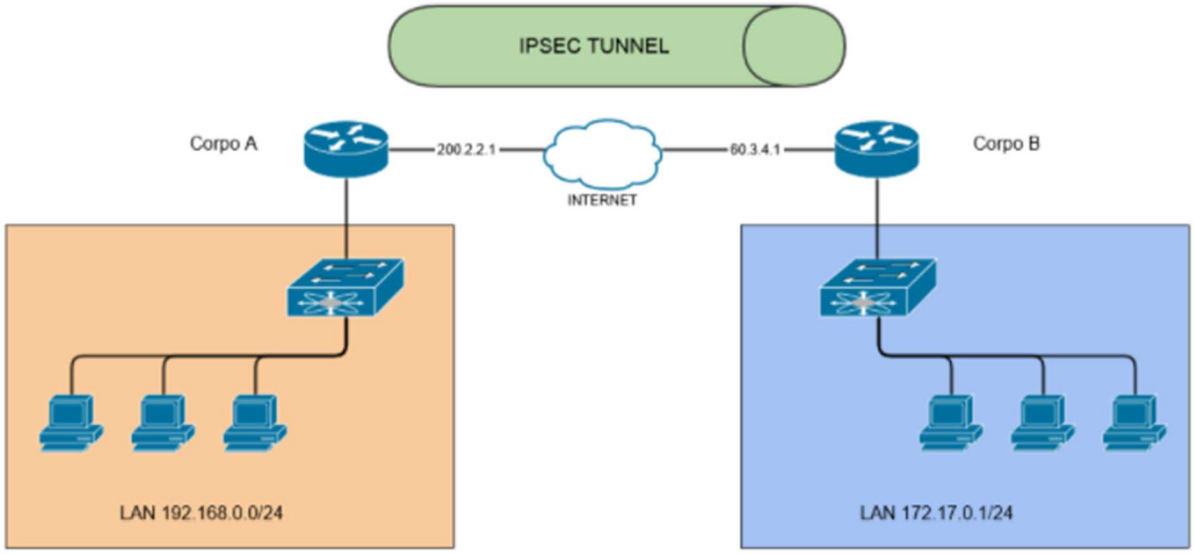


Рисунок 1.4 – Site-to-site VPN

Технологія створення тунелів має широкий спектр застосовування при формуванні захищених каналів доступу. Для реалізації цього використовуються протоколи на таких рівнях: канальний, мережевий і транспортний.

1. Канальний рівень. Використовуються протоколи PPTP та L2TP.

PPTP (Point-to-Point Tunnelling Protocol) працює лише на пристроях, робота яких базується на Windows, та використовує TCP / IP. За допомогою даного протоколу будується тунель до сервера одержувача, по якому передаються PPP-пакети. Після

цього сервер і комп'ютер-клієнт починають обмінюватись службовими пакетами. Далі відбувається інкапсуляція даних: PPP-кадр інкапсулюється в пакет GRE, який у свою чергу інкапсулюється в кадр з додаванням IP-заголовку. У цьому заголовоку зазначаються адреси одержувача та відправника пакету. Далі PPTP вказує відповідні PPP закінчення та заголовок (рис.1.5). [14,64,66]

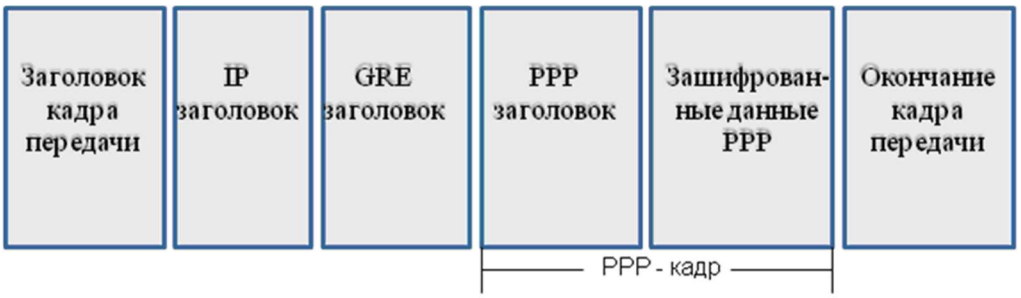


Рисунок 1.5 – Структура даних для пересилання по тунелю PPTP

У PPTP виявлено велику кількість недоліків. Замість нього рекомендується використовувати L2TP (Layer 2 Tunneling Protocol). Він створює VPN-мережі з розмежуванням прав доступу. L2TP використовує UDP протокол як транспорт. А також застосовує аналогічний формат повідомлень для управління сконфігуреним тунелем і передачі пакетів. Даний прокол інкапсулює кадри PPP у протокол мережевого рівня, попередньо проводить аутентифікацію користувача. L2TP додає заголовок PPP, потім заголовок L2TP до поля інформаційних даних PPP. Отриманий пакет інкапсулюється за допомогою UDP. «L2TP може шифрувати UDP повідомлення та додавати до них заголовок і закінчення Encapsulating Security Payload (ESP). Після цього відбувається інкапсуляція в IP. Додається IP-заголовок, який містить адреси одержувача та відправника. [14,36,64,66] Вже після цього L2TP виконує другу PPP-інкапсуляцію по підготовці даних до відправлення.» [14]

Комп'ютер користувача одержує пакети. Далі відбувається обробка PPP закінчення та PPP заголовку, при цьому заголовок IP видаляється з пакету. Після цього обробляється UDP заголовок, і для визначення тунелю вже використовується L2TP

заголовок (рис.1.6). Після виконання вищевказаних дій у PPP пакеті залишаться лише актуальні дані, які будуть направлені користувачеві. [14,31]

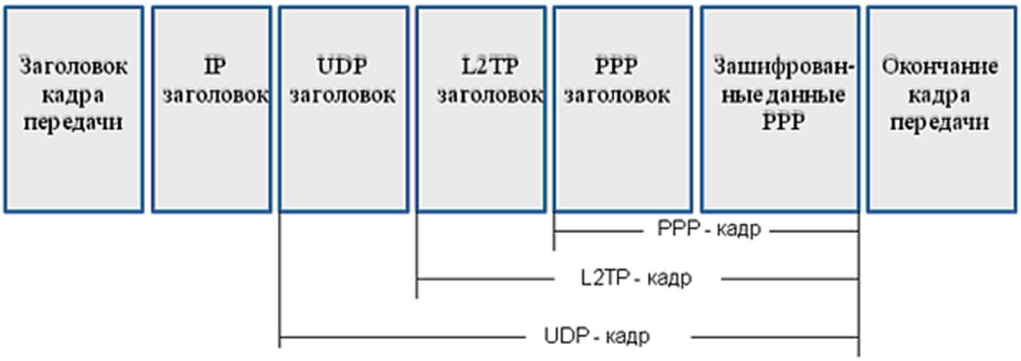


Рисунок 1.6 – Структура даних для пересилання по тунелю L2TP

2. Мережевий рівень представлений набором протоколів IPSec:

– AH (Authentication Header) гарантує цілісність заголовків та даних всередині пакетів, однак не в змозі забезпечити їх конфіденційність; [43]
– ESP (Encapsulating Security Payload) – шифрує та захищає цілісність інкапсульованих IP пакетів, додатково аутентифікує ESP заголовок і гарантує конфіденційність цих даних; [54]
– IKE (Internet Key Exchange). Передає граничним вузлам захищеного каналу згенеровані шифрувальні ключі. [54]

Існує два режими роботи IPSec: тунельний (забезпечує захист пакета та його заголовку) та транспортний (захищає дані всередині пакету).

Тунельний режим IPSec (рис. 1.7):

– здійснюється додавання нового заголовка в IP-пакет;
– здійснюється інкапсуляція та шифрування первинного IP-заголовку;
– адреса відправника та отримувача може бути змінена на адресу граничного шлюзу;
– шлюз VPN або вузол отримувача здійснює інкапсуляцію. [48,46,54]

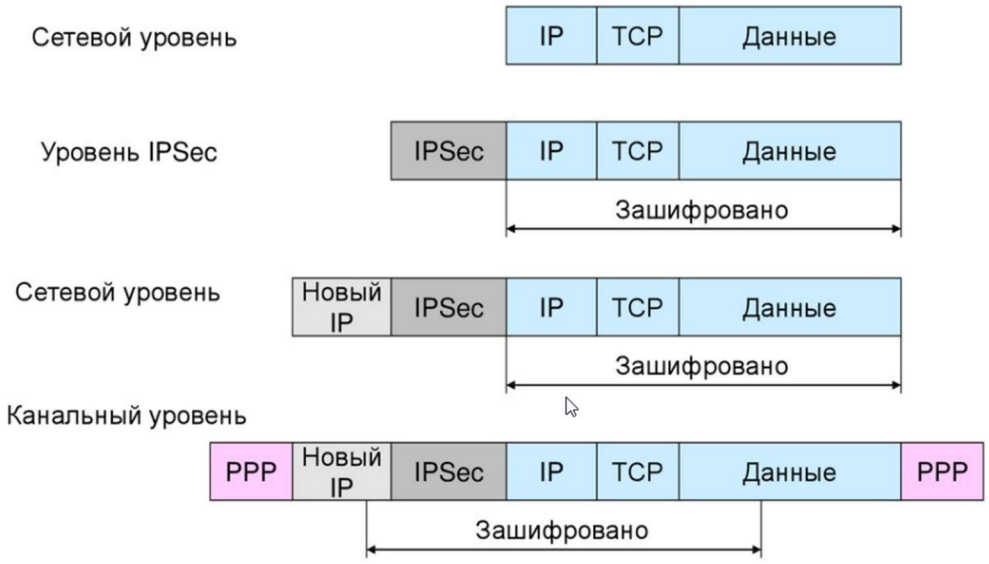


Рисунок 1.7 – Інкапсуляція IPSec для тунельного режима

Транспортний режим IPSec (рис. 1.8):

- використовується первинний IP-заголовок;
- не змінюються адреси відправника та отримувача;
- кінцеві пристрої здійснюють інкапсуляцію даних. [48,46,54]

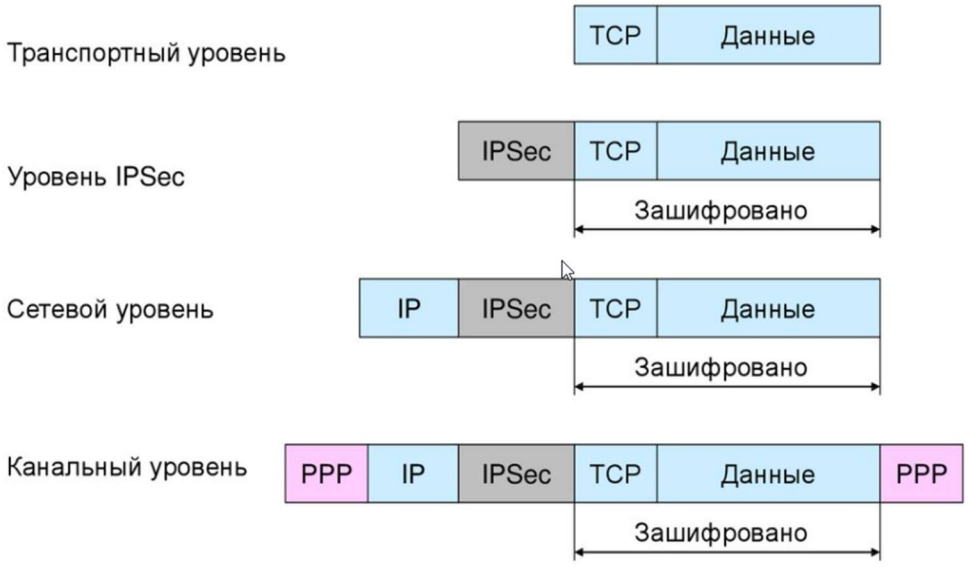


Рисунок 1.8 – Інкапсуляція IPSec для транспортного режиму

3. На транспортному рівні використовується протокол SSL/TLS. Даний протокол надає шифрування та можливість аутентифікації на транспортному рівні між отримувачем та відправником. Протокол складається з наступних фаз:

- для встановлення діалогу між учасниками сесії обирається алгоритм шифрування;
- відбувається аутентифікація за допомогою сертифікатів або за допомогою обміну ключами;
- здійснюється обмін даними, які зашифровані за допомогою симетричних алгоритмів шифрування. [55]

Протокол SSL складається з наступних протоколів:

- Протокол запису SSL (SSL record protocol);
- Протокол рукостискання (Handshake protocol)
- Протокол специфікації шифру змін (Change-cipher spec protocol)
- Протокол оповіщення (Alert protocol) [15,49,53]

Протокол SSL record за допомогою сесій забезпечує цілісність та конфіденційність. Даний протокол надає можливість інкапсулювати протоколи вищого рівня. SSL record протокол здійснює поділ даних на окремі частини. Надалі до усіх поділених частин додається аутентифікаційний код, шифруються дані та додається новий SSL заголовок. [15,53]

Протокол Handshake направляє короткі повідомлення учасникам сесії, за допомогою яких здійснює їх аутентифікацію. Таким чином, забезпечується надійне з’єднання. Протокол працює наступним чином:

- відбувається пінг між сервером та клієнтом;
- після вдалого пінгу клієнт отримує від серверу ключ обміну та сертифікат;
- у відповідь сервер отримує від клієнта його ключ-обмін та сертифікат ;
- запускається Change-cipher spec протокол. [15,49,53]

Change-cipher spec протокол складається з зашифрованого повідомлення розміром в один байт. Він потрібен для копіювання очікуваного стану у поточний. Очікуваний стан буде в тому випадку, якщо не буде завершений протокол Handshake. В іншому випадку, стан зміниться на поточний. [15,53]

Передача сповіщень для SSL реалізується за допомогою протоколу Alert. Записуватись може або попереджуюче, або фатальне повідомлення. Кожне повідомлення в цьому протоколі складаються з двох байтів та є зашифрованим. [15,53]

1.4 Постановка задачі

У сучасних умовах дистанційної роботи зростає увага до безпеки корпоративних мереж. Аналіз, проведений в рамках першого розділу показав, що питання організації віддаленого доступу вирішує VPN, використовуючи різні протоколи на кожному рівні.

Враховуючи актуальність проблеми, в ході дипломної роботи необхідно:

1. Порівняти технології побудови VPN мережі та визначити яку з них краще використовувати для з’єднання між офісами, а яку – для організації віддаленого доступу до робочого місця.

2. Визначити способи підсилення захисту VPN мережі.

