

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 магістра
на тему:

«Проектування підсистеми захищеного мережного обміну гетерогенної мережі на базі
технологій DMVPN»

Виконав,

студент II-го курсу, групи КБм-21-1
спеціальності 125 «Кібербезпека»

 Волинець Б. О.

Керівник,

доцент кафедри комп'ютерної інженерії та
кібербезпеки, доктор педагогічних наук, доцент

 Марцева Л.А..

Рецензент,

доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Пулеко І. В.

Житомир – 2022

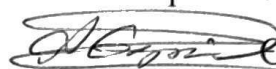
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«22» жовтня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Волинця Богуслава Олеговича**

Тема роботи: **Проект підсистеми захищеного мережного обміну гетерогенної мережі на базі технологій DMVPN**

затверджена Наказом по університету від «25» жовтня 2022 р. №501/с

Термін здачі студентом закінченої роботи – «19» грудня 2022р.

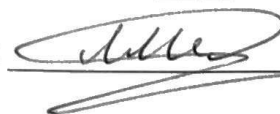
Вихідні дані для роботи:

1. Логічна топологія мережі
2. Маршрутизатори Cisco
3. Операційні системи Cisco IOS, Windows 10, Windows 7, Kali linux,
4. Графічний емулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	15.06.2022	15.06.2022
2	Єфіменко А.А.	06.09.2022	06.09.2022
3	Єфіменко А.А.	04.10.2022	04.10.2022

Керівник



Марцева Л.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 вересня 2022 – 7 вересня 2022	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	8 вересня 2022 – 15 вересня 2022	Виконано
3	Аналіз протоколів та технологій DMVPN.	16 вересня 2022 – 20 вересня 2022	Виконано
4	Аналіз можливих вразливостей протоколів які використовують технології DMVPN	21 вересня 2022 – 27 вересня 2022	Виконано
5	Проектування мережної інфраструктури	28 вересня 2022 – 2 жовтня 2022	Виконано
6	Проектування тестування оцінки безпеки комп'ютерної мережі	3 жовтня 2022 – 10 жовтня 2022	Виконано
7	Вибір засобів тестування безпеки комп'ютерної мережі	11 жовтня 2022 – 17 жовтня 2022	Виконано
8	Базове налагодження пристроїв мережі	18 жовтня 2022 – 22 жовтня 2022	Виконано
9	Налагодження роботи підсистеми динамічних багатоточкової приватної віртуальної мережі	23 жовтня 2022 – 30 жовтня 2022	Виконано
10	Тестування роботи віртуальних приватної мережі	1 листопада 2022 – 9 листопада 2022	Виконано
11	Тестування безпеки мережі DMVPN	10 листопада 2022 – 30 листопада 2022	Виконано
12	Аналіз результатів тестування	31 листопада 2022 – 2 грудня 2022	Виконано
13	Написання пояснювальної записки	3 грудня 2022 – 10 грудня 2022	Виконано
14	Підготовка презентації та виступу	11 грудня 2022 – 14 грудня 2022	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	14 грудня 2022 – 18 грудня 2022	Виконано
16	Захист	24 грудня 2022 р.	

Студент Коб Волинець Б.О.

Керівник Марцева Марцева Л.А.

РЕФЕРАТ

Випускна кваліфікаційна робота магіста містить проект підсистеми захищеного мережного обміну гетерогенної мережі на базі технологій DMVPN, пояснювальну записку та ілюстративний матеріал до нього. Пояснювальна записка до випускної роботи містить 58 сторінки, 30 ілюстрацій та 1 таблицю.

Метою роботи є проектування та налаштування мережної інфраструктури, які створюють захищений тунель до користувачів віддаленого доступу за допомогою технології DMVPN.

В роботі проаналізовано теоретичні відомості та визначено завдання на розробку підсистеми забезпечення гетерогенних віддалених підключень. Також у роботі спроектовано план тестування безпеки даної мережі та проведене тестування за складеним планом. У роботі наведено сценарій тестування безпеки гетерогенної мережі та розглянуті методи покращення захисту нашої побудованої мережі.

КЛЮЧОВІ СЛОВА: DYNAMIC MULTIPPOINT VPN, ТЕСТУВАННЯ БЕЗПЕКИ, МЕРЕЖА, ТУНЕЛЮВАННЯ.

Житомирська політехніка.22.125.03.001

Змн	Арк.	№ докум.	Підпис	Дата
-----	------	----------	--------	------

Розроб.		Волшинець Б.О.		19.11.22
---------	--	----------------	--	----------

Керівник		Марцева Л.А.		19.11.22
----------	--	--------------	--	----------

Реценз.		Пудеко І.В.		
---------	--	-------------	--	--

Н. Контр.				
-----------	--	--	--	--

Затверд.		Сфіменко А.А.		19.11.22
----------	--	---------------	--	----------

Проект підсистеми захищеного
мережного обміну гетерогенної
мережі на базі технологій DMVPN

Літ.	Арк.	Аркушів
------	------	---------

	4	71
--	---	----

Державний Університет
«Житомирська політехніка»
ФІКТ, група. КБм-21-1

ABSTRACT

The master's graduation thesis contains a project of protected network exchange subsystem of a heterogeneous network based on DMVPN technologies, an explanatory note and illustrative material for it. The explanatory note to the final thesis contains 58 pages, 30 illustrations and 1 tables.

The goal of the work is to design and configure network infrastructure that creates a secure tunnel to remote access users using DMVPN technology.

The paper analyzes theoretical information and defines the task of developing a subsystem for providing heterogeneous remote connections. The work also designed a security testing plan for this network and conducted testing according to the prepared plan. The paper provides a scenario for testing the security of a heterogeneous network and considers methods for improving the protection of our constructed network.
KEYWORDS: DYNAMIC MULTIPOINT VPN, SECURITY TESTING, NETWORK, TUNNELING.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

VPN – Virtual Private Network - віртуальна приватна мережа

ПК – Персональний комп'ютер

PPTP – Point to Point Tunneling Protocol

L2TP – Layer 2 Tunneling Protocol

NAT - Network Address Translation — перетворення мережевих адрес

IPsec - IP Security

MPLS - Multiprotocol Label Switching

IKE – Internet Key Exchange

SLA - Service Level Agreement

DMPVN - dynamic multipoint virtual private network

GRE - Generic Routing Encapsulation

NHRP - Next Hop Resolution Protocol

NAT - Network address translation

TCP - The Transmission Control Protocol

PSK - Pre-shared key

PKE - public key

RPKE - replayable public-key

ARP - Address Resolution Protocol

IGP- Interior Gateway Protocol

GRE - Generic Routing Encapsulation

SHA - Secure Hash Algorithm

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

AES-CBC - Advanced Encryption Standard - Cipher Block Chaining

TCP- Transmission Control Protocol

TED - Tunnel Endpoint Discovery

mGRE - Multipoint Generic Routing Encapsulation

WAN - Wide area network

NBMA - Non-broadcast multiple access

NHC - Next Hop Resolution Protocol client

NHS - Next Hop Servers

NHRP - Next Hop Resolution Protocol

TED - Tunnel Endpoint Discovery

QoS - Quality of Service

FQDN - Fully Qualified Domain Name

UDP - User Datagram Protocol

MTU - Maximum Transmission Unit

IPX - internetwork packet exchange

DOS/DDOS - Disk Operating System / Distributed Denial-of-service attack

MitM - Man-in-the-middle attack

MAC - Media Access Control Protocol

BSD - The Berkeley Software Distribution or Berkeley Standard Distribution

GUI - Graphical user interface

CLI - Command-line interpreter

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ЗМІСТ

ЗМІСТ	8
ВСТУП	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЙ ДИНАМІЧНИХ БАГАТОТОЧКОВИХ ВІРТУАЛЬНИХ МЕРЕЖ В ГЕТЕРОГЕНОМУ СЕРЕДОВИЩІ	11
1.1 Організація приватних віртуальних мереж.	11
1.2 Технології та протоколи віддаленого досупу.....	13
1.3 Аналіз вразливостей мереж на базі технологій DMVPN	30
1.4 Технічне завдання.	32
1.5 Висновки до розділу 1.	34
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО МЕРЕЖНОГО ОБМІНУ НА БАЗІ ТЕХНОЛОГІЙ DMVPN	35
2.1 Проектування мережної інфраструктури	35
2.2 Проектування тестування оцінки безпеки комп'ютерної мережі.....	37
2.3 Засоби тестування безпеки комп'ютерної мережі.....	41
2.4 Висновки до розділу 2.	46
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ	47
3.1 Налаштування віддаленого доступу.	47
3.2 Перевірка роботи та дослідження віддаленого доступу.	52
3.3 Висновки до розділу 3.	56
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	60
ДОДАТКИ	63

ВСТУП

Основні конвенції та компоненти системного адміністрування не захищають від атак (наприклад, прослуховування телефонних розмов, зміна інформації тощо). Безпека системи є ключовим питанням на тій підставі, що розвивається деструктивне поведіння в системі. Безпека включає в себе численні аспекти, які включають підтвердження, надійність, невідховування та класифікацію. Творці вирішили перевірити конфіденційність у світлі того факту, що обмін інформацією між штаб-квартирою компанії і віддаленим відділенням або бізнес-спільниками, клієнтами або контракторами, які використовують відкриті системи (Інтернет). Питання інформаційної таємниці в організації з численними філіями, які є динамічними в усьому світі, є життєво важливим. Підприємства використовують різну техніку для побудови безпечної мережі між штаб-квартирою та багатьма філіями та корпоративними для передачі інформації, обміну даними ресурсів і додатками. Для безпечного зв'язку більшість компаній використовує традиційний метод виділеної лінії для підключення віддалених користувачів і філій. Але цей спосіб орендованої лінії недешевий у плануванні і займає велику кількість часу та витрат на встановлення та активацію. Керівництво підприємства більше, а філії окремі по всій країні. Підприємство, клієнт, співробітник завжди потребують підвищення безпеки передачі даних і доступності мережі. Багато корпоративних мереж використовують техніку VPN для створення безпечної корпоративної мережі в різних регіонах. Але IPsec VPN не підтримує динамічний маршрут. Проблема традиційного VPN полягає в тому, що мережа та розширення не піддаються, вартість обслуговування та експлуатації надзвичайно дорога.

