

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 захищеної корпоративної мережі
організації на базі технології FlexVPN»

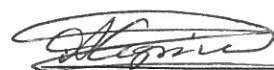
Виконав студент 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Бабіч Дмитро

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

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

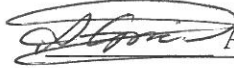
 Андрій Єфіменко

Житомир – 2022

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Бабіч Дмитро Володимирович

Тема роботи: «Проект захищеної корпоративної мережі організації на базі технології FlexVPN»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

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

Віртуальні приватні мережі, процес забезпечення безпечної передачі даних у комп'ютерних мережах за допомогою технології FlexVPN.

Обладнання та програмне забезпечення:

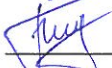
1. мережевий симулятор GNS3, VirtualBox
2. операційні системи Windows Server 2019, Windows 10
3. маршрутизатори Cisco c7200, 3725

4. Cisco AnyConnect Secure Mobility Client, VPN Profile Editor

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О. А.	1.03.22	 1.03.2022

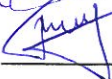
Студент  Дмитро Бабіч

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.03.2022 – 01.04.2022	
2	Написання вступної частини кваліфікаційної роботи	01.04.2022 – 03.04.2022	
3	Аналіз основних теоретичних відомостей VPN технологій	03.04.2022 – 11.04.2022	
4	Проектування мережі та топології мережі головного офісу та філіалу	11.04.2022 – 18.04.2022	
5	Вибір обладнання та технологій	18.04.2022 – 24.04.2022	
6	Налаштування мережі головного офісу та філіалу в емуляторі GNS3	24.04.2022 – 01.05.2022	
7	Налаштування Site-to-Site VPN	01.04.2022 – 08.05.2022	
8	Налаштування Remote Access VPN	08.05.2022 – 16.05.2022	
9	Написання висновків	16.05.2022 – 20.05.2022	
10	Оформлення кваліфікаційної роботи	20.05.2022 – 25.05.2022	
11	Підготовка презентації до захисту	25.05.2022 – 02.06.2022	

Студент  Дмитро Бабіч

Керівник  Олександра Покотило

АНОТАЦІЯ

Пояснювальна записка містить: 93 сторінки текстової частини, 48 рисунків, 3 таблиці та 12 джерел.

Метою роботи є побудова захищеної корпоративної мережі та філіалу з використання технології FlexVPN для безпечної передачі трафіку через загальнодоступні мережі.

В даній роботі розглянуто основні методи VPN та протоколи безпеки мережевого трафіку. Розглянуто особливості обладнання Cisco Systems. В практичній частині показано розробку мережі в емуляторі GNS3, випробувано дві основні реалізації захищених VPN – Site-to-Site та Remote Access та наведено результати тестування.

Ключові слова: ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, ТУНЕЛЮВАННЯ, БЕЗПЕКА МЕРЕЖЕВОГО ТРАФІКУ, МІЖСАЙТОВИЙ VPN, ТЕХНОЛОГІЯ ВІДДАЛЕНОГО ДОСТУПУ

					КІК.КР.Б – 123 – 02 – ПЗ			
Зм.	З	Арк.	Ар	№ докум.	№	Підпис	Під	Дата
Розроб.				Бабіч Д.				10.00
Керівник				Покотило О. А.				20.06
Реценз.				Єфіменко А.А.				20.06
Н. контр.				Покотило О. А.				20.06
Затверд.				Єфіменко				20.06

Проект захищеної корпоративної мережі організації на базі технології FlexVPN

Літ.	Арк.	Аркуші
	4	93

ФІКТ, Гр. КІ-4

ANNOTATION

The explanatory note contains: 93 pages of text, 48 figures, 3 tables and 12 sources.

The purpose of the work is to build a public network and a branch using Flex VPN technology for secure traffic through public networks.

This paper discusses the main VPN methods and network traffic security protocols. Features of Cisco Systems equipment are considered. In the practical part of network development in GNS3 emulators, testing of two main implementations of secure VPNs – Site-to-Site and Remote access and test results.

Keywords: VIRTUAL PRIVATE NETWORK, TUNNELING, NETWORK SECURITY TRAFFIC, INTERSITE VPN, REMOTE ACCESS TECHNOLOGY

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ПОБУДОВУ ТА ЗАХИСТ VPN МЕРЕЖ.....	9
1.1 Призначення технології віртуальних приватних мереж.....	9
1.2 Протокол безпеки IPsec.....	10
1.3 Site-to-Site та Remote Access VPN.....	19
1.4 Інфраструктура відкритого ключа	21
Висновки до першого розділу	26
РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ГОЛОВНОГО ОФІСУ ТА ФІЛІАЛУ.....	28
2.1 Проєктування моделей та схем адресацій.....	28
2.2 Вимоги до обладнання	36
Висновки до другого розділу.....	42
РОЗДІЛ 3 НАЛАШТУВАННЯ VPN ТЕХНОЛОГІЙ У СИМУЛЯТОРІ GNS3.....	43
3.1 Базове налаштування пристроїв.....	43
3.2 Налаштування Site-to-Site VPN	46
3.2.1 Налаштування головного офісу	46
3.2.2 Конфігурація РКІ-сервера на маршрутизаторі Cisco	49
3.2.3 Налаштування тунелю на аутентифікація по сертифікатам	52
3.3 Налаштування Remote Access VPN	57
3.3.1 Налаштування AAA серверу	58
3.3.2 Налаштування аутентифікатора.....	61
3.3.3 Налаштування VPN клієнта	64
Висновки до третього розділу	67
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	72

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

ACL – Access Control List

AH – Authentication Header

ESP – Encapsulating Security Payload

EAP – Extensible Authentication Protocol

DMVPN – Dynamic Multipoint VPN

VTI Virtual – Virtual Tunneling Interface

IKE – Internet Key Exchange

OSI – Open System Interconnection

OSPF – Open Shortest Path First

ISP – Internet Service Provider

PKI – Public Key Infrastructure

SSL – Secure Sockets Layer

IPsec – Internet Protocol Security

ISAKMP – Internet Security Association and Key Management Protocol

GRE – Generic Routing Encapsulation

SA – Security Association

SPI – Security Parameters Index

HMAC – Hash-based message authentication code

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі, де різні інформаційні технології тісно інтегровані не тільки у великі корпоративні мережі, а й у побут звичайних користувачів, реалізація VPN з обов'язковим використанням протоколів безпеки стає критично необхідною. Захищатися мають персональні дані як звичайних користувачів, так і мережі великих корпорацій та сервіс-провайдерів. Все частіше збитки від різноманітних кіберзагроз навіть важко оцінити.

Метою кваліфікаційної роботи є побудова захищеної корпоративної мережі та філіалу з використання технології FlexVPN для безпечної передачі трафіку через загальнодоступні мережі.

Визначена мета обумовлює наступні завдання:

- Дослідити основні теоретичні відомостей про побудову захищених VPN.
- Спроектувати топологію мережі, схему адресації та підібрати відповідне обладнання.
- Налаштувати мережу головного офісу та філіалу.
- Налаштувати Site-to-Site та Remote Access VPN з використанням технології FlexVPN.

Об'єктом дослідження є віртуальні приватні мережі.

Предметом дослідження є процес забезпечення безпечної передачі даних у комп'ютерних мережах за допомогою технології FlexVPN.

У процесі виконання кваліфікаційної роботи було розроблено проект ієрархічної моделі головного офісу, з можливістю підключати віддалених користувачів та з'єднуватися через VPN тунель з філіалом.

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ПОБУДОВУ ТА ЗАХИСТ VPN МЕРЕЖ

1.1 Призначення технології віртуальних приватних мереж

VPN – віртуальна приватна мережа, що створюється поверх іншої, наприклад Internet. Не дивлячись на те, що комунікація відбувається по публічним мережам з використання небезпечних протоколів, за рахунок шифрування створюються закриті від посторонніх канали обміну інформації.

VPN використовуються у світі, для створення зашифрованого підключення до Інтернету. Шифрування приховує діяльність користувачів від сторонніх очей, а також VPN може замінити справжню IP-адресу на іншу, що дасть змогу отримувати інформацію, доступ до якої був заблокований раніше.

У VPN зазвичай застосовуються такі технології тунелювання, як IPsec, PPP, L2TP, SSL VPN, GRE VPN. Тунелювання забезпечує передачу даних між двома точками – таким чином, що для джерела і приймача даних є схованою вся мережева інфраструктура, що лежить між ними. Перед передачею пакету вони інкапсулюються у пакет із новим заголовком. Цей заголовок надає публічну ір-адресу, що маршрутизується, щоб вона могла пройти загальнодоступну мережу, перш ніж досягти своєї кінцевої точки тунелю. Цей логічний шлях, по якому проходять інкапсульовані пакети, називається тунелем. Коли кожен пакет досягає кінцевої точки тунелю, він "декапсулюється" і пересилається до кінцевого пункту призначення. Обидві кінцеві точки тунелю повинні підтримувати один і той же протокол тунелювання.

VPN використовує шифрування для забезпечення конфіденційності даних. Пакети, що передаються через загальнодоступну мережу таким чином, не можна було б прочитати без належний ключів для розшифровки.

VPN забезпечує перевірку цілісності інформації. За допомогою дайджесту повідомлень отримувач перевіряє чи не були дані в середині пакета змінені під час їх передачі по мережі.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Для аутентифікації віддалених користувачів VPN можна використовувати логін та пароль, сертифікати, смарт-карти, жетони та RADIUS. Крім того, можлива комбінації різних рівнів аутентифікації. Наприклад, логін і пароль та сертифіката з використанням електронного USB-ключа.

1.2 Протокол безпеки IPsec

VPN можна налаштувати і без шифрування. Налаштування тунелю GRE, де інкапсуляція оригінального пакету відбувається з використанням GRE header (заголовок інкапсуляції), який вкладається в delivery header (заголовок доставки), який безпосередньо вкладається в Ethernet[1].

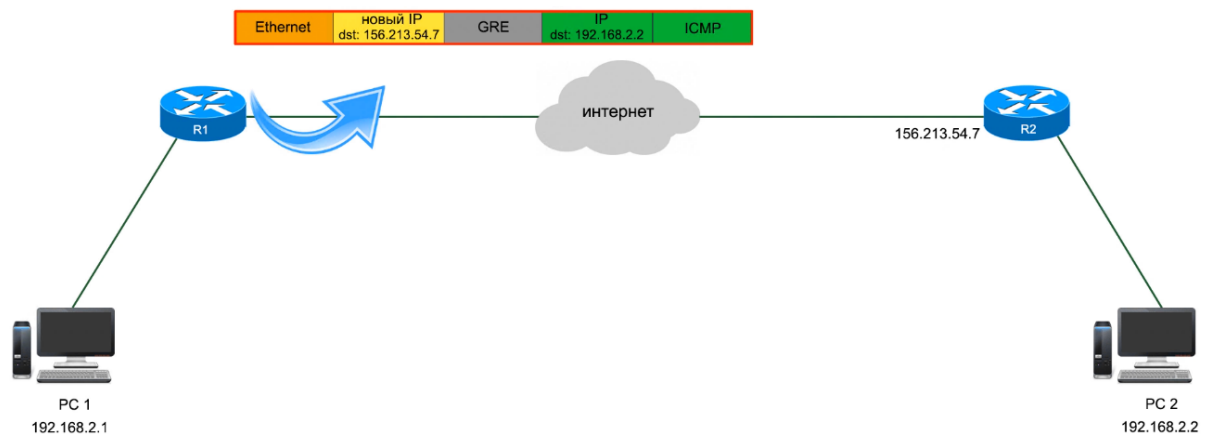


Рисунок 1.1 – GRE тунель

Однак побудований тунель GRE не забезпечує шифрування трафіка. Для забезпечення шифрування використовується IPsec. IPsec – це набір протоколів, що забезпечує захист даних, що передаються всередині IP. IPsec розроблений IETF для забезпечення захисту даних, що працює на мережевому рівні моделі OSI через незахищену мережу.

Алгоритми перевірки цілісності, хешування та шифрування потрібно якось керувати, управління цими алгоритмами відбувається за допомогою групи протоколів IPsec: ESP, AH, ESP+AH, IKE. Працюючи спільно вони забезпечують перевірку цілісності, хешування та шифрування.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

IPsec пакети передані через загальнодоступну мережу таким чином, не можуть бути «прочитані» без належних ключів, тим самим забезпечуючи конфіденційність даних під час передачі. Після відпрацювання групи протоколів IPsec, GRE пакет поміститься в ESP (рис.1.2). Всі дані в середині ESP будуть зашифровані.



Рисунок 1.2 – IPsec over GRE

ESP – один з протоколів, що входить до групи протоколів IPsec, в середині якого всі заголовки шифруються, також даний протокол налічує не тільки header, а й trailer - кінцевик. На рис. 1.2 зображена інкапсуляція пакета, за допомогою GRE, дана технологія називається IPsec over GRE, однак IPsec в змозі шифрувати дані самостійно, за допомогою ACL, який підключений до крипто карти (crypto-map)[10].

Туннельный режим:



Рисунок 1.3 – IPsec без GRE

IPsec використовує протоколи AH та ESP для надання служб безпеки[8]:

1. ESP забезпечує:

- Конфіденційність даних (encryption) за допомогою AES, 3DES, DES
- Цілісність даних (data integrity) і аутентифікація пакетів за допомогою SHA, MD5
- Аутентифікація пакетів за допомогою HMAC
- Захист від відтворення даних (antireplay) за допомогою SN

Які поля шифруються, а від яких рахується хеш, який поміщається в поле ESP Authentication, зображено на рис.1.4.

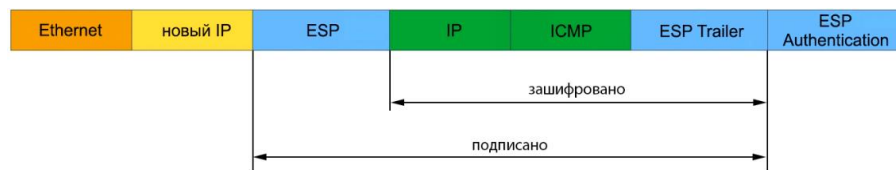


Рисунок 1.4 – ESP

2. Протокол АН (Authentication Header) забезпечує аутентифікацію джерела та цілісність IP-пакетів, але не шифрує. Заголовок АН (рис. 1.5), вкладений в пакет IP, містить хеш даних, порядковий номер та інформацію, яка може бути використана для перевірки відправника, забезпечення цілісності даних та запобігання повторним атакам:

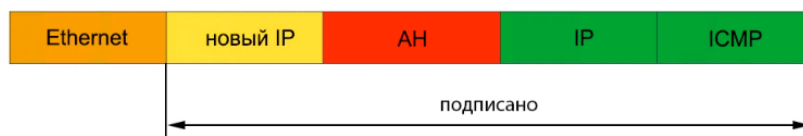


Рисунок 1.5 – АН

АН захищає зовнішній IP заголовок, але не шифрує дані, а ESP навпаки. Якщо потрібно використані дві можливості, то можна скористатися комбінованим режимом. Однак він використовується досить рідко, оскільки потрібно рахувати хеш окремо для ESP та АН, що додатково навантажує процесор пристрою, а захист зовнішнього IP заголовку може знадобитися в вузькоспеціалізованих випадках.

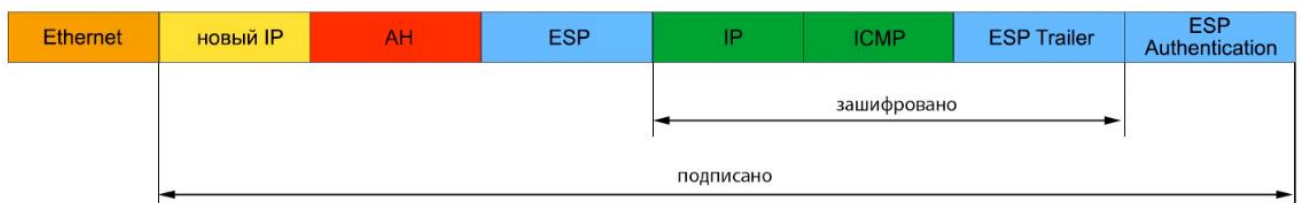


Рисунок 1.6 – ESP + АН

ESP, АН, ESP+АН являються робочими інструментами IPsec, завдяки ним відбувається шифрування, перевірка цілісності даних та аутентифікація. Однак перед тим, як передавати трафік, будується тунель. Щоб побудувати тунель, потрібно узгодити алгоритми шифрування, хешування, згенерувати ключі та передати їх на другий кінець тунелю. За все це відповідає протокол IKE (Internet Key Exchange). Можна сказати, що IKE займається побудовою тунелю, а ESP, АН, ESP+АН передають по ньому шифрований трафік. Протокол IKE – це гібридний протокол в його основі лежать протоколи: ISAKMP, Oakley, SKEME[7].

- ISAKMP програмна конструкція, завдяки якій працюють протоколи обміну ключами
- Oakley забезпечує генерацію і обмін ключового матеріалу
- SKEME забезпечує додаткові механізми обміну, яких не має в Oakley

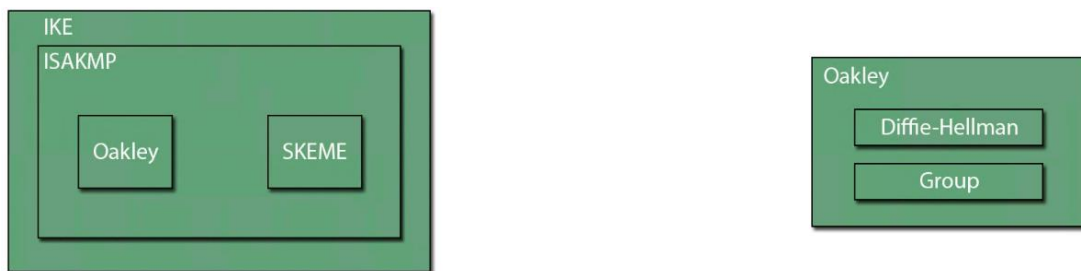


Рисунок 1.7 – IKE протоколи

Побудова тунелю поділяється на два етапи:

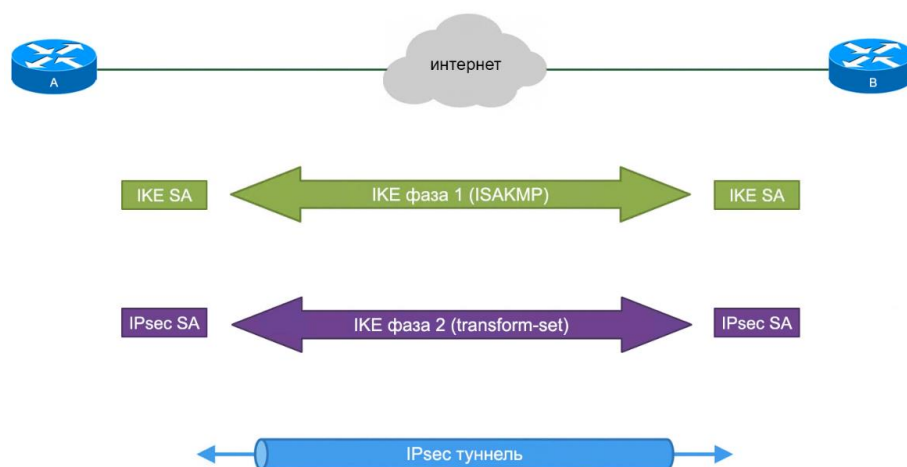


Рисунок 1.8 – Побудова IPsec тунелю

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

На першій фазі відбувається побудова міні-тунелю, що захищає інформацію, яка передається на другій фазі. На другій фазі відбувається обмін інформацією вже в зашифрованому вигляді для побудови основного IPsec тунелю, в кінці якого буде побудовано основний IPsec тунель.