3. Розробити та побудувати схему максимально захищеного доступу віддалених співробітників до корпоративної мережі з розподіленими офісами за допомогою IPSec VPN та SSL VPN.

Розроблена модель дозволе компаніям швидко налаштувати вискозахищений доступ до корпоративної мережі.

2 ВИБІР VPN ТЕХНОЛОГІЇ ДЛЯ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ВИСОКОЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

2.1 Вибір VPN технології

Для вирішення задачі організації високозахищеного віддаленого доступу співробітників до корпоративної мережі з доступом до інформації в декількох офісах слід перш за все обрати яка технологія створення VPN мережі буде використовуватися між офісами та між власним пристроєм користувача та офісом, в якому знаходиться його робоча станція.

Існує велика різноманітність технологій створення VPN мереж [32] (рис. 2.1):

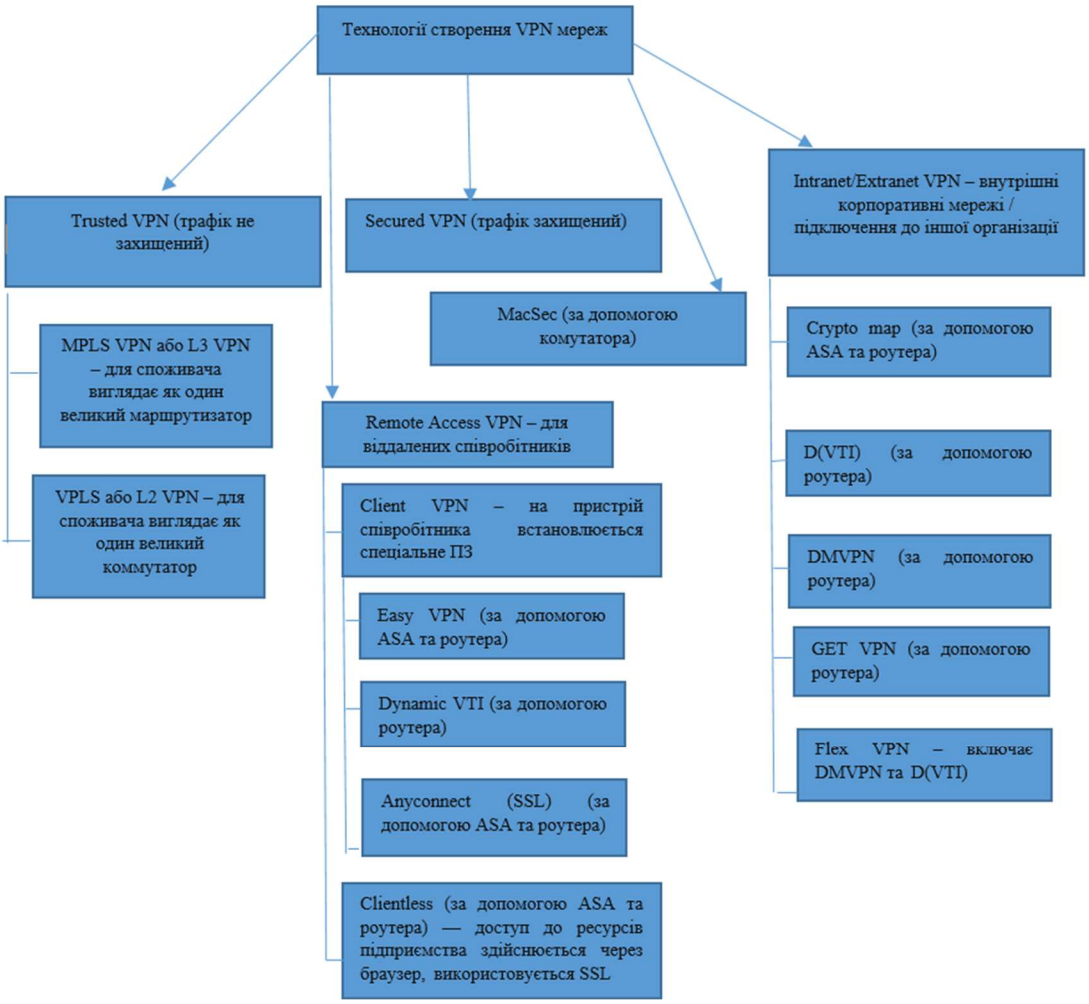


Рисунок 2.1 – Технології створення VPN мереж

Найчастіше виникає питання що краще обрати при реалізації VPN технології – IPsec або SSL VPN. Для вирішення цієї задачі можна побудувати наступний майндмепінг (рис. 2.2):

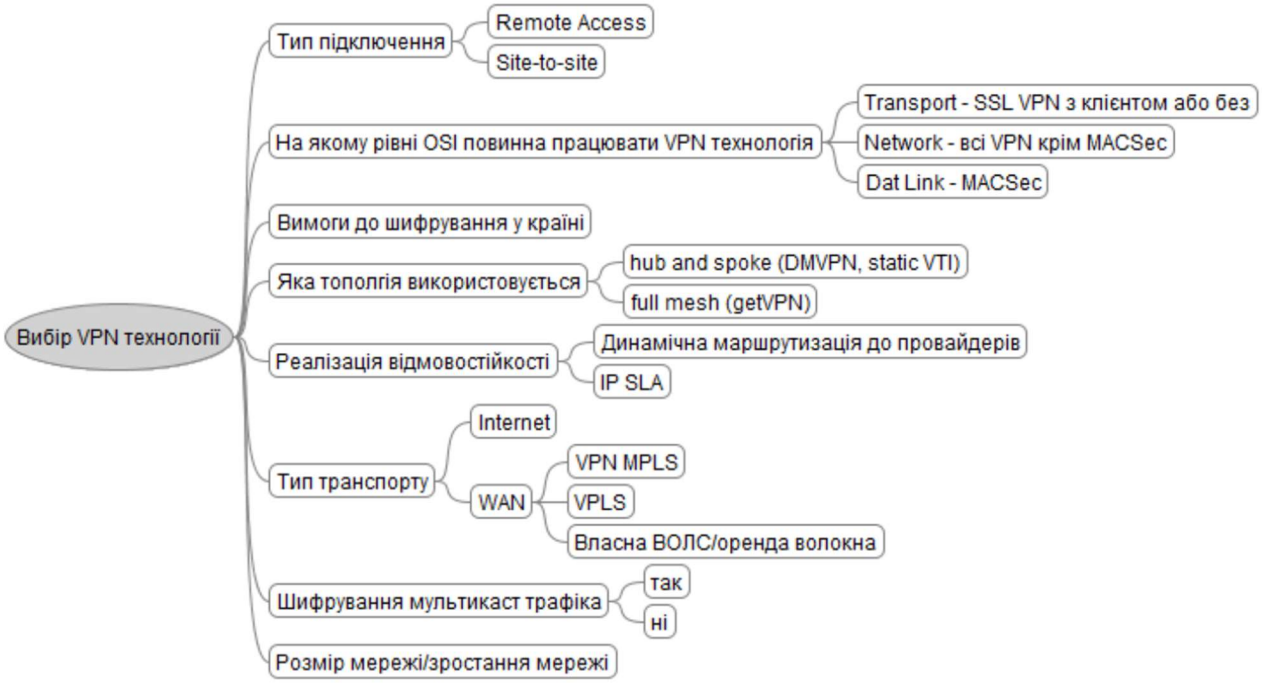


Рисунок 2.2 – Майндмепінг для вибору VPN технології

За допомогою рис 2.2. можна вирішити яку технологію VPN обрати. Оскільки найбільш безпечними є IPsec VPN та SSL VPN, то вибір будемо здійснювати серед даних технологій. Але для початку визначимо їх основі особливості.

Для з’єднання декількох офісів компанії IPsec VPN є найбільш економічним варіантом. Тому що для організації даної технології немає потреби витрачатися на відокремлені лінії зв’язку, все засновано лише на Інтернет. Безперебійний зв’язок між офісами створюється за допомогою єдиного IP-простору за рахунок налаштування високозахищених тунелів. Для того, щоб застосувати IPsec технологію на існуючих пристроях потрібно зробити відповідні налаштування та встановити додаткове ПЗ, а це в свою чергу сприяє підвищенню захисту. [42,49,58]

З іншого боку, крім вище зазначених переваг, існує ряд недоліків IPsec VPN:

- якщо розглядати IPsec для відділених співробітників, то у цьому випадку компанія повинна буде запровадити додаткові налаштування VPN клієнту з індивідуальною конфігурація IPsec. А це призведе до додаткових витрат;
- робота IPsec може погіршуватися за рахунок того, що шифрування сприяє збільшення трафіку в мережі;
- IPsec немає можливості розмежувати доступ до ресурсів компанії, тому кожен користувач має необмежений доступ;
- для встановлення IPsec тунелю необхідно пройти процедуру узгодження відкриття необхідних портів, які за замовченням можуть бути закритими. [58]

При використанні SSL VPN таких проблем не виникає. Для SSL VPN необхідне просте налаштування та використанні відкритих портів. Додаткове встановлення ПЗ на пристрої користувачів не є необхідним. Співробітник повинен знати лише логін та пароль, а також необхідну ip адресу. [55]

SSL VPN може бути двох видів:

1. Client SSL VPN з використанням ПЗ Cisco AnyConnect:

- може бути встановлений на пристрої як мобільний додаток;
- оцінується стан ПК віддаленого клієнта;
- структура клієнта є модульною;
- трафік спрямовується до Cisco Web Security Appliance. [32,55,58]

2. Clientless SSL: Публікація http та https ресурсів повинна бути здійснена на сервері компанії. На Cisco ASA завантажуються відповідні модулі.

Таким чином, SSL VPN має наступні переваги:

- організовує високозахищений доступ до ресурсів організації з зовнішніх вузлів;
- налаштування на стороні користувачів майже не потрібні;
- не потребує додаткового ПЗ з боку віддаленого клієнта;
- можна виділити ресурси, доступ до яких будуть мати лише окремі користувачі. [32,55,58]

Проте, SSL VPN має і свої недоліки:

– потрібно проводити певні налаштування для додатків, які працюють без використання Інтернет
– швидкість передачі трафіку знижується через необхідність шифрування та подальшого дешифрування. [32,55,58]

З характеристик IPsec VPN та SSL VPN можна зробити висновок, що вони можуть функціонувати одночасно або окремо. Можна виділити наступні критерії для вибору IPsec VPN та SSL VPN для певних випадків та вибрати відповідну технологію для кожного з них (рис. 2.3).

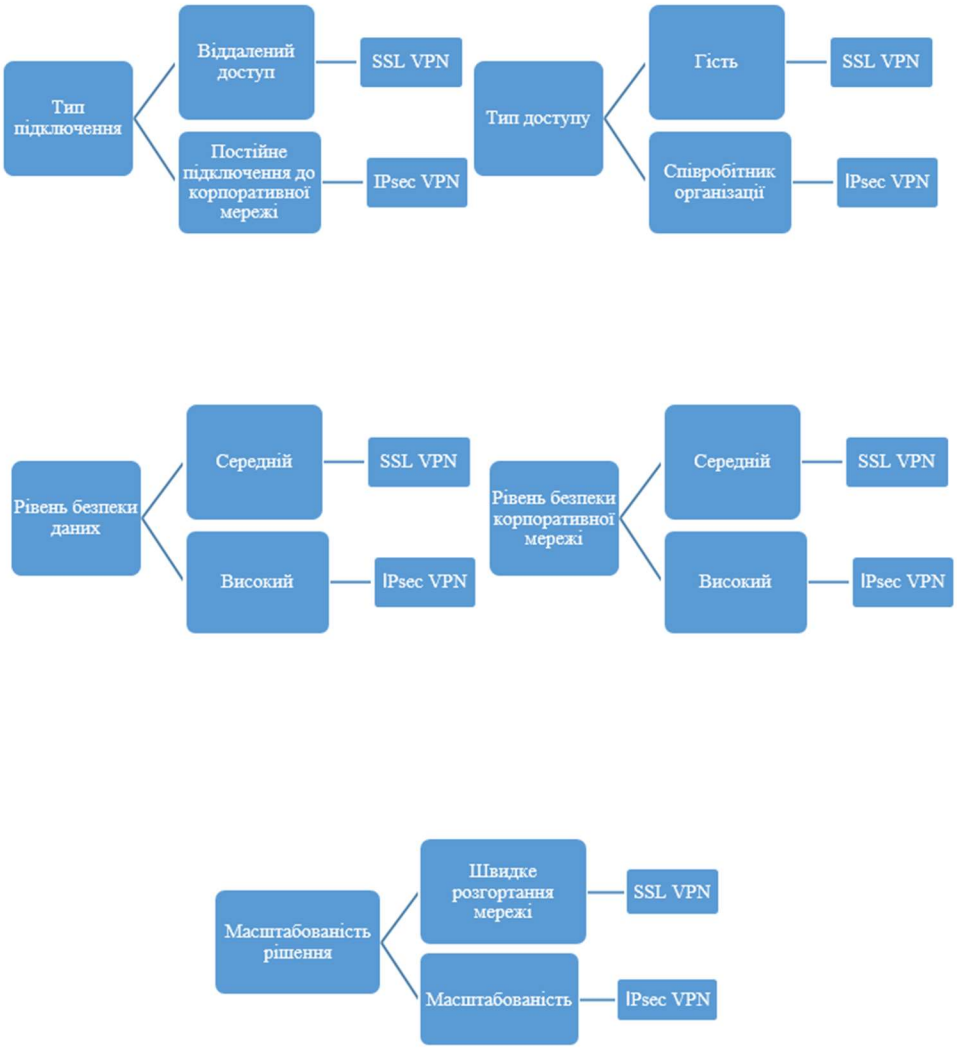


Рисунок 2.3 – Критерії вибору між IPsec VPN та SSL VPN

На основі вище вказаного можна порівняти можливості IPsec VPN та SSL VPN (табл. 2.1).

Таблиця 2.1 – Порівняння можливостей IPsec VPN та SSL VPN

Характеристика	IPsec VPN	SSL VPN
Підтримка термінального доступу	+	+
Підтримка доступу до файлових серверів	+	+
Підтримка HTTP додатків	+	+
Підтримка бізнес додатків	+	+
Мобільний ПК	+	+
Корпоративний ПК	+	+
Публічний ПК	- (необхідна установка клієнта)	+
Робота із іншої мережі (за межмережевим екраном)	- (відкриття портів)	+ (через https)
Централізована авторизація	+	+
Можливість підвищеної аутентфифікації	+ (у більшості випадків)	+
Автоматичне застосування політик	- (вимагає додаткових рішень)	+
Легкість впровадження	Залежить від рішення	+
Безклієнтська технологія	-	+ (достатньо Internet)

Таким чином, найбільш захищеним варіантом буде поєднання використання IPsec VPN та SSL VPN. Для побудови захищеної корпоративної мережі між

віддаленими офісами будемо використовувати IPsec VPN, а для налаштування віддаленого доступу для співробітників – SSL VPN.