При розробці корпоративної мережі забезпечується безпека передачі даних, мінімізуються витрати на технічне обслуговування та експлуатація, а з'єднання між штаб-квартирою та філією завжди доступне. З цією метою ми проектуємо корпоративну мережу з використанням технології DMVPN через IPsec для встановлення безпечної мережі та використовуємо протоколи маршрутизації гарячого резервування (HSRP), щоб гарантувати, що мережі не перериваються через

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

втрату з'єднання, а мережа завжди доступна для з'єднання з кожним пунктом призначення.[1]

Апробація результатів:

1. Волинець Б. О., Єфіменко А. А., Вакалюк Т. А. Аналіз та дослідження технологій багатоточкових динамічних віртуальних мереж // Тези доповідей IV Всеукраїнської науково-практичної інтернет- конференції здобувачів вищої освіти і молодих учених «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», м. Житомир, 25 – 26 листопада 2021 р. – Житомир: Житомирська політехніка, 2021. – 186 с

2. Волинець Б. О., Єфіменко А. А., Вакалюк Т. А. Аналіз технології групового зашифрованого транспортування у віртуальних приватних мереж // V Всеукраїнській науково-практичній інтернет-конференції молодих вчених та студентів «Сучасні інформаційні системи та технології», м. Херсон, 30 листопада 2022р. – Херсон: Херсонський національний технічний університет, 2022. – 1с.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЙ ДИНАМІЧНИХ БАГАТОТОЧКОВИХ ВІРТУАЛЬНИХ МЕРЕЖ В ГЕТЕРОГЕНОМУ СЕРЕДОВИЩІ

1.1 Організація приватних віртуальних мереж.

Замість того, щоб покладатися на дороге апаратне забезпечення для налаштування закритих мереж, більшість компаній надають перевагу VPN де використовують відкриту мережу Інтернет для безпечної передачі даних через зашифровані тунелі. Оскільки Інтернет є загальнодоступним за задумом, шифрування служить стримуючим фактором для зловмисників, які ховаються в тому самому середовищі.

Загалом існують два основних типи VPN: Remote VPN, Site-to-Site VPN.

Remote VPN (VPN віддаленого доступу) – це тимчасове зашифроване з'єднання між центром обробки даних компанії та пристроєм користувача. Він стає активним лише тоді, коли користувач його вмикає. В іншому випадку він не матиме постійного підключення. Компанії в основному використовують цей тип для безпечного доступу до програм і даних у центральному хабі через тунель VPN . Ви можете думати про це як про VPN-з'єднання, що створює безпечний шлях від вашого пристрою до доступу до конфіденційних документів або матеріалів компанії на іншому кінці.

Дана технологія працює наступним чином:

— Спочатку сервер VPN перевіряє, чи дозволено користувачеві доступ до мережі. Від користувача вимагають введення пароля або використання біометричних даних, таких як відбиток пальця, щоб ідентифікувати себе. У деяких рішеннях можуть використовувати сертифікати безпеки для автоматичної автентифікації користувача у фоновому режимі, що забезпечує швидше з'єднання. Це особливо корисно, коли користувачеві потрібно підключитися до кількох серверів VPN – наприклад, для доступу до різних мереж сайту.

— Після автентифікації користувача клієнт і сервер встановлюють між собою зашифрований тунел який захищає трафік через Інтернет. Існує багато різних

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

протоколів VPN , які можна використовувати для налаштування тунелю шифрування: IPsec і SSL – це два, які часто використовуються.

—Користувач отримує доступ до ресурсів через сервер VPN.

Найкращими прикладами Remote VPN можна назвати:

—OpenVPN Access Server

—Cisco AnyConnect VPN

—Perimeter 81

У той час як VPN віддаленого доступу розроблено, щоб дозволити окремим користувачам підключатися до мережі та використовувати її ресурси, VPN типу site-to-site - це постійне з'єднання між декількома офісами для створення об'єднаної постійно ввімкненої мережі. Його потрібно налаштувати окремо для обох мереж, і він найкраще працює у випадках, коли у вас є кілька віддалених сайтів. Його можна налаштувати на локальних маршрутизаторах або на брандмауерах.

Дане рішення не дуже часто використовують, якщо користувачі хочуть підключатися з дому. Зазвичай адміністратори не дозволяють з'єднання з мереж, які вони не контролюють, з міркувань безпеки. По суті, вони жертвують доступністю на користь безпеки. З іншого боку, це один із найдешевших методів об'єднання окремих мереж в єдину інтранет. Кожен окремий пристрій може працювати так, ніби він знаходиться в одній локальній мережі, що полегшує обмін даними та робить його закритим від спроб стеження ззовні.

Залежно від того, кому належать мережі, до яких приєднуються, загалом існують дві різні форми VPN типу " site-to-site ":

—VPN на основі інтрамережі: якщо підключені мережі належать одній компанії, така об'єднана мережа називається VPN на основі інтрамережі. Це дозволяє компанії створити єдину глобальну мережу (WAN), яка охоплює два чи більше офісів. Користувачі компанії можуть отримати доступ до ресурсів з інших сайтів так само легко, як якщо б вони були на своєму власному сайті.

—VPN на основі екстрамережі: якщо підключені мережі належать різним компаніям, об'єднана мережа називається VPN на основі екстрамережі. Екстранет

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

VPN використовується, наприклад, коли компанія хоче підключитися до мережі свого постачальника, щоб вони могли торгувати ефективніше.

Існують три основні способи реалізації VPN типу "сайт-сайт":

- Побудовані на тунелях IPsec
- З використанням VPN третього рівня (L3VPN)
- Динамічна багатоточкова VPN (DMVPN)

1.2 Технології та протоколи віддаленого досугу.

Динамічна багатоточкова віртуальна приватна мережа (DMVPN, Dynamic Multipoint VPN) – це технологія розроблена компанією Cisco, що забезпечує захищений обмін даними між сайтами (маршрутизаторами) без проходження трафіку через центральний сервер (маршрутизатор) віртуальної приватної мережі компанії. DMVPN дозволяє організаціям створювати мережу VPN з декількома сайтами без необхідності статичного налаштування пристроїв. DMVPN будує сітчасту VPN топологію «Hub and Spoke», в якій маршрутизатор кожного віддаленого сайту налаштований на підключення до центральної точки VPN компанії, щоб забезпечити доступ до необхідних ресурсів. У той же час кожен сайт («клієнт») може з'єднуватися безпосередньо з усіма іншими клієнтами, незалежно від їх розташування і без необхідності проходження через центральний вузол [1].

За допомогою DMVPN підключення між філіями забезпечуються через загальнодоступне підключення до глобальної мережі або Інтернет. DMVPN працює як на маршрутизаторах, так і на міжмережних екранах компанії Cisco. Кожен віддалений сайт має маршрутизатор, налаштований для підключення до VPN-хабу, що знаходиться в головному офісі компанії.

Коли два користувача обмінюються даними (наприклад, для забезпечення виклику Voice over IP) один із клієнтів зв'яжеться з центральною інстанцією (Hub) та отримає необхідну інформацію про іншого клієнта для створення між ними динамічного тунелю IPsec VPN. Користувачі не використовують постійне VPN-з'єднання, натомість вони спілкуються через з використанням централізованої

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

модель «Hub-and-Spoke», яка застосовує захист VPN та детальний контроль доступу за потреби [1].

DMVPN складається з таких ключових складових [4]:

- багатоточкові тунельні інтерфейси (mGRE, Multipoint Generic Routing Encapsulation);
- протокол наступного переходу (NHRP, Next Hop Resolution Protocol);
- механізм виявлення кінцевої точки тунелю (TED, Tunnel Endpoint Discovery);
- протокол маршрутизації.

Загальна інкапсуляція маршрутизації (GRE) — це протокол інкапсуляції IP, який використовується для транспортування IP-пакетів по мережі. Загальна інкапсуляція маршрутизації (GRE) спочатку була розроблена компанією Cisco, а пізніше стала промисловим стандартом (RFC 1701, RFC 2784 і RFC 2890).

GRE (Generic Routing Encapsulation) датаграма IP тунелюється (інкапсулюється) в іншу IP-датаграму. GRE (Generic Routing Encapsulation) також підтримує інкапсуляцію широкомовного та багатоадресного трафіку IPv4. Явною перевагою GRE перед іншими протоколами тунелювання є те, що він може інкапсулювати широкомовний, багатоадресний трафік (протоколи багатоадресної потокової передачі або маршрутизації) або інші протоколи, які не є IP. Пакети GRE можна захистити за допомогою Internet Protocol Security (IPSec), що забезпечує конфіденційність і цілісність тунельованого трафіку.

Тунелі загальної інкапсуляції маршрутизації (GRE) не є безпечними, оскільки загальна інкапсуляція маршрутизації (GRE) не шифрує корисне навантаження даних. У режимі реального часу загальна інкапсуляція маршрутизації (GRE) використовується разом з іншими безпечними протоколами тунелювання, такими як IPSec, для забезпечення безпеки мережі.

GRE не має стану і не знає про конфігурацію або навіть про існування кінцевої точки віддаленого тунелю. Після налаштування GRE пакети інкапсулюються та пересилаються незалежно від того, є пристрій декапсуляції чи ні.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

На відміну від тунелювання IP-to-IP , тунелювання GRE може транспортувати багатоадресний трафік і трафік IPv6 між мережами. Переваги тунелів GRE включають наступне:

- Тунелі GRE охоплюють декілька протоколів через одну протокольну магістраль.
- Тунелі GRE надають обхідні шляхи для мереж з обмеженими стрибками.
- Тунелі GRE з'єднують розривні підмережі.
- Тунелі GRE дозволяють використовувати VPN в глобальних мережах (WAN).