IKEv1, фаза 1 (main mode):

- Визначення політик;
- ДН обмін ключами;
- Аутентифікація піра.

Політика – це набір атрибутів, що вказує алгоритми шифрування, хешування та обміну ключами та тривалість життя SA (lifetime)[2]. Під час встановлення з'єднання ініціатор присилає набір створених політик, а отримувач зрівнює їх зі своїми, окрім атрибуту lifetime. В результаті політка, що співпала буде відправлена ініціатору, а у випадку не співпадиння жодної з політик, перша фаза закінчиться помилкою і тунель не буде побудований.

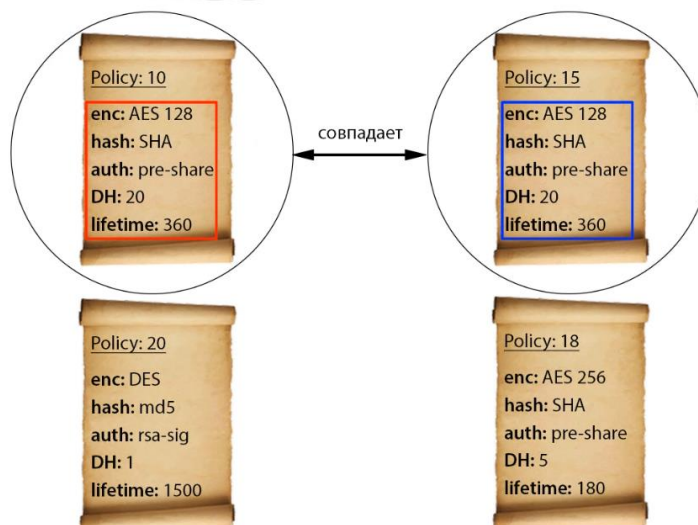


Рисунок 1.9 – Порівняння політик

На другому етапі першої фази IKEv1 генерується спільний shared secret за допомогою алгоритму Diffie-Hellman. На основі shared secret розраховується SKEYID (в залежності від типу аутентифікації), а на його основі розраховуються ще 3 сесійних ключа:

- SKEYID_a (authentication key) – для підпису ISAKMP повідомлень

- KEYID_e (encryption key) – для шифрування ISAKMP повідомлень
- KEYID_d (derivative key) – для генерації IPsec ключів

IKE підтримує аутентифікація по preshared key. IKE також підтримує використання цифрових сертифікатів. Користувачі аутентифікуються, попередньо підписуючи дані своїм цифровим підписом. Потім інша кінцева точка підтверджує підпис. В залежності від типу аутентифікації розраховується SKYID.

На третьому етапі першої фази вже з розрахованим ключовим матеріалом, аутентифікація пірів відбувається обміном HASH_Initiator та HASH_Responder, вже в зашифрованому вигляді за допомогою розрахованих ключів відбувається дешифрування хешу симетричним алгоритмом шифрування та його порівняння з новим розрахованим хешем. В результаті співпадіння розрахованих хешів, віддалений пір вважається аутентифікованим.

Друга фаза складається з двох етапів: обміном IPsec політик та їх підтвердження. Всього 3 повідомлення: 2 на обмін політиками та 1 на підтвердження ініціатором. Завдяки алгоритмам, вибраними в 1-й фазі, всі повідомлення 2-ої фази зашифровані. В політиках другої фази вказуються алгоритми, якими буде шифруватися трафік користувачів.

Результатом узгодження 2-ої фази являється Security Association (SA). SA – договір між двома пристроями, як саме захищати інформацію[3]. В такому договорі вказано: pre-share, AES and SHA, SOURCE IP, DST IP, mode tunnel, crypto ACL, key, SPI, lifetime, anti-replay window, SN, SN overflow, Path MTU. Існує два типи SA. Перший тип IKE SA (bidirectional) служить для узгодження політик на першому етапі. Другий тип IPsec SA вказує як конкретно захищати трафік (алгоритми) користувачів. За кожної SA закріплюється SPI номер. SPI являється псевдовипадковим числом. В результаті створюється головний IPsec тунель.

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

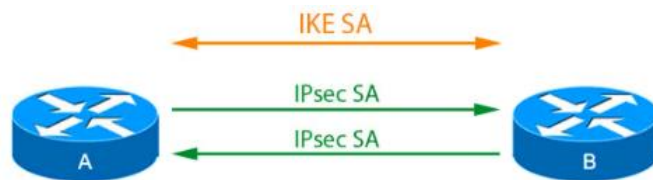


Рисунок 1.10 – Типи IPsec SA

Протокол IKEv2 був випущений у 2005 році. Він зберігає більшість функцій протоколу IKEv1, але також підтримує трансляцію мережних адрес (NAT) та забезпечує більшу гнучкість. Ідеологія IKEv2 залишилася без змін, аналогічно використовується дві фази. Однак, змінилася термінологія, тепер перша фаза тепер називається IKE_SA_INIT (IKE Security Association Initialization), а друга IKE_AUTH (IKE Authentication). Найменування SA першої фази тепер Parent SA, а другої Child SA. Тунель тепер будується за 4 повідомлення.

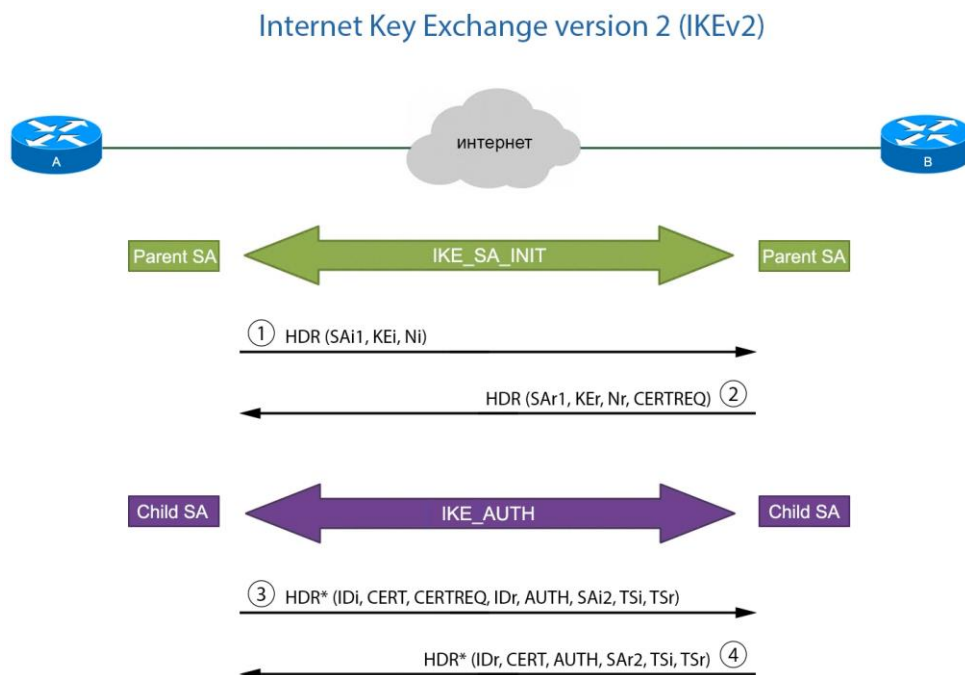


Рисунок 1.11 – IKEv2

Розрахунок ключового матеріалу тепер не залежить від типу аутентифікації як в IKEv1. На основі SKEYSEED тепер розраховується 7 ключів на основі них відбувається шифрування та перевірка аутентифікації.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

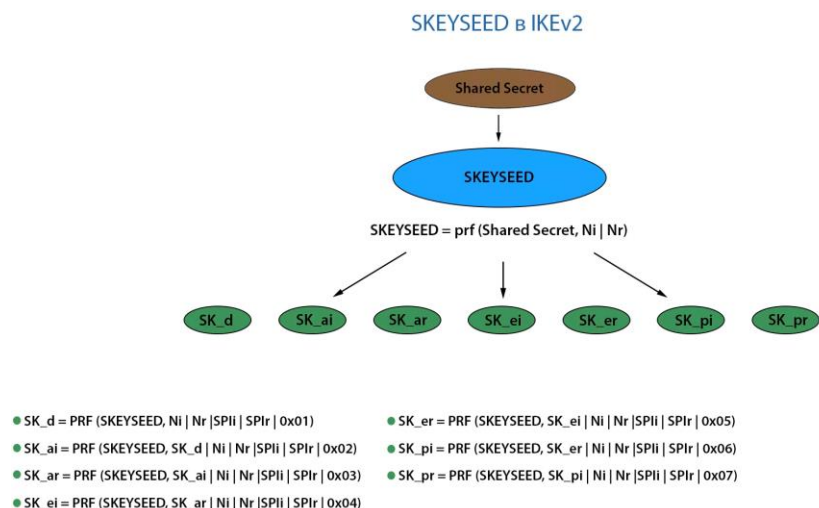


Рисунок 1.12 – Розрахунок ключового матеріалу IKEv2

Крім того, IKEv2 має можливість захисту від DoS (Denial-of-Service) атак. Режим захисту вмикається в IKEv2 вмикається автоматично, як тільки відповідач виявляє велику кількість напіввідкритих асоціацій першої фази, він зупиняє генерувати shared secret. Далі відповідач генерує Cookie і чекає на відповідь з аналогічним Cookie. Загальний обмін повідомлення збільшується до 6.



Cookie = <VersionIDofSecret> | Hash(Ni | IPi | SPIi | <secret>)

Рисунок 1.13 – Denial-of-Service Protection

Проведення порівняння двох технологій, визначення основних відмінностей відображено в табл.1.1.

Таблиця 1.1

Порівняння IKEv1 та IKEv2

Функція	IKEv1	IKEv2
Обмін повідомленнями	<u>Перша фаза:</u> 6 повідомлень в Main Mode 4 повідомлення в Aggressive Mode <u>Друга фаза:</u> 3 повідомлення	Мінімально 4 повідомлення (може змінюватися в залежності від типу аутентифікації)
Термін «фаза 1»	Наявний	IKE_SA_INIT
Термін «фаза 2»	Наявний	IKE_SA_AUTH
Методи аутентифікації	Pre-Shared Key (PSK) RSA Encrypted Nonce (RSA-encryption) Digital Signature (RSA-signature)	Pre-Shared Key (PSK) Digital Signature (RSA-signature) ECDSA Signature (ecdsa-sig) Extensible Authentication Protocol (EAP)
Асиметрична аутентифікація	Обидва піра повинні використовувати один і той же метод аутентифікації	Піри можуть використовувати різні методи аутентифікації
Час життя SAs	Час життя повинно бути узгоджено	Час життя може не узгоджуватись. В будь який момент пір може видалити SA, пославши повідомлення “delete”

Порівняння IKEv1 та IKEv2

Функція	IKEv1	IKEv2
Захист від DoS атак	Не підтримується	Використовує cookie для мінімізації DoS атак
Зміна ключового матеріалу (rekeying)	Використовує повторну аутентифікацію	Не вимагає повторної аутентифікації
Підтвердження повідомлень	Відсутнє	Кожне інформаційне повідомлення підтверджується
NAT Traversal, Dead Peer Detection, Remote Access VPN	Являється розширенням	Підтримується за замовчуванням

1.3 Site-to-Site та Remote Access VPN

Типи тунелів, які буде налаштовано в даній кваліфікаційні роботі[5]:

- Remote Access VPN – це тунель, що з'єднує клієнта з попередньо встановленим ПЗ та пристрій, що виконує роль сервера і реалізує підключення клієнтів.
- Site-to-Site VPN – передбачає постійний тунель між двома пристроями (сайтами).

Приклади використання цих технологій [3]:

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

2) Site-to-Site VPN – тунель між віддаленими мережами, наприклад, філії з центральним офісом. Побудову тунелю виконує сам граничний маршрутизатор. Він будує віддалене з'єднання між маршрутизаторами, які об'єднуються в одну

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

мережу, відтак, співробітник без спеціалізованого ПЗ працює у локальній мережі офісу.

На обладнанні Cisco можливо реалізувати наступні типи захищених Site-to-Site та Site-to-Multisite VPN тунелів: DMVPN, Static and Dynamic VTI, Crypto Maps, GRE. Remote Access можна налаштувати за допомогою EasyVPN та SSL VPN.

Flex VPN – це універсальна технологія від Cisco, за допомогою якої всі типи тунелів конфігуруються через внесення незначних змін в IKEv2 протокол. До того ж, важливою перевагою даної технології є автоматичний захист VPN мережі від DDoS-атак [2]. Технологія сумісна з мережами VPN, побудованими на обладнанні інших виробників. Тепер такі вирішення як EasyVPN, DMVPN, DynamicVTI, VPN на базі crypto-map можуть бути замінені одною технологією – Flex VPN. Роблячи невеликі зміни в конфігурації за допомогою FlexVPN можна гнучко створити VPN з'єднання як Site-to-Site, так і Remote Access.

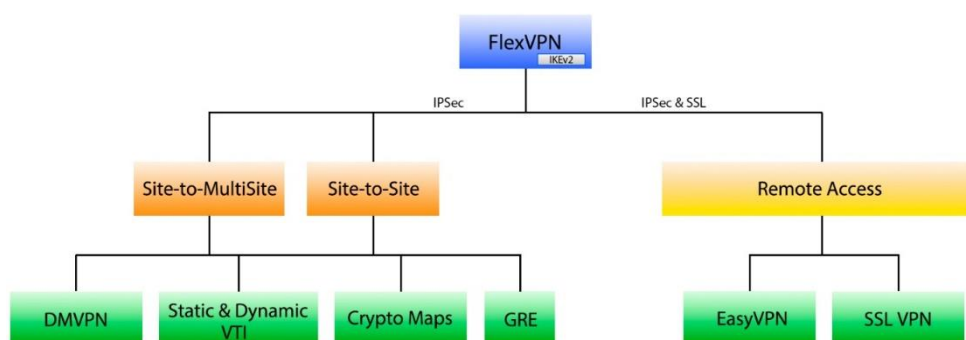


Рисунок 1.14 – Об'єднання технологій FlexVPN

Можна сказати, що FlexVPN – це фреймворк, тобто спільна система управління протоколом IKEv2, що дає змогу через єдиний синтаксис команд IOS реалізовувати внесення незначних налаштувань в конфігурацію налаштовувати різні версії VPN. За допомогою FlexVPN можна підключати віддалених працівників як за допомогою IPsec, так і SSL. Для налаштування SSL зручно використовувати ASA, а для IPsec маршрутизатор, тим не менше не завжди так, деякі маршрутизатори підтримують SSL, а IPsec на ASA був присутнім завжди.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

1.4 Інфраструктура відкритого ключа

На ряду з IPsec, інфраструктура відкритого ключа є важливою технологією на якій базується мережева безпека. Різниця між симетричним та асиметричним шифруванням:

- Шифрування з симетричними ключами — схема шифрування, у якій ключ шифрування, та ключ дешифрування збігаються, або один легко обчислюється з іншого та навпаки
- Шифрування з асиметричними ключами — схема шифрування, у якій для шифрування використовують один ключ, а для розшифрування — інший.

Недоліком симетричного шифрування є те, що ключ потрібно якось передати сусідньому пристрою по мережі. На допомогу приходить алгоритм Diffie-Hellman. За допомогою цього алгоритму ключ взагалі не передається по Internet, а генерується однаковий на обох маршрутизаторах.

Недоліком асиметричного шифрування є те, що алгоритми RSA, ECDSA, DSA, Diffie-Hellman шифрують трафік повільно, тому користувацький трафік шифрується симетричними алгоритмами.

При асиметричному шифруванні відкритий ключ передається вільно по мережі, де потім за допомогою нього маршрутизатор В шифрує дані та посилає до назад маршрутизатору А, після чого маршрутизатор А розшифровує дані своїм закритим ключем (рис.1.15).

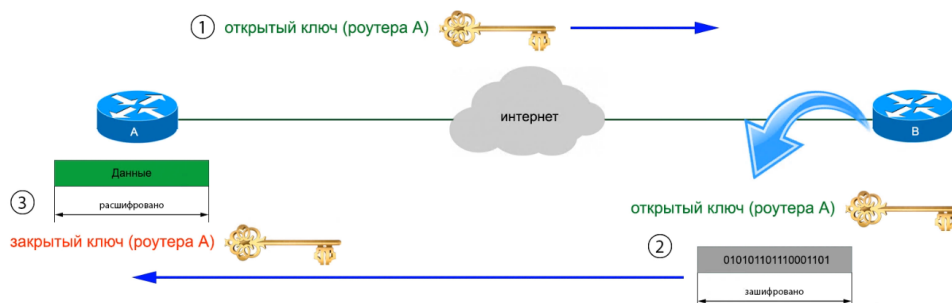


Рисунок 1.15 – Асиметричне шифрування

У випадку якщо зломиснику вдасться перехопити відкритий ключ маршрутизатора А у момент передачі дані можуть бути прочитані (рис. 1.16).

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

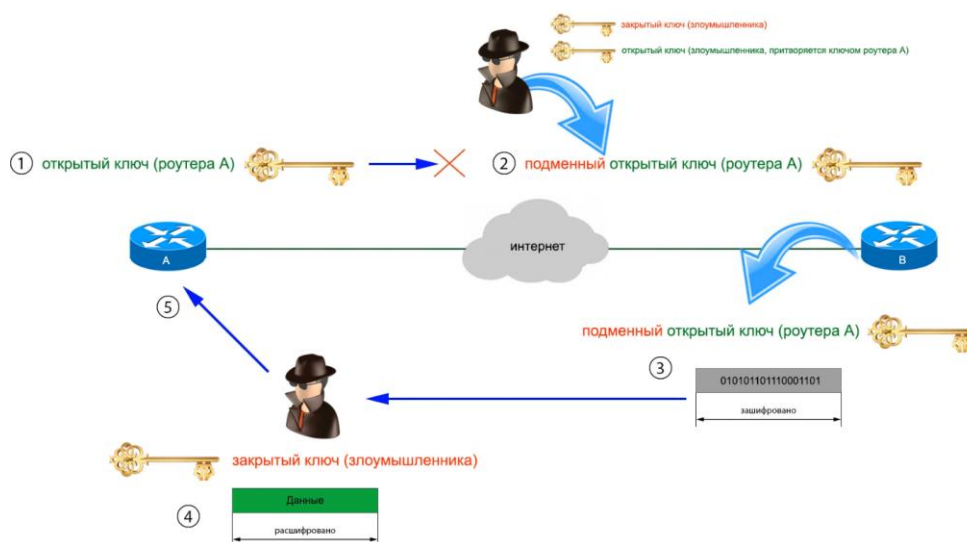


Рисунок 1.16 – Man-in-the-middle атака

Згідно рисунку 1.16 маршрутизатор А посилає свій ключ маршрутизатору Б, однак ключ не доходить до маршрутизатора Б, зломисник перехоплює ключ та відкладає в сторону, після чого зломисник генерує свою пару відкритого та закритого ключа. Згенерований відкритий ключ зломисника надсилається маршрутизатору Б. Маршрутизатор Б нічого не підозрюючи шифрує дані ключем зломисника, думаючи, що шифрує ключем маршрутизатора А. Після чого відправляє дані маршрутизатору А, де їх перехоплює та сама «людина по середині», розшифровує їх. В результаті чого конфіденційність була порушена. Однак на цьому атака не завершується зломисник знов зашифровує дані відкритим ключем маршрутизатора А та посилає маршрутизатору А. Таким чином не хто з учасників не здогадається, що є третє лице, яке перехоплює і читає дані. У зв'язку з цим потрібно якось підтвердити, що це саме ключ маршрутизатора А, а не зломисника. Для цього відкритий ключ потрібно зв'язати з деякою інформацією, кому він належить, який його серійний номер, яким алгоритмом він був згенерований. Крім цього, якщо маршрутизатор А виявить, що ключ був викрадений, то потрібний механізм для відкликання сертифіката, щоб маршрутизатор Б більше не приймав його.