2.2 Підсилення захисту VPN

Оскільки для віддаленого доступу співробітників ми будемо використовувати SSL VPN технологію, то потрібно враховуючи всі ризики та підсилити захист. Для підключення через SSL VPN та підвищення захисту для користувачів запроваджується певна кількість перевірок. В першу чергу, це стосується проходження аутентифікації. Така аутентифікації може бути трьох видів: сертифіката, імені користувача та пароля, або їх комбінація.

Процес аутентифікації імені користувача та пароля відбувається за наступними етапами:

1. Користувач для входу в систему вводить логін та пароль, які відправляються на SSL VPN шлюз.

2. Аутентифікація користувача відбувається на AAA сервері, який отримує пароль та логін від SSL VPN шлюзу. [53,56]

Для авторизації лише сертифікатів не потрібно вводити логін і пароль. Сервер отримує сертифікат авторизації, обліку та аутентифікації від користувача. Дана авторизація відбувається в такій послідовності:

1. Користувач намагається отримати доступ до WebVPN за допомогою сертифікату аутентифікації AAA.

2. Шлюз WebVPN перевіряє клієнта за допомогою сертифікату автентифікації AAA, який був надісланий клієнтом.

З’єднання не буде встановлено у випадку підтвердження недійсності сертифікату. В іншому випадку з’єдання успішно встановлюється.

3. Відбувається перевірка даних користувача на AAA сервері для підтвердження їх відповідності даним в сертифікаті. [53,56]

У комбінованій авторизації користувач вводить логін і пароль та надає сертифікат аутентифікації AAA. Даний процес відбувається наступним чином:

1. Здійснюється перевірка особи клієнта та сертифіката.

2. Для користувача відкривається сторінка авторизації

3. Користувач зазначає логін та пароль.

4. На AAA сервер надходить запит від WebVPN про аутентифікацію та авторизацію.

5. Далі списки користувачів, налаштовані на AAA, будуть використовуватись для авторизації та аутентифікації. [56]

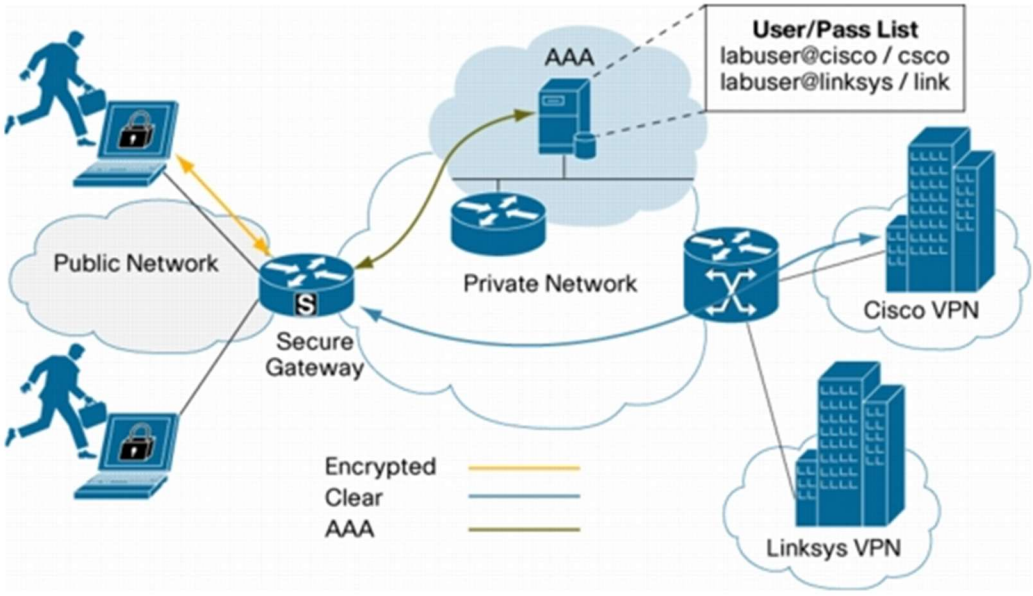


Рисунок 2.4 – Топологія Cisco SSL VPN з AAA Server

Для забезпечення більшої безпеки при підключенні віддалених співробітників до мережі компанії рекомендується зробити VPN більш захищеним за рахунок встановлення VPN клієнта та двофакторної авторизації.

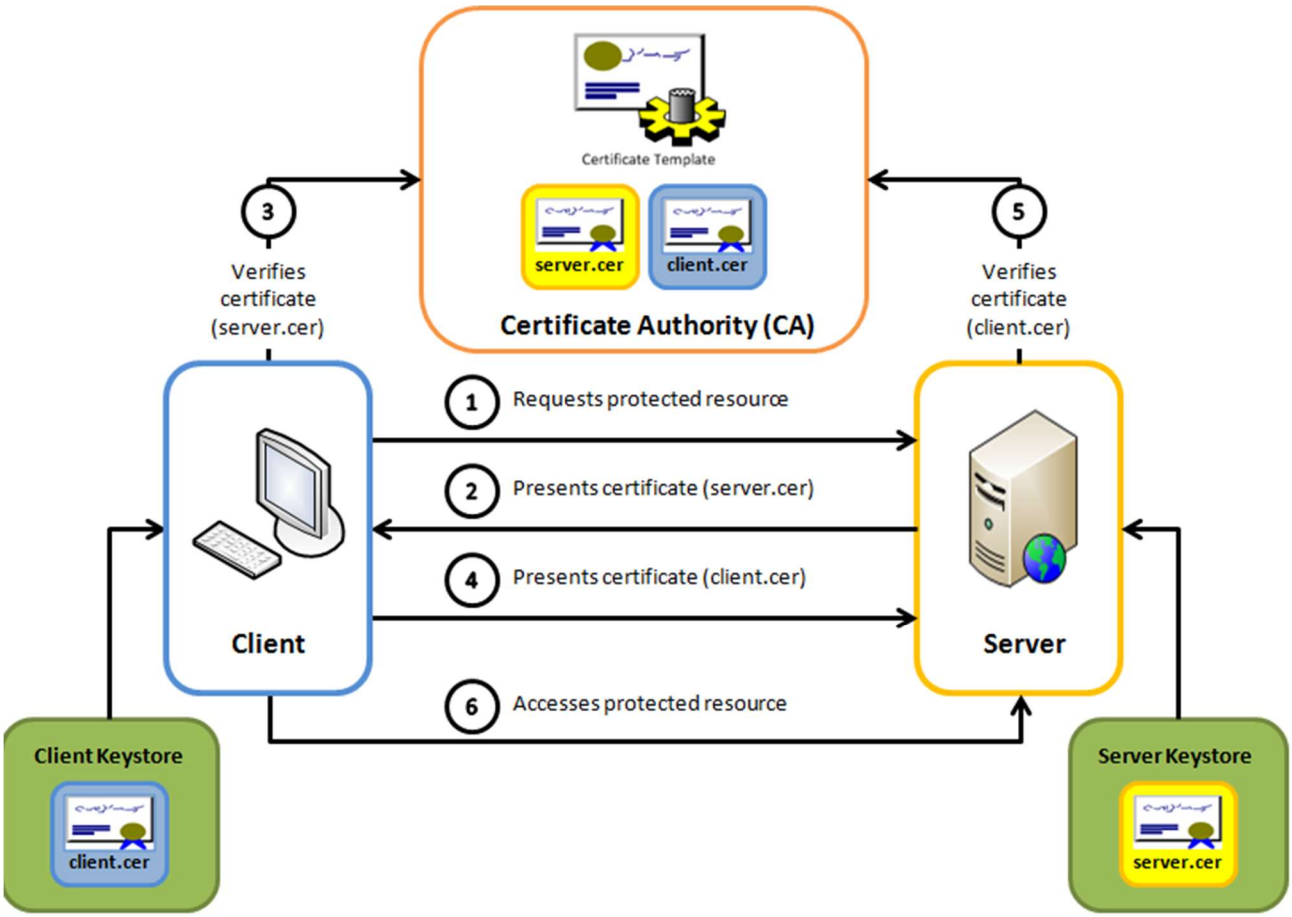


Рисунок 2.5 – Взаємна аутентифікація SSL на основі сертифікатів

«Двофакторна аутентифікація (2FA) – це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи аутентифікаційних даних.» [21]

Для підвищення захисту облікових даних користувачів крім звичайних паролів 2FA запроваджує додаткову перевірку особи. Це збільшує захист обікового запису від зловмисників. [21,62]

Реалізація 2FA вимагає від користувача наявність хоча б двох з наведених нижче видів ідентифікаційних даних:

– те, що йому відомо (те, що співробітник буде вводити при намаганні увійти в систему, наприклад пін-код або пароль);
– те, чим він володіє (токен, яким користувач володіє);

– те, що йому властиве (біометричні дані: відбитки пальців, сканери обличчя або сітківки ока). [21]

2FA можна організувати наступними способами:

1. Одноразовий пароль

У процесі 2FA користувач вводить свій обліковий логін та пароль, а також одноразовий пароль, який йому надійшов на телефон або електрону пошту. Такий пароль забезпечує більш високий захист після перевірки пароля користувача. Він надсилається у вигляді цифр та є короткостроковим.

2. Аутентифікація на основі програмного забезпечення

Забезпечується за рахунок завантаження користувачем відповідного додатку на мобільний телефон. Коли користувач здійснює вхід у такий додаток, то автоматично генерується певна комбінація символів кожну хвилину, які також отримує і сервер. Користувач вводить згенерований пароль, який звіряється з тим кодом, який отримав сервер. І якщо вони є однаковими, то вхід буде дозволено. [61,62,65,67]

3. Резервний код

Якщо з певних причин користувач немає доступу до телефону, додатку, електронної пошти та відповідно не має змоги ввести другий пароль, то можна запросити резервний код, яким можна скористатися один раз. [62,65]

4. Апаратна аутентифікація

Реалізується за допомогою ключа, який знаходиться на USB-накопичувачі. Такий ключ є так званим ідентифікатором користувача, за яким буду здійснена перевірка. Таким чином, це зменшує шанси доступу небажаних осіб до ресурсів компанії, навіть якщо вони отримали доступ до мобільного телефону користувача). [62]

Найбільш популярним VPN клієнтом для 2FA є Cisco AnyConnect. Даний додаток можна легко завантажити та встановити або на мобільний телефон або ПК з будь-якою ОС. Завдяки цьому компанія може швидко організувати віддалений доступ для користувачів, які працюють за межами офісу.

У табл. 2.2 наведено порівняння Clientless SSL VPN та AnyConnect.

Таблиця 2.2 – Порівняння Clientless SSL VPN та AnyConnect

	Clientless SSL VPN	AnyConnect
Досвід користувача	Web-браузер для доступу до різних додатків	Такий як для офісних додатків
Контроль доступу	На URL-рівні	Мережевий ACL: IP, TCP/UDP-порти, SGT
Інсталяція клієнтського ПО	Не потрібно, використовується браузер	Потрібно, товстий клієнт
Можливі проблеми сумісності	Нові версії браузерів та додатків	Не потребує повторної інсталяції та підтримки

Крім зазначених переваг у використанні, Cisco AnyConnect може підтримувати додаткові функцій:

1. Always-On VPN. Дана функція забезпечує постійний захист, якщо співробітник працює за межами корпоративної мережі через автоматичне підключення VPN. [1]

2. Split tunneling. Підходить для співробітників, які працюють віддалено за власним ПК. Функція розподілу тунелів реалізується через забезпечення шифрування лише трафіку до мережі компанії, інший трафік залишається без шифрування. [1]

3. Per App VPN. Компанія може встановлювати різні правила для груп співробітників, таким чином лише окремий трафік буде шифруватися. [1]

На прикладі клієнта Cisco AnyConnect розглянемо як відбувається 2FA (рис. 2.6):

1. Користувач відкриває Cisco AnyConnect Client. Вводить свій логін, пароль та другий пароль, який він отримав за допомогою додатку.

2. ASA відправляє до ISE для аутентифікації логін та пароль.

3. Для аутентифікації ISE використовує Active Directory (AD), результат відправляється до ASA.

4. VIP Enterprise Gateway (VIP EGW) отримує від ASA пароль та логін.

5. EGW відправляє запит на аутентифікацію до Symantec VIP Authentication Service.

6. До VIP EGW надходить відповідь на аутентифікацію.
7. Міжмережевий екран ASA отримує кінцевий результат аутентифікації.
8. Користувач отримує доступ, якщо аутентифікації пройшла успішно. [39]

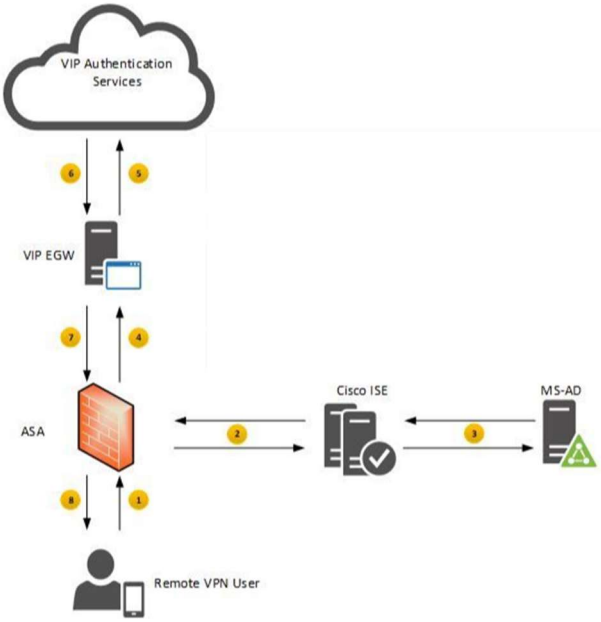


Рисунок 2.6 – Топологія 2 FA

Не рекомендується встановлювати більше одного захисного клієнта на ПК. Більш доцільно для вирішення широкого спектру задач встановити один VPN клієнт, який буде відповідати за безпеку доступу, аутентифікацію та ідентифікацію. Такий підхід дозволить заощадити ресурси ПК та вплине на його продуктивність.