Деякі характеристики тунелів GRE включають наступне:

— Інкапсуляція даних – тунелі GRE інкапсулюють пакети, які використовують протоколи, несумісні з проміжною мережею (пасажирські протоколи), у межах сумісних протоколів (транспортні протоколи). Це дозволяє надсилати дані через мережі, які інакше не можна було б пройти. Наприклад, ви можете реалізувати тунель GRE, щоб з'єднати дві мережі AppleTalk через мережу лише з IP або для маршрутизації пакетів IPv4 через мережу, яка використовує лише IPv6.

— Простота – у тунелях GRE за замовчуванням відсутні механізми, пов'язані з керуванням потоком і безпекою. Ця відсутність функцій може полегшити процес налаштування. Однак ви, ймовірно, не захочете передавати дані в незашифрованому вигляді через загальнодоступну мережу; тому тунелі GRE можуть бути доповнені набором протоколів IPSec з метою безпеки. Крім того, тунелі GRE можуть пересилати дані з суміжних мереж через один тунель, чого не можуть зробити VPN.

— Переадресація багатоадресного трафіку – тунелі GRE можна використовувати для пересилання багатоадресного трафіку, тоді як VPN – ні. Через це багатоадресний трафік, такий як рекламні оголошення, надіслані протоколами маршрутизації, можна легко передавати між віддаленими сайтами при використанні тунелю GRE.

Заголовок загальної інкапсуляції маршрутизації складається із таких складових:

— Flag C (Присутня контрольна сума) - використовується для вказівки, що поле контрольної суми присутнє та містить дійсну інформацію, якщо встановлено значення 1;

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

- Flag R (Присутня контрольна сума) - використовується для вказівки, що поля маршрутизації присутні та містять дійсну інформацію, якщо встановлено значення 1;
- Flag K (Ключ присутній) - використовується для вказівки, що поле Key є в заголовку GRE, якщо встановлено значення 1;
- Flag S (присутній порядковий номер) - використовується для вказівки, що поле порядкового номера присутнє, коли встановлено значення 1;
- Flag s (Strict Source Route) – Якщо встановлено значення 1, інформація про маршрутизацію складається з Strict Source Route;
- Контроль рекурсії та номер версії (Recursion Control and Version Number) зазвичай встановлені на 0;
- Тип протоколу (Protocol Type)- поле типу протоколу використовується для згадки корисного навантаження протоколу пакета GRE. Для IP це поле встановлено на 0x800;
- Контрольна сума (Checksum) - значення поля контрольної суми використовується для перевірки цілісності заголовка GRE та корисного навантаження;
- Ключ (Key) - значення поля ключа використовується для аутентифікації інкапсулятора пакета GRE;
- Sequence Number - значення в файлі Sequence Number використовується для відстеження послідовності пакетів GRE;

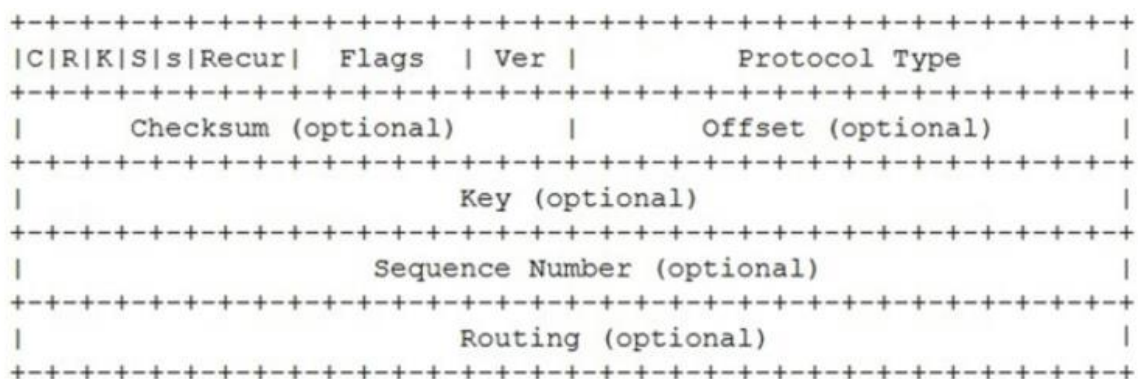


Рисунок 1.1 – Складові заголовка GRE

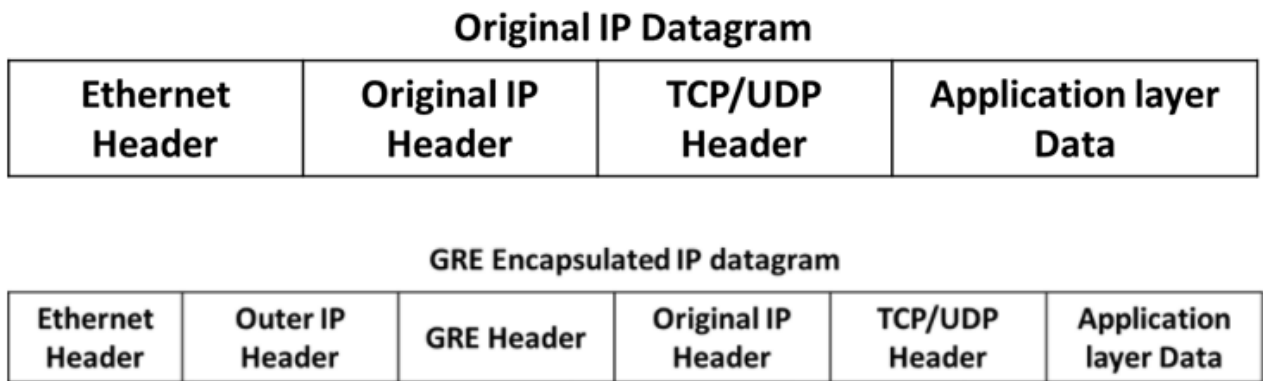


Рисунок 1.2 – Різниця між оригінальною IP-дейтаграмою та інкапсульованою IP-дейтаграмою Generic Routing Encapsulation (GRE).

Next Hop Resolution Protocol (NHRP) — це технологія автоматичного налаштування, яка маршрутизує дані в розподіленій мережі, виявляючи найкращий шлях маршрутизації між кінцевими точками. Це дозволяє комп'ютеру, що надсилає дані на інший комп'ютер, дізнатися найбільш прямий маршрут – найменшу кількість стрибків – до комп'ютера-отримувача.

У багатоточковій топології GRE/DMVPN маршрутизатор, який відіграє роль хаба є сервером NHRP, а всі інші маршрутизатори відіграють роль клієнтів. Кожен клієнт реєструється на сервері та повідомляє свою публічну IP-адресу, яку сервер відстежує у своєму кеші. Завдяки процесу, який включає реєстрацію та запити на вирішення від клієнтських маршрутизаторів, а також відповіді на вирішення від маршрутизатора сервера, увімкнено трафік між різними маршрутизаторами в DMVPN [4].

Якщо комп'ютер-одержувач знаходиться в тій самій підмережі, використання NHRP повідомляє комп'ютеру-одержувачу, що комп'ютер-одержувач є локальним, і він може надсилати наступні пакети даних безпосередньо на комп'ютер-отримувач, використовуючи адресу своєї підмережі, а не адресу глобальної мережі. Однак якщо комп'ютер-отримувач не входить до тієї ж підмережі, використання NHRP повідомляє комп'ютеру-відправнику про комп'ютер у підмережі, чий маршрутизатор забезпечує найбільш прямий шлях до комп'ютера-

NHRP схожий на протокол розділення адрес (ARP), який можна використовувати для динамічного відображення мереж. Алгоритм роботи цього протоколу розділений на кілька частин, як показано нижче



Ці з'єднання «точка-точка» можуть бути фізичним оптоволоконним каналом, віртуальною приватною мережею (VPN) або тунелем загальної інкапсуляції маршрутизації (GRE). Це може призвести до кількох можливих шляхів від одного клієнта до іншого. Крім того, WAN блокує широкомовні запити на дозвіл адреси.

Такі типи мережі є мережною множинною доступу без широкомовної передачі (NBMA). Через це весь трафік повинен проходити через основний маршрутизатор, що призводить до складної конфігурації, неоптимальної маршрутизації на вузьких місць пропускної здатності.

У мережі NBMA кінцеві точки та маршрутизатори-учасники не знають фізичного шляху один до одного. Цю інформацію про маршрутизацію можна створити вручну, але її важко підтримувати.

NHRP дозволяє маршрутизаторам автоматично знаходити правильний фізичний шлях та адреси Інтернет-протоколу (IP). NHRP використовує сервери наступного переходу (NHS) для реєстрації та надання інформації про маршрутизацію клієнтам наступного переходу (NHC). NHS також можна назвати центром, а NHC — клієнтом. Кожен NHC реєструє свою фізичну IP-адресу та свою логічну локальну IP-адресу в NHS. Коли один NHC хоче виявити маршрут для зв'язку з кінцевою точкою на іншому маршрутизаторі NHC, він виконує дозвіл NHRP. Він зв'язується з NHS, щоб знайти фізичну адресу наступного NHC. Потім він може надсилати трафік безпосередньо на правильний NHC — між розмовними каналами — не надсилаючи його спочатку через центральний хаб. Це значно збільшує загальну ємність усієї мережі NBMA за рахунок зменшення навантаження на центральну NHS.

NHRP була розроблена Робочою групою Internetworking Over NBMA Робочої групи Internet Engineering Task Force (IETF). Він є основним компонентом багатопроTOCOLного режиму асинхронної передачі і описаний у Запиті IETF на коментарі 2332, «Протокол NBMA Next Hop Resolution Protocol» і RFC 2333, «Заява про застосовність протоколу NHRP».