Сертифікат – це відкритий ключ, плюс інформаційна обв'язка. Приклад сертифікату стандарту X.509 (рис. 1.17).

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

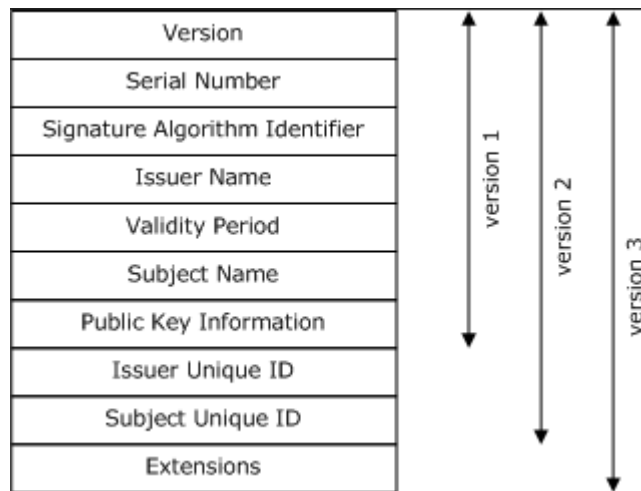


Рисунок 1.17 – Сертифікат формату X.509

Однак, сам по собі сертифікат не гарантує безпеку, оскільки його можна так само підмінити як відкритий ключ. Для вирішення цієї проблеми сертифікат потрібно завірити, необхідний третій учасник який підтвердить належність сертифікату віддаленому пристрою.

Механізмом для завірення сертифікату буде виступати Certificate Authority (центр сертифікації). Алгоритм даного механізму наступний: маршрутизатор А генерує пару відкритий та закритий ключ, згодом відправляє свій відкритий ключ з додатковою службовою інформацією, одним словом запит на СА сервер. Для запиту сертифікату по мережі буде використовуватися протокол SCEP (Simple Certificate Enrollment Protocol). На основі переданої інформації, СА формує сертифікат, заповнюючи відповідні поля сертифікату стандарту X.509. Після чого СА розраховує хеш від полів сертифікату. Розрахований хеш шифрується закритим ключем СА та поміщається в сертифікат в поле digital signature. Зашифрований хеш, отриманий від полів сертифіката і вкладений в одне з полів того ж самого сертифіката, і є цифровим підписом цього сертифіката. Тепер це підписаний або завірений сертифікат. Маршрутизатор Б проводить аналогічну операцію, після чого обидва маршрутизатори мають по завіреному сертифікату.

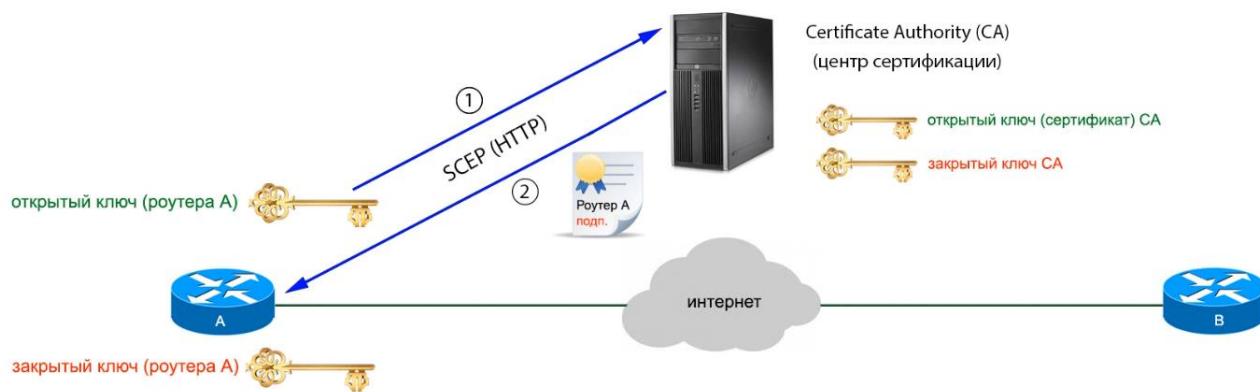


Рисунок 1.18 – Public Key Infrastructure

Окрім цього СА виписує ще сертифікат для кожного пристрою. Пристрій, що має СА сертифікат може довіряти всім сертифікатам випущеним даним СА. Виписаний сертифікат (відкритий ключ) СА використовується для перевірки піра, ним розшифровується поле digital signature та порівнюється

Тепер атака man-in-the-middle зазнає невдачі, оскільки зломисник змінюючи поля сертифікату не має закритого ключа СА для шифрування підпису. Якщо сертифікат буде викрадено, тоді зломиснику вдасться ініціювати аутентифікацію.

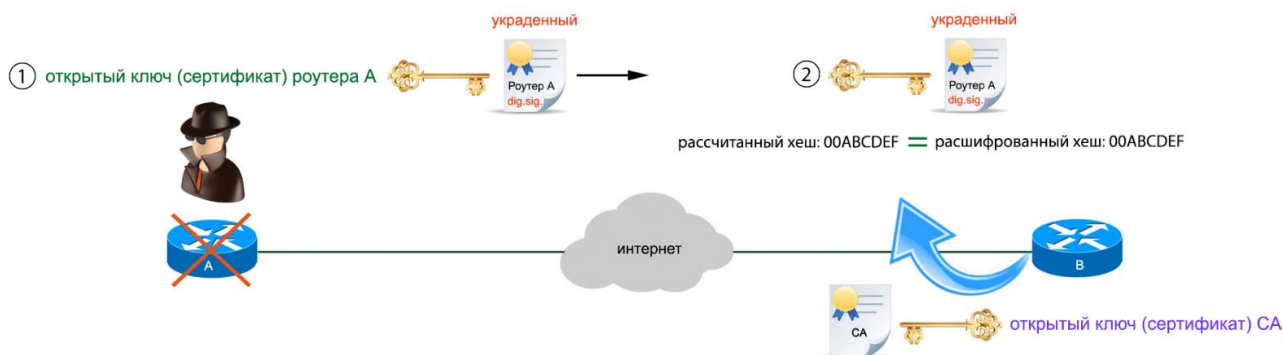


Рисунок 1.19 – Викрадений сертифікат

Однак цього трапляється, оскільки маршрутизатор Б проводить ще одну перевірку. В аутентифікації по pre-shared ключу маршрутизатори генерували HASH_I та HASH_R та обмінювалися ними. В аутентифікації по сертифікати вони розраховуються, але нікуди не передаються, замість цього від них береться хеш, який шифрується закритим ключем самого маршрутизатора. Розраховані

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

підписи відповідно називаються SIG_I та SIG_R, тому вже вони передаються на маршрутизатори.

У випадку коли зловмисник отримає і доступ до закритого ключа самого маршрутизатора, тоді йому нічого не завадить встановити з'єднання. Таке можливо, якщо зловмисник отримав повний доступ до IOS та закритий ключ був помічений як експортований. Потрібно механізм, щоб маршрутизатор, який отримує сертифікат мав змогу перевірити чи сертифікат не відкликаний. Такими механізмами може бути Certificate Revocation List (CRL), Online Certificate Status Protocol (OSCP) або AAA Server (Cisco-пропрієтарна альтернатива OCSP).

Всі вони виконують працюють за єдиною логікою, файл чи база даних, що містить список сертифікатів, які помічають як відкликані. Якщо сертифікат був скомпрометований, системний адміністратор має змогу відкликати сертифікат на CA сервері.

Отримавши команду на відкликання сертифікату, CA внесе зміни в CRL, на кшталт сертифікат з id 33394 був відкликаний та опублікує його на веб-сервері. Крім того CA розрахує хеш CRL файлу та підпише своїм закритим ключем.

Маршрутизатор, крім всіх попередніх перевірок, ще завантажить CRL файл з сервера та перевірить чи CRL файл був випущений не підробленим СА. Для цього самостійно розрахує хеш та розшифрує зашифрований хеш СА маршрутизатора відкритим ключем СА, після чого порівняє їх. У випадку якщо хеші зійдуться, перевірить отриманий сертифікат на факт відклику.

Недоліком цього методу являється, те що файл постійно потрібно завантажувати з сервера, а у випадку коли пристроїв може буде багато, то і розмір файлу значний. Але перевагою CRL файлу, те що він є простий в налаштуванні і якщо пристроїв не багато, то розмір файлу не великий.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

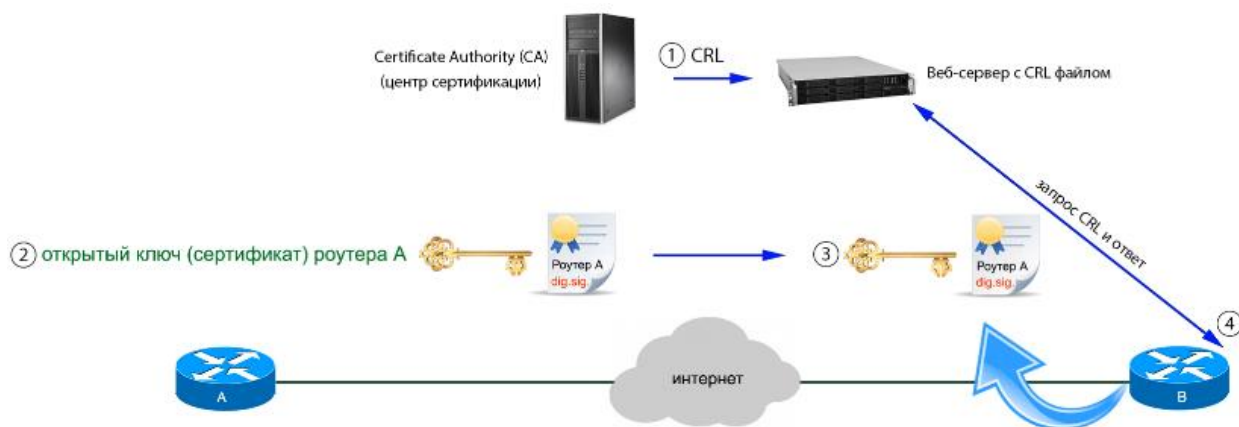


Рисунок 1.20 – Перевірка сертифікату на факт відклику

Отже, все, що було розглянуто й називається PKI. Інфраструктура відкритого ключа – це інтегрований комплекс методів та засобів, призначених забезпечити впровадження та експлуатацію криптографічних систем.

Висновки до першого розділу

У першому розділі досліджено, що використання VPN забезпечує безпеку мережевого трафіку в загальнодоступних мережах. Було детально проаналізовано загальну концепцію, що використовуються для захисту тунельного з'єднання через незахищену мережу.

Детально розглянуто VPN шифрування трафіку за допомогою технології IPsec, які алгоритми використовуються для забезпечення конфіденційності даних, аутентифікації користувача та алгоритми забезпечення цілісності даних. Визначено основні відмінності між протоколами ESP, AH та ESP+AH. ESP шифрує та підписує дані, AH – підписує включаючи зовнішній IP заголовок, але не шифрує, а ESP + AH – шифрує та підписує дані, включаючи зовнішній IP заголовок, але використовується рідко.

Зазначено, основні етапи на першій фазі IPsec тунелю: обмін політиками для узгодження алгоритмів шифрування та перевірки цілісності пакетів, генерування спільного shared secret, аутентифікація піра. Описано, як на другій фазі по вже зашифрованому міні-тунелю передаються політики для узгодження

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

алгоритмів шифрування користувацьких даних, де в разі співпадіння політик вже будується головний тунель.

Проведено порівняння між IKEv1 та IKEv2 протоколами. Основні переваги IKEv2: підтримка сучасних VPN клієнтів, асиметрична аутентифікація, захист від DoS-атак та підтримка розширень за замовчуванням.

Наведено класифікацію віртуальних приватних мереж на основі доступних на обладнанні Cisco. Проаналізовано їх можливості та особливості. Досліджено основні теоретичні відомості про фреймворк FlexVPN, насамперед що він підтримує тільки IKE версії 2 та SSL.

Досліджено інфраструктуру відкритого ключа, а саме як відбувається аутентифікація пірів за допомогою сертифікатів. Детально розібрано структуру сертифікату, які поля він в собі містить, як СА підписує сертифікат та захищає від атаки Man-in-the-middle. Наведено приклад перевірки сертифікату на факт відклику за допомогою CRL сертифікату.

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ГОЛОВНОГО ОФІСУ ТА ФІЛІАЛУ

2.1 Проєктування моделей та схем адресацій

Для побудови великих мереж підприємств використовується ієрархічний мережевий дизайн, оскільки дозволяє розподілити трафік на рівні.

– Access рівень призначається для підключення кінцевих абонентів: робочих станцій, принтерів, телефонів, тощо. Основна ціль – прокомутувати трафік від користувача на рівень вище (distribution).

– Distribution рівень збирає трафік від access рівня, який згодом передає або на рівень вище або назад на access. Окрім цього комутатори рівня розподілення повинні підтримувати велику кількість функцій, оскільки основні мережеві задачі виконується на ньому, такі як: маршрутизація, пріоритет, безпека та фільтрація трафіка.

– Core рівень призначається для передачі від одного distribution блока до іншого, тобто від одної будівлі до іншої.

– Enterprise edge – це рівень де знаходяться маршрутизатори, які з'єднується з Internet. Також на них працює NAT, Firewall, вони ж являються VPN пристроями. До edge рівня також належать ASA, IDS та IPS.

На основі ієрархічної моделі було побудовано наступну структурну схему мережі головного офісу (рис. 2.1).

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

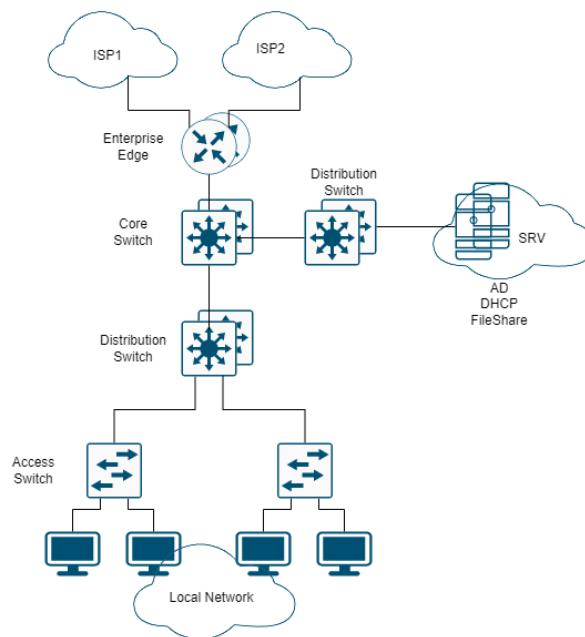


Рисунок 2.1 Структурна схема мережі головного офісу

На основі структурної схеми було розроблено L2 схему мережі головного офісу:

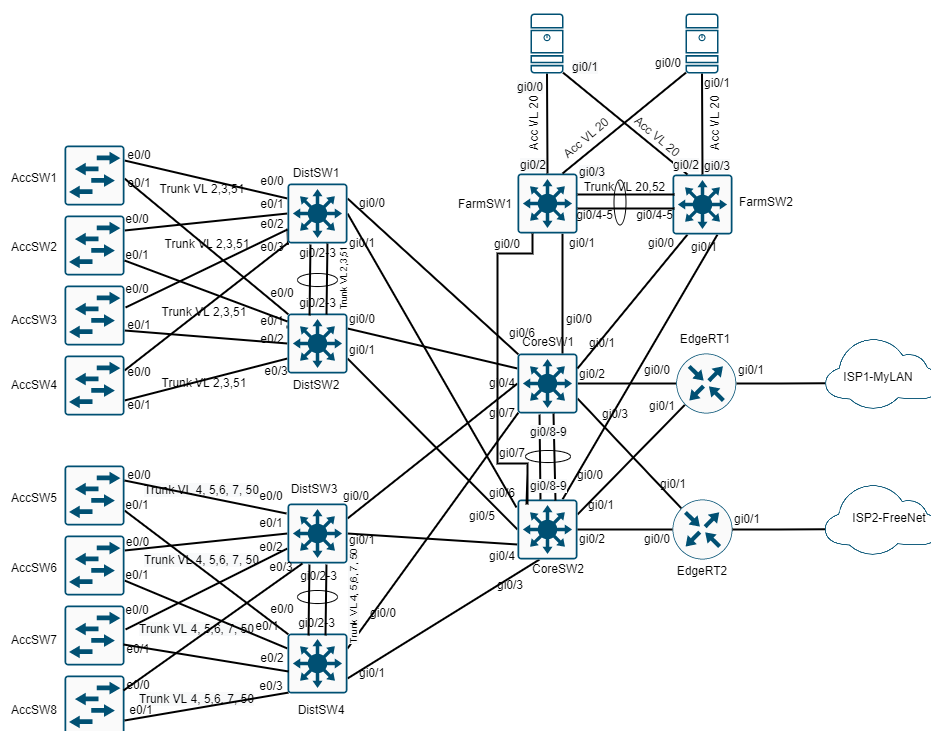


Рисунок 2.2 Схема мережі головного офісу

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Для побудови мережі головного офісу була обрана модель Switched Campus Architecture, де L3 частина мережі виконує маршрутизацію, а нижня комутацію.