3 РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ ВИСОКОЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

3.1 Реалізація моделі високозахищеного віддаленого доступу для підприємства

На рис. 3.1 наведена схема захищеного доступу до серверів офісу в м. Київ для співробітників офісів у м. Київ та м. Суми. Тунель між офісами побудований на основі IPsec VPN. Доступ до серверів обмежується за технологією Client SSL VPN (Cisco AnyConnnect).

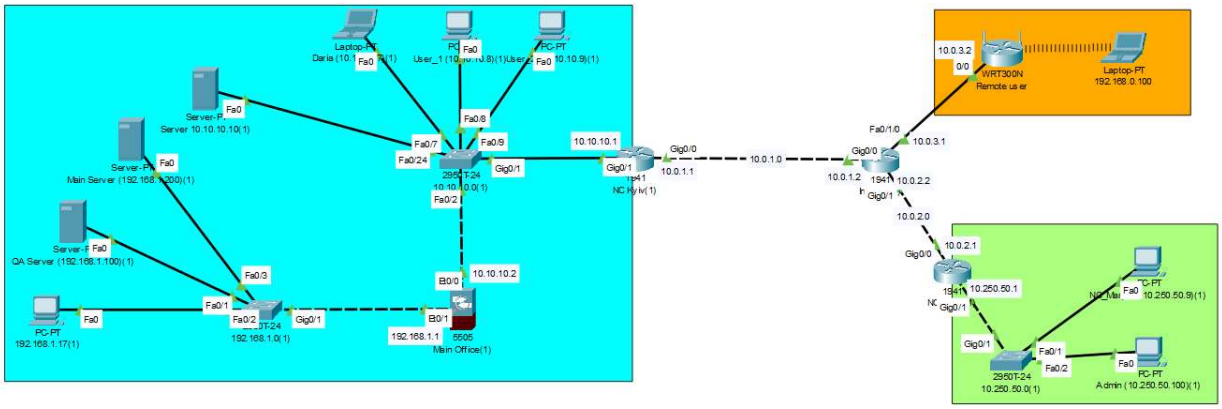


Рисунок 3.1. – Схема IPsec VPN та SSL VPN для віддаленого офісу та віддаленого співробітника

Конфігурація роутерів, серверу та необхідні команди наведені в Додатку А. За допомогою вказаних команд можна зробити відповідні налаштування на ASA та AAA сервері, до якого ASA буде звертатися при спробі співробітників компанії підключитися до захищених серверів за допомогою Cisco AnyConnect. При цьому за допомогою налаштувань на граничних роутерах офісів компанії встановлюється IPsec тунель.

3.2 Реалізація технології IPsec VPN та SSL VPN для віддаленого офісу за допомогою Cisco Packet Tracer

Модель віддаленого доступу була реалізована за допомогою Cisco Packet Tracer. Але враховуючи особливості та обмеження даної програми, насамперед додавання SSL клієнта, неможливо показати Client SSL (Anyconnect VPN), а також IPsec VPN для віддаленого офісу та SSL VPN для віддаленого співробітника в одній схемі. Тому було побудовано дві моделі:

- IPsec VPN та SSL VPN для віддаленого офісу
- Clientless SSL VPN для віддаленого співробітника

На рис. 3.2 наведена схема захищеного доступу до серверів офісу в м. Київ для співробітників офісів у м. Київ та м. Суми. Тунель між офісами побудований на основі IPsec VPN. Доступ до серверів обмежується за технологією SSL VPN.

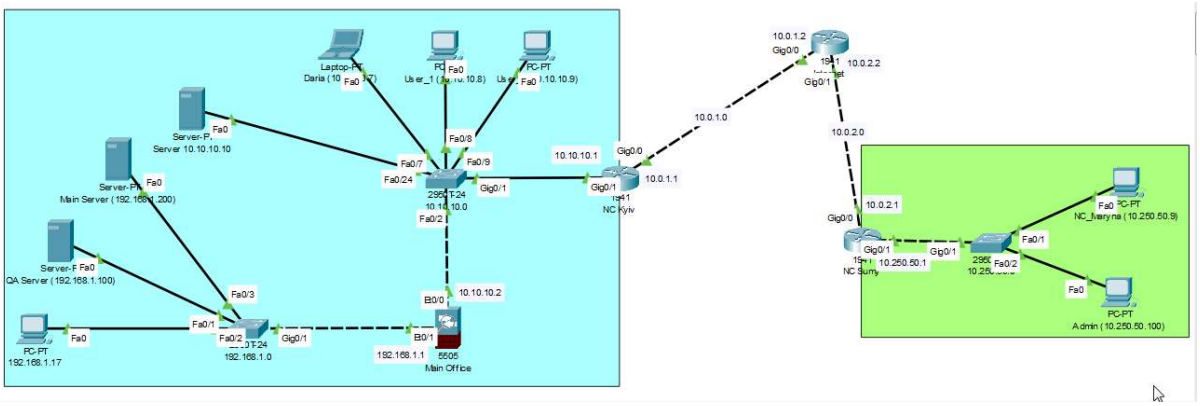


Рисунок 3.2 – Схема IPsec VPN та SSL VPN для віддаленого офісу

У табл. 3.1 та табл. 3.2 наведено IP адреси пристроїв та права доступу користувачів до серверів.

Таблиця 3.1 – IP адреси пристроїв

Device	Interface	IP address	Subnet mask	Default gateway
NC Sumy router	g0/1	10.250.50.1	255.255.255.0	N/A
	g0/0	10.0.2.1	255.255.255.0	N/A
Internet router	g0/1	10.0.2.2	255.0.0.0	N/A
	g0/0	10.0.1.2	255.0.0.0	N/A
NC Kyiv router	g0/1	10.10.10.1	255.0.0.0	N/A
	g0/0	10.0.1.1	255.0.0.0	N/A
Main office ASA	vlan 1	192.168.1.1	255.255.255.0	N/A
	vlan 2	10.10.10.2	255.255.255.0	N/A
PC NC_Maryna	Fa0	10.250.50.9	255.0.0.0	10.250.50.1
PC Admin	Fa0	10.250.50.100	255.0.0.0	10.250.50.1
PC-PT	Fa0	192.168.1.17	255.255.255.0	192.168.1.1
Laptop PT-Daria	Fa0	10.10.10.7	255.255.255.0	10.10.10.1
PC-PT User1	Fa0	10.10.10.8	255.255.255.0	10.10.10.1
PC-PT User2	Fa0	10.10.10.9	255.255.255.0	10.10.10.1

Таблиця 3.2 – Права доступу користувачів до серверів

Login	Password	Available servers
Maryna	123123123	Main Server
Admin	999777555	Main Server
Daria	12345678	N/A

Для вирішення поставленої задачі були виконані наступні налаштування на пристроях мережі.

Конфігурація IPsec на NC Sumy router:

Configure terminal

1. Задаємо IP адреси інтерфейсам:

interface g0/1

ip address 10.250.50.1 255.255.255.0

no shut

interface g0/0

ip address 10.0.2.1 255.255.255.0

no shut

2. Додаємо на роутер необхідний модуль безпеки:

license boot module c1900 technology-package securityk9

exit

3. Зберігаємо налаштування:

copy running-config startup-config

reload

show version

Configure terminal

4. Налаштовуємо IPSec тунель:

access-list 100 permit ip 10.250.50.0 0.0.0.255 10.10.10.0 0.0.0.255

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

exit

crypto isakmp key password address 10.0.1.1

crypto ipsec transform-set NC_Sumy-to-NC_Kyiv esp-aes 256 esp-sha-hmac

crypto map IPSEC 10 ipsec-isakmp

set peer 10.0.1.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set NC_Sumy-to-NC_Kyiv

match address 100

5. Перевіряємо роботу сконфігурованого IPSec шлюзу (рис. 3.3):

interface GigabitEthernet0/0

crypto map IPSEC

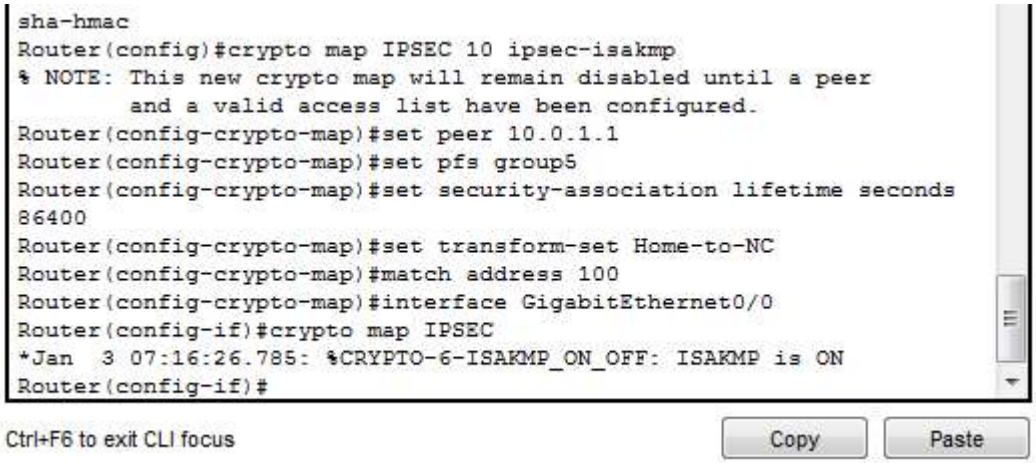


Рисунок 3.3 – Перевірка стану IPSec на NC Sumy router

Конфігуарція Internet router:

1. Задаємо IP адреси інтерфейсам:

Configure terminal

interface g0/1 ip address 10.0.2.2 255.0.0.0

no shut

interface g0/0 ip address 10.0.1.2 255.0.0.0

no shut

Конфігурація Ip sec на NC Kyiv router:

1. Задаємо IP адреси інтерфейсам:

Configure terminal

interface g0/1 ip address 10.10.10.1 255.0.0.0

no shut

interface g0/0 ip address 10.0.1.1 255.0.0.0

no shut

conf t

2. Додаємо на роутері необхідний модуль безпеки:

license boot module c1900 technology-package securityk9

exit

3. Зберігаємо налаштування (рис.3.4):

copy running-config startup-config

reload

show version

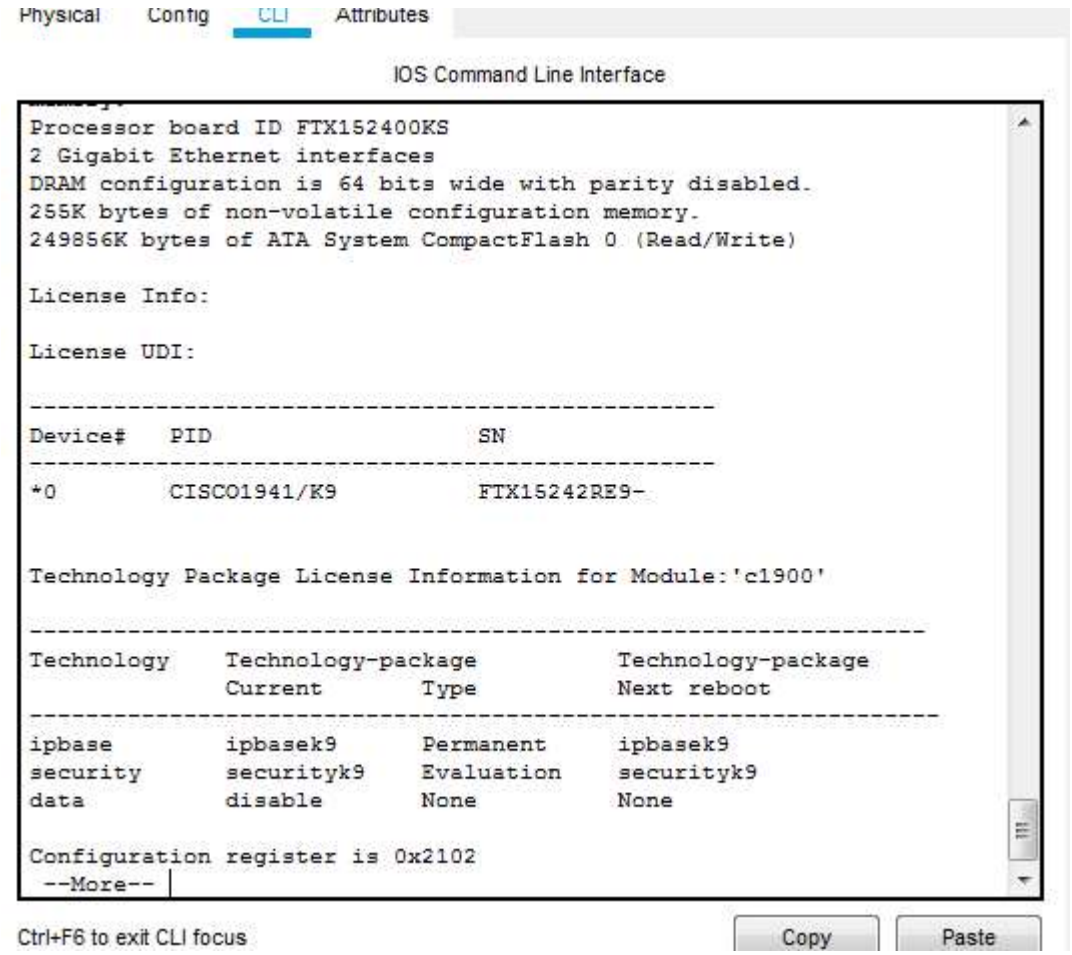


Рисунок 3.4 – Перевірка підключення додаткових модулей безпеки

Configure terminal

4. Налаштовуємо IPSec тунель:

access-list 100 permit ip 10.10.10.0 0.0.0.255 10.250.50.0 0.0.0.255

crypto isakmp policy 10 encryption aes 256 authentication pre-share group 5

exit

crypto isakmp key password address 10.0.2.1

crypto ipsec transform-set NC_Kyiv-to-Home esp-aes 256 esp-sha-hmac

crypto map IPSEC 10 ipsec-isakmp

set peer 10.0.2.1

set pfs group5

set security-association lifetime seconds 86400

set transform-set NC-to-Home

match address 100

5. Перевіряємо роботу сконфігурованого IPSec шлюзу (рис. 3.5):

interface GigabitEthernet0/0

crypto map IPSEC

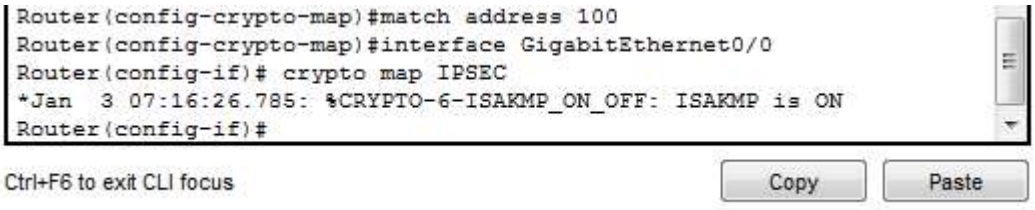


Рисунок 3.5 – Перевірка стану IPSec на NC Kyiv router

Конфігурація Main office ASA:

Configure terminal

1. Встановлюємо IP адреси Vlan-ів:

Hostname ASA1

Interface vlan 1

Nameif inside

Security-level 100

Ip address 192.168.1.1 255.255.255.0

exit

Interface vlan 2

Nameif outside

Security-level 0

Ip address 10.10.10.2 255.255.255.0

Exit

2. Вмикаємо функцію Webvpn для роботи віддалених користувачів:

Webvpn

Enable outside

Object network lan

Subnet 192.168.1.0 255.255.255.0

Exit

3. Додаємо дані користувачів:

username Maryna password 123123123

username Admin password 999777555

username Daria password 12345678

4. Конфігуруємо адреси серверів (рис. 3.6):

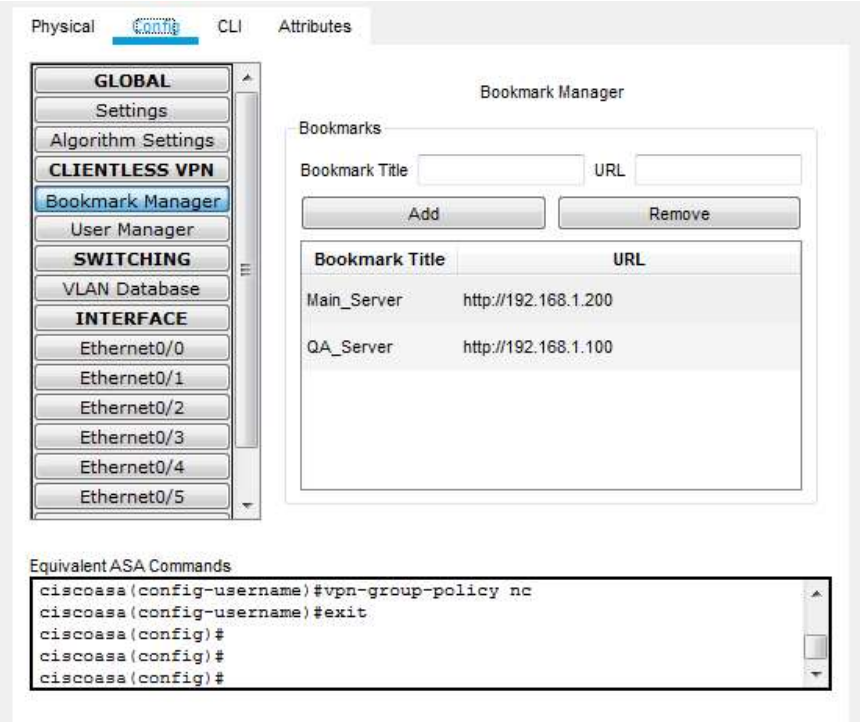


Рисунок 3.6 – Налаштування адрес серверів на Main office ASA

5. Налаштовуємо доступ для користувачів (рис. 3.7):

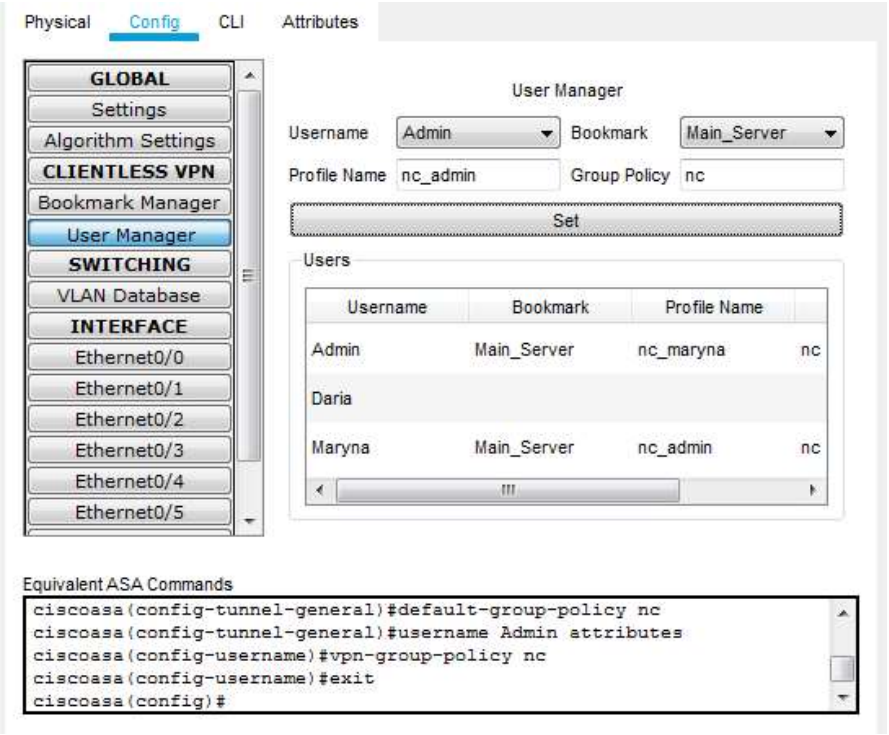


Рисунок 3.7 – Налаштування доступу для користувачів на Main office ASA

Перевіримо шифрування трафіку за допомогою команди show crypto ipsec sa (рис. 3.8):

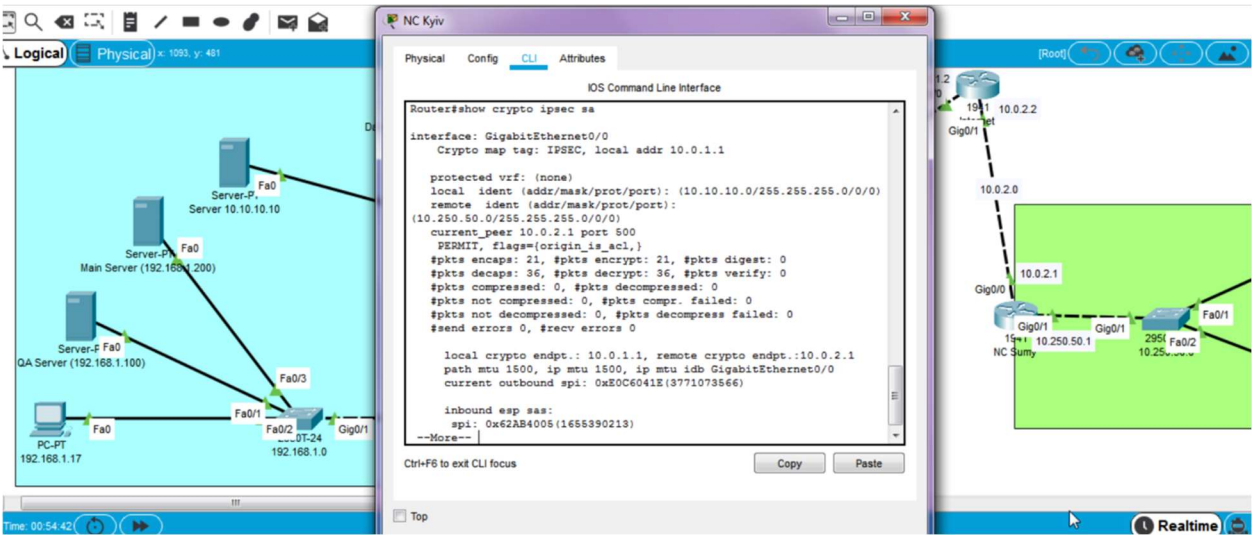


Рисунок 3.8 – Перевірка шифрування трафіку за технологією IPsec

Після налаштування IPsec та SLL можна протестувати доступи користувачів до серверів. Користувач Maryna має доступ до Server 10.10.10.10 без необхідності введення пароля, тільки через IPsec (рис. 3.9).

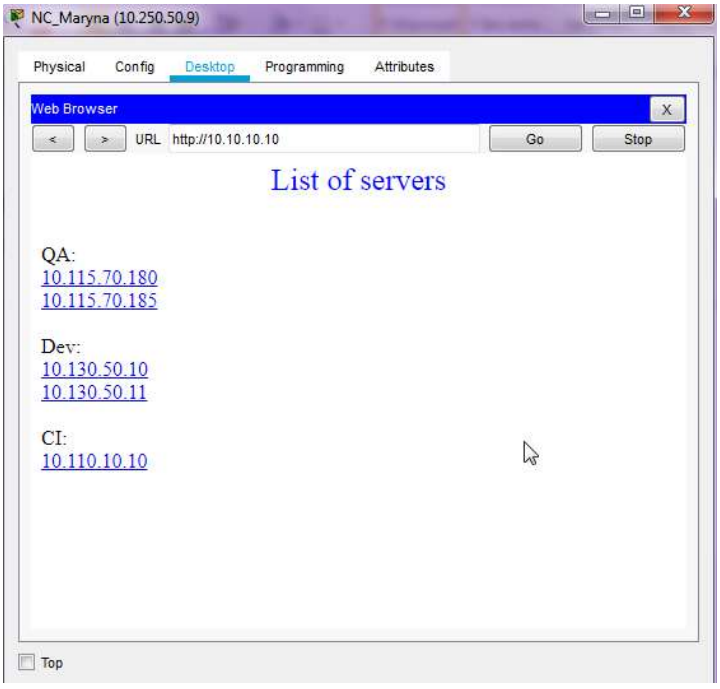


Рисунок 3.9 – Доступні сервери для користувача Maryna

Але при намаганні зайти на сервери за межами ASA, система запитає вже логін та пароль для входу (рис. 3.10). При цьому користувач зможе зайти лише на ті сервери, до яких у нього є доступ (рис. 3.11).

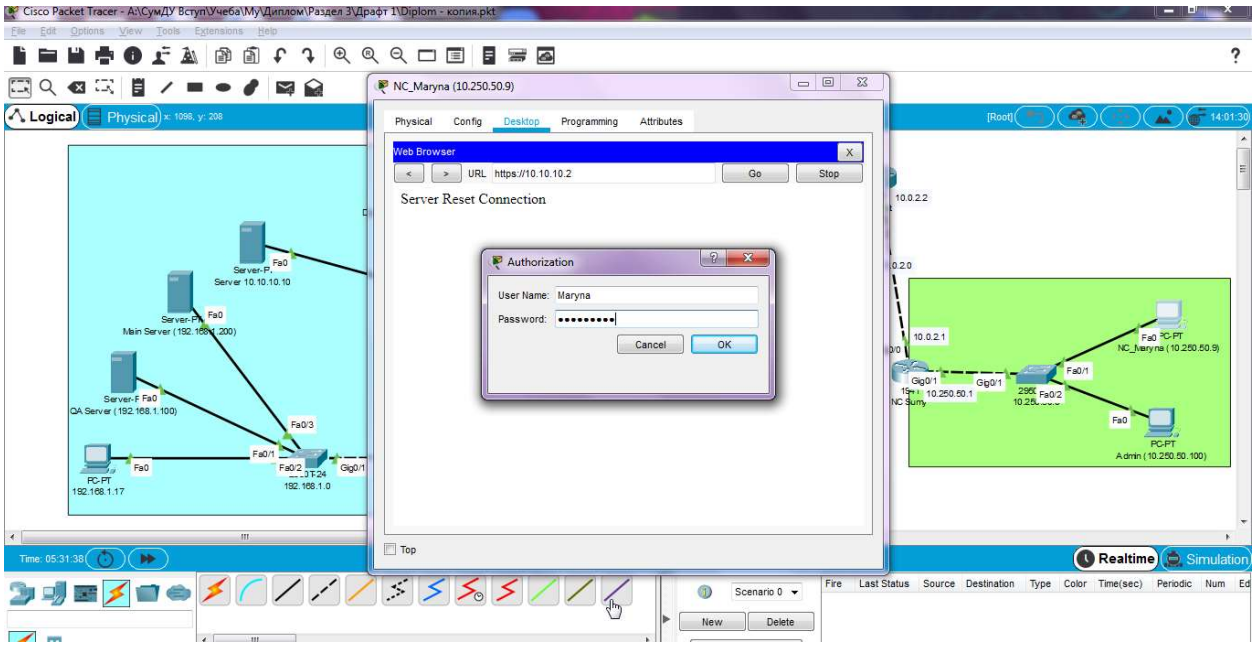


Рисунок 3.10 – Окно авторизації користувача

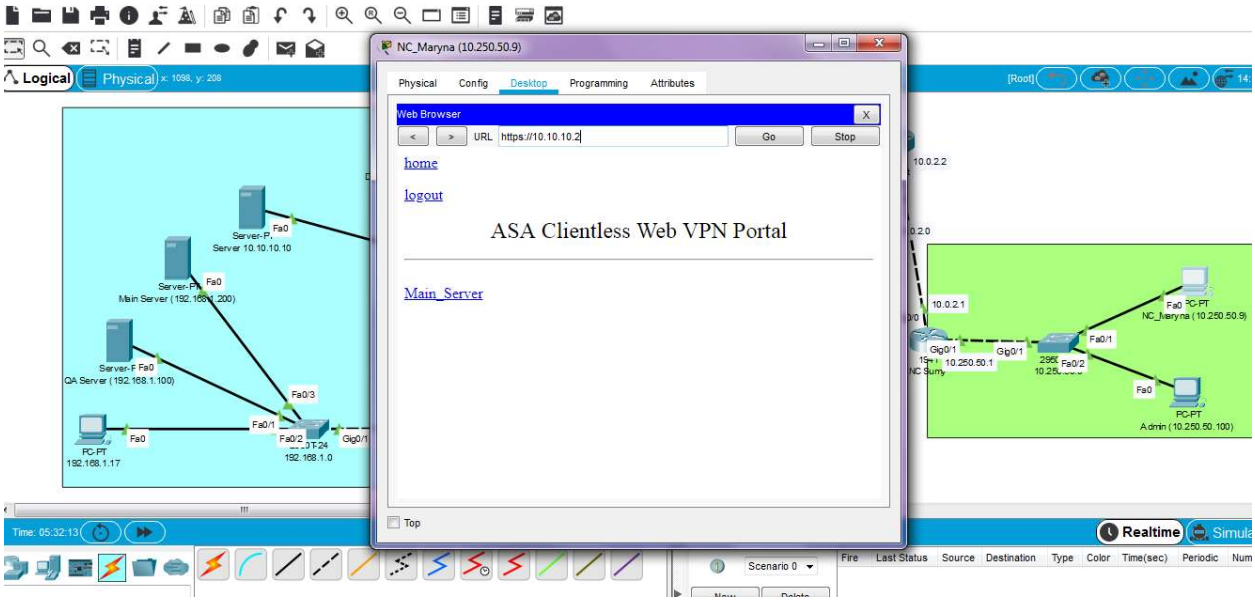


Рисунок 3.11 – Доступні сервери для користувача Maryna

Користувач Daria немає доступу на серверів за межами ASA (рис. 3.12, рис. 3.13):