NHRP працює на рівні 2 моделі взаємозв'язку відкритих систем, подібно до ARP. Він також може працювати в мережах GRE та IP. NHRP не має спеціального номера протоколу, присвоєного Internet Assigned Numbers Authority.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

NHRP є відкритим стандартом, який підтримується більшістю великих виробників маршрутизаторів. Сюди входять Cisco, Juniper, Hewlett Packard Enterprise та інші. OpenNHRP існує як реалізація з відкритим кодом.

Tunnel Endpoint Discovery (TED) — протокол від Cisco, який покращує масштабованість та доступність VPN, розширюючи можливості динамічних криптокарт. [1] Динамічні крипто-карти значно зменшують вашу роботу, усуваючи конфігурацію конкретних однорангових IPsec. Однак динамічні крипто-карти (за замовчуванням) є лише одержувачами запитів узгодження IKE. Тобто, на відміну від звичайних криптовалютних карт, вони не можуть ініціювати вихідні SA з віддаленими одноранговими користувачами — динамічні крипто-карти покладаються на те, що інші однорангові партнери спочатку зв'язуються з ними.

Поведінка лише прослуховування динамічних криптокарт прийнятна в більшості середовищ доступу VPN, де центральний маршрутизатор приймає запити IKE від багатьох користувачів, які підключені до телефону. Однак у середовищі внутрішньої мережі VPN підхід лише для прослуховування не дуже корисний, оскільки ви хочете надати кожному одноранговому можливість ініціювати IKE з будь-яким іншим одноранговим. Це означає, що ви повинні використовувати звичайні статичні крипто-карти.

Коли у вас є великий інтранет VPN — скажімо, понад 20 або 30 маршрутизаторів — налаштування статичних крипто-карт для з'єднання з усіма можливими одноранговими користувачами стає трудомістким і складним у керуванні. Коли настав час додати новий одноранговий вузол, вам доведеться повернутися до всіх інших однорангових вузлів і змінити кожен конфігурацію, щоб вмістити додавання, а це в свою чергу займе багато часу та ресурсів.

Отже, ось TEB з TED динамічною криптокартой може динамічно досліджувати й виявляти віддалені однорангові вузли. З TED це означає, що динамічна криптокарта може використовуватися для автоматичного ініціювання SA для кількох однорангових партнерів за запитом та з мінімальною конфігурацією (віддалений однорангові пристрої також мають увімкнути TED). Таким чином, сітка

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

топології «багать-до-багатьох» можлива без необхідності налаштовувати величезні статичні крипто-карти.

TED працює, надсилаючи пакет проби та прослуховуючи відповідь, щоб визначити інший кінець IKE SA. Коли вихідний пакет потребує захисту IPsec, TED відправляє пробний пакет. Запит направляється через ненадійну мережу до кінцевого пункту призначення даних, поки не досягне віддаленого однорангового пристрою з підтримкою TED. Коли віддалений одноранговий вузол відповідає ініціатору проби, віддалений одноранговий вузол «виявляється», і два пристрої встановлюють IKE SA. Решта процесу IPsec продовжується як зазвичай.

TIP TED зручний, коли ви розгортаєте резервні однорангові вузли для високодоступних VPN. Якщо віддалений одноранговий вузол вийде з ладу, TED динамічно виявить новий віддалений одноранговий вузол (якщо ви розгорнули його як резервну копію). Коли ви додаєте резервний одноранговий пристрій, вам не потрібно переналаштовувати інші маршрутизатори в мережі — TED автоматично виявляє нову резервну копію.

Протоколи маршрутизації дозволяють DMVPN ефективно та ефективно знаходити маршрути між різними кінцевими точками. Щоб створити масштабований і стабільний DMVPN, важливо вибрати правильний протокол маршрутизації. Одним з варіантів є використання протоколу внутрішньої маршрутизації. OSPF найкраще підходить для розгортання невеликих мереж на базі DMVPN. Для середніх та великих мереж більше підходять протоколи EIGRP або BGP. EIGRP не обмежений обмеженнями топології протоколу стану каналу, і його легше розгорнути та масштабувати в топології DMVPN. BGP може масштабуватися до багатьох однорангових і маршрутів, і це створює менше навантаження на маршрутизатори в порівнянні з іншими протоколами маршрутизації [2].

Існує три різні типи або так звані фази дизайну DMVPN: Фаза 1, Фаза 2, Фаза 3.

На першій фазі користувачі DMVPN реєструють на хабі. На цій початковій стадії немає прямого зв'язку між клієнтами, тому весь трафік проходить через головний

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

сервер. Кожна кінцева точка використовує звичайні інтерфейси тунелю GRE типу «Point-to-Point» і вимагає лише маршруту за замовчуванням до вузла, щоб досягти інших кінцевих точок. В результаті конфігурація маршрутизації на цьому етапі проста.

На другій фазі можна розгортати тунель типу «Spoke-to-Spoke» з усіма сполучними маршрутизаторами, які використовують багатоточкові тунелі GRE. Ці прямі тунелі запускаються на основі трафіку клієнта. Це означає, що дані не повинні передаватися до вузла. Хоча центральна точка використовується для площини керування, йому не обов'язково знаходиться в кругообігу даних.

На третій фазі розгортаються прямі тунелі без використання певних заздалегідь прокладених маршрутів. Для забезпечення безпеки цих маршрутів на льоту на даному етапі використовуються сигнальні повідомлення NHRP про рух (перенаправляють та використовують короткі шляхи) з вузла зв'язку.

Переваги використання DMVPN є такими:

- спрощена конфігурація маршрутизації;
- підтримка динамічного розгортання кінцевих вузлів за допомогою NHRP;
- низькі адміністративні витрати;
- підтримка QoS;
- висока масштабованість та доступність [4].

Розглянемо дані переваги дещо детальніше. У DMVPN не потрібні кілька тунельних інтерфейсів для кожної гілки (клієнта) VPN. Замість цього проста конфігурація вузла і користувачів забезпечує мережеве підключення на вимогу з динамічною маршрутизацією та багатоадресною IP-адресою. DMVPN також підтримує розгортання "Zero Touch", щоб додати більше віддалених сайтів. Ця спрощена, масштабована топологія ідеально підходить для організацій, яким потрібне зашифроване підключення до глобальної мережі між віддаленими сайтами, включаючи мереж типу SOHO, мережі середнього та великого розміру. За допомогою DMVPN і NHRP можна розгортати користувачів за допомогою

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

динамічно призначених публічних IP-адрес. Кожен клієнт може створити VPN-тунель з іншими, знайшовши їх загальнодоступні IP-адреси . DMVPN спрощує топологію WAN-мережі, зменшуючи витрати на конфігурування. Не потрібно налаштовувати крипто-карти, прив'язані до фізичного інтерфейсу, або вносити зміни в центрі, щоб додати більше користувачів. Крім того, централізовані зміни конфігурації в хабі контролюють поведінку розділеного тунелювання, що ще більше спрощує конфігурацію та знижує витрати .

DMVPN підтримує численні механізми розширеної якості обслуговування (QoS), включаючи формування трафіку в інтерфейсах вузла за принципом Per-Spoke/Per-Spoke-Group, а також політику QoS Hub-to-Spoke/Spoke-to-Spoke. Також підтримує динамічні політики якості обслуговування QoS, які автоматично приєднують шаблони QoS до тунелів у міру їх встановлення [1].

DMVPN інтегрує шифрування в систему балансування навантаження сервера або поширюється на виділені головні VPN-маршрутизатори. Є можливість масштабуватися до тисяч користувачів з ієрархічним розгортанням вузла для більшої масштабованості. Щоб підвищити продуктивність, тунелі розподіляються між доступними вузлами.

DMVPN також забезпечує підвищену безпеку для під мереж кінцевих користувачів, підтримуючи сполучні маршрутизатори, які виконують трансляцію мережних адрес (NAT) або розміщені за динамічними пристроями NAT. Він також забезпечує ефективний і масштабований розподіл трафіку "One-to-Many" і " Many-to-Many" з підтримкою багатоадресного IP-трафіку між користувачем та вузлом .

Якщо порівнювати технологію DMVPN із звичайною VPN, то перша забезпечує багато переваг, включаючи наступні переваги: високу швидкість мережі і характерна надійність, покращення зв'язку між філіями за рахунок інтеграції VPN в існуючі методи комунікації, збереження пропускної здатності WAN та підвищена стійкість і резервування мережі [1].

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Також існує розширення технології DMVPN – технологія FlexVPN, яка ще має назву як четверта фаза DMVPN. За своєю суттю FlexVPN створена на тих же фундаментальних технологіях як і DMVPN, але має певні відмінності.

FlexVPN — це структура конфігурації (набір команд CLI/API), спрямована на спрощення налаштування віддаленого доступу, топологій «сайт-сайт» і DMVPN. З точки зору технології, FlexVPN — це спосіб налаштування IKEv2 [RFC] від Cisco[2]. Більшість конфігураційних команд починаються з `crypto ikev2` «розумних налаштувань за замовчуванням», які представляють погляд Cisco на найкращий дизайн. Конфігурація динамічного тунелю була спрощена, тому теоретично вам потрібен лише один шаблон інтерфейсу на сайті Hub, щоб дозволити всі типи вхідних VPN-з'єднань. Однак у цій публікації ми зосередимося на розгортанні FlexVPN DMVPN, тому для стислості та мінімізації кількості випадків, коли слово «VPN» з'являється в цій публікації, я буду називати цю технологію просто FlexVPN.