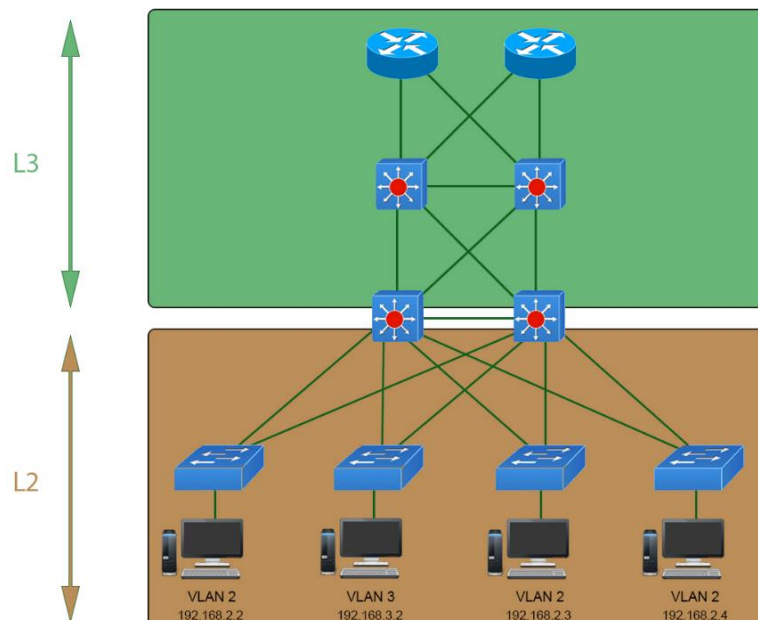


Рисунок 2.3 – модель Switched Campus Architecture

Переваги даної моделі:

- можливість побудови end-to-end VLANs
- одні і ті ж політики (безпеки, QoS) можуть примінитися до одних і тих же користувачів не залежно від їх фізичного розташування
- можливість використання дешевих комутаторів на access (L2+) без підтримки маршрутизації

Недоліки даної моделі:

- broadcast повідомлення розсилаються на всі комутатори
- необхідність використання spanning-tree
- ускладнений troubleshooting
- distribution комутатори повинні знати про всі VLAN

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

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Таблиця 2.1 – Схема адресації головного офісу

Пристрій	Інтерфейс	ІР-адреса	Маска підмережі	Шлюз за замовчуванням	Пристрій підключення	Порт
Маршрутизатор EdgeRT1	F2/0	165.25.24.12	/24	N/A	ISP	-
	F1/0	10.0.11.2	/24	N/A	CoreSW2	E1/0
	F0/0	10.0.10.2	/24	N/A	CoreSW1	E1/0
	Lo0	50.0.7.1	/24	N/A	-	-
Маршрутизатор EdgeRT2	F2/0	218.22.1.3	/24	N/A	ISP	-
	F1/0	10.0.12.2	/24	N/A	CoreSW2	E1/1
	F0/0	10.0.13.2	/24	N/A	CoreSW1	E1/1
	Lo0	50.0.8.1	/24	N/A	-	-
Комутатор CoreSW1	E1/0	10.0.10.1	/24	N/A	EdgeRT1	F0/0
	E1/1	10.0.13.1	/24	N/A	EdgeRT2	F0/0
	E1/3	10.0.14.2	/24	N/A	FarmDistSW1	F0/0
	E1/2	10.0.9.1	/24	N/A	CoreSW2	E1/2
	E2/0	10.0.17.2	/24	N/A	FarmDistSW2	F0/0
	E0/3	10.0.7.2	/24	N/A	DistSW4	F0/1
	E0/2	10.0.5.2	/24	N/A	DistSW3	F0/1
	E0/0	10.0.3.2	/24	N/A	DistSW2	F0/0
	E0/0	10.0.1.2	/24	N/A	DistSW1	F0/0
	Lo0	50.0.5.1	/24	N/A	-	-
Комутатор CoreSW2	E1/0	10.0.11.1	/24	N/A	EdgeRT1	F1/0
	E1/1	10.0.12.1	/24	N/A	EdgeRT2	F1/0
	E1/3	10.0.15.2	/24	N/A	FarmDistSW1	F0/1
	E2/0	10.0.16.2	/24	N/A	FarmDistSW2	F0/1
	E0/3	10.0.8.2	/24	N/A	DistSW4	F0/0
	E0/2	10.0.6.2	/24	N/A	DistSW3	F0/0
	E0/1	10.0.4.2	/24	N/A	DistSW2	F0/1
	E0/0	10.0.2.2	/24	N/A	DistSW1	F0/1

Продовження таблиці 2.1

	E1/2	10.0.9.2	/24	N/A	CoreSW1	E1/2
	Lo0	50.0.6.1	/24	N/A	-	-
Комутатор DistSW1	F0/0	10.0.1.1	/24	N/A	CoreSW1	E0/1
	F0/1	10.0.2.1	/24	N/A	CoreSW2	E0/0
	vlan 2	192.168.2.50	/24	N/A	-	-
	vlan 3	192.168.3.50	/24	N/A	-	-
	Lo0	50.0.1.1	/24	N/A	-	-
Комутатор DistSW2	F0/0	10.0.3.1	/24	N/A	CoreSW1	E0/0
	F0/1	10.0.4.1	/24	N/A	CoreSW2	E0/1
	vlan 2	192.168.2.51	/24	N/A	-	-
	vlan 3	192.168.3.51	/24	N/A	-	-
	Lo0	50.0.2.1	/24	N/A	-	-
Комутатор DistSW3	F0/0	10.0.3.1	/24	N/A	CoreSW1	E0/2
	F0/1	10.0.3.1	/24	N/A	CoreSW2	E0/2
	vlan 4	192.168.4.50	/24	N/A	-	-
	vlan 5	192.168.5.50	/24	N/A	-	-
	vlan 6	192.168.6.50	/24	N/A	-	-
	vlan 7	192.168.7.50	/24	N/A	-	-
	Lo0	50.0.3.1	/24	N/A	-	-
Комутатор DistSW4	F0/0	10.0.8.1	/24	N/A	CoreSW2	E0/3
	F0/1	10.0.7.1	/24	N/A	CoreSW1	E0/3
	vlan 4	192.168.4.51	/24	N/A	-	-
	vlan 5	192.168.5.51	/24	N/A	-	-
	vlan 6	192.168.6.51	/24	N/A	-	-
	vlan 7	192.168.7.51	/24	N/A	-	-
	Lo0	50.0.4.1	/24	N/A	-	-
Комутатор FarmDistSW1	F0/0	10.0.14.1	/24	N/A	CoreSW1	E1/3
	F0/1	10.0.15.1	/24	N/A	CoreSW2	E1/3
	F1/2	20.0.1.2	/24	N/A	Сервер CS	E0/1
	vlan 20	123.20.20.50	/24	N/A	-	-
	Lo0	50.0.9.1	/24	N/A	-	-

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Продовження таблиці 2.1

Комутатор FarmDistSW2	F0/1	10.0.16.1	/24	N/A	CoreSW1	E2/0
	F0/0	10.0.17.1	/24	N/A	CoreSW2	E2/0
	F1/2	20.0.2.2	/24	N/A	Сервер CS	E0/0
	vlan 20	123.20.20.51	/24	N/A	-	-
	Lo0	50.0.10.1	/24	N/A	-	-
Switch AccSW1	Vlan 51	50.0.12.2	/24	N/A	-	-
Switch AccSW2	Vlan 51	50.0.12.3	/24	N/A	-	-
Switch AccSW3	Vlan 51	50.0.12.4	/24	N/A	-	-
Switch AccSW4	Vlan 51	50.0.12.5	/24	N/A	-	-
Switch AccSW5	Vlan 50	50.0.11.2	/24	N/A	-	-
Switch AccSW6	Vlan 50	50.0.11.3	/24	N/A	-	-
Switch AccSW7	Vlan 50	50.0.11.4	/24	N/A	-	-
Switch AccSW8	Vlan 50	50.0.11.5	/24	N/A	-	-
Сервер CS	E0/0	20.0.1.1	/24	N/A	FarmDistSW2	F1/2
	E0/1	20.0.2.1	/24	N/A	FarmDistSW1	F1/2
	Lo0	60.0.1.1	/24	N/A	-	-
Сервер WinServer	E0	123.20.20.5	/24	123.20.20.1	FarmDistSW1	F1/3
	E1				FarmDistSW2	F1/3

Альтернативною Switched Campus Architecture являється Routed Campus Architecture. Верхня L3 зона відповідає тепер за маршрутизацію, а нижня за комутацію. Саме ця модель обрана для побудови мережі філіалу.

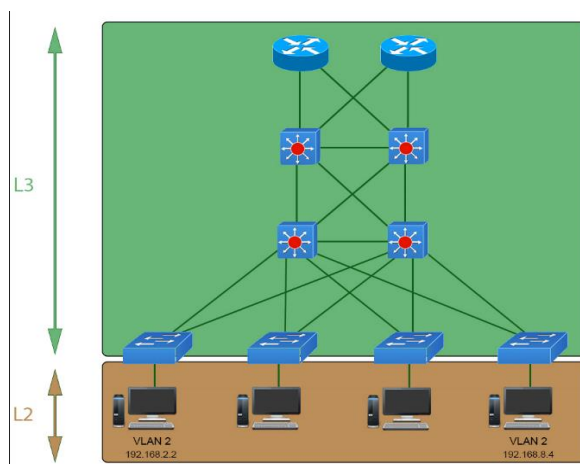


Рисунок 2.4 – модель Routed Campus Architecture

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Переваги даної моделі:

- відсутня необхідність використовувати spanning-tree;
- полегшений troubleshooting;
- не потрібно створювати VLANs на distribution комутаторах;
- broadcast повідомлення розповсюджуються тільки в межах одного access комутатора.

Недоліки даної моделі:

- тільки local VLANs;
- користувачі належать до одного широкомовного домену тільки тоді, коли вони підключені до одного access комутатора;
- необхідність використання дорогих комутаторів на access (L3) з підтримкою маршрутизації;
- одній й ті ж політики (безпеки, QoS) не можуть примінитися до одних й тих же користувачів, якщо вони підключені до різних access комутаторів.

На основі моделі Routed Campus Architecture була побудована наступна схеми мережі філіалу:

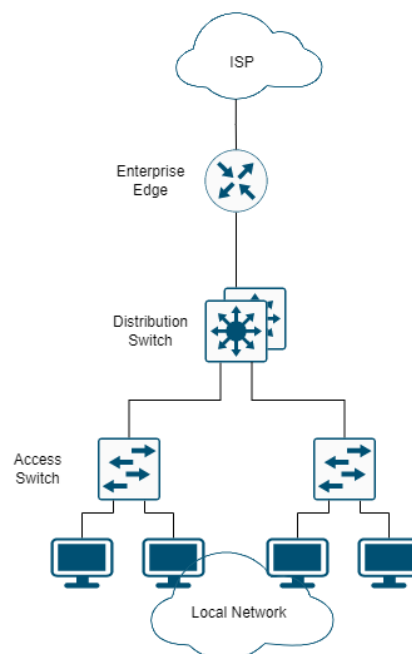


Рисунок 2.5 – Структурна схема мережі філіалу

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

На основі структурної схеми було сконструювано наступну схему L2 (рис. 2.6).

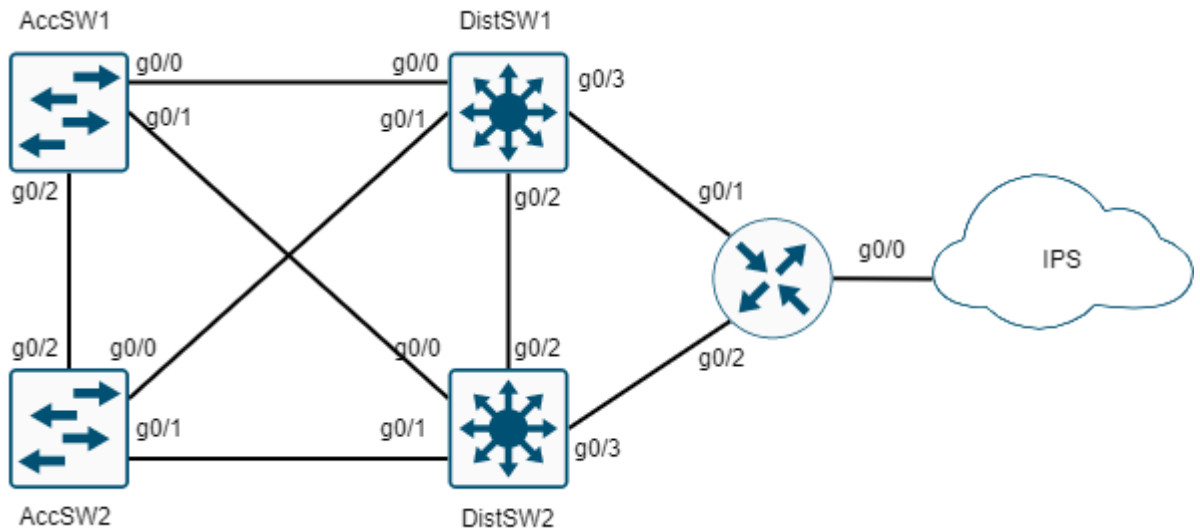


Рисунок 2.6 – L2 схема мережі філіалу

Таблиця 2.2 – Схема адресації філіалу

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням	Пристрій підключення	Порт
Маршрутизатор BrEdgeRT1	E0/2	30.0.20.2	/24	N/A	ISP	-
	E0/0	30.0.1.2	/24	N/A	BrDistSW1	E0/0
	E0/1	30.0.2.2	/24	N/A	BrDistSW1	E0/0
	Lo0	70.0.1.1	/24	N/A	-	-
Маршрутизатор BrDistSW1	E0/0	30.0.1.1	/24	N/A	BrEdgeRT1	E0/0
	E0/1	30.0.6.2	/24	N/A	BrAccSW2	E1/1
	E0/2	30.0.4.1	/24	N/A	BrAccSW1	E1/1
	E0/3	30.0.3.2	/24	N/A	BrDistSW2	E1/1
	Lo0	70.0.2.1	/24	N/A	-	-
Маршрутизатор BrDistSW2	E0/0	30.0.2.1	/24	N/A	BrEdgeRT1	E0/1
	E0/1	30.0.3.1	/24	N/A	BrDistSW1	E1/1
	E0/2	30.0.5.1	/24	N/A	BrAccSW1	E1/0
	E0/3	30.0.7.1	/24	N/A	BrDistSW2	E1/0
	Lo0	70.0.3.1	/24	N/A	-	-

Продовження таблиці 2.2

BrAccSW1	E0/0	30.0.4.2	/24	N/A	BrDistSW1	E0/2
	E1/0	30.0.7.2	/24	N/A	BrDistSW2	E0/2
	E0/1	30.0.8.2	/24	N/A	BrAccSW1	E0/2
	vlan 2	172.20.20.1	/24	N/A	-	-
	Lo0	70.0.4.1	/24	N/A	-	-
BrAccSW2	E0/0	30.0.6.1	/24	N/A	BrDistSW1	E0/1
	E0/1	30.0.5.2	/24	N/A	BrDistSW2	E0/2
	E0/2	30.0.8.1	/24	N/A	BrAccSW1	E0/1
	vlan 3	172.20.21.1	/24	N/A	-	-
	Lo0	70.0.5.1	/24	N/A	-	-
PC-A	E0	172.20.20.2	/24	172.20.20.1	BrAccSW1	E0/2
PC-B	E0	172.20.21.2	/24	172.20.21.1	BrAccSW2	E0/3

2.2 Вимоги до обладнання

Для створення мережі необхідно підібрати обладнання, яке б відповідало вимогам. Вибір обладнання буде відбуватися з асортименту компанії Cisco. Cisco – ведучий виробник телекомунікаційного обладнання, яка гарантує надійність обладнання, підтримку Інтернет спільнотою та можливість навчання з використанням програмних симуляторів чи емуляторів, таких як Cisco Packet Tracer чи GNS3.

Оскільки, в мережі використовується ієрархічна модель, то обладнання потрібно обрати до кожного рівня: Access Layer, Distribution Layer, Core Layer та Edge Layer.

Крім того, існують 4 основні версії IOS, яку версію використовувати залежить від поставлених задач.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Comparison	LAN Lite	LAN Base	IP Base	IP Services
Scale of business	Small	Small-to-medium	Medium-large	Large
Layer 2	Yes	Enterprise access	Complete access	Complete access
Layer 3	No	Yes	Enterprise access	Complete access
Security	Basic	Enterprise access Security	Complete access Security	Complete access Security
QoS	Basic	Enterprise access QoS	Complete access QoS	Complete access QoS

Рисунок 2.7 – Порівняння 4 версій

Рівень доступу – це точка входу для користувачів, принтерів, сканерів, ір-телефонів, ір-камер, тощо. Як правило на рівні доступу застосовуються комутатори другого рівня моделі OSI (L2). Комутатори серії 2960 – найбільш економічне рішення (найбільш низька ціна за порт). Access рівень має підтримувати наступний функціонал: керування, підтримка VLAN, агрегація каналів, підтримка Voice VLAN, QoS, DHCP Snooping, Port security, IP Source guard, Dynamic ARP Inspection, логування та моніторинг.

Виходячи з вище перерахованих функцій, які має містити в собі комутатор та бюджету було обрано Cisco Catalyst 2960-Plus з версією прошивки LAN Base на 24 порти.



Комутатор Cisco WS-C2960+24LC-L

Будьте першим, хто відгукнеться про цей товар

Catalyst 2960 Plus 24 10/100 (8 PoE) + 2 T/SFP LAN Base

Артикул (SKU): WS-C2960+24LC-L

Состояние: **Новий**

Наличие: **Доступний під замовлення**

Срок поставки: **14-21 день**

GPL Price: ~~4981\$~~

35 955 грн

Рисунок 2.8 – Cisco Catalyst 2960-Plus

Комутатор має наступні характеристики:

- 24 або 48 Fast Ethernet портів;
- наявність PoE портів (в залежності від моделі);

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

- 2 Gigabit комбо порта, або 2 sfp + 2 Gigabit;
- 128 Мб оперативної пам'яті;
- 64 Мб флеш пам'яті;
- не стикується;
- Lan Base/Lan Lite прошивка;
- Підтримка IOS 15.0(2) SE і вище.

Основні переваги LAN Base перед LAN Lite:

- підтримка статичної маршрутизації (до 16 маршрутів);
- підтримка розширених функцій безпеки: можливість налаштування ACL на порт, IPSG, DAI, NAC, DHCP Snooping, IP source guard;
- підтримка до 255 VLAN для LAN Base і 64 для LAN Lite;
- підтримка RSPAN;
- підтримка розширених функцій QoS (ingress policing, AutoQoS).

Наступний крок – це вибір L3 пристрою для рівня розподілення, головна задача якого - агрегація каналів комутатора доступу, відмовостійкість та підключення інших модулів. Рівень розподілення є важливою ланкою в роботі всієї мережевої інфраструктури і потребує високо продуктивного відмовостійкого обладнання. Модель Cisco SBA LAN передбачає використання технології стикування і агрегованих з'єднань між мережевими пристроями, тоді як традиційна модель використовує принцип надлишковості.

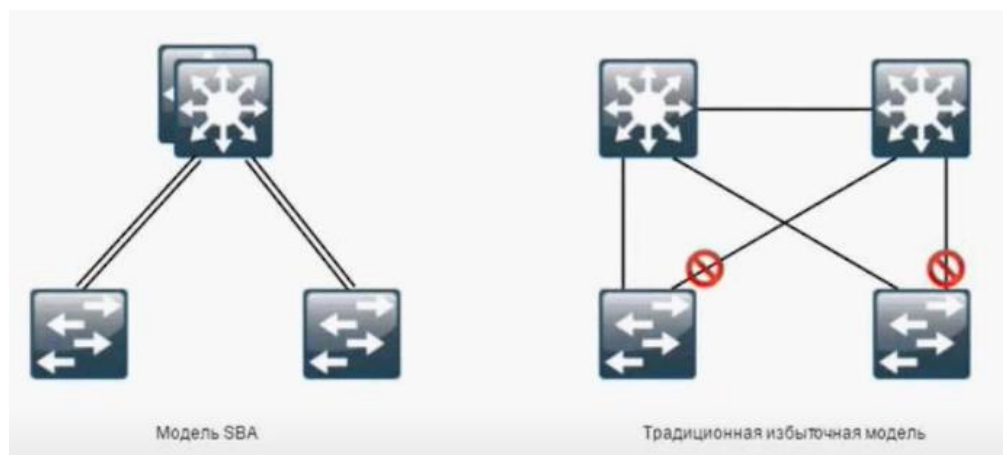


Рисунок 2.9 – Моделі підключення між рівнем доступу та розподілення

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Можливі серії, які можуть бути використані в мережі є Cisco Catalyst 3560-X, Cisco Catalyst 3750-X, Cisco Catalyst 4500-X.