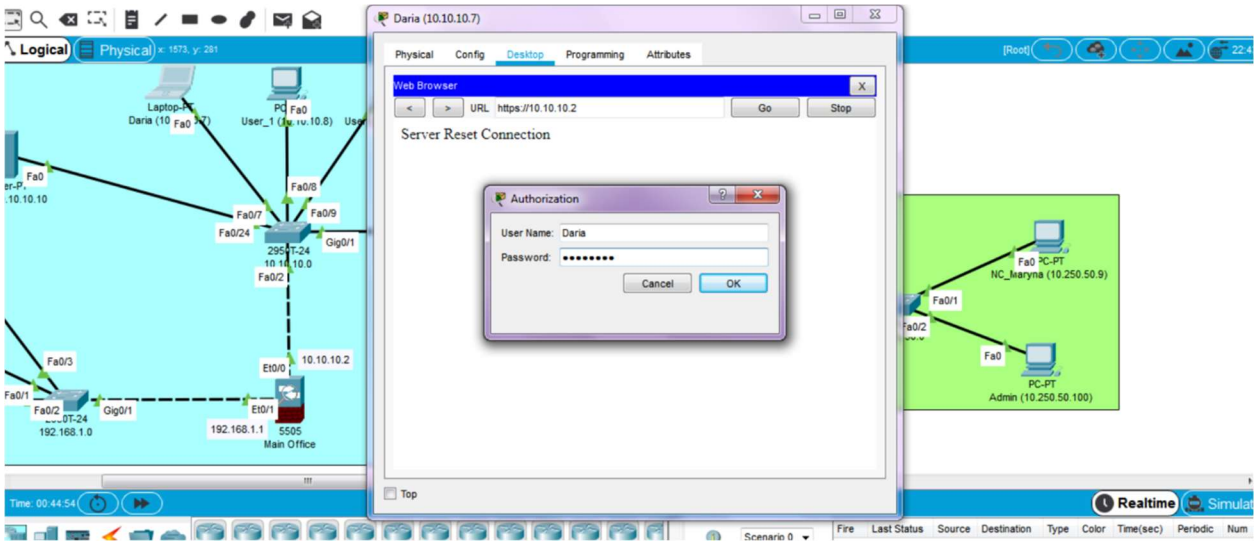


Рисунок 3.12 – Окно авторизації користувача

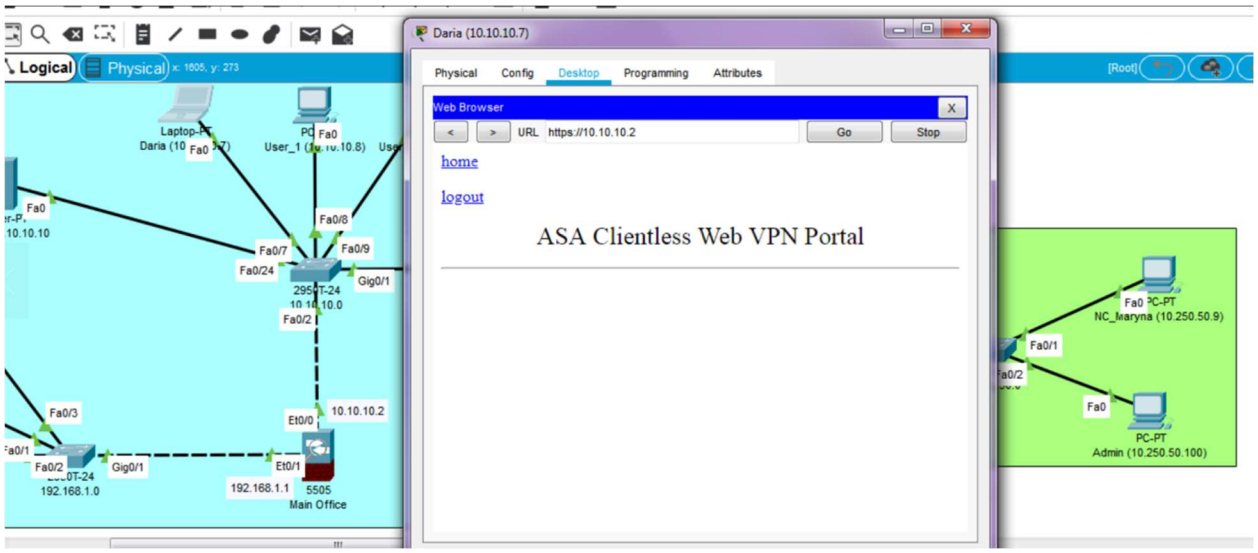


Рисунок 3.13 – Доступні сервери для користувача Daria

Користувач PC-PT має доступ до всіх серверів за межами ASA (рис. 3.14):

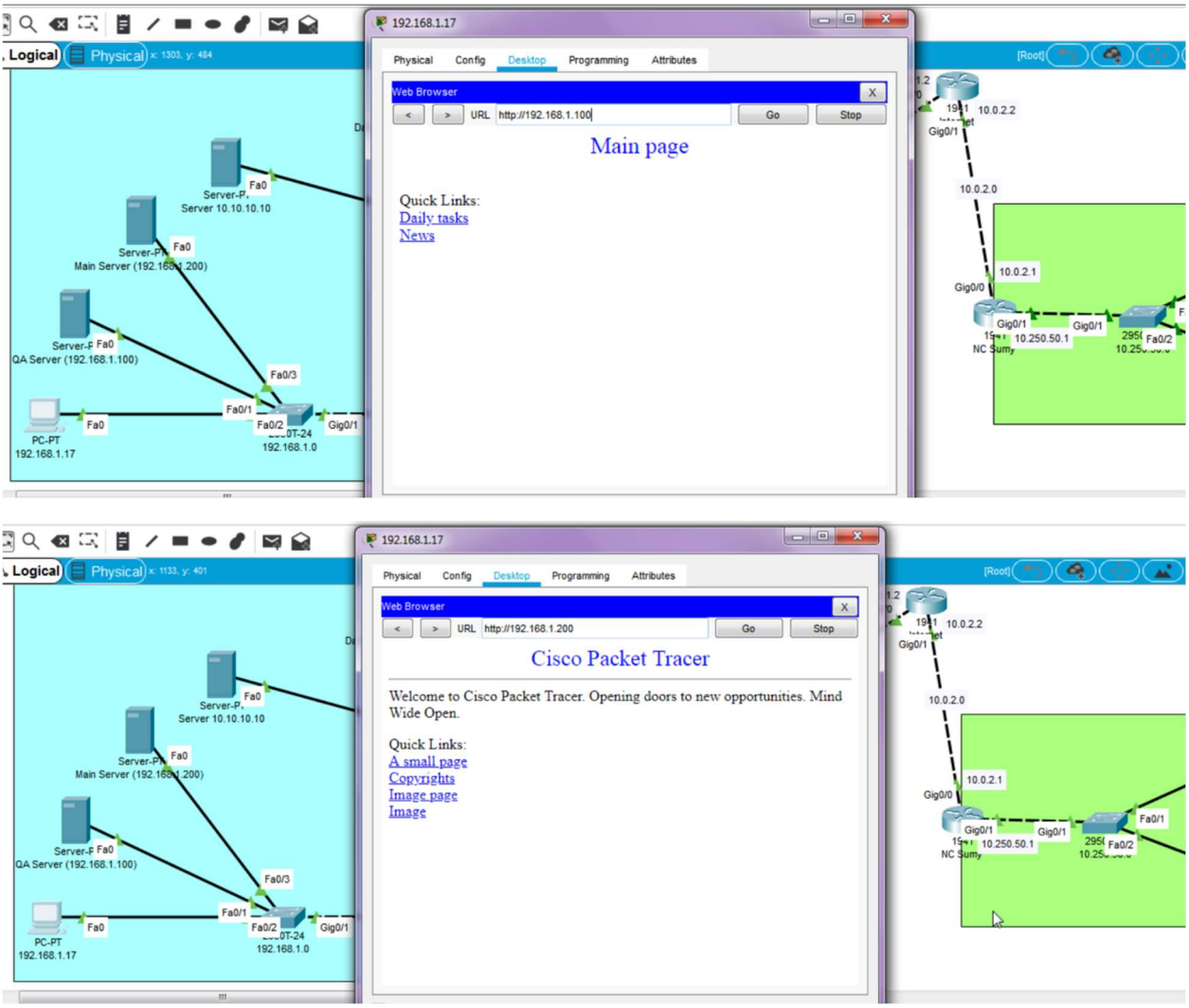


Рисунок 3.14 – Доступні сервери для користувача PC-PT

3.3 Реалізація технології Clientless SSL VPN для віддаленого співробітника за допомогою Cisco Packet Tracer

На рис. 3.15 наведена схема захищеного доступу до серверів офісу в для віддаленого співробітник. Доступ до серверів обмежується за технологією SSL VPN.

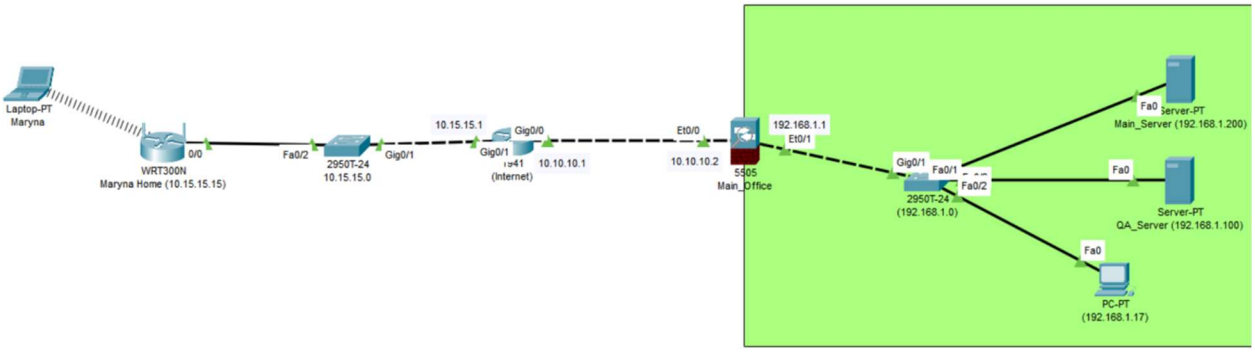


Рисунок 3.15 – Схема SSL VPN для віддаленого співробітника

У табл. 3.3 та табл. 3.4 наведено IP адреси пристроїв та права доступу користувачів до серверів

Таблиця 3.3 – IP адреси пристроїв

Device	Interface	IP address	Subnet mask	Default gateway
(Internet) router	g0/1	10.15.15.1	255.0.0.0	N/A
	g0/0	10.10.10.1	255.0.0.0	N/A
Main office ASA	vlan 1	192.168.1.1	255.255.255.0	N/A
	vlan 2	10.10.10.2	255.255.255.0	N/A
Maryna Home router	0/0	10.15.15.15	255.255.255.0	10.15.15.1
Laptop Maryna	Fa0	192.168.0.100	255.255.255.0	192.168.0.1

Таблиця 3.2 – Права доступу користувачів до серверів

Login	Password	Available servers
Maryna	123123123	Main Server

Для вирішення поставленої задачі були виконані наступні налаштування на пристроях мережі.