За своєю суттю FlexVPN – це те саме, що і DMVPN. З'єднання між пристроями все ще залишаються тунелями GRE «точка-точка», зв'язок «спокійний зв'язок» все ще досягається за допомогою повідомлення перенаправлення NHRP, маршрутизатори IOS навіть запускають один і той самий код NHRP як для DMVPN, так і для FlexVPN, що також означає, що обидва є власними технологіями Cisco. Однак є деякі серйозні відмінності:

Тунелі P2P GRE тепер є або статичними (спікер-концентратор), або віртуальним доступом (концентратор-то-спік і спікер-то-спік) інтерфейсами. На відміну від mGRE, який був просто синтаксичним цукром для набору тунелів P2P GRE, інтерфейси віртуального доступу дозволяють нам точно побачити, яка конфігурація конкретного P2P-тунелю (за допомогою спеціальної команди `show derived-config interface Virtual-Access X`).

Якщо традиційна конфігурація «крипто» DMVPN була лише варіантом, то FlexVPN тепер сильно пов'язаний з конфігурацією IPSec. Однак це дозволяє значно спростити використання NHRP, оскільки більше не потрібно виконувати реєстрацію Spoke на Hub.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

FlexVPN використовує новий протокол керування ключами – IKEv2, тоді як більшість традиційних мереж DMVPN використовують IKEv1. IKEv2 дозволяє детальну конфігурацію налаштувань QoS, ZBF і VRF без необхідності покладатися на інші протоколи, як це було з QoS NHRP і DMVPN для кожного тунелю[2].

З FlexVPN є лише один стандартний спосіб операцій NHRP і протоколів маршрутизації, а не 3 фази DMVPN.

Все вищесказане вказує на те, що FlexVPN є кращим варіантом порівняно з DMVPN. Існує також низка презентацій Cisco Live, що містять більш детальне, навіть дещо сумнівне, порівняння за функціями різних технологій VPN, усі віддаючи перевагу FlexVPN

Однією з найважливіших речей у оволодінні будь-якою технологією є вміння розкласти її на найдрібніші частини та зрозуміти їхню взаємодію. З FlexVPN є два найважливіші будівельні блоки:

- Конфігурація IPsec IKEv2
- Конфігурація тунельного інтерфейсу

Як зазначалося раніше, у FlexVPN є два типи тунелів – статичні VTI і віртуальні шаблонні тунелі. Перший використовується в маршрутизаторі Spoke для визначення статичного тунелю до концентратора і в будь-якому іншому випадку, коли буде достатньо статичних тунелів (наприклад, міжконцентровий тунель у подвійних хмарних топологіях). Статичні тунелі VTI налаштовуються точно так само, як і будь-який інший тунель P2P GRE.

Інший тип, Virtual-template, схожий на VPDN. Віртуальний шаблон — це буквально шаблон, з якого Hub створює (створює копію) іншого інтерфейсу — Virtual-Access щоразу, коли надходить запит від одного з Spokes. Цей інтерфейс не прив'язаний до жодного джерела чи місця призначення і на нього посилається пізніше з конфігурації IKEv2. Його потрібно налаштувати на центральному маршрутизаторі (щоб створити екземпляр Tunnels to Spokes), а також на Spokes (щоб дозволити тунелі Spoke-to-Spoke).

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Найважливішою частиною конфігурації IKEv2 є криптопрофіль. Тут ви визначаєте свій локальний ідентифікатор IKEv2, метод автентифікації, який використовує кожна сторона (з IKEv2 віддалена та локальна автентифікація можуть відрізнятися), правила відповідності вхідних запитів, який інтерфейс віртуального шаблону використовувати та який метод авторизації використовувати. Цей криптопрофіль прив'язаний до вихідного інтерфейсу за допомогою tunnel protection ipsecкоманди. Існує також ряд додаткових елементів конфігурації, які можуть або не можуть використовуватися залежно від загального дизайну. Ці елементи включають:

- Конфігурація інфраструктури PKI;
- Конфігурація AAA та політики авторизації для застосування індивідуальних налаштувань до кожного нового інтерфейсу віртуального доступу
- Пропозиції та політики IKEv2 (еквівалент налаштувань IKEv1 фази 1)

За допомогою топології з двома концентраторами можна розгорнути їх в одній підмережі в так званій топології з подвійним концентратором і однією хмарою. Spokes-маршрутизатор буде використовувати «блок конфігурації клієнта», який дозволяє йому динамічно вибирати тунельні адреси джерела та призначення на основі IP SLA та об'єктів відстеження або спробувати їх послідовно.

Деякі з плюсів і мінусів описано в прикладі конфігурації Cisco. Ось деякі важливі особливості, на які варто звернути увагу.

Гнучкість – за допомогою топології подвійної хмари трафік може бути перенаправлений до обох концентраторів на основі політик маршрутизації, визначених на Spoke, таким чином досягаючи певного рівня розподілу навантаження трафіку.

Складність – топологію однієї хмари може здатися легше налаштувати, оскільки вона покладається на вбудований у IKEv2 механізм виявлення мертвих однорангових (DPD) для перемикання збоїв Hub і не вимагає окремого інтерфейсу тунелю для другого Hub. Однак початкова простота швидко зникає, коли ви додаєте повторну активацію, відстеження однорангового зв'язку та IP SLA для

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

детермінованого вибору концентратора. Також можна зробити, щоб протоколи динамічної маршрутизації поклалися на таймери DPD з мінімальними налаштуваннями конфігурації (як я продемонструю в наступній публікації), що робить топологію подвійної хмари такою ж простою (з точки зору перемикання збоїв концентратора), як і однохмарну топологію.

Технічне обслуговування. Коли резервний концентратор стає недоступним (через втрату з'єднання WAN або зміну конфігурації) у топології з подвійною хмарою, це стає відразу очевидним на всіх інших пристроях (тунельний інтерфейс виходить з ладу), тоді як у топології з однією хмарою (навіть з відстеженням IP SLA) ви ніколи не можете гарантувати, що конфігурація резервного концентратора не змінилася, і перехід на помилку буде успішним.

Це може здатися досить очевидним на поверхні. Звичайно, PKI є більш гнучким рішенням і дає змогу детально керувати списями за допомогою протоколу Simple Certificate Enrollment Protocol (SCEP) і списків відкликання сертифікатів (CRL). Додайте до цього той факт, що сервер СА можна легко налаштувати на будь-якому маршрутизаторі IOS, і взагалі не повинно бути причин використовувати попередньо спільні ключі. Однак є ще один дуже важливий аргумент для PKI, специфічний для FlexVPN, і він стосується функції конфігурації на спиці.

Коли PKI не використовується у нас є лише ідентифікатор IKEv2 (FQDN або адреса електронної пошти) для кодування специфічних атрибутів (наприклад, пропускна здатність каналу WAN). Той самий ідентифікатор IKEv2 потрібно використовувати для збігу вхідних запитів у криптопрофілі і, отже, має бути унікальним. Не існує гарного та масштабованого способу досягнення обох цих цілей, і єдиний спосіб, який я знаю, вимагає змін конфігурації на всіх пристроях FlexVPN щоразу, коли вводиться нова пропускна здатність каналу WAN.

За допомогою PKI ми можемо використовувати будь-яке поле всередині сертифіката X.509 для виконання запитів зіставлення та авторизації. Наприклад, ім'я суб'єкта може містити унікальний ідентифікатор мовлення, а організаційний підрозділ може кодувати пропускну здатність каналу («10 Мбіт/с»). FlexVPN Hub

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідатиме вхідному запиту на основі «asme.com» і авторизує його (наприклад, призначає параметри QoS) на основі значення OU.

Деякі сайти можуть мати додаткові вимоги до високої доступності WAN-посилань. Існують різні способи задовольнити цю вимогу залежно від режиму HA.

Active/Standby – найпростіший спосіб перемикання збоїв у режимі активного/резервного режиму як для Hub, так і для Spoke – це використовувати згаданий раніше «блок конфігурації клієнта». Це дозволяє прив'язати об'єкти відстеження як до адреси джерела тунелю, так і до адреси призначення та зробити їх вибір динамічним. Якщо Hub має подвійні WAN-лінії в цьому режимі, обидва канали повинні знаходитися в одному FVRF, а додаткове відстеження має бути прив'язане до статичних маршрутів за замовчуванням.

Активний/неактивний – єдиний спосіб розподілити навантаження трафіку – це мати два окремих маршрутизатора (або розділити існуючий маршрутизатор на кілька VRF), встановити суміжність маршрутів по обох каналах і керувати трафіком за допомогою засобів, доступних протоколом маршрутизації. За замовчуванням розподіл трафіку між двома каналами буде статичним, проте динамічну поведінку можна ввести за допомогою таких технологій, як Performance Routing (PfR).

FlexVPN дозволяє змінювати конфігурацію кожного тунелю за допомогою політики авторизації AAA. Найбільш гнучким рішенням є використання Radius-сервера, який повинен бути розміщений разом із кожним хабом і призначати специфічні налаштування Spoke за допомогою атрибутів AAA. Наприклад, Radius-сервер може повернутися ip:interface- config="bandwidth qos-reference 5000", якщо сертифікат X.509 містить «5Mbps» у полі OU, і це значення буде призначено новоствореному інтерфейсу віртуального доступу[2]. Використовуючи атрибути радіусу, також можна змінити конфігурацію на маршрутизаторі Spoke, наприклад, натиснути статичний маршрут хоста для IP-адреси тунелю віртуального шаблону Hub.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Якщо виділений радіус-сервер недоступний, авторизацію AAA можна налаштувати локально на маршрутизаторі-концентраторі. Однак це означає, що всі атрибути радіусу мають бути попередньо налаштовані на всіх пристроях, що робить оновлення конфігурації та обслуговування громіздкими для середнього масштабованого розгортання.

Конфігурація QoS в топологіях DMVPN завжди була проблемою. На жаль, це все ще стосується FlexVPN. Немає «приємного» рішення, яке б врахувало всі сценарії перевантаження. Однак існує ряд речей, які можна зробити, щоб полегшити деякі з найгірших наслідків перевантажень WAN-каналів:

Налаштуйте формувач класу за замовчуванням на фізичному інтерфейсі. Це обмежить загальну пропускну здатність каналу WAN і забезпечить верхню межу для всіх політик QoS в тунелі. Зауважте, що згідно з поточними застереженнями, ви не можете налаштувати CBWFQ на цьому інтерфейсі, і будь-які наступні зміни QoS на фізичному інтерфейсі вимагатимуть відключення всіх тунелів (закриття/вимкнення).