Рисунок 2.10 – Catalyst 3750-X

Основні характеристики Cisco Catalyst 3750-X:

- 24 або 48 gigabit портів;
- Пропускна здатність 160 Гб/с
- Наявність PoE+ портів (в залежності від моделі)
- 256 Мб оперативної пам'яті
- 128 Мб флеш пам'яті
- Стикуються за замовчуванням
- Резервні джерела живлення
- Прошивка LAN Base, IP Base та IP Services (можливо оновлення між версіями)

Підтримка технології StackWise Plus:

- До 9 пристроїв в стеці
- Пропускна здатність 64 Гбіт/с
- Розподілення живлення
- Сумісність з L3 моделлю 3750

Дизайн великих корпоративних мереж, які охоплюють дві і більше будівлі зобов'язує використання рівня ядра. Головні задачі рівня ядра ж агрегація комутаторів рівня розподілення, відмовостійкість та висока продуктивність. Комутатори ядра найпотужніші в мережі. Наявність рівня ядра дозволяє зменшити кількість з'єднань. На рисунку 2.10 наведено приклад з'єднань з ядром і без ядра.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

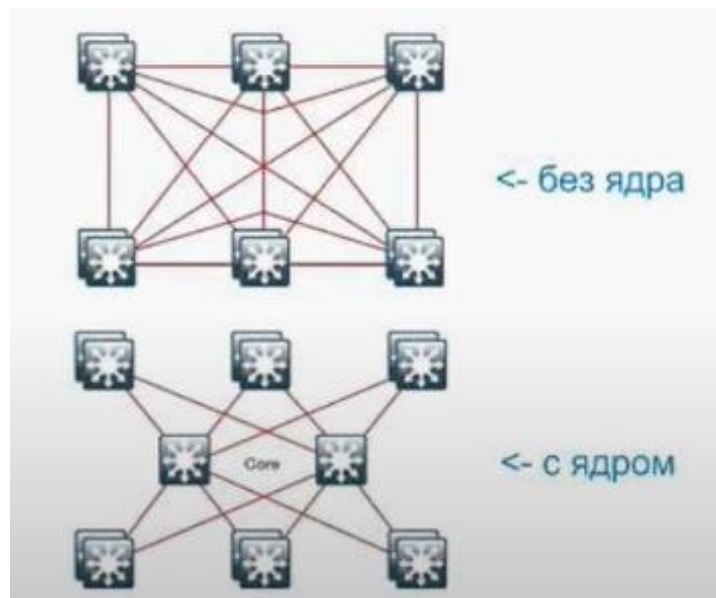


Рисунок 2.11 – Cisco Catalyst 2960-Plus

Для рівня ядра була обрана серія Cisco Catalyst 6500-E:



Рисунок 2.12 – Cisco Catalyst 6500-E серія

Cisco Catalyst 6500-E підтримує:

- Підтримка лінків до 100 Гбіт/с
- Підтримка модулів: NAM до 3 штук (15 Гбіт/с), WiSM (безпроводний контролер) – до 2 штук (20 Гбіт/с), ASA-SM (20 Гбіт/с)
- Sup2T, Sup2T-XL
- Комутація – 2 Тбіт/с (4 Тбіт/с – VSS)
- 80 Гбіт/с на слот
- MSFC5, PFC4/DFC4

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- 3x1GE (SFP) + 2x10GE (x2)

Для рівня ядра було обрано комутатор Cisco VS-C6504E-SUP2T:



Рисунок 2.13 – Cisco VS-C6504E-SUP2T

Edge маршрутизатори мають відповідати наступним вимогам:

- Підтримка всіх функцій Cisco VPN
- Підтримка версії Cisco IOS не нижче 15.2(1) T
- Компактність та енергоефективність обладнання.

Маршрутизатор Cisco 1921-ADSL2/K9 відповідає даним вимогам та має наступні характеристики:

- Кількість портів 2
- Загальна кількість слотів розширення 2 (HWIC)
- Безпекові функції: IPsec, SSL, PKI, GRE, AAA
- Стандартної пам'яті 512
- Флеш пам'яті 256



Рисунок 2.12 – Маршрутизатор Cisco 1921-ADSL2/K9

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

Висновки до другого розділу

Даний розділ присвячено проектування корпоративної мережі головного офісу та філіалу, в результаті чого було спроектовано відповідні схеми мережі, таблиці адресації пристроїв та визначена архітектура мереж. Крім того, в процесі вибору обладнання були здобуті наступні навички:

- Ознайомлення з асортиментом комутаторів та маршрутизаторів Cisco, які б ефективно та економічно доцільно могли б бути використані у проєкті.
- Вибору та установки програмного забезпечення з використанням сервісів та документації Cisco.
- Вивчення особливостей різних версій Cisco IOS та визначення оптимальної для налаштування VPN з відповідною безпекою.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

РОЗДІЛ 3 НАЛАШТУВАННЯ VPN ТЕХНОЛОГІЙ У СИМУЛЯТОРІ GNS3

3.1 Базове налаштування пристроїв

У цій частині кваліфікаційної роботи буде побудована та налаштована мережа та використана Cisco IOS для налаштування VPN реалізації Site-to-Site та Remote Access.

Крок 1: Підключення мережі, як показано в топології (рис. 2.3).

Крок 2: Налаштування основних параметрів для кожного пристрою (табл. 2.1 та 2.2).

- Налаштування імен хостів;
- Налаштування IP адрес інтерфейсів, згідно таблиць IP-адресації;
- Вимкнення пошуку DNS, встановлення таймерів на консольне з'єднання, тощо;

Крок 3: Налаштування протоколу маршрутизації OSPF на пристроях мережі:

```
router ospf 1
router-id 7.7.7.7
network 10.0.0.0 0.0.255.255 area 2
network 50.0.7.0 0.0.0.255 area 2
default-information originate metric 1 route-map DEFAULT-INFORMATION
```

Крок 4: Налаштування DEFAULT-INFORMATION в залежності в IP SLA.

Створення IP SLA, який буде надсилати ICMP-пакети в мережу Інтернет, в даному випадку на DNS сервер Google.

```
ip sla 1
icmp-echo 8.8.8.8 source-interface Ethernet0/2
frequency 10
ip sla schedule 1 life forever start-time now
```

Прив'язування IP SLA до track:

```
track 1 ip sla 1 reachability
```

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Створення маршруту, замкненого на null інтерфейс. Маршрут буде знаходитися в таблиці маршрутизації до тих пір track 1 знаходить в активному стані.

```
ip route 155.155.155.155 255.255.255.255 Null0 track 1
```

Створення префікс-листа з іменем control_route, який буде перевіряти наявність маршруту 155.155.155.155/32.

```
ip prefix-list control_route seq 10 permit 155.155.155.155/32
```

Налаштування route-map з іменем DEFAULT-INFORMATION, який буде відстежувати стан префікс-листа і буде активна, якщо в таблиці маршрутизації буде маршрут 155.155.155.155/32:

```
route-map DEFAULT-INFORMATION permit 10  
match ip address prefix-list control-route control_route
```

Якщо route-map буде активний, тоді маршрутизатор буде анонсувати маршрут за замовчуванням:

```
default-information originate metric 1 route-map DEFAULT-INFORMATION
```

Крок 5: Налаштування NAT Overload на Edge маршрутизаторах.

```
access-list 7 permit 192.168.0.0 0.0.255.255  
access-list 7 permit 60.0.1.0 0.0.0.255  
access-list 7 permit 20.0.0.0 0.0.255.255
```

```
ip nat inside source list 7 interface Ethernet0/2 overload
```

Крок 6: Налаштування структури NTP на пристроях мережі.

```
EdgeRT1#sh run | sec ntp  
ntp source Ethernet0/2  
ntp access-group peer 1  
ntp access-group serve-only 2  
ntp master 3  
ntp update-calendar  
ntp server 193.106.144.6 prefer
```

Крок 7: Налаштування HSRP на distribution рівні.

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Для початку потрібно створити vlan та відповідні віртуальні SVI інтерфейси. Приклад налаштування SVI інтерфейсу та налаштування HSRP на ньому:

```
interface Vlan2
ip address 192.168.2.50 255.255.255.0
ip helper-address 123.20.20.5
standby 1 ip 192.168.2.1
standby 1 priority 110
standby 1 preempt
```

Крок 8: Налаштування Spanning Tree Protocol за кожен vlan.

```
spanning-tree vlan 2 priority 8192
spanning-tree vlan 3 priority 16384
```

Крок 9: Налаштування резервного копіювання конфігурації за розкладом.

```
CoreSW2#sh run | sec archive
archive
path ftp://@123.20.20.5/$H-$T
write-memory
time-period 360
```

Крок 10: Налаштування DHCP з використанням відповідної ролі на Windows Server 2019.

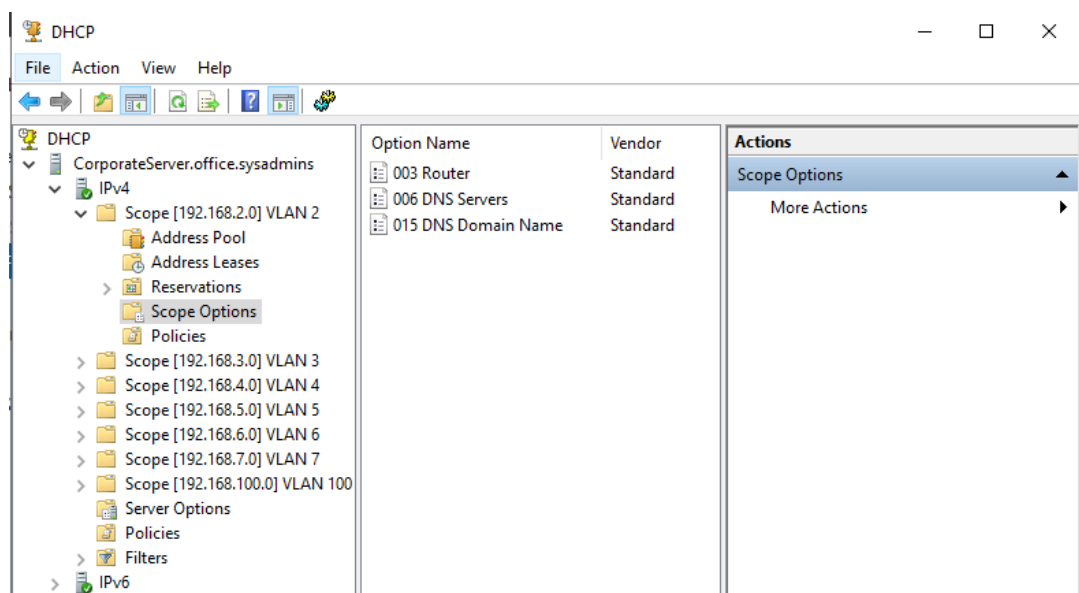


Рисунок 3.1 – Налаштування DHCP ролі

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування DHCP-Relay на Access рівні пристроїв мережі:

```
interface Vlan2
ip address 192.168.2.50 255.255.255.0
ip helper-address 123.20.20.5
standby 1 ip 192.168.2.1
standby 1 priority 110
standby 1 preempt
interface Vlan3
ip address 192.168.3.50 255.255.255.0
ip helper-address 123.20.20.5
standby 2 ip 192.168.3.1
standby 2 preempt
```

3.2 Налаштування Site-to-Site VPN

У даній частині буде налаштовано VPN IPsec між маршрутизаторами головного офісу (EdgeRT1) та філіялу (BrEdgeRT).

3.2.1 Налаштування головного офісу

Налаштування атрибутів першої фази IKEv2:

```
EdgeRT1(config-ikev2-proposal)#do sh run | sec prop
crypto ikev2 proposal SITE_PHASE_1
encryption aes-cbc-256
integrity sha512
group 24
```

Підключення атрибутів до політики IKEv2:

```
crypto ikev2 policy POL_SITE_1
proposal SITE_PHASE_1
```

Визначення використовуваних ключів:

```
EdgeRT1(config-ikev2-keyring-peer)#crypto ikev2 keyring RING_1
EdgeRT1(config-ikev2-keyring)#peer BrEdgeRT
EdgeRT1(config-ikev2-keyring-peer)#address 56.94.24.23
EdgeRT1(config-ikev2-keyring-peer)#pre-shared-key cisco
```

Визначення IKEv2 профілю:

```
crypto ikev2 profile SITE_PROF
match identity remote address 56.94.24.23 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local RING_1
lifetime 36700
```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Налаштування політик IPsec (фаза 2):

```
EdgeRT1(cfg-crypto-trans)#do sh run | sec trans
crypto ipsec transform-set SITE_PEER_BRANCH esp-aes esp-sha-hmac
mode tunnel
```

Створення IPsec профілю:

```
crypto ipsec profile SITE_IPSEC_PROF
set transform-set SITE_PEER_BRANCH
set ikev2-profile SITE_PROF
```

Налаштування тунельного інтерфейсу:

```
interface Tunnel0
ip unnumbered Loopback0
tunnel source Ethernet0/2
tunnel destination 56.94.24.23
tunnel protection ipsec profile SITE_IPSEC_PROF
```

Аналогічно налаштовується філіальний маршрутизатор, відрізняючись тільки публічним адресом віддалено піру.

```
BrEdgeRT1(config)#do sh run | sec cry
no service password-encryption
crypto ikev2 proposal SITE_PHASE_1
  encryption aes-cbc-256
  integrity sha512
  group 24
crypto ikev2 policy POL_SITE_1
  proposal SITE_PHASE_1
crypto ikev2 keyring RING_1
  peer EdgeRT1
    address 165.25.24.12
    pre-shared-key cisco
!
crypto ikev2 profile SITE_PROF
  match identity remote address 165.25.24.12 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local RING_1
  lifetime 36700
crypto ipsec transform-set SITE_PEER_BRANCH esp-aes esp-sha-hmac
mode tunnel
crypto ipsec profile SITE_IPSEC_PROF
  set transform-set SITE_PEER_BRANCH
  set ikev2-profile SITE_PROF
```

Для отримання маршрутів віддалених мереж налаштовується маршрутизація. Для маршрутизація між мережами було обрано протокол BGP, оскільки дає змогу зручно фільтрувати та сумаризувати маршрути.

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Налаштування BGP на маршрутизаторі головного офісу:

```
EdgeRT1#show run | sec bgp
router bgp 10
  bgp log-neighbor-changes
  aggregate-address 192.168.0.0 255.255.0.0 summary-only
  redistribute ospf 1
  neighbor 100.0.1.1 remote-as 20
  neighbor 100.0.1.1 route-map FROM_BRANCH in
```

Налаштування BGP на маршрутизаторі:

```
BrEdgeRT1(config)#do sh run | sec bgp
router bgp 20
  bgp log-neighbor-changes
  aggregate-address 172.20.0.0 255.255.0.0 summary-only
  aggregate-address 70.0.0.0 255.255.0.0 summary-only
  redistribute ospf 1
  neighbor 100.0.1.2 remote-as 10
  neighbor 100.0.1.2 route-map FROM_MAIN_OFFICE in
```

Згідно налаштувань, у BGP відбувається редистрибуція маршрутів з OSPF. BGP дає змогу більш зручно налаштувати фільтрацію маршрутів з використання route-map та сумаризацію.

```
access-list 3 permit 172.20.0.0 0.0.255.255
access-list 3 permit 70.0.0.0 0.0.255.255
```

```
route-map FROM_BRANCH permit 10
match ip address 3
```

Route-map перевіряє чи маршрути, які прийшли від сусіда підпадають під дію ACL, тільки ті маршрути, що підпадають будуть внесені в таблицю маршрутизації.

```
EdgeRT1#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 165.25.24.98 to network 0.0.0.0

    70.0.0.0/16 is subnetted, 1 subnets
B       70.0.0.0 [20/0] via 100.0.1.1, 00:31:58
B      172.20.0.0/16 [20/0] via 100.0.1.1, 00:31:58
B      192.168.0.0/16 [200/0], 00:33:18, Null0
```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

З таблиці маршрутизації видно, що фільтрація route-map працює правильно. Пересвідчимося в працездатності тунелю:

```
EdgeRT1#show crypto ipsec sa
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 165.25.24.12

  protected vrf: (none)
  local ident (addr/mask/prot/port): (165.25.24.12/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (56.94.24.23/255.255.255.255/47/0)
  current_peer 56.94.24.23 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 699, #pkts encrypt: 699, #pkts digest: 699
    #pkts decaps: 689, #pkts decrypt: 689, #pkts verify: 689
    #pkts compress: 0, #pkts decompress: 0
```

Лічильник інкапсуляції та декапсуляції пакетів не дорівнює нулю, що свідчить про роботу IPsec.

З комп'ютера філіалу звертаємось до комп'ютера головного офісу.

```
PC-A> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1  172.20.20.1    0.620 ms  0.463 ms  0.705 ms
 2  30.0.4.1       0.690 ms  0.745 ms  0.629 ms
 3  30.0.1.2       0.895 ms  0.696 ms  0.903 ms
 4  100.0.1.2      1.356 ms  1.118 ms  1.065 ms
 5  10.0.11.1      1.352 ms  1.298 ms  1.552 ms
 6  10.0.2.1      17.783 ms 9.929 ms  9.125 ms
 7  * * *
 8  *192.168.2.2  36.150 ms (ICMP type:3, code:3, Destination port unreachable)

PC-A> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=58 time=20.565 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=58 time=16.685 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=58 time=27.515 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=58 time=23.574 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=58 time=26.572 ms
```

З виводу утиліти tracert видно, що трафік направляється в тунель. Пінг проходить.

3.2.2 Конфігурація PKI-сервера на маршрутизаторі Cisco

Аутентифікація по відкритому ключу не вважається безпечною, надійніший метод – аутентифікація по сертифікатам. Переведемо тунель на аутентифікацію по сертифікатам, для цього потрібно розгорнути CA сервер.

Створюється пара ключів з використанням алгоритму RSA довжиною 2048 біт:

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

CS(config)#crypto key generate rsa label CS-KEYS modulus 2048 exportable
The name for the keys will be: CS-KEYS

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 4 seconds)

```

Створюється trust point та підключаємо створену ключову пару до нього:

```

CS(config)#crypto pki trustpoint MY-CS
CS(ca-trustpoint)#rsakeypair CS-KEYS

```

Вмикається http сервер (необхідно для того, щоб клієнти могли подавати заявки на сертифікати):

```

CS(config)#ip http server

```

Створення та перехід в налаштування сервера:

```

CS(config)#crypto pki server MY-CS
CS(cs-server)#

```

Поля кореневого сертифікату:

```

CS(cs-server)#issuer-name CN=MY-CS,OU=VPN,O=Cisco,C=US

```

Місце де зберігатимуться сертифікати, а також CRL файл на СА:

```

CS(cs-server)#database url unix:/cerbase
% Server database url was changed. You need to move the
% existing database to the new location.

```

Шлях по якому СА сервер буде дублювати CRL файл:

```

database url crl publish ftp://178.20.20.1/ username dmytro password 7 05080F1C2243

```

Місце, де клієнти будуть перевіряти сертифікати на стан «відкликаний/ не відкликаний»:

```

CS(cs-server)#cdp-url http://178.20.20.1/my-cs/my-cs.crl

```

Налаштування частини інформації про сертифікати, яку буде зберігати сервер, в даному випадку повну:

```

CS(cs-server)#database level complete

```

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Встановлення алгоритмів хешування, життя сертифікату в днях, життя кореневого сертифіката та час життя CRL файлу:

```
CS(cs-server)#hash sha256
CS(cs-server)#lifetime certificate 730
CS(cs-server)#lifetime ca-certificate 1000
CS(cs-server)#lifetime crl 336
```

Відмінна автоматичного погодження запитів, для підвищення безпеки мережі та вмикання серверу:

```
CS(cs-server)#no grant auto
CS(cs-server)#gra
CS(cs-server)#no sh
% Ambiguous command: "no sh"
CS(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Re-enter password:
```

Оскільки вивантажувати файл CS-сервер буде по протоколу FTP, потрібно налаштувати клієнта, для цього скористаємося програмою Home Ftp Server. В даному випадку FTP сервер буде завантажувати файл у папку my-cs на веб сервері:

Home Ftp Server						
New account	Username	Password	Home directory	Address	Last time	
	Anonymous			-	-	
Modify account	CA	disco	C:\WebServers\home\112.24.24.3\www\my-cs	165.25.24.12:11022	16.06.2022 22:07	

Рисунок 3.2 – Створення користувача на FTP сервері

Веб-сервером слугуватиме програма Denwer. Шлях до CRL файлу буде наступний:

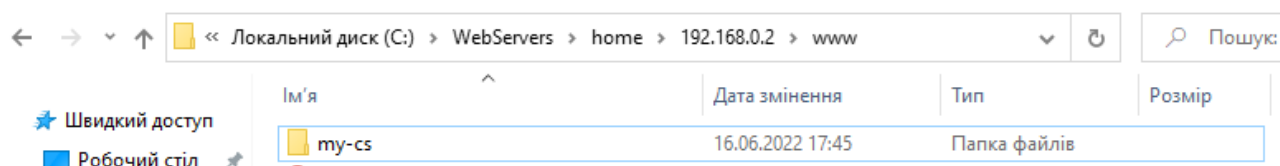


Рисунок 3.3 – Шлях до CRL файлу на сервері

3.2.3 Налаштування тунелю на аутентифікація по сертифікатам

Генеруємо ключову пару за допомогою алгоритму RSA:

```
EdgeRT1(config)#generate rsa label VPN-KEYS modulus 2048 exportable
The name for the keys will be: VPN-KEYS

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 2 seconds)
```

Створюємо trustpoint:

```
EdgeRT1(config)#crypto pki trustpoint VPN-PKI
```

Вказуємо URL адресу нашого CA (PKI) сервера:

```
EdgeRT1(ca-trustpoint)#enrollment url http://60.0.1.1
```

Те що буде написано в полях сертифікату:

```
EdgeRT1(ca-trustpoint)#subject-name CN=EdgeRT1,OU=VPN,O=Cisco,C=US
```

Для початку відміняємо перевірку на факт відкликання сертифікату:

```
EdgeRT1(ca-trustpoint)#revocation-check none
```

Прив'язка ключової пари до trustpoint:

```
EdgeRT1(ca-trustpoint)#rsa-keypair VPN-KEYS
```

Завантаження CA сертифікату (відкритий ключ CA сервера):

```
EdgeRT1(ca-trustpoint)#crypto pki authenticate VPN-PKI
EdgeRT1(ca-trustpoint)#crypto pki authenticate VPN-PKI
Certificate has the following attributes:
  Fingerprint MD5: F2E7BEA9 DEABC27F 85FF5769 F57FD521
  Fingerprint SHA1: 7EBFBD3A B3BF3849 D909EA95 07CE2C0A B04C9879

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Створюємо запит на отримання свого сертифікату від CA (відкритий ключ маршрутизатора):

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

EdgeRT1(config)#crypto pki enroll VPN-PKI
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: CN=EdgeRT1,OU=VPN,O=Cisco,C=US
% The subject name in the certificate will include: EdgeRT1
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose VPN-PKI' command will show the fingerprint.