Конфігурація (Internet) router:

1. Налаштовуємо IP адреси для інтерфейсів:

```
Configure terminal
interface g0/1 ip address 10.15.15.1 255.0.0.0
no shut
interface g0/0 ip address 10.10.10.1 255.0.0.0
no shut
```

Конфігурація Main office ASA:

```
Configure terminal
```

1. Налаштовуємо IP адреси для Vlan-ів:

```
Hostname ASA1
Interface vlan 1
Nameif inside
Security-level 100
Ip address 192.168.1.1 255.255.255.0
exit
Interface vlan 2
Nameif outside
Security-level 0
Ip address 10.10.10.2 255.255.255.0
Exit
```

2. Вмикаємо функцію Webvpn для віддалених користувачів:

```
Webvpn
Enable outside
Object network lan
Subnet 192.168.1.0 255.255.255.0
```

Exit

3. Додаємо дані користувачів:

username Maryna password 123123123

4. Задаємо конфігурацію серверів (рис. 3.16):

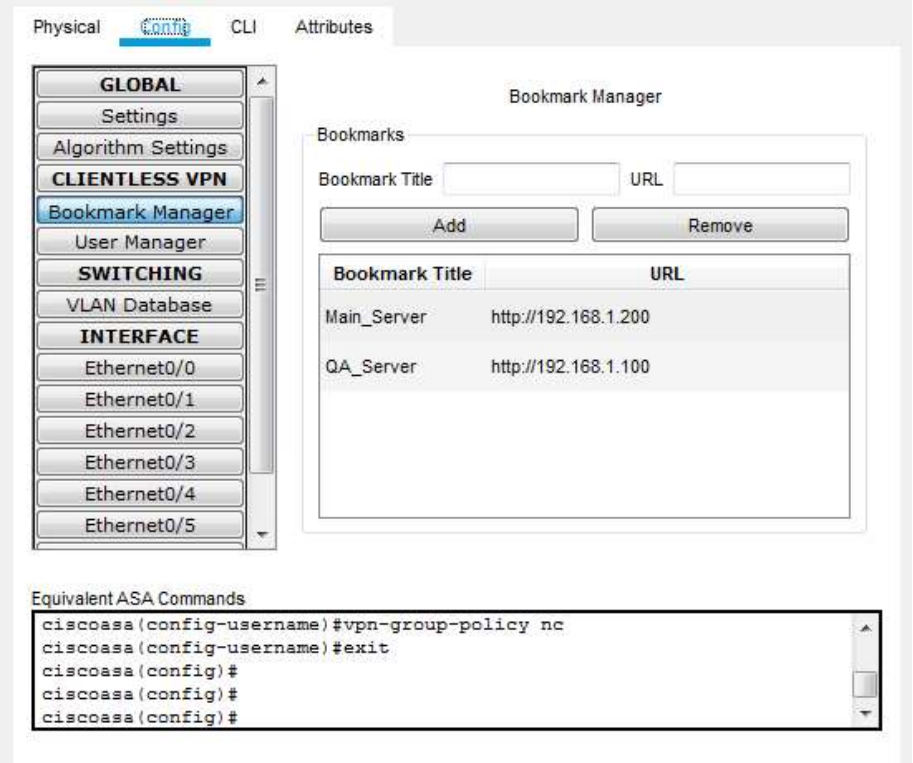


Рисунок 3.16 – Налаштування адрес серверів на Main office ASA

5. Конфігуруємо доступ для користувачів (рис. 3.17):

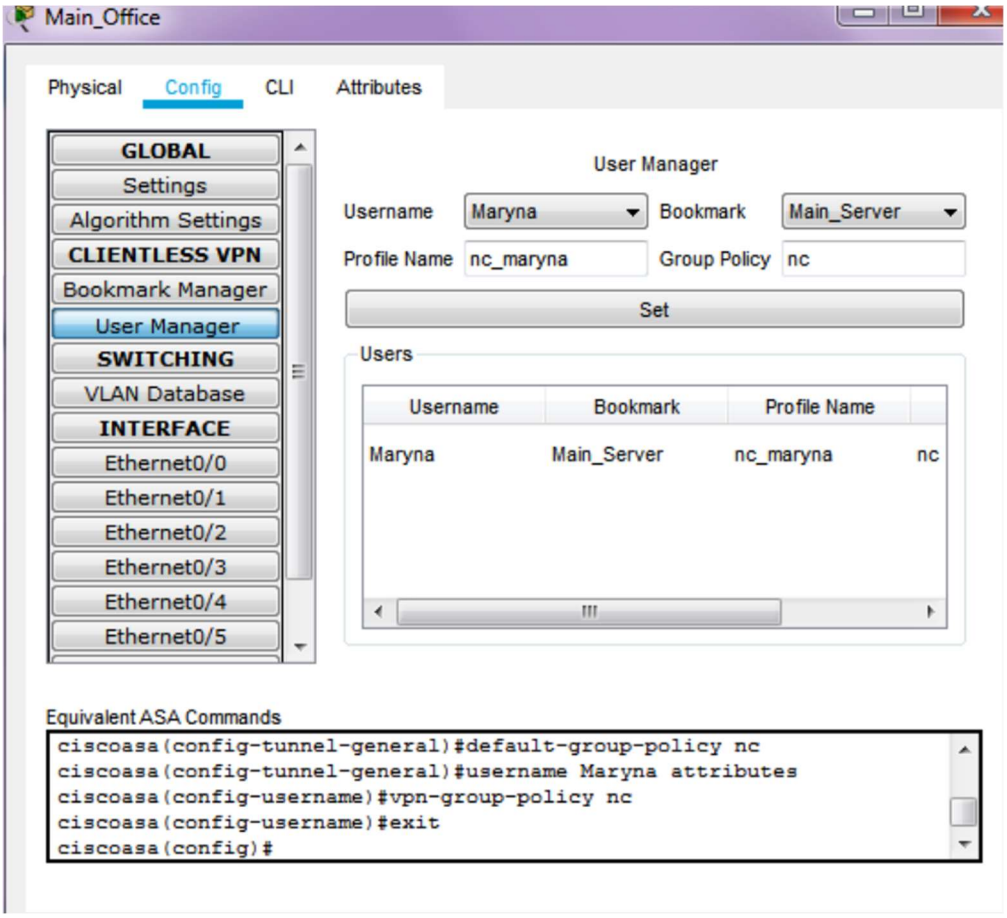


Рисунок 3.17 – Налаштування доступу для користувачів на Main office ASA

Після налаштування SLL можна протестувати доступ користувача до серверів. У користувач Maryna при намаганні зайти на сервери за межами ASA, система запитає логін та пароль для входу. При цьому користувач зможе зайти лише на ті сервери, до яких у нього є доступ (рис. 3.18).

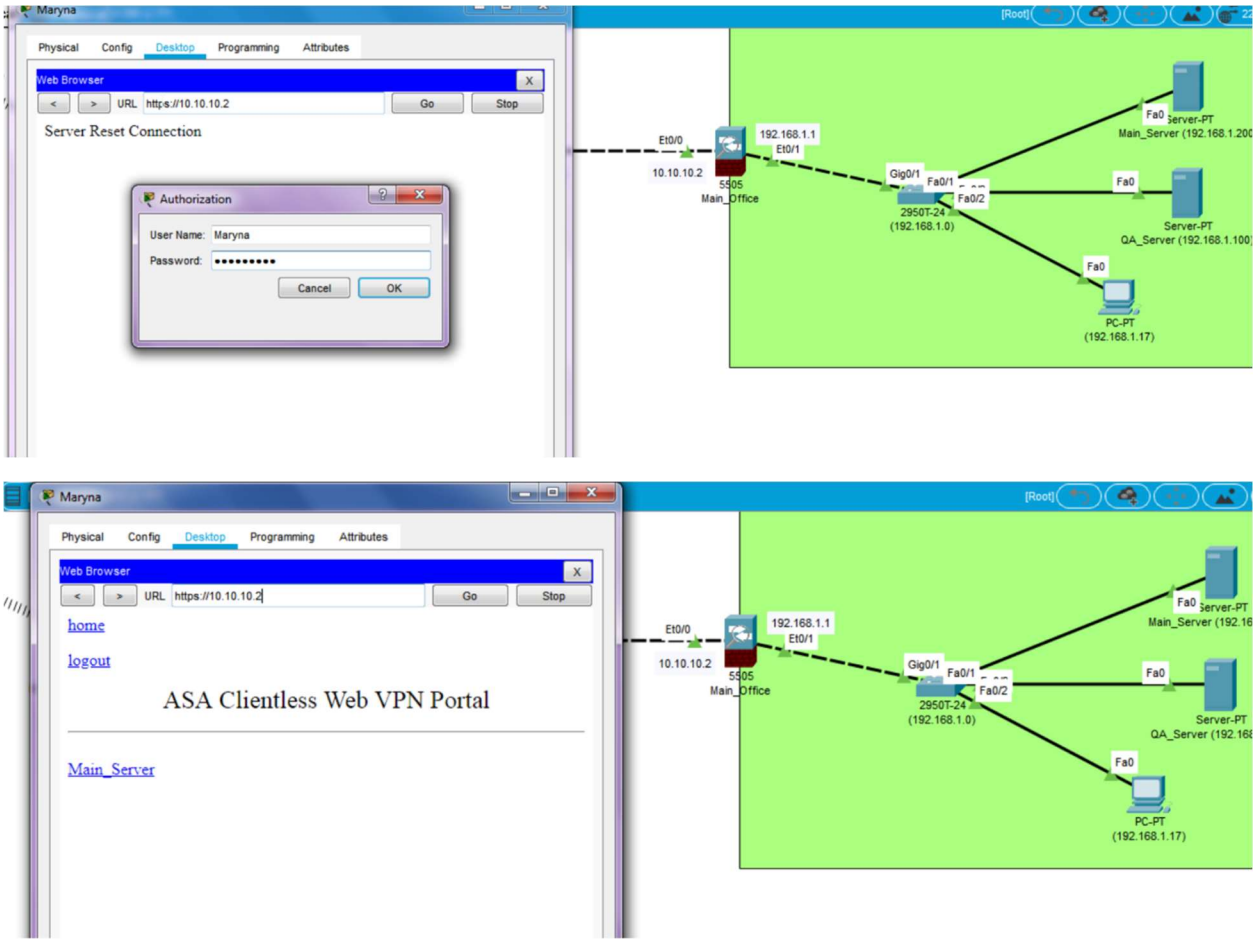


Рисунок 3.18 – Доступ до серверів для користувача Maryna

Таким чином, в третьому розділу була розроблена модель високозахищеного доступу до ресурсів компанії з віддаленими офісами та віддаленими співробітниками, які працюють за межами офісів. Реалізація моделі була виконана в програмі Cisco Packet Tracer. Було протестовано, що при IPsec VPN шифруються пакети, та при цьому за допомогою SSL VPN можна обмежити доступ до ресурсів компанії для певних груп користувачів.

ВИСНОВКИ

VPN – це логічна мережа, створена поверх існуючої мережі, яка за допомогою шифрування створює нові закриті канали для обміну даними. Завдяки створенню тунелів, застосуванню протоколів та аутентифікації VPN дозволяє об'єднати в одну мережу різні офіси компанії, організує приватну мережу з партнерами та створює віддалений доступ для співробітників. Існує велике різноманіття видів VPN, кожен з яких слід використовувати для спеціальних цілей, визначених компанією.

Для функціонування VPN має великий вибір протоколів, які можуть працювати на різних рівнях моделі OSI. Вони відповідають за безпеку підключення за допомогою особливостей шифрування і авторизації. Це призводить до відмінностей у безпеці та швидкості підключень.

Для розробки найбільш захищеного VPN доступу віддалених співробітників до корпоративної мережі з розподіленими офісами було обрано поєднання використання IPsec VPN та SSL VPN. Для побудови захищеної корпоративної мережі між віддаленими офісами було залучено технологію IPsec VPN, а для налаштування віддаленого доступу для співробітників – SSL VPN. При цьому для забезпечення більш захищеного доступ для віддалених співробітників слід підсилити SLL VPN за допомогою двофакторної аутентифікації на основі Cisco AnyConnect.

Реалізація моделі була виконана в програмі Cisco Packet Tracer. Було протестовано, що при Ip sec VPN шифруються пакети, та при цьому за допомогою SSL VPN можна обмежити доступ до ресурсів компанії для певних груп користувачів. Розроблена модель дозволе компаніям швидко налаштувати вискозахищений доступ до корпоративної мережі.

СПИСОК ЛІТЕРАТУРИ

1. Алексей Лукацкий. Почему Cisco AnyConnect — это не просто VPN-клиент [Електронний ресурс] – https://m.habr.com/ru/company/cisco/blog/493590/
2. Александр Панасенко. SSL VPN – шаг вперед в технологии VPN сетей [Електронний ресурс] – https://www.anti-malware.ru/node/449
3. Базовые понятия и классификация VPN [Електронний ресурс] – https://hidemy.name/ru/articles/bazovye-ponjatija-i-klassifikacija-vpn/
4. Безопасность сетей. Лекция 11. Виртуальные частные сети [Електронний ресурс] – https://intuit.ru/studies/courses/102/102/lecture/2991
5. Вариант удаленного доступа к корпоративной сети предприятия посредством VPN с разграничением доступа к внутренним ресурсам и аутентификацией в AD [Електронний ресурс] – https://m.habr.com/ru/post/111215/
6. Википедия. VPN [Електронний ресурс] – https://ru.wikipedia.org/wiki/VPN
7. Виртуальные Частные Сети (VPN) [Електронний ресурс] – https://www.insotel.ru/press/articles/virtualnye_chastnye_seti_vpn/
8. Владимир Хазов. VPN – типы подключения и проверка безопасности [Електронний ресурс] – https://vasexperts.ru/blog/vpn-tipy-podklyucheniya-i-proverka-bezopasnosti/
9. Віртуальні приватні мережі (VPN) [Електронний ресурс] – https://compbest.com.ua/ua/virtualnye-chastnye-seti-vpn/
10. В чем отличия между Cisco ASA и Cisco ISR и как выбрать устройство для вашей сети [Електронний ресурс] – https://cbs.ru/lib/technical-articles/10403/
11. Двухфакторная авторизация для VPN-соединений [Електронний ресурс] – https://m.habr.com/ru/company/panda/blog/337800/
12. Двухфакторная аутентификация пользователей VPN посредством MikroTik и SMS [Електронний ресурс] – https://m.habr.com/ru/post/505714/

13. Денис Коденцев. «Удаленка» с маршрутизатором Cisco [Електронний ресурс] – https://habr.com/ru/company/cisco/blog/493150/
14. Информация. Лекция 6. Технологии защиты информации в компьютерных сетях [Електронний ресурс] – https://intuit.ru/studies/courses/16655/1300/lecture/25509
15. Информация. Лекция 11. Технологии туннелирования [Електронний ресурс] – https://intuit.ru/studies/courses/14248/1285/lecture/24227
16. Казаков Дмитрий. Оптимизация облачных сервисов в AnyConnect VPN туннеле на Cisco ASA [Електронний ресурс] – https://habr.com/ru/company/cisco/blog/493774/
17. Казаков Дмитрий. Развертывание ASA VPN Load-Balancing кластера [Електронний ресурс] – https://habr.com/ru/company/cisco/blog/493098/
18. Казаков Дмитрий. Реализация концепции высокозащищенного удаленного доступа [Електронний ресурс] – https://m.habr.com/ru/company/cisco/blog/497618/
19. Классификация сетей VPN [Електронний ресурс] – https://ozlib.com/825055/informatika/klassifikatsiya_setey
20. Национальная библиотека им. Н. Э. Баумана [Електронний ресурс] – https://ru.bmstu.wiki/VPN_(Virtual_Private_Network)
21. Немного о 2FA: Двухфакторная аутентификация [Електронний ресурс] – https://habr.com/ru/company/1cloud/blog/277901/
22. Николай Колдовский. Построение безопасных сетей на основе VPN [Електронний ресурс] – https://3dnews.ru/190130
23. Олифер Виктор и Олифер Наталья. Виртуальные частные сети: администраторы требуют гарантий. Часть I [Електронний ресурс] – https://www.olifer.co.uk/articles/vpn/vpn.htm