Інтерфейс тунелю може мати стандартний вкладений формувач CBFQ з qos pre-classify командою. Якщо пропускну здатність тунелю не визначена явно (через bandwidth або bandwidth qos-reference команди), він успадковує свою пропускну здатність від значення для формування класу за замовчуванням фізичного інтерфейсу. Це означає, що кілька тунелів можуть легко передплатити канал WAN, і в такому випадку всі інтерфейси отримають рівну частку пропускну здатності фізичного каналу, незалежно від їхніх власних вимог до пропускну здатності (незважаючи на справедливий черга). Це одне з найбільших застережень дизайну QoS FlexVPN, і, наскільки мені відомо, для цього не існує рішення. «Найкращим» рішенням, яке я чув досі, було «не передплачувати» послання WAN. Якщо буде достатньо інтересу, я можу написати додаткову публікацію з описом деталей того, як QoS для кожного тунелю реалізовано в DMVPN і FlexVPN.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Окрім технологій DMVPN від компанії Cisco існують схожі рішення від інших розробників. Так, наприклад, компанія Huawei розробила технологію розумного динамічного VPN (DSVPN, Dynamic Smart VPN), яка ідентична DMVPN, завдяки чому їх часто використовують разом у випадках, коли неможливо забезпечити використання пристроїв лише однієї компанії [5]. Також існує рішення DMVPN на платформі Vyatta, для якої спільнота розробників створила власну реалізацію протоколу NHRP з відкритим кодом, назвавши його OpenNHRP. Цей проект не є повністю закінченим рішенням, але показує можливості відкритої реалізації фірмових складових технології DMVPN. Код проекту доступний через SourceForge.

1.3 Аналіз вразливостей мереж на базі технологій DMVPN

Хоча використання багатьох протоколів забезпечує високий рівень модульності та гнучкості, з іншого боку збільшує вразливість усієї мережі та кожного протоколу який використовують у DMVPN. Серед цих загроз можна виділити найбільш розповсюджених у використанні зловмисниками:

- Перенаправити всі повідомлення на комп'ютер хакера;
- Нанести шкоду серверам мережі шляхом фальсифікації або зриву передачі пакетів (повідомлень);
- Можливість проникнути в корпоративну мережу як законне обладнання та отримати доступ до конфіденційних ресурсів;
- Дозволити розшифровку частини повідомлень які були захищені механізмами шифрування.[11]

Так наприклад IPsec, який є основним протоколом технології DMVPN, незважаючи на високий рівень безпеки, він залишається вразливим до певних типів атак, спрямованих на порушення доступності тунелів DMVPN і надання додаткових затримок, які можуть зробити деякі транспортовані потоки непридатними. Незважаючи на його надійність з точки зору шифрування, IPsec можна легко використати для дешифрування певних повідомлень, які мають бути захищені ESP, це складне завдання, але воно також здійсненне для повторюваних повідомлень, насправді деякі протоколи та програми генерують ті самі дані, прикладом є

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

повідомлення «Оголошення маршрутизатора» протоколу IPv6, відстань Хеммінга, іншими словами, кількість різних бітів між пакетами мала або нульова, особливо для додатків на основі протоколів UDP або IP.

Наступним прикладом може бути протокол керуючих повідомлень Інтернету (ICMP) який відповідає за сигналізацію у IP-мережі. Знаючи, що IP є ненадійним і неорієнтованим протоколом з'єднання, тобто він не забезпечує жодного підтвердження для переданих даних, важливо забезпечити безперебійне функціонування мережі. і сповіщати обладнання у разі збою доставки. ICMP виконує ці завдання, наразі існує дві версії ICMP, для IPv4 і IPv6, повідомлення ICMP класифікуються за двома категоріями: повідомлення про помилки та повідомлення керування. Протокол ICMP можна використовувати як вектор атаки проти загроз IPsec: Влаштувати збій продуктивності всієї мережі шляхом зменшення або збільшення MTU шляху. Використовуючи цей механізм, зловмисник може провести атаку на відмову в обслуговуванні або зменшити пропускну здатність між обладнанням DMVPN.

Ще одну вразливість має протокол GRE, який дозволяє інкапсулювати кілька повідомлень у вигляді одноадресних, багатоадресних і широкомовних повідомлень різних протоколів IP, IPX і AppleTalk в IP-пакет [11]. Незважаючи на те, що сьогодні він широко поширений завдяки своїй ефективності та простоті з точки зору розгортання, він страждає від тих самих обмежень, що й протокол IP, щодо безпеки, таких як конфіденційність, цілісність та автентифікація. GRE розгортає механізм автентифікації, але цей механізм залишається надто слабким проти атак за словником або грубої сили. Тунель GRE є ключовим компонентом у термінології мережі DMVPN, він може бути як «точка-точка», так і «точка-багатоточка», у першому випадку адреси шлюзів повинні бути призначені статично, у другому випадку, багатоточка-точка, IP-адреси можуть бути динамічними, їх виявлення здійснюється за протоколом NHRP. Відсутність механізмів конфіденційності та розрахунку цілісності дає хакерам можливість перенаправляти встановлені тунелі, підробляти пакети та вставляти їх як законні пакети або запобігати зв'язку між станціями, що належать до різних сайтів або навіть в межах одного сайту.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Як і протокол ARP, протокол NHRP базується на кеш-пам'яті для зберігання зіставлення адрес тунелю та пов'язаних із ними загальнодоступних адрес кожного обладнання, що належить до однієї хмари DMVPN, що означає, що цей протокол уразливий передусім для двох типів атак: відмова в обслуговуванні та отруєння NHRP. Отруєння кешу NHRP полягає у зміні динамічних записів або додаванні нових у кеші резолвера на NHC або NHS [9]. Ця атака зазвичай використовується для перенаправлення трафіку від одного сайту до іншого посередника, часто сайту хакера, щоб досягти успіху в цій атаці. хакер повинен знати ідентифікатор хмари NHRP і використані рядки автентифікації тунелю. На жаль, останні вразливі до атак грубої сили та словникових атак, насправді довжина ключа автентифікації NHRP не може перевищувати 8 символів, це полегшує завдання для хакера, який може провести розподілену атаку, щоб швидко зламати рядки автентифікації.

1.4 Технічне завдання.

Після розгляду теорії можемо зробити певні висновки та розробити технічне завдання проекту призначенням якого буде захист мережної інфраструктури підприємства для збору, зберігання, зв'язку між робочими станціями та перегляд інформації та дії персоналу та інших осіб.

В мережі буде використовуватися два види робочих станцій:

- Клієнтська, яка буде отримувати через мережу доступ до інших робочих станцій і через віддалений доступ до головної робочої станції.
- Головна(сервер), яка містить всі основні ресурси мережі і доступна лише користувачам, яким надано доступ.

При розробці мережі потрібно одразу логічно її структурувати. Дана підсистема буде складатися з декількох LAN та окремої підмережі з сервером також для кожної LAN має бути можливість масштабованості в майбутньому.

Для кожної локальної буде використовуватися таке обладнання як: робочі станції, комутатори, маршрутизатори (DHCP-сервера, Branch\HUB DMVPN).

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Обладнання та програмне забезпечення будуть наступними:

- Cisco 4000 Series Integrated Services Routers
- Маршрутизатор MikroTik hEX PoE (RB960PGS)
- Робочі станції під управлінням windows 7/8/xp linux/ununtu/centOS

Таблиця 1.1 - Параметри LAN

Назва мережі	Кількість робочих станцій	DHCP-сервер	DMVPN
LAN A	3 робочі станції і сервер (Можливість додавання робочих станцій)	Сервер під керуванням Windows 10 Server	Маршрутизатори використовуються як головний та резервний Hub
LAN B	2 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор	Маршрутизатор використовується як Branch
LAN C	3 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор	
LAN D	2 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор	Маршрутизатор використовується як Branch
LAN E	3 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор	

1.5 Висновки до розділу 1.

Під час написання першого розділу було проведено аналіз теоретичних відомостей які надали характеристики організації приватних віртуальних мереж. Проаналізували основні переваги протоколів на яких на даному моменті працюють технології DMVPN. Під кінець було розглянуто приклади вразливостей безпеки у технологій багатоточкових динамічних віртуальних приватних мереж. Також розробили технічне завдання.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО МЕРЕЖНОГО ОБМІНУ НА БАЗІ ТЕХНОЛОГІЙ DMVPN

2.1 Проектування мережної інфраструктури

На підставі попереднього розділу де було розібрано теорію та механізми впровадження ми моделюємо практичний механізм реалізації технології DMVPN з протоколами HSRP для захищеної корпоративної мережі в деякій організації. Проектування та моделювання виконано за допомогою Graphical Network Simulator-3. Ми створили центральний сервер у головному офісі та створили дві філії. Головний сервер підключено до однієї локальної мережі з двома концентраторами через комутатор, а два концентратори підключено до Інтернету, який надає постачальник послуг Інтернету (ISP). У філіях дві різні міські філії підключені до Інтернету, і філії мають своїх клієнтів з однаковою мережевою локальною мережею.