EdgeRT1(config)#
Jun 16 15:38:13.204: CRYPTO_PKI: Certificate Request Fingerprint MD5: 7CAD734C C4391D54 5045737F C857A885
Jun 16 15:38:13.204: CRYPTO_PKI: Certificate Request Fingerprint SHA1: B7954DD6 FD28E31F 3D8595D4 639682E5
403D914B

```

Виведемо список сертифікатів на СА сервері:

```

CS(cs-server)#do show crypto pki server MY-CS requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
RA certificate requests:
ReqID  State      Fingerprint                               SubjectName
-----
Router certificates requests:
ReqID  State      Fingerprint                               SubjectName
-----
1      pending    7CAD734CC4391D545045737FC857A885 hostname=EdgeRT1,cn=EdgeRT1,ou=VPN,o=Cisco,c=US

```

Підтвердження запиту на CS сервері:

```
CS#crypto pki server MY-CS grant 1
```

Підтвердження отримання сертифікату:

```

EdgeRT1(ca-trustpoint)#
Jun 16 18:47:15: %PKI-6-CERTRET: Certificate received from Certificate Authority
EdgeRT1(ca-trustpoint)#show run

```

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

Отриманні сертифікати:

```

crypto pki certificate chain VPN-PKI
certificate 02
3082035A 30820242 A0030201 02020102 300D0609 2A864886 F70D0101 0B050030
3B310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310C
300A0603 55040B13 0356504E 310E300C 06035504 0313054D 592D4353 301E170D
32323036 31363135 34323435 5A170D32 34303631 35313534 3234355A 3055310B
30090603 55040613 02555331 0E300C06 0355040A 13054369 73636F31 0C300A06
0355040B 13035650 4E311030 0E060355 04031307 45646765 52543131 16301406
092A8648 86F70D01 09021607 45646765 52543130 82012230 0D06092A 864886F7
0D010101 05000382 010F0030 82010A02 82010100 B583F55F A8BEC8B4 CFFE4AA2
7195332D 6CCCC14A 441BE160 2E1502AB 80B073C1 00671A92 887D29CA 6D64AA3C
1ABF255C A846CE83 D70737F9 61B9B2F8 B898F12B 7ACAA12D 0959D6F5 9EFC59DE
B1E59C14 6379A06D E322B9D1 858E55C4 28B17831 D5CE8F46 715B08AE 70BC0153
1F9B3FE2 FE2F7564 17FC30C2 D3CA5801 BA62955D C1C27089 1AFE501B 7BB6AEED
B1EB7DC8 CED5C9B1 9561F440 3B05F139 1F16E7C2 24FA7843 63A66C51 A91AA56B
4628CFC3 2F141436 D5EA5D63 828F4CB2 8A166CD3 EB46A64B 71585248 96B73CC6
6685668C 80E99FE7 71A659F1 95547FCA 182834D2 51B7D99B C5C7BDD5 AF4B69E9
D3DBB30E 29E6E0A1 6F592CCA 458AA072 CD13065B 02030100 01A34F30 4D300B06
03551D0F 04040302 05A0301F 0603551D 23041830 1680145A C14AD7DF C743EEFC
5E5A4FA6 B377B597 92E77930 1D060355 1D0E0416 04148DF9 2B3C2378 09B4C75E
8291CB5B F8846DD5 40A5300D 06092A86 4886F70D 01010B05 00038201 0100BEC7
918C68DC 7CE36ABB 264CA3A4 E5A98632 4A911154 80702B3C 2F566506 3A796492
65F43880 416B683D 4B6CD5A1 2711E6F3 EBA0B64B 3786BE18 211E7326 49DE8DDA
FFEBA60B 1EF52350 5AF1661B B7B35B63 70D821D3 B6447774 709032C3 A89AD14B
9A1DD70E C584D346 B0BFD891 6E17CD38 2BBE7D8D D77C3886 6F9C5498 F0016545
9C451C1A 6C147D4C B4382799 7119A81C F2DC79E6 D4D85424 204D0A87 82D0D98D
5D55A63F B23DBA7C 7D8C3073 EAB1D140 007F034C E02BDCF4 690C0BA0 3F090F17
12683181 8F3AAD9E 3B7B96EF BA89454B 0E6FA5A8 3A2FC565 08D5B210 6E7802A2
B1C094FA 169E4E11 133ECE08 A8F3B11A 1865A5A7 0E80DB25 0AC63E41 BD5C
quit
certificate ca 01
3082035A 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
3B310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310C
300A0603 55040B13 0356504E 310E300C 06035504 0313054D 592D4353 301E170D
32323036 31363135 30323033 5A170D32 35303331 32313530 3230335A 303B310B
30090603 55040613 02555331 0E300C06 0355040A 13054369 73636F31 0C300A06
0355040B 13035650 4E310E30 0C060355 04031305 4D592D43 53308201 22300D06
092A8648 86F70D01 01010500 0382010F 00308201 0A028201 0100E6A1 20B7A0D7
5C823685 57603C57 549FD8FD 68F92EE4 E90CB8DF 99B11026 0FD7B650 93BF86F6
7187DB08 8E4F2844 FB561E8D 9D2792B6 D8D4F249 2C2AA8D0 50B11A7C A132D1C7
5F2D59BA 565786E4 F85886DA 709F8DAC 13F4FD6A 0E75CC1F 5C8AC7BB 6506609E
D32E9D0A 52D96F09 4EC26542 774E68EF E873FB05 9B5F9EA5 519607CA 049D23E7
E09ED7C5 B9A42E01 446C0A05 6551EB17 64D0BE43 068CA062 0F73877D 89F5BBE2
ED001CC5 7863B667 3D65AAE4 52D60BE1 5AC3ABC8 28F8128E C2390D1C 998B1663
F96A76A1 5E566D9A 91E3DBB1 112F0F14 D61A6280 97B30016 410AE500 AB403C38
3F87F7B2 80BF6387 DECEC7F3 053C9E25 ACD327E4 ACCEB83D C3F10203 010001A3
63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404
03020186 301F0603 551D2304 18301680 145AC14A D7DFC743 EEFC5E5A 4FA6B377
B59792E7 79301D06 03551D0E 04160414 5AC14AD7 DFC743EE FC5E5A4F A6B377B5
9792E779 300D0609 2A864886 F70D0101 0B050003 82010100 17F1D2E2 F866CCCF
9F5D7353 195C597C 5766D0F9 512A40E3 3FD061D4 9768148B 627C050F 1435C363
71E3B637 42DE52D9 6253D5BE BA254446 86B77673 D7AF5E5F 0916262C 4B31E788
A8CB12AE 9BB78455 3B60C0B0 427D3E24 F215071B 9EC53478 8DB6BDAB 0D2BFA81

```

Аналогічні дії виконано на маршрутизаторі філіалу.

Переведення налаштувань VPN тунелю аутентифікації по сертифікатам на маршрутизаторі, для цього було додано карту сертифікатів та вказано критерії по яких вона має спрацьовувати:

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

```
EdgeRT1(config)#crypto pki certificate map IDENTITY_MAP 10
EdgeRT1(ca-certificate-map)#subject-name co ou = VPN
```

В IKEv2 профілі було змінено параметри аутентифікації:

```
EdgeRT1(ca-trustpoint)#crypto ikev2 profile SITE_PROF
EdgeRT1(config-ikev2-profile)#no authentication remote pre-share
EdgeRT1(config-ikev2-profile)#no authentication local pre-share
EdgeRT1(config-ikev2-profile)#no key
EdgeRT1(config-ikev2-profile)#no keyring local RING_1
```

Налаштований профіль:

```
EdgeRT1(config-ikev2-profile)#do sh run | sec crypto ikev2 profile
crypto ikev2 profile SITE_PROF
match certificate IDENTITY_MAP
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint VPN-PKI
```

Аналогічні зміни в налаштування було встановлено на філіальному маршрутизаторі. Після чого було розірвано сесію за допомогою команди clear crypto session для ініціювання нового тунелю.

Перевірка на працездатність утилітою ping:

```
PC-A> ping 192.168.2.2
192.168.2.2 icmp_seq=1 timeout
192.168.2.2 icmp_seq=2 timeout
192.168.2.2 icmp_seq=3 timeout
84 bytes from 192.168.2.2 icmp_seq=4 ttl=58 time=15.747 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=58 time=16.740 ms
```

Ввімкнути перевірку на факт відклику сертифікату на обох маршрутизаторах:

```
BrEdgeRT1(ca-trustpoint)#revocation-check crl
```

Відкликання сертифікату під номером 3 (сертифікат філіального маршрутизатора):

```
CS#crypto pki server MY-CS revoke 3
Writing MY-CS.crl !
```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Перевірка CRL файлу на сервері:

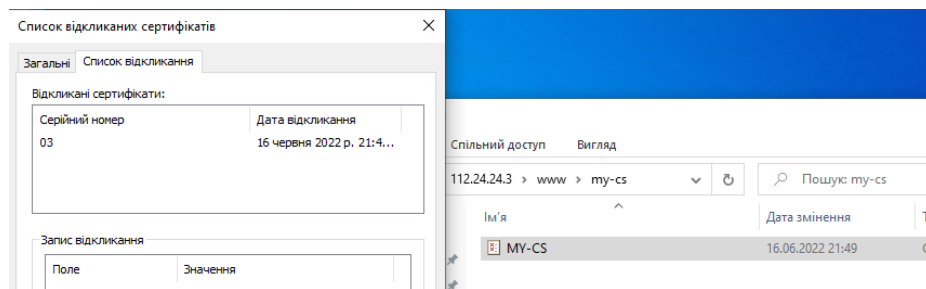


Рисунок 3.4 – Завантажений CRL файл на сервері

Розривання тунелю та ініціювання нового з'єднання:

```
Jun 16 22:06:06: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 03) is revoked
Jun 16 22:06:06: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 03) is revoked
EdgeRT1(config)#
```

Аутентифікація не можлива, оскільки сертифікат під номером 3 був відкликаний.

Відновлення відкликаного сертифікату та публікація нового CRL файлу на сервер повторно:

```
CS#crypto pki server MY-CS unrevoke 0x3
Writing MY-CS.crl !
```

Розривання тунелю та ініціювання нового з'єднання:

```
BrEdgeRT1#clear crypto sess
```

Успішне встановлення тунелю:

```
*Jun 16 19:08:06.898: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
BrEdgeRT1(config)#ebd
*Jun 16 19:08:10.453: %BGP-5-ADJCHANGE: neighbor 100.0.1.2 Up
```

Перевірка працездатності тунелю. Використовуючи утиліту trace подивимось через які вузли проходить пакет.

```
PC-A> trace 192.168.2.2
Trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1  172.20.20.1    0.697 ms  0.463 ms  0.583 ms
 2  30.0.4.1       0.827 ms  0.587 ms  0.691 ms
 3  30.0.1.2       1.030 ms  0.782 ms  0.824 ms
 4  100.0.1.2      1.480 ms  1.345 ms  1.555 ms
 5  10.0.10.1      1.434 ms  1.654 ms  1.737 ms
 6  10.0.1.1      10.136 ms 9.281 ms  9.525 ms
 7  *192.168.2.2  21.007 ms (ICMP type:3, code:3, Destination port unreachable)
```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Перевірка за допомогою утиліти ping:

```
PC-A> ping 192.168.2.2
192.168.2.2 icmp_seq=1 timeout
192.168.2.2 icmp_seq=2 timeout
84 bytes from 192.168.2.2 icmp_seq=3 ttl=58 time=17.744 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=58 time=16.627 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=58 time=17.066 ms
```

Перевірка працездатності пройшла успішно.

3.3 Налаштування Remote Access VPN

У даній частині буде налаштовано Remote Access з використанням технології Flex VPN з налаштуванням індивідуальної аутентифікації і авторизації на Radius методом EAP.

У великих мережах слідкувати хто, і до чого має доступ ускладняється великою кількістю пристроїв, на допомогу приходить зовнішній AAA-сервер. AAA-сервер – це пристрій, що дозволяє контролювати доступ до ресурсів мережі і записувати дії користувачів в єдиному місці. Тепер всі облікові записи користувачів та політики для кожної групи користувачів будуть зберігатися на AAA-сервері. Зовнішньо AAA сервера працюють на трьох основних протоколах: Radius, Tacsacs+, Diameter. Для реалізації наших завдань для аутентифікації та авторизації користувачі на AAA сервері буде використовуватися протокол Radius. Radius входить в склад ролі Network Police Server (NPS). NPS – це програмне забезпечення, яке робить з простого сервера AAA сервер.

В моделі з AAA сервером існує суплікант, аутентифікатор та сервер аутентифікації. Суплікантом виступає VPN клієнт, аутентифікатором виступає граничний маршрутизатор підприємства, AAA сервером Windows Server. Суплікант надсилає аутентифікатору дані для аутентифікації, в залежності від типу це можуть бути сертифікат чи логін та пароль або і те і інше. Аутентифікатор виступає як посередник, він передає дані AAA серверу за допомогою запиту Radius: Access-Request. Зовнішній AAA сервер перевіряє аутентифікаційні дані, у випадку якщо дані коректні, тоді AAA сервер висилає AAA атрибути в повідомленні Radius: Access-Accept. Отримавши підтвердження

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

від AAA сервера, аутентифікатор надішле відповідні атрибути супліканту. У випадку, якщо аутентифікація провалиться, AAA сервер надішле повідомлення типу Radius: Access-Reject.

3.3.1 Налаштування AAA серверу

Встановлення ролі NPS:

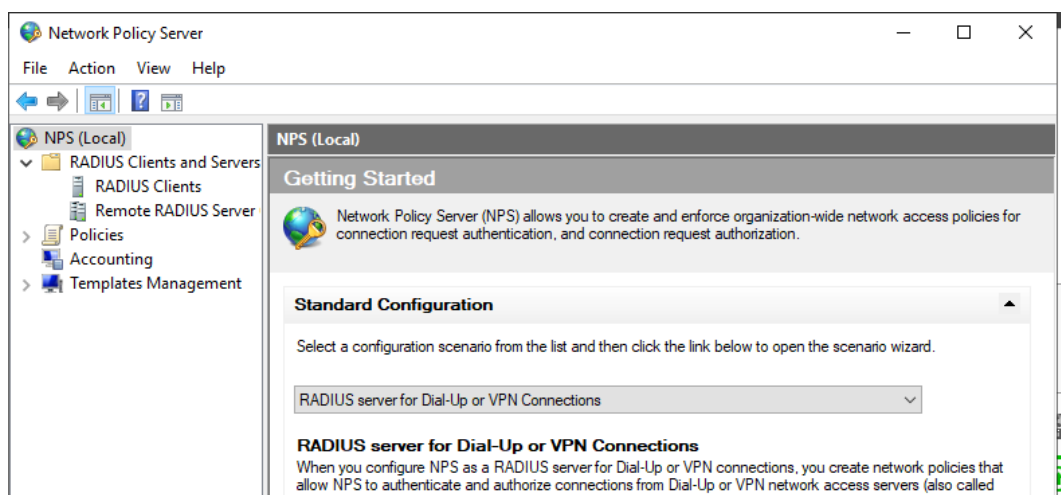


Рисунок 3.5 – Встановлення ролі NPS

Додавання Radius-клієнта:

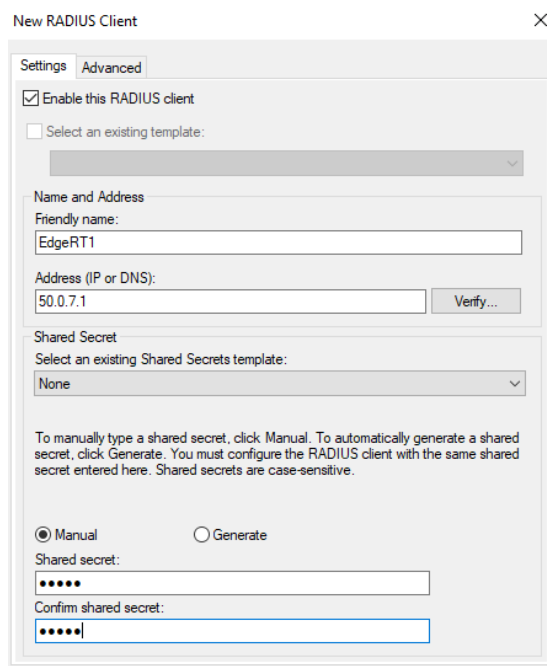


Рисунок 3.6 – Створення Radius клієнта

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Створення клієнтів яким буде дозволено доступ в Active Directory:

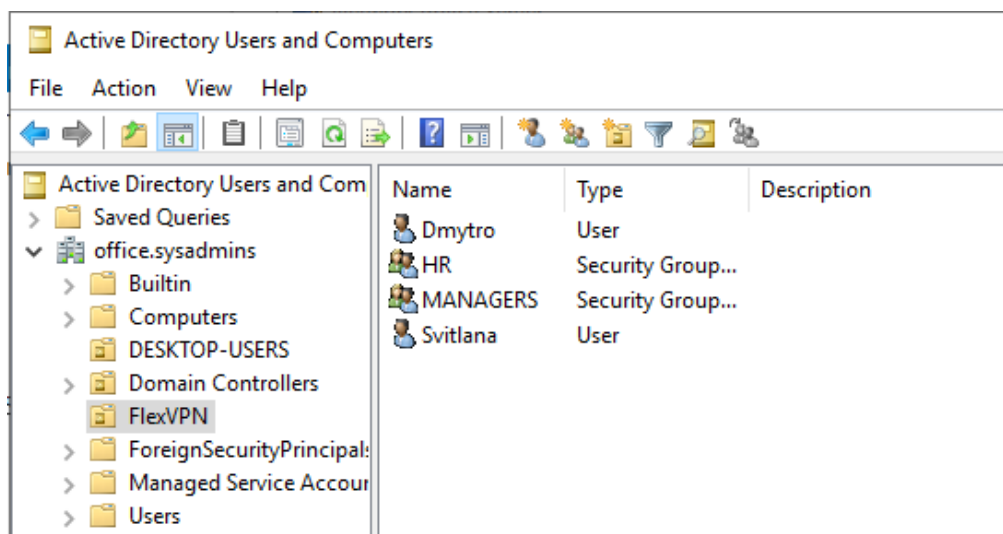


Рисунок 3.7 – Створення клієнтів та груп

В даному випадку для тестування було створено два користувачі: Dmytro, який є членом групи MANAGERS та Svitlana, яка належить до групи HR.

Далі відбувається створення політик на основі, яких будуть видаватися відповідні атрибути. Дана політика спрацюватиме, якщо буде підключатися користувач з групи MANAGERS:

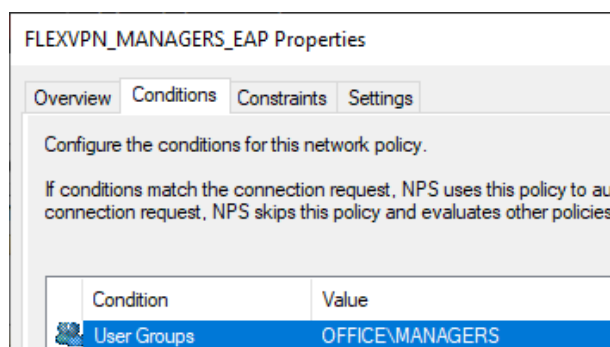


Рисунок 3.8 – Умова спрацювання політики

Встановлення AAA атрибути, які будуть надсилатися аутентифікатору, в даному випадку адреса буде братися з пулу з ім'ям FLEX_POOL_MANAGERS, а маршрути з ACL на ім'я SPLIT-MANAGERS. ACL та pool з відповідними іменами мають бути попередньо створені на маршрутизаторі. Отримавши відповідні атрибути, маршрутизатор відправить їх клієнту:

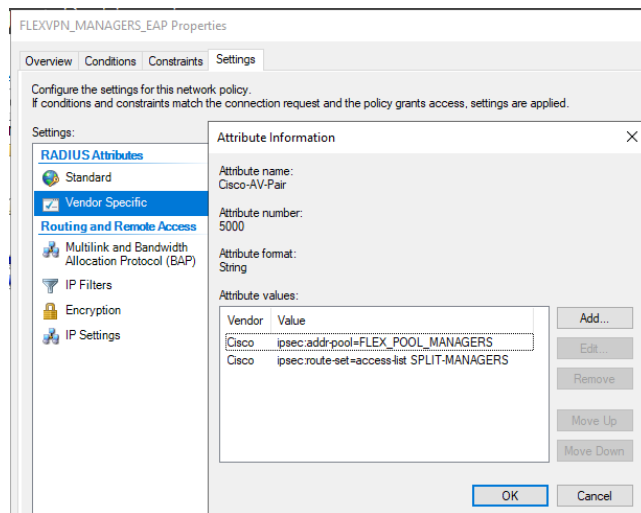


Рисунок 3.9 – Атрибути, які видаються клієнту

Аналогічно налаштовуємо політику для HR користувачів:

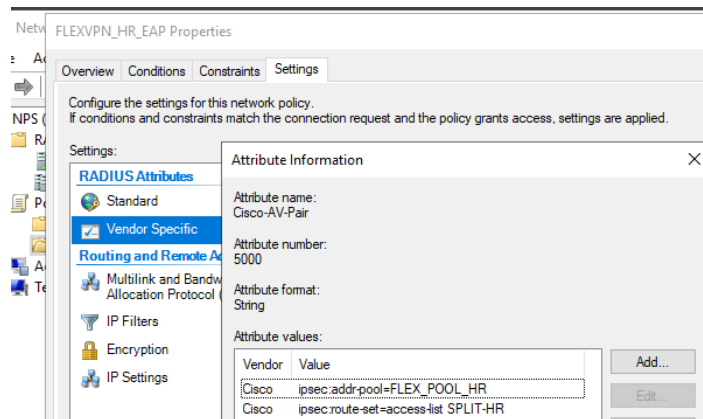


Рисунок 3.10 – Умова спрацювання політики

Необхідно підвищити пріоритетність політик:

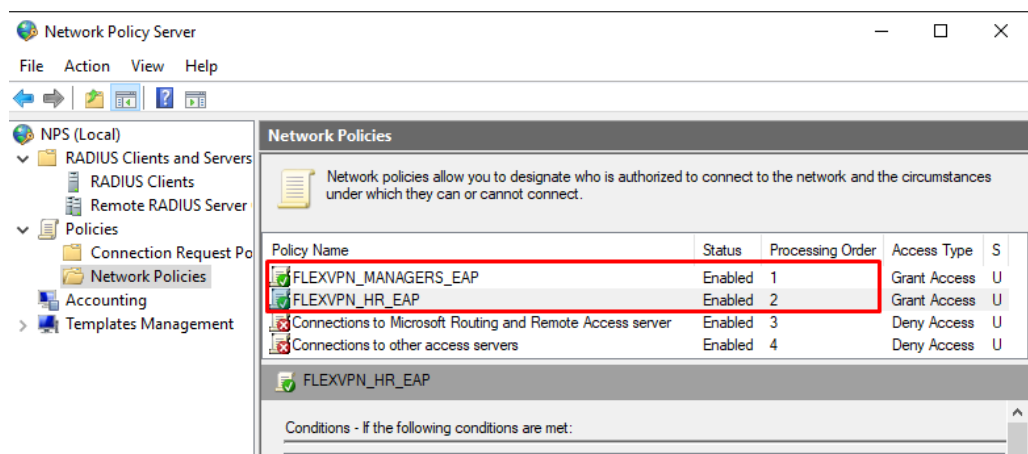


Рисунок 3.11 – Створені політики

3.3.2 Налаштування аутентифікатора

Створення пари RSA ключів та налаштування trustpoint для запиту на сертифікат:

```
EdgeRT1(config)#crypto key generate rsa label FLEXVPN-KEYS-CS2 modulus 2048
The name for the keys will be: FLEXVPN-KEYS-CS2

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

EdgeRT1(config)#crypto pki trustpoint FlexVPN-TP-CS2
EdgeRT1(ca-trustpoint)# enrollment url http://60.0.1.1:80
EdgeRT1(ca-trustpoint)# subject-name CN=165.25.24.12
EdgeRT1(ca-trustpoint)# crl cache none
EdgeRT1(ca-trustpoint)# revocation-check none
EdgeRT1(ca-trustpoint)# rsakeypair FLEXVPN-KEYS-CS2
```

Створення запитів на сертифікати:

```
EdgeRT1(config)#crypto pki authenticate FlexVPN-TP-CS2
```

```
EdgeRT1(config)#crypto pki enroll FlexVPN-TP-CS2
```

Додавання атрибутів, які будуть передаватися на VPN клієнти:

```
EdgeRT1(config)#ip local pool FLEX_POOL_MANAGERS 77.0.12.0 77.0.12.254
EdgeRT1(config)#ip local pool FLEX_POOL_HR 77.0.13.0 77.0.13.254
EdgeRT1(config)#ip access-list standard SPLIT-HR
EdgeRT1(config-std-nacl)# permit 123.20.20.5
EdgeRT1(config-std-nacl)#ip access-list standard SPLIT-MANAGERS
EdgeRT1(config-std-nacl)# permit 123.20.20.5
EdgeRT1(config-std-nacl)# permit 192.168.2.0 0.0.0.255
```

Налаштування першої фази:

```
EdgeRT1(config)#crypto ikev2 proposal PROP1_FOR_FLEX
IKEv2 proposal MUST either have a set of an encryption algorithm other than aes-gcm, an integrity algorithm
and a DH group configured or
  encryption algorithm aes-gcm, a prf algorithm and a DH group configured
EdgeRT1(config-ikev2-proposal)# encryption aes-cbc-256
EdgeRT1(config-ikev2-proposal)# integrity sha256
EdgeRT1(config-ikev2-proposal)# group 15
EdgeRT1(config-ikev2-proposal)#crypto ikev2 policy IKEv2_POL_FOR_FLEX
IKEv2 policy MUST have atleast one complete proposal attached
EdgeRT1(config-ikev2-policy)# proposal PROP1_FOR_FLEX
```

Налаштування другої фази:

```
EdgeRT1(config)#crypto ipsec transform-set TSET_FOR_FLEX esp-gcm 192
EdgeRT1(cfg-crypto-trans)# mode tunnel
```

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

Створення IKEv2 профілю:

```
EdgeRT1(config)#crypto ikev2 profile FLEX_IKEv2_PROF
```

Для встановлення VPN з'єднання, маршрутизатор надсилає клієнту свій власний сертифікат.

```
EdgeRT1(config-ikev2-profile)#authentication local rsa-sig
```

Встановлюємо метод аутентифікації клієнти EAP:

```
EdgeRT1(config-ikev2-profile)#authentication remote eap query-identity
```

Дана команда вказує, що AAA атрибути будуть передаватися в процесі аутентифікації:

```
EdgeRT1(config-ikev2-profile)#aaa authorization user eap cached
```

Умовою спрацювання IKEv2 профілю буде будь-який identity:

```
EdgeRT1(config-ikev2-profile)#match identity remote address 0.0.0.0
```

Для аутентифікації (в даному випадку і авторизації) буде використовуватися метод, вказаний в листі з іменем A_EAP_AUTHEN_LOCAL_LIST:

```
EdgeRT1(config-ikev2-profile)#aaa authentication eap A_EAP_AUTHEN_LOCAL_LIST
```

Прив'язка trustpoint:

```
EdgeRT1(config-ikev2-profile)#pki trustpoint FlexVPN-TP-CS2
```

Підключення до профілю VTI інтерфейс з номером 100. VTI інтерфейс буде створений пізніше:

```
EdgeRT1(config-ikev2-profile)#virtual-template 100
```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

Налаштований IKEv2 профіль:

```
crypto ikev2 profile FLEX_IKEv2_PROF
match identity remote address 0.0.0.0
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-CS2
aaa authentication eap A_EAP_AUTHEN_LOCAL_LIST
aaa authorization user eap cached
virtual-template 100
```

Створення IPsec профілю:

```
EdgeRT1(config)#crypto ipsec profile FLEX_IPSEC_PROF
EdgeRT1(ipsec-profile)# set transform-set TSET_FOR_FLEX
EdgeRT1(ipsec-profile)# set ikev2-profile FLEX_IKEv2_PROF
```

Створення VTI:

```
EdgeRT1(config)#interface Virtual-Template100 type tunnel
EdgeRT1(config-if)# ip unnumbered Ethernet0/2
EdgeRT1(config-if)# ip mtu 1400
EdgeRT1(config-if)# tunnel mode ipsec ipv4
EdgeRT1(config-if)# tunnel protection ipsec profile FLEX_IPSEC_PROF
```

Активуємо та налаштовуємо AAA New Model:

```
aaa new-model
aaa authentication login A_EAP_AUTHEN_LOCAL_LIST group RADIUS-GROUP
```

Вказуємо адресу Radius сервера:

```
EdgeRT1(config)#radius server FLEX-VPN-RAD
EdgeRT1(config-radius-server)#$v4 123.20.20.5 auth-port 1645 acct-port 1646
EdgeRT1(config-radius-server)# key cisco
```

Інтерфейс з під якого будуть відправлятися запити на Radius:

```
EdgeRT1(config)#ip radius source-interface lo0
```

Додаємо створений сервер до Radius групи:

```
EdgeRT1(config)#aaa group server radius RADIUS-GROUP
EdgeRT1(config-sg-radius)#server name FLEX-VPN-RAD
```

Radius група вже підключена до AAA моделі:

```
aaa new-model
aaa authentication login A_EAP_AUTHEN_LOCAL_LIST group RADIUS-GROUP
```

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

3.3.3 Налаштування VPN клієнта

На комп'ютері користувача встановлюється VPN клієнт, в даному випадку було встановлено Cisco AnyConnect Secure Mobility Client. Крім цього ще встановлена програма VPN Profile Editor для редагування профілів на основі, яких здійснюється підключення.

Налаштування профілю підключення:

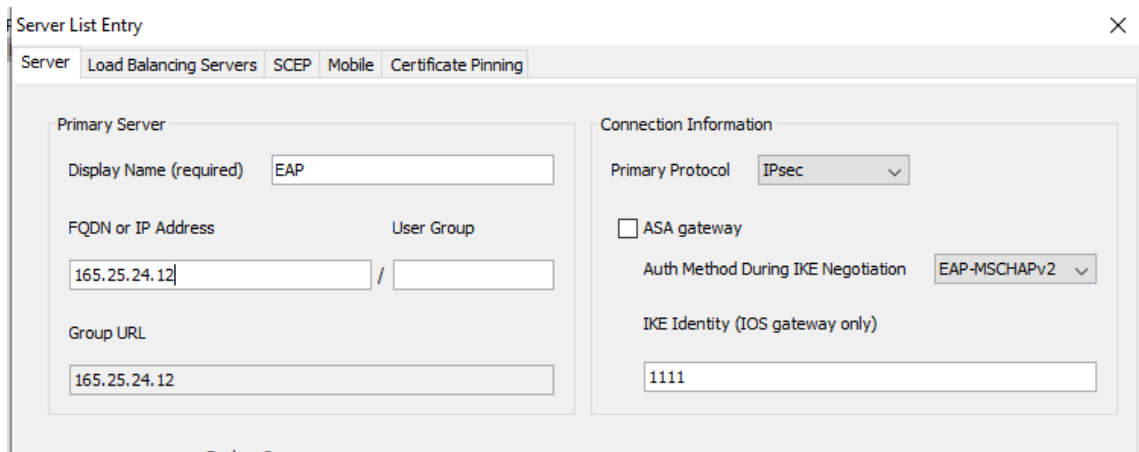


Рисунок 3.11 – Створення профілю підключення

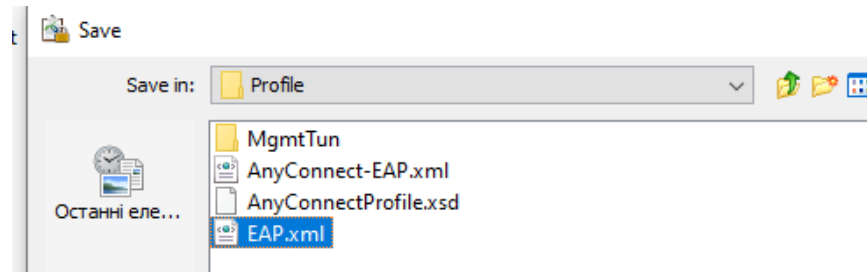


Рисунок 3.12 – Збереження профілю

Підключення VPN клієнта під користувачем Dmytro:

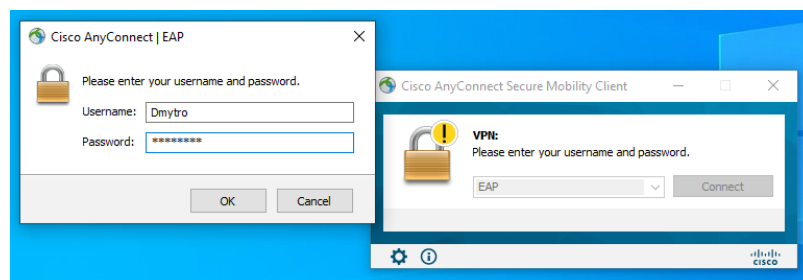


Рисунок 3.13 – Підключення користувача Dmytro

Після підключення перевіряємо, яка адреса була назначена клієнту:

```
C:\Users\Student>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2547:329a:7470:8edd%3
    Link-local IPv6 Address . . . . . : fe80::2957:a68c:577e:ac33%3
    IPv4 Address. . . . . : 77.0.12.1
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : ::
```

Отримані маршрути:

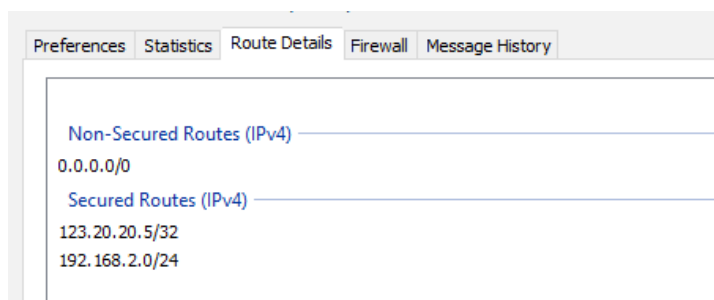


Рисунок 3.14 – Отримані маршрути для користувача Dmytro

Перевірка доступу до ресурсу за допомогою утиліти tracert:

```
C:\Users\Student>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  165.25.24.12
  2     1 ms     1 ms     1 ms  10.0.10.1
  3     6 ms     9 ms     9 ms  10.0.1.1
  4    27 ms    19 ms    19 ms  192.168.2.2
```

Перевірка маршрутів в таблиці маршрутизації:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.2	281
	77.0.0.0	255.0.0.0	On-link	77.0.12.2	257
	77.0.12.2	255.255.255.255	On-link	77.0.12.2	257
	77.255.255.255	255.255.255.255	On-link	77.0.12.2	257
	123.20.20.5	255.255.255.255	77.0.0.1	77.0.12.2	2
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
	165.25.24.12	255.255.255.255	192.168.0.1	192.168.0.2	26
	192.168.0.0	255.255.255.0	On-link	192.168.0.2	281
	192.168.0.2	255.255.255.255	On-link	192.168.0.2	281
	192.168.0.255	255.255.255.255	On-link	192.168.0.2	281
	192.168.2.0	255.255.255.0	77.0.0.1	77.0.12.2	2
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	331

Підключення під іншим користувачем:

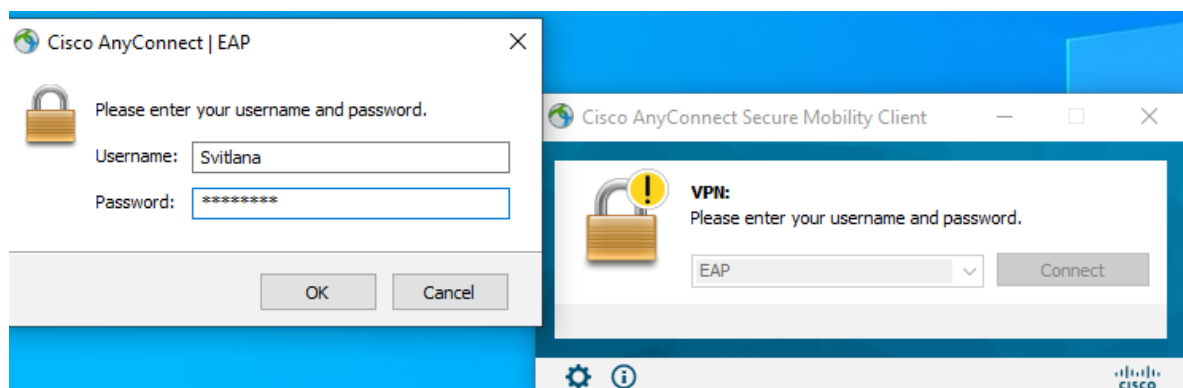


Рисунок 3.15 – Підключення користувачки Svitlana

Адреса назначена на інтерфейс:

```

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::2957:a68c:577e:ac33%3
Link-local IPv6 Address . . . . . : fe80::bd26:62a1:3dd0:39fe%3
IPv4 Address. . . . . : 77.0.13.1
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : ::
    
```

Отримані маршрути:

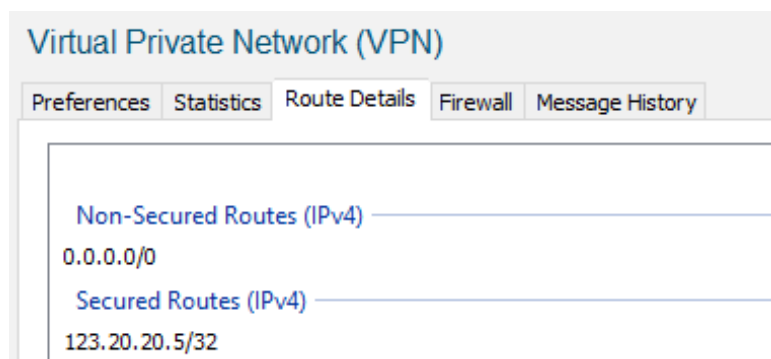


Рисунок 3.16 – Отримані маршрути для користувачки Svitlana

Отримані маршрути в таблиці маршрутизації користувача:

Active Routes:					
Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.2	281
77.0.0.0	255.0.0.0	255.0.0.0	On-link	77.0.13.1	257
77.0.13.1	255.255.255.255	255.255.255.255	On-link	77.0.13.1	257
77.255.255.255	255.255.255.255	255.255.255.255	On-link	77.0.13.1	257
123.20.20.5	255.255.255.255	255.255.255.255	77.0.0.1	77.0.13.1	2
127.0.0.0	255.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331

Перевірка через які вузли мережі проходить трафік:

```
C:\Users\Student>tracert 123.20.20.5

Tracing route to 123.20.20.5 over a maximum of 30 hops

  1      4 ms      2 ms      1 ms    165.25.24.12
  2      1 ms      1 ms      1 ms    10.0.10.1
  3      6 ms      9 ms      9 ms    10.0.14.1
  4     20 ms     19 ms     20 ms    123.20.20.5
```

Перевірка доступності пристрою:

```
C:\Users\Student>ping 123.20.20.5

Pinging 123.20.20.5 with 32 bytes of data:
Reply from 123.20.20.5: bytes=32 time=27ms TTL=125
Reply from 123.20.20.5: bytes=32 time=14ms TTL=125
Reply from 123.20.20.5: bytes=32 time=17ms TTL=125
Reply from 123.20.20.5: bytes=32 time=15ms TTL=125
```

3.4 Висновки до розділу 3

Даний розділ присвячено налаштуванню:

- технології Site-to-Site VPN з використанням технології тунелювання IPSec;
- технології Remote Access VPN з використанням технології тунелювання IPSec;

Всі налаштування виконувались в симуляторі GNS3 за схемою описаною у попередньому розділі. В процесі роботи над розділом були здобуті наступні навички:

- налаштування базових технологій для роботи мережі, таких як протокол маршрутизації OSPF, NAT, NTP, DHCP, STP, HSRP та збереження конфігурацій пристроїв на сервер за розкладом;
- налаштування маршрутизаторів для створення захищених тунелів при реалізації технології Site-to-Site VPN;

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

- налаштування VPN серверу та клієнтських маршрутизаторів для створення захищених тунелів при реалізації технології Remote Access VPN;
- освоєння програмного забезпечення Cisco AnyConnect Secure Mobility Client з використання VPN Profile Editor.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ВИСНОВКИ

У сучасному світі, де різні інформаційні технології тісно інтегровані не тільки у великі корпоративні мережі, а й у побут звичайних користувачів, реалізація VPN з обов'язковим використанням протоколів безпеки стає критично необхідною.

В даній кваліфікаційній роботі проаналізовано засоби забезпечення безпеки мережевого трафіку, пояснені призначення та особливості VPN, необхідність тунелювання, шифрування, аутентифікації та забезпечення цілісності даних.

Безпеку передачі даних може бути досягнуто різними методами, в залежності критичності даних та технічних можливостей самих мереж. Найкращим є рішення, що водночас забезпечує тунелювання, шифрування, аутентифікацію та цілісність даних. Основою створення захищених VPN є застосування протоколу безпеки IPsec у побудованих тунелях, оскільки його принцип створення та обміну ключами, аутентифікації вже довгий час є стандартом для мереж з критичним трафіком.

У даній кваліфікаційній роботі було детально проаналізовано технологію IPsec. Досліджено та проаналізовано групи протоколів для шифрування трафіку ESP, AH, ESP+AH. Детально описано побудову тунелю з використанням IKEv1 та IKEv2, проведено порівняння даних протоколів з врахуванням сучасних задач. Особливу увагу було присвячено PKI, що гарантує більшу безпеку при побудові тунелю.

Провідним виробником активного обладнання для мережі Інтернет вже кілька десятиліть залишається корпорація Cisco Systems, яка не тільки є виробником обладнання, але й розробником міжнародних стандартів в області телекомунікацій. Тому особливу увагу в цій роботі було приділено реалізації віртуальних приватних мереж саме на рішеннях від Cisco.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Робота також має велику практичну цінність, оскільки значну її частину становить технічна реалізація віртуальних приватних мереж на основі власноруч побудованого проєкту в емуляторі GNS3. Опанування синтаксису командного рядку операційної системи Cisco IOS дозволило налаштувати та перевірити роботу Site-to-Site та Remote Access VPN – двох базових реалізацій даної технології з використання технології FlexVPN.

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. [Електронний ресурс] – Режим доступу:
<https://www.comparitech.com/vpn/vpn-statistics/>
2. IPSec VPN Configuration, Cisco, 2009. – 28 с.
3. The Complete Cisco VPN Configuration Guide By Richard Deal, 2005. – 1032с.
4. 9. Point-to-Point GRE over IPsec Design Guide. – Cisco, 2006. – 106 с.
5. [Електронний ресурс] – Режим доступу:
<https://www.cisco.com/c/en/us/support/docs/security/flexvpn/115782-flexvpn-site-to-site-00.html>
6. [Електронний ресурс] – Режим доступу:
<https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html>
7. Cisco IOS VPN Configuration Guide, 2005. – 131 с.
8. VPN Security - The Government of the Hong Kong Special Administrative Region, 2008 – 24 с.
9. Скорик Ю.В., Богун М.О. Аналіз принципів побудови корпоративної мережі підприємства / Одинадцята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» 8-9 квітня 2021 року. Баку – Харків – Київ – Жиліна – 2021. – С. 86
10. [Електронний ресурс] – Режим доступу:
<https://packetpushers.net/flexvpn-configuration/>
11. [Електронний ресурс] – Режим доступу:
<https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2018/pdf/BRKSEC-2881.pdf>
12. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / Л.Гончарова, А. Возненко, О. Стасюк, Ю. Коваль. – К., 2013. – 435 с. (дата звернення: 08.05.2020)

		Бабіч Д. В.			<i>KIK.KP.B – 123 – 02 – ПЗ</i>	Арк.
		Покотило О. А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Конфігураційний файл комутатора рівня доступу

Current configuration : 2115 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime localtime

no service password-encryption

service compress-config

!

hostname AccSW1

!

boot-start-marker

boot-end-marker

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone KYIV 3 0

no ipv6 cef

ipv6 multicast rpf use-bgp

no ip icmp rate-limit unreachable

!

no ip domain-lookup

ip cef

!

archive

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

path ftp://@123.20.20.5/$H-$T
write-memory
time-period 360
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ftp source-interface Loopback0
!
interface Loopback0
no ip address
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/2
switchport access vlan 2
switchport mode access
duplex auto

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet0/3
    switchport access vlan 2
    switchport mode access
    duplex auto
!
interface Vlan51
    ip address 50.0.12.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 50.0.12.1
!
access-list 1 permit 50.0.2.1
access-list 1 permit 50.0.1.1
!
control-plane
!
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login
!
ntp source Vlan51

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ntp access-group peer 1
ntp update-calendar
ntp server 50.0.1.1 prefer
ntp server 50.0.2.1
end

```

Додаток В – Конфігураційний файл комутатора рівня розподілу

Current configuration : 3899 bytes

```

!
version 12.4

service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname DistSW1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
clock timezone KYIV 3
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!

```

		Бабіч Д. В.			<i>KIK.KP.B – 123 – 02 – ПЗ</i>	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

!
spanning-tree vlan 2 priority 8192
spanning-tree vlan 3 priority 16384
archive
log config
hidekeys
path ftp://123.20.20.5/$H
write-memory
time-period 360
!
ip tcp synwait-time 5
ip ftp source-interface Loopback0
!
interface Loopback0
ip address 50.0.1.1 255.255.255.0
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/0
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

!
interface FastEthernet1/0
  switchport mode trunk
!
interface FastEthernet1/1
  switchport mode trunk
!
interface FastEthernet1/2
  switchport mode trunk
!
interface FastEthernet1/3
  switchport mode trunk
!
interface FastEthernet1/4
  switchport mode trunk
  channel-group 1 mode on
!
interface FastEthernet1/5
  switchport mode trunk
  channel-group 1 mode on
!
interface Vlan1
  no ip address
!
interface Vlan2
  ip address 192.168.2.50 255.255.255.0
  ip helper-address 123.20.20.5
  standby 1 ip 192.168.2.1

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

standby 1 priority 110
standby 1 preempt
!
interface Vlan3
ip address 192.168.3.50 255.255.255.0
ip helper-address 123.20.20.5
standby 2 ip 192.168.3.1
standby 2 preempt
!
interface Vlan51
ip address 50.0.12.50 255.255.255.0
standby 1 ip 50.0.12.1
standby 1 priority 110
standby 1 preempt
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 10.0.0.0 0.0.255.255 area 2
network 50.0.1.0 0.0.0.255 area 2
network 50.0.12.0 0.0.0.255 area 2
network 192.168.0.0 0.0.255.255 area 2
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

access-list 1 permit 50.0.2.1
access-list 1 permit 50.0.6.1
access-list 1 permit 50.0.5.1
access-list 2 permit 50.0.12.4
access-list 2 permit 50.0.12.5
access-list 2 permit 50.0.12.2
access-list 2 permit 50.0.12.3
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
!
ntp clock-period 17179839
ntp source Loopback0
ntp access-group peer 1
ntp access-group serve-only 2
ntp master 5
ntp peer 50.0.2.1

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

ntp server 50.0.5.1 prefer

ntp server 50.0.6.1

!

Додаток С – Конфігураційний файл комутатора рівня ядра

Current configuration : 2556 bytes

!

version 15.1

service timestamps debug datetime msec

service timestamps log datetime localtime

no service password-encryption

service compress-config

!

hostname CoreSW1

!

boot-start-marker

boot-end-marker

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

clock timezone KYIV 3 0

no ipv6 cef

ipv6 multicast rpf use-bgp

no ip icmp rate-limit unreachable

!

no ip domain-lookup

		Бабіч Д. В.			KIK.KP.B – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

ip cef
!
archive
path ftp://@123.20.20.5/$H-$T
write-memory
time-period 360
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Loopback0
ip address 50.0.5.1 255.255.255.0
!
interface Ethernet0/0
no switchport
ip address 10.0.1.2 255.255.255.0
!
interface Ethernet0/1
no switchport
ip address 10.0.3.2 255.255.255.0
!
interface Ethernet0/2
no switchport
ip address 10.0.5.2 255.255.255.0
!

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

interface Ethernet0/3
  no switchport
  ip address 10.0.7.2 255.255.255.0
!
interface Ethernet1/0
  no switchport
  ip address 10.0.10.1 255.255.255.0
!
interface Ethernet1/1
  no switchport
  ip address 10.0.13.1 255.255.255.0
!
interface Ethernet1/2
  no switchport
  ip address 10.0.9.1 255.255.255.0
!
interface Ethernet1/3
  no switchport
  ip address 10.0.14.2 255.255.255.0
!
interface Ethernet2/0
  no switchport
  ip address 10.0.17.2 255.255.255.0
!
interface Vlan1
  no ip address
  shutdown
!

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

router ospf 1
  router-id 5.5.5.5
  network 10.0.0.0 0.0.255.255 area 2
  network 50.0.5.0 0.0.0.255 area 2
!
no ip http server
!
access-list 1 permit 10.0.9.2
access-list 1 permit 50.0.7.1
access-list 1 permit 50.0.8.1
access-list 2 permit 50.0.3.1
access-list 2 permit 50.0.2.1
access-list 2 permit 50.0.1.1
access-list 2 permit 50.0.4.1
access-list 2 permit 50.0.10.1
access-list 2 permit 50.0.9.1
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

login
!
ntp source Loopback0
ntp access-group peer 1
ntp access-group serve-only 2
ntp master 4
ntp update-calendar
ntp peer 50.0.6.1
ntp server 50.0.7.1
ntp server 50.0.8.1 prefer
end

```

Додаток D – Конфігураційний файл комутатора граничного маршрутизатора

Current configuration : 14656 bytes

```

!
! No configuration change since last restart
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname EdgeRT1
!
boot-start-marker
boot-end-marker
!
aaa new-model
!

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

aaa group server radius RADIUS-GROUP
server name FLEX-VPN-RAD
!
aaa authentication login A_EAP_AUTHEN_LOCAL_LIST group RADIUS-GROUP
!
aaa session-id common
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
clock timezone KYIV 3 0
clock calendar-valid
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
crypto pki trustpoint VPN-PKI
enrollment url http://60.0.1.1:80
subject-name CN=EdgeRT1,OU=VPN,O=Cisco,C=US

```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

revocation-check crl
source interface Ethernet0/2
rsa-keypair VPN-KEYS
!
crypto pki trustpoint FlexVPN-TP-CS2
  enrollment url http://60.0.1.1:80
  subject-name CN=165.25.24.12
  crl cache none
  revocation-check none
  source interface Loopback0
  rsa-keypair FLEXVPN-KEYS-CS2
!
crypto pki certificate map IDENTITY_MAP 10
  subject-name co ou = vpn
!
crypto pki certificate chain VPN-PKI
  certificate 01
  certificate 02
!
redundancy
!
track 1 ip sla 1 reachability
!
ip tcp synwait-time 5
!
crypto ikev2 proposal PROP1_FOR_FLEX
  encryption aes-cbc-256
  integrity sha512

```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

```

group 16 19 24
crypto ikev2 proposal SITE_PHASE_1
  encryption aes-cbc-256
  integrity sha512
group 24 16 15
!
crypto ikev2 policy IKEv2_POL_FOR_FLEX
  proposal PROP1_FOR_FLEX
crypto ikev2 policy POL_SITE_1
  proposal SITE_PHASE_1
!
crypto ikev2 keyring RING_1
  peer BrEdgeRT
    address 56.94.24.23
    pre-shared-key cisco
!
crypto ikev2 profile SITE_PROF
  match certificate IDENTITY_MAP
  authentication remote rsa-sig
  authentication local rsa-sig
  pki trustpoint VPN-PKI
  lifetime 36700
!
crypto ikev2 profile FLEX_IKEv2_PROF
  match identity remote address 0.0.0.0
  match identity remote key-id 1111
  authentication remote eap query-identity
  authentication local rsa-sig

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

pki trustpoint FlexVPN-TP-CS2
aaa authentication eap A_EAP_AUTHEN_LOCAL_LIST
aaa authorization user eap cached
virtual-template 100
!
crypto ipsec transform-set SITE_PEER_BRANCH esp-aes esp-sha-hmac
mode tunnel
crypto ipsec transform-set TSET_FOR_FLEX esp-gcm 192
mode tunnel
!
crypto ipsec profile FLEX_IPSEC_PROF
set transform-set TSET_FOR_FLEX
set ikev2-profile FLEX_IKEv2_PROF
!
crypto ipsec profile SITE_IPSEC_PROF
set transform-set SITE_PEER_BRANCH
set ikev2-profile SITE_PROF
!
interface Loopback0
ip address 50.0.7.1 255.255.255.0
!
interface Tunnel0
ip address 100.0.1.2 255.255.255.0
tunnel source Ethernet0/2
tunnel destination 56.94.24.23
tunnel protection ipsec profile SITE_IPSEC_PROF
!
interface Ethernet0/0

```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

```

ip address 10.0.10.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
ip ospf priority 100
!
interface Ethernet0/1
ip address 10.0.11.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
!
interface Ethernet0/2
ip address 165.25.24.12 255.255.255.0
ip nat outside
ip virtual-reassembly in
!
interface Virtual-Template100 type tunnel
ip unnumbered Ethernet0/2
ip mtu 1400
tunnel mode ipsec ipv4
tunnel protection ipsec profile FLEX_IPSEC_PROF
!
router ospf 1
router-id 7.7.7.7
network 10.0.0.0 0.0.255.255 area 2
network 50.0.7.0 0.0.0.255 area 2
default-information originate metric 1 route-map DEFAULT-INFORMATION
!
router bgp 10

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

```

bgp log-neighbor-changes
aggregate-address 192.168.0.0 255.255.0.0 summary-only
redistribute ospf 1
neighbor 100.0.1.1 remote-as 20
neighbor 100.0.1.1 route-map FROM_BRANCH in
!
ip local pool FLEX_POOL_MANAGERS 77.0.12.0 77.0.12.254
ip local pool FLEX_POOL_HR 77.0.13.0 77.0.13.254
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 7 interface Ethernet0/2 overload
ip route 155.155.155.155 255.255.255.255 Null0 track 1
ip route 0.0.0.0 0.0.0.0 165.25.24.98
!
ip access-list standard SPLIT-HR
permit 123.20.20.5
ip access-list standard SPLIT-MANAGERS
permit 123.20.20.5
permit 192.168.2.0 0.0.0.255
!
!
ip prefix-list OSPF seq 5 permit 192.168.0.0/16
!
ip prefix-list control_route seq 10 permit 155.155.155.155/32
ip radius source-interface Loopback0

```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip sla 1
  icmp-echo 8.8.8.8 source-interface Ethernet0/2
  frequency 10
ip sla schedule 1 life forever start-time now
!
route-map DEFAULT-INFORMATION permit 10
  match ip address prefix-list control-route control_route
!
route-map FROM_BRANCH permit 10
  match ip address 3
!
!
access-list 1 permit 193.106.144.6
access-list 2 permit 50.0.6.1
access-list 2 permit 50.0.5.1
access-list 3 permit 172.20.0.0 0.0.255.255
access-list 3 permit 70.0.0.0 0.0.255.255
access-list 7 permit 192.168.0.0 0.0.255.255
access-list 7 permit 60.0.1.0 0.0.0.255
access-list 7 permit 20.0.0.0 0.0.255.255
access-list 10 permit 70.0.0.0 0.0.255.255
access-list 10 permit 172.20.0.0 0.0.0.255
!
!
radius server FLEX-VPN-RAD
  address ipv4 123.20.20.5 auth-port 1645 acct-port 1646
  key cisco
!

```

		Бабіч Д. В.			KIK.KP.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

```

!
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
  transport input none
!
ntp source Ethernet0/2
ntp access-group peer 1
ntp access-group serve-only 2
ntp master 3
ntp update-calendar
ntp server 193.106.144.6 prefer
!
end

```

		Бабіч Д. В.			КІК.КР.Б – 123 – 02 – ПЗ	Арк.
		Покотило О. А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93