24. Организация корпоративных сетей на основе VPN: построение, управление, безопасность [Електронний ресурс] –https://www.kp.ru/guide/korporativnaja-set.html
25. Платунова С.М. Построение корпоративной сети с применением коммутационного оборудования и настройкой безопасности. Учебное пособие по дисциплине «Корпоративные сети». – СПб: НИУ ИТМО, 2012. – 85 с.
26. Поговорим о VPN-ах? Типы VPN соединений. Масштабирование VPN [Електронний ресурс] – https://m.habr.com/ru/post/246281/
27. Принципы организации VPN [Електронний ресурс] – http://ciscotips.ru/vpn
28. Рябко Е.И. Калейдоскоп VPN-технологий [Електронний ресурс] – https://cyberleninka.ru/article/n/kaleydoskop-vpn-tehnologiy/viewer
29. Сергей Калашников. Что поставить на периметр сети: Cisco маршрутизатор или Cisco ASA? [Електронний ресурс] – https://habr.com/ru/company/cbs/blog/279857/
30. Сергей Орлов. Виртуальные частные сети: от IPSec к SSL [Електронний ресурс] – https://www.osp.ru/lan/2008/03/4870297
31. Сравнительный обзор реализаций технологии VPN: что выбрать? [Електронний ресурс] – https://1cloud.ru/help/network/comparevpntypes
32. Технологии Cisco VPN и выбор VPN технологии туннелирования [Електронний ресурс] – https://blog.telecom-sales.ru/tehnologii-cisco-vpn-i-vybor-vpn-tehnologii/
33. Хілах Мазіяр. Що таке VPN? І чому вона вам [ДІЙСНО] потрібна у 2020 році [Електронний ресурс] – https://uk.vpnmentor.com/blog
34. Что такое RDP/VPN. Что лучше выбрать и как настроить [Електронний ресурс] – https://5socks.net/Manual/rdp_vpn_ru.htm
35. 7 Best Practices For Securing Remote Access for Employees [Електронний ресурс] – https://phoenixnap.com/blog/secure-remote-access-best-practices

36. A Complete Guide to Remote Access Protocols [Електронний ресурс] – https://www.solarwindsmsp.com/blog/remote-access-protocols-complete-guide
37. Alex Leemon. 5 IT Best Practices that Also Mitigate Cyber Security Vulnerabilities in OT [Електронний ресурс] – https://www.cyberark.com/resources/blog/5-it-best-practices-that-also-mitigate-cyber-security-vulnerabilities-in-ot
38. Charlotte Empey. Что такое VPN и как это работает: базовое руководство Avast [Електронний ресурс] – https://blog.avast.com/ru/chto-takoe-vpn-i-kak-eto-rabotaet-bazovoe-rukovodstvo-avast
39. Configure two factor authentication on ASA for cisco ANYconnect [Електронний ресурс] – https://community.cisco.com/
40. Daniel Petri. Understanding VPN Remote Access Mechanism [Електронний ресурс] – https://petri.com/understanding-vpn-remote-access-mechanism
41. Dan Kaplan. 8 Best Practices for Secure Remote Work Access [Електронний ресурс] – https://www.siemplify.co/blog/8-best-practices-for-security-remote-work-access/
42. Difference between IPSec and SSL [Електронний ресурс] – https://www.geeksforgeeks.org/difference-between-ipsec-and-ssl/?ref=rp
43. IPsec made simple [Електронний ресурс] – https://briolidz.wordpress.com/2012/01/23/ipsec-made-simple/amp/
44. IP security (IPSec) [Електронний ресурс] – https://www.geeksforgeeks.org/ip-security-ipsec/
45. Michael Cobb. What's the difference between two-step verification and 2FA? [Електронний ресурс] – https://searchsecurity.techtarget.com/answer/Whats-the-difference-between-two-step-verification-and-2FA
46. IPsec Packet Flow [Електронний ресурс] – https://docs.oracle.com/cd/E23823_01/html/816-4554/ipsec-ov-54.html
47. IPSec VPN клиент/сервер [Електронний ресурс] – https://help.keenetic.com/hc/ru/articles

48. IPSec VPN: Статический виртуальный туннельный интерфейс SVTI [Електронний ресурс] – https://learncisco.ru/security/security.html
49. Paul Bischoff. VPN encryption explained: IPSec vs SSL [Електронний ресурс] – https://www.comparitech.com/blog/vpn-privacy/ipsec-vs-ssl-vpn/
50. Protect your business online. Remote access security issues [Електронний ресурс] – https://www.nibusinessinfo.co.uk/content/remote-access-security-issues
51. Remote access [Електронний ресурс] – https://searchsecurity.techtarget.com/definition/remote-access
52. Remote Access Security Best Practices [Електронний ресурс] – https://www.netwrix.com/remote_access_security_best_practices.html
53. Secure Socket Layer (SSL) [Електронний ресурс] – https://www.geeksforgeeks.org/secure-socket-layer-ssl/?ref=lbp
54. Sheila Frankel, Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W.Ritchey, Steven R. Sharma. Guide to IPsec VPNs. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] – https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf
55. SSL Full Form [Електронний ресурс] – https://www.geeksforgeeks.org/ssl-full-form/
56. SSL VPN Configuration Guide, Cisco IOS Release 15M&T [Електронний ресурс] – https://www.cisco.com/
57. SSL VPN Security [Електронний ресурс] – https://tools.cisco.com/security/center/resources/ssl_vpn_security
58. SSL VPN vs IPSec VPN – Pros & Cons Of Both VPNs [Електронний ресурс] – https://www.limevpn.com/ssl-vpn-vs-ipsec-vpn-pros-cons-of-both-vpns/
59. Technologies for Optimized Remote Access [Електронний ресурс] – https://www.remoteaccessworks.com/Remote-Access-Technologies.asp

60. The best VPN protocols [Електронний ресурс] – https://nordvpn.com/uk/blog/protocols/
61. Two-Factor Authentication (2FA) for Cisco AnyConnect [Електронний ресурс] – https://www.miniorange.com/two-factor-authentication-for-cisco-any-connect
62. Two Factor Authentication Implementation Methods and Bypasses [Електронний ресурс] – https://www.geeksforgeeks.org/two-factor-authentication-implementation-methods-and-bypasses/
63. VPN-шифрование (всё что нужно знать) [Електронний ресурс] – https://www.cactusvpn.com/ru/beginners-guide-to-vpn/vpn-encryption/
64. Will Ellis. VPN Protocols: PPTP vs L2TP/IPSec vs SSTP vs IKEv2/Ipsec [Електронний ресурс] – https://privacyaustralia.net/vpn-protocols/
65. What Is Remote Access? Definition and Best Software List [Електронний ресурс] – https://www.dnsstuff.com/what-is-remote-access-definition
66. What Is a VPN Protocol & What Is the Best VPN Protocol? [Електронний ресурс] – https://www.cactusvpn.com/beginners-guide-to-vpn/vpn-protocol/
67. Yuki Arbel. Remote Access Security: Risks & Best Practices [Електронний ресурс] – https://securityboulevard.com/2020/04/remote-access-security-risks-best-practices/

ДОДАТОК А

Конфігурація NC Sumy router:

```
Configure terminal
interface g0/1
ip address 10.250.50.1 255.255.255.0
no shut
interface g0/0
ip address 10.0.2.1 255.255.255.0
no shut
license boot module c1900 technology-package securityk9
exite
copy running-config startup-config
reload
show version
Configure terminal
access-list 100 permit ip 10.250.50.0 0.0.0.255 10.10.10.0 0.0.0.255
crypto isakmp policy 10
encryption aes 256
authentication pre-share
group 5
exit
crypto isakmp key password address 10.0.1.1
crypto ipsec transform-set NC_Sumy-to-NC_Kyiv esp-aes 256 esp-sha-hmac
crypto map IPSEC 10 ipsec-isakmp
set peer 10.0.1.1
set pfs group5
```

set security-association lifetime seconds 86400

set transform-set NC_Sumy-to-NC_Kyiv

match address 100

interface GigabitEthernet0/0

crypto map IPSEC

Конфігурація Internet router:

Configure terminal

interface g0/1 ip address 10.0.2.2 255.0.0.0

no shut

interface g0/0 ip address 10.0.1.2 255.0.0.0

no shut

Конфігурація NC Kyiv router:

Configure terminal

interface g0/1 ip address 10.10.10.1 255.0.0.0

no shut

interface g0/0 ip address 10.0.1.1 255.0.0.0

no shut

conf t

license boot module c1900 technology-package securityk9

exite

copy running-config startup-config

reload

show version

Configure terminal

access-list 100 permit ip 10.10.10.0 0.0.0.255 10.250.50.0 0.0.0.255

crypto isakmp policy 10 encryption aes 256 authentication pre-share group 5

exit

crypto isakmp key password address 10.0.2.1

crypto ipsec transform-set NC_Kyiv-to-Home esp-aes 256 esp-sha-hmac

crypto map IPSEC 10 ipsec-isakmp

set peer 10.0.2.1

set pfs group5

set security-association lifetime seconds 86400

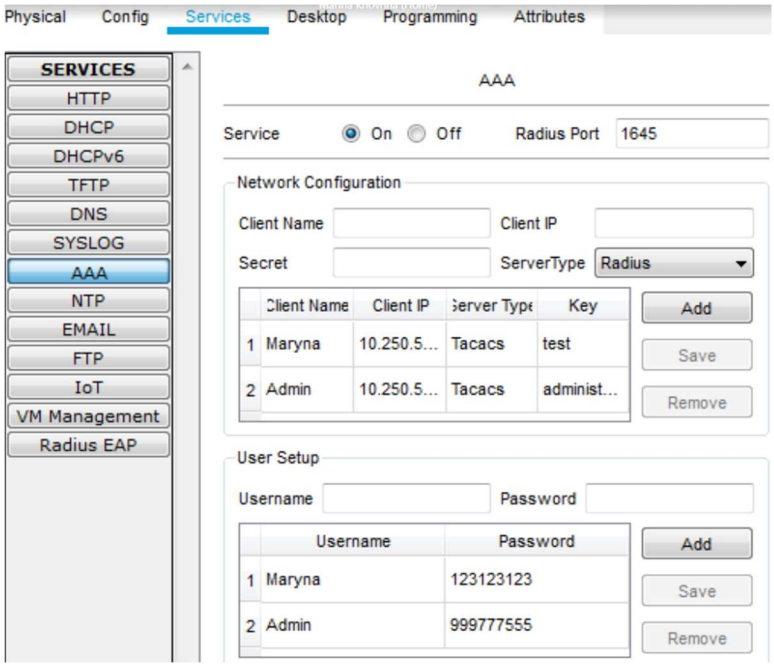
set transform-set NC-to-Home

match address 100

interface GigabitEthernet0/0

crypto map IPSEC

Конфігураці AAA серверу за допомогою інтерфейсу:



Конфігурація Main office ASA:

Configure terminal

Hostname ASA1

Interface vlan 1

Nameif inside

Security-level 100

Ip address 192.168.1.1 255.255.255.0

exit

Interface vlan 2

Nameif outside

Security-level 0

Ip address 10.10.10.2 255.255.255.0

hostname firewall1

names

name 192.168.1.100 QA_Server name 192.168.1.100 QA_Server

name 192.168.1.200 Main_Server name 192.168.1.200 Main_Server

name 10.1.1.10 OUT_DB_server name 10.10.10.10. Server

object-group network Privat_servers

network-object host QA_Server

network-object host Main_Server

access-list OUT_IN remark ***ftp traffic to Privat servers***

access-list OUT_IN extended permit tcp any object-group Privat_servers eq ftp

access-list OUT_IN extended permit tcp any object-group Privat_servers eq ftp-data

access-list OUT_IN remark ***DB traffic between DB servers***

access-list OUT_IN remark ***Virtual Telnet for Authentication***

access-list OUT_IN extended permit tcp any host 10.50.10.10 eq https

access-list OUT_IN extended deny ip any any log

logging enable

logging buffered informational

static (outside) 10.50.10.10 10.50.10.10 netmask 255.255.255.255

access-group OUT_IN in interface outside

route outside 0.0.0.0 0.0.0.0 10.10.10.254 1

timeout xlate 4:00:00

timeout conn 1:00:00 half-closed 0:10:00 udp 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

timeout uauth 4:00:00 absolute

aaa-server ACS_1 protocol tacacs+

aaa-server ACS_1 host 10.10.10.10

key password

aaa authentication serial console ACS_1 LOCAL

aaa authentication enable console ACS_1 LOCAL

aaa authentication ssh console ACS_1 LOCAL

aaa authentication include ip outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ACS_1

aaa authentication exclude tcp/1526 outside OUT_DB_server 255.255.255.255 ACS_1

aaa authorization include ip outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 ACS_1

aaa authorization exclude tcp/1526 outside OUT_DB_server 255.255.255.255 ACS_1

aaa authentication include https outside 10.50.10.10 255.255.255.255 0.0.0.0 0.0.0.0 ACS_1

aaa proxy-limit 128

aaa authentication listener https outside port 1443 redirect

virtual telnet 10.50.10.10

telnet timeout 5

ssh 10.10.10.0 255.255.255.0 outside

ssh timeout 5

ssh version 2

console timeout 5

no threat-detection basic-threat

no threat-detection statistics access-list

ssl encryption des-sha1 rc4-md5

username Maryna password PaSsWoRd privilege 15

username Admin password PaSsWoRd privilege 15

Exit

Webvpn

Enable outside

Object network lan

Subnet 192.168.1.0 255.255.255.0

exit

crypto key generate rsa label ssl-anyconnect

crypto ca trustpoint localtrust

enrollment self

fqdn sslvpn. nc.com

subject-name CN=sslvpn.nc.com

keypair ssl-anyconnect

crypto ca enroll localtrust noconfirm

ssl trust-point localtrust outside

copy tftp://10.150.81.50/anyconnect-win-2.0.0343-k9.pkg flash

webvpn

svc image disk0:/anyconnect-win-2.3.0254-k9.pkg 1

enable outside

svc enable

ip local pool SSLClientPool 10.0.3.1-10.0.3.50 mask 255.255.255.0

group-policy SSLCLient internal

group-policy SSLCLient attributes

dns-server value 10.10.10.10

vpn-tunnel-protocol svc

default-domain value nc.com

address-pools value SSLClientPool

sysopt connection permit-vpn

tunnel-group SSLClientProfile type remote-access

tunnel-group SSLClientProfile general-attributes

default-group-policy SSLCLientPolicy

tunnel-group SSLClientProfile webvpn-attributes

group-alias SSLVPNClient enable

webvpn

tunnel-group-list enable

access-list 100 extended permit ip any 10.0.3.2 255.255.255.0

nat (inside) 0 access-list 100

username Maryna password 123123123 privilege 0

username Maryna attributes

username Admin password 999777555 privilege 0

username Admin attributes

service-type remote-access