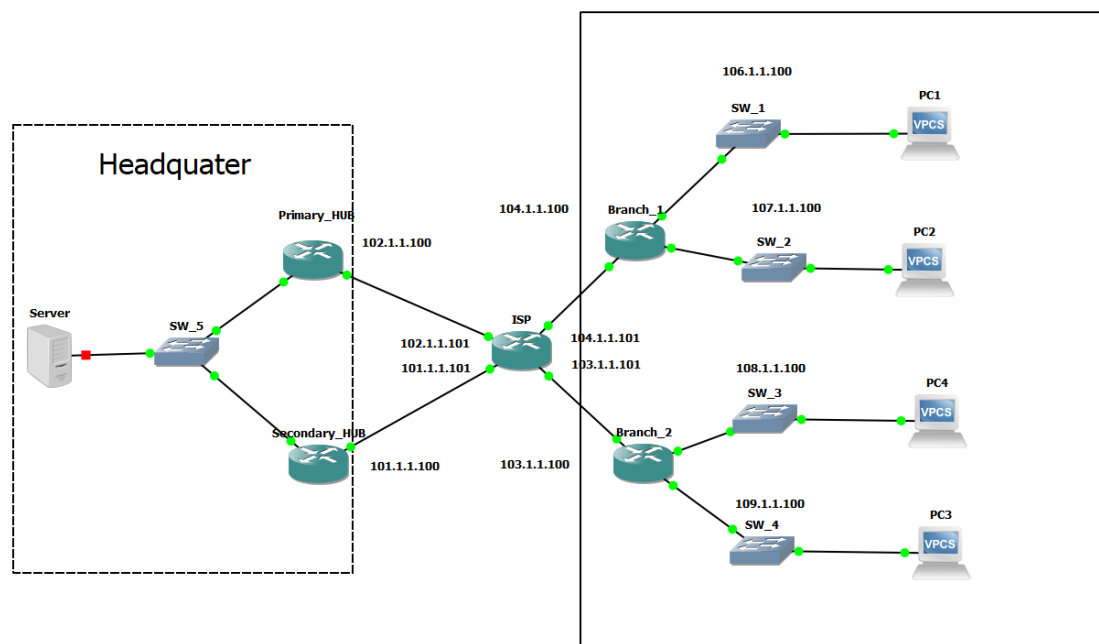


Рисунок 2.1 – Загальна топологія мережі

Вся топологія розроблена в програмному забезпеченні GNS3, вся команда інтерфейсу з зображенням організована крок за кроком. Для кращого розуміння ми розділили всю топологію на дві частини

- 1) Кінцева топологія штаб-квартири.
- 2) Топологія кінця гілок.

В кінцевій топології штаб-квартири буде налаштована топологія мережі для цієї дослідницької мети, метод проектування описано крок за кроком. Перш за все, ми встановили один iso-файл сервера та два iso-файли маршрутизатора в gns3 і підключили обидва маршрутизатори до порту сервера через послідовний кабель. зображення показано на малюнку.

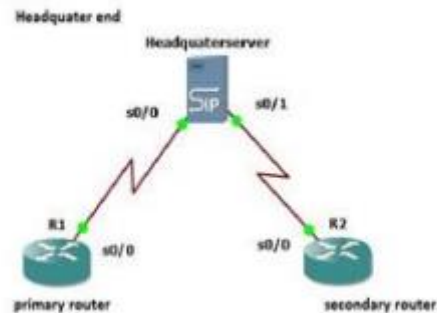


Рисунок 2.2 – Топологія штаб-квартири

Топологія мережі, показана вище, налаштовується за допомогою команди Cryptographic, GRE tunnel, профілю NHRP і протоколів маршрутизації в GNS3 (Graphical Network Simulator 3).

В топології кінця гілок кожна філія підключена до зацікавленого маршрутизатора постачальника послуг Інтернету, який є шлюзом для досягнення головного місця призначення. Кінцева топологія гілок показана нижче, гілки підключені до ISP через послідовний кабель.

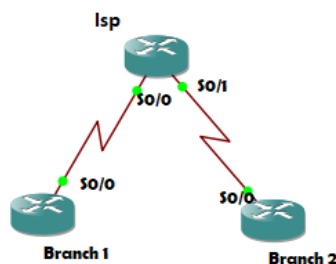


Рисунок 2.3 – Топологія кінцевих гілок

Топологія мережі, показана вище, налаштована за допомогою команди Cryptographic, тунелю GRE, профілю NHRP і протоколів маршрутизації для гілок, що підтримуються на GNS3

2.2 Проектування тестування оцінки безпеки комп'ютерної мережі

Після того як ми спроектували топологію нашої корпоративної мережі, її схему та механізми її реалізації нам потрібно також потрібно спроектувати тести нашої DMVPN. Точні етапи тесту на проникнення залежатимуть від типу VPN, який використовується. Незалежно від типу, оцінку безпеки (тестування) VPN можна навести наступною схемою.

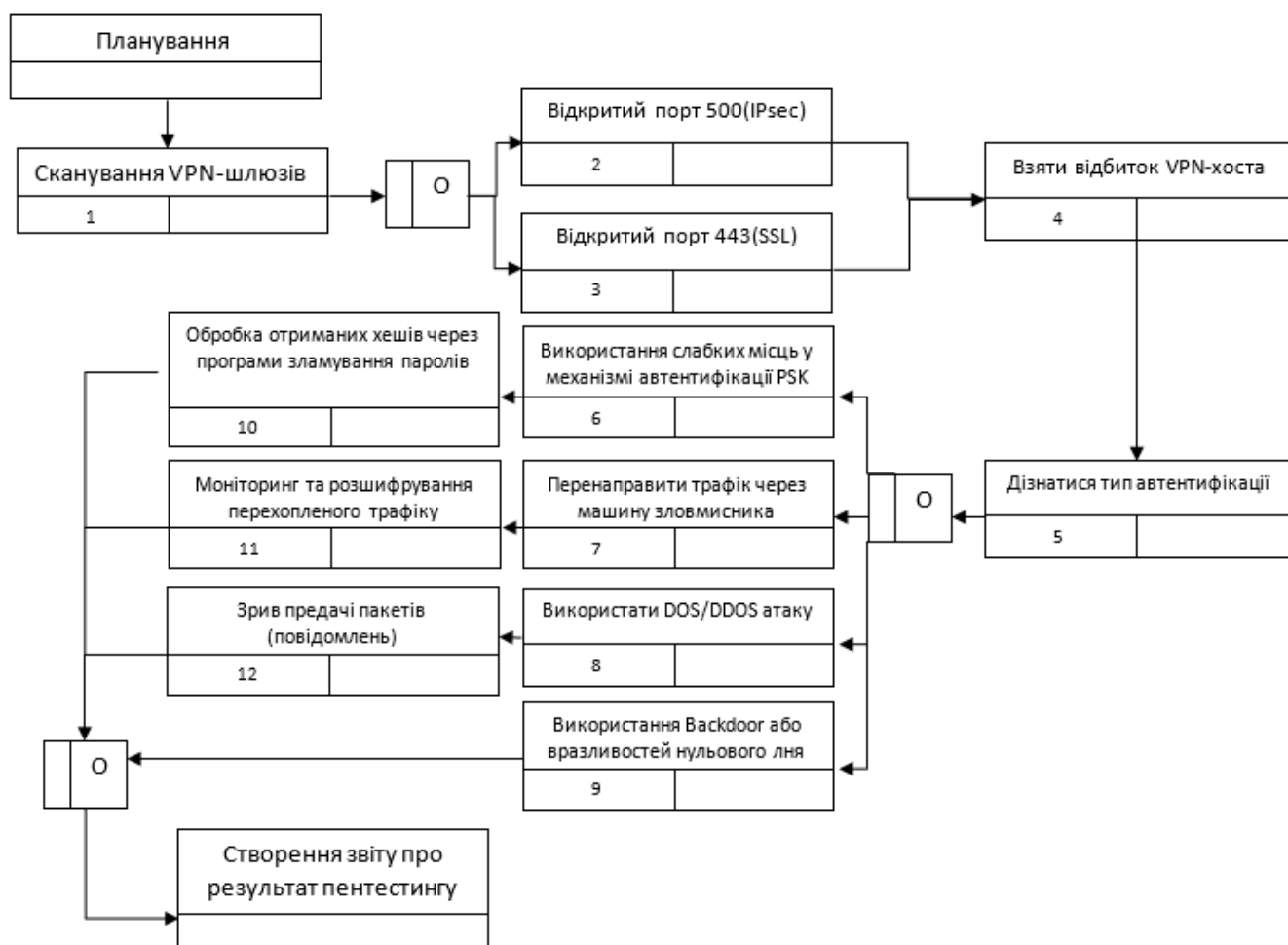


Рисунок 2.4 – Побудована IDEF0 діаграма по пентестингу VPN

Тестування починається з планування. Цей крок задає тон решті діяльності. Основна увага повинна бути зосереджена на визначенні обсягу та реалістичних термінів із чітким розподілом наших дій.

Наступним кроком є сканування VPN-шлюзів. Сканування портів допомагає ідентифікувати тип VPN. Оскільки ми вже знаємо, де знаходиться наша DMVPN

мережа, можна швидко спрямувати свій інструмент сканування на певний діапазон IP-адрес, а не на всю мережу. Тип VPN можна визначити, перевіривши список відкритих портів. Для сканування шлюзів VPN, прийнято використовувати nmap або ike-scan які ми розглянемо більш детально.

Після сканування ми можемо встановити рукописання зі шлюзом VPN, де можемо провести зняття відбитків пальців пристрою, щоб повернути таку інформацію: постачальник/виробник і модель, версія програмного забезпечення. Отримана інформація використовується для ідентифікації атаки на постачальника або точного налаштування загальної атаки. Якщо VPN розміщено на брандмауері, відбитки пальців також ідентифікують брандмауер, який використовується.

Основна причина полягає в тому, що IKE не гарантує надійність переданих пакетів, більшість постачальників шлюзів VPN використовують власний протокол для роботи з трафіком, який виглядає втраченим. Цей інструмент надсилає тестові пакети IKE до шлюзу VPN, але не відповідає на отриману відповідь. Сервер відповідає так, ніби пакети були втрачені, і реалізує свою стратегію відстрочки, щоб повторно надіслати пакети. Аналізуючи різницю в часі між пакетами та кількість повторних спроб, можна визначити відбиток постачальника та дізнатися модель та версію ОС машини жертви.[15]

Після того як було зрозуміло за допомогою типу автентифікації модель та версії операційної системи обладнання жертви ми маємо декілька сценаріїв дій: використати слабкі місця у механізмі автентифікації PSK, спробувати перенаправити весь трафік через машину зломисника та спробувати розшифрувати або частково розшифрувати зашифрований трафік, провести DOS/DDOS для зриву передачі пакетів, або використати іншу вразливість яка доступна саме на певному обладнанні та на певній версії.

В першому сценарії будемо пробувати захопити попередньо надані ключі. Це можливо, оскільки агресивний режим IPSec не захищає попередні спільні ключі. Облікові дані автентифікації надсилаються як відкритий текст, який можна захопити, а потім зламати за допомогою офлайн-інструментів.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Перш ніж зламати отриманий хеш спільного ключа за допомогою офлайн-інструменту потрібно буде відредагувати вихідний файл, щоб включати лише значення хешу (він має містити дев'ять значень, розділених двокрапками).

В другому сценарії буде використано вразливості у протоколах ARP, NHRP, а саме атаки типу MitM. Спочатку хакер надсилає підроблені пакети, які пов'язують MAC-адресу зловмисника з IP-адресою обладнання, який уже є в локальній мережі, після хакер змінює таблицю маршрутизації компанії, щоб вона містила фальсифіковані карти MAC.

В третьому сценарії ми можемо спробувати перевантаживши ціль або навколишню інфраструктуру заради того щоб завдати збитки компанії через так званий простій.

Також використовують відомі уразливості які ґрунтуються на результатах попереднього етапів тестування. Цей крок зосереджується на використанні виявлених уразливостей або уразливостей нульового дня, які необхідно б негайно виправити але з тих чи інших причин вони не були виправлені (наприклад через складність будови протоколів). Одним з прикладом таких вразливостей можна назвати атаку яка націлена на реалізацію рукостискання IKE та використовується для VPN-з'єднань на основі IPsec, відкриваючи двері для атак MiTM або для зловмисників для доступу до даних, що передаються в сеансах VPN. Нова криптографічна атака Bleichenbacher oracle була випущена в усьому світі, використовуючи помилку протоколу 20-річної давності для компрометації протоколу Internet Key Exchange (IKE), який використовується для захисту IP-зв'язку. Зокрема, атака спрямована на реалізацію рукостискання IKE, яка використовується для VPN-з'єднань на основі IPsec. Зловмисники можуть скористатися цією вразливістю, щоб отримати ключі сеансу IKEv1 і розшифрувати з'єднання, що зрештою відкриває двері для атак типу «людина посередині» (MitM) або для доступу зловмисників до даних, що передаються в сеансах VPN. Наслідки можуть бути далекосяжними; Як відомо, VPN дозволяють співробітникам отримувати безпечний доступ до корпоративної мережі, коли вони знаходяться поза

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

офісом. Методика, розкрита групою академічних дослідників з Рурського університету Бохума, Німеччини та Університету Ополя, Польща, передбачає повторне використання пари ключів у різних версіях і режимах IKE, що може призвести до обходу міжпротокольної автентифікації. Це дозволяє зловмиснику підробити цільову кінцеву точку IPSec і зрештою зламати механізм шифрування. Атака охоплює всі доступні механізми автентифікації IKE. Атаки базуються на Bleichenbacher oracle – протокольний загрози 20-річної давнини, яка роками використовувалася для порушення конфіденційності TLS при використанні з шифруванням RSA. Тепер дослідники виявили, що ці ж оракули можна дуже ефективно використовувати для розшифровки одноразових кодів, які порушують аутентифікацію, зашифровану за допомогою RSA, у фазі 1 IKE. Крім того, документ показує, що їх можна використовувати для підробки цифрових підписів, що порушує автентифікацію на основі підпису на етапі 1, а на фронті PSK можливі офлайн-словникові атаки, на думку дослідників, завершуючи компроміси захисту.

Для Cisco недолік існує у її флагманській операційній системі Internetworking Operating System (IOS), яка працює на більшості маршрутизаторів і комутаторів, а також у її відгалуженні на базі Linux, IOS XE, якщо ввімкнено параметр «автентифікації rsa-encr». Інша гілка операційної системи, IOS XR, використовується для інфраструктури операторського рівня, і це не впливає. Уразливість існує через те, що уражене програмне забезпечення неправильно реагує на збої дешифрування. Зловмисник може використати цю вразливість, надсилаючи створені зашифровані тексти на пристрій, налаштований за допомогою IKEv1, який використовує одноразові коди з шифруванням RSA, — пояснила Cisco у своєму пораді щодо безпеки. З боку Huawei проблема стосується реалізацій IPSec IKEv1 продуктів Huawei Firewall. Віддалені зловмисники можуть розшифрувати дані зашифрованого тексту тунелю IPSec, використовуючи оракул заповнення RSA Bleichenbacher. Успішне використання цієї вразливості може вплинути на безпеку тунелю IPSec. Відомо, що атака впливає на впровадження IKEv1 від Cisco (CVE-2018-0131), Huawei (CVE-2017-17305), Clavister (CVE-2018-8753, Clavister cOS

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Core) і ZyXEL (CVE-2018). -9129, ZyWALL/USG). Команда науковців раніше приватно розкрила проблему чотирьом постачальникам. Однак всі версії та варіанти протоколу IKE IPsec можуть бути зламані, якщо присутні слабкі PSK і Bleichenbacher oracle у варіантах IKEv1 PKE і RPKE – таким чином, це може вплинути на більше реалізацій у основних операційних системах і мережевих пристроях, в залежності від конфігурації.

Та завершує тестування звіт. Як і будь-яке інше тестування на проникнення, у звіті підсумовуються результати та перераховуються пункти дій, які мали бути виконані. Ці пункти дій допоможуть команді або тестувальнику з тим, що їй потрібно зробити для виправлення виявлених вразливостей.

2.3 Засоби тестування безпеки комп'ютерної мережі

Тепер коли ми розробили план тестування нам потрібно вибрати засоби якими ми будемо проводити тестування.

Першим в наше використання можна записати Nmap, який стає корисним під час тестування на проникнення в мережу. Даний додаток не лише надає інформацію про мережу, але й допомагає виявити проблеми безпеки в системі. Nmap не залежить від платформи та може працювати на різних стандартних операційних системах, включаючи Linux, Windows, macOS і BSD. Він простий у використанні та містить як інтерфейс командного рядка (CLI), так і графічний інтерфейс користувача (GUI). Деякі із завдань, які може виконувати nmap:

- Виявлення підключених хостів у мережі
- Аналіз вільних портів на цільовому хості
- Виявлення запущених служб у системі разом із номером версії
- Виявлення вразливостей мережі та системних лазівок [15]

Процес сканування мереж складається з трьох етапів, причому Nmap виконує перші два етапи, а третій залишається хакеру В першому етапі Nmap надсилає необроблені IP-пакети, щоб виявити доступні хости в мережній системі. Відповідно до конфігурації мережі, ці пакети потребують відповіді від комп'ютера

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

призначення. Наступному етапі ми отримуємо відповіді від цілі. Оскільки ці запити вимагають відповіді, хост надсилає відповіді, підсвічуючи порти, які можуть обмінюватися даними з іншими машинами. Відкриті порти надсилатимуть деякі відповіді, а закриті можна відфільтрувати, оскільки вони не матимуть відповіді. Останій етап складається з аналізу отриманих даних. Коли хакери отримують певну інформацію з боку цілі, вони повинні пройти через вразливі служби та відкрити порти. Після цього кроку можна переходити до третьої фази етичного хакерства, отримуючи доступ до машини-жертви.



Рисунок 2.5 – Принцип роботи утиліти Nmap

Nmap має безліч режимів роботи але найбільшими його перевагами будуть:

— Ping sweep – це просте сканування Nmap, яке перевіряє всі доступні IP-адреси, щоб побачити, які з них відповідають ICMP (Internet Control Message Protocol). Цей Ping Sweep чудово підходить для людей, яким потрібно знати кількість IP-адрес.

— Сканування SYN надсилає повідомлення SYN через TCP на всі цільові порти. Якщо система отримує підтвердження, порт відкрито. Відсутність відповіді означає закритий або що даний порт недоступний.

— Сканування TCP як і сканування SYN, воно використовує рівень TCP для надсилання пакетів на всі порти. Відмінність полягає в тому, що пакети підтвердження завершують з'єднання. Журнали можуть легко знайти сканування TCP і використовувати додаткову обчислювальну потужність.

— Сканування в режимі очікування - це сканування використовується, щоб перевірити, чи заплановані зловмисні атаки на мережу. Сканування Nmap переміщуються від порту для пошуку зловмисного програмного забезпечення. Однак зовнішньому хосту слід призначити IP-адресу та порт.

— Сканування Remote Procedure Calls (RPC) хакери використовують, щоб зробити системи вразливими до вірусних атак. Рекомендується періодично сканувати мережу на наявність команд RPC, оскільки ці процедури можуть виконуватися в системі та збирати дані.

— Сканування Windows: коли надходять пакети SYN, програма шукає в портах пакети підтвердження. Це сканування виявляє будь-які порушення в отриманих пакетах ACK і допомагає визначити, які порти не працюють.

— Сканування відмов - це сканування яке перевіряє безпеку рівня протоколу передачі файлів. Рівні FTP рідко приймають пакети, а якщо приймають, вони можуть бути перенаправлені на внутрішній рівень для доступу до комп'ютерів. Сканування відмов оцінює той самий недолік і визначає, чи є ваш рівень FTP вразливим.

— Сканування UDP - це сканування в основному ефективно в Windows, щоб перевірити, чи є рівень UDP вразливим. Не завжди важливо отримати відповідь від рівня UDP, але корисно знати, чи активні якісь троянські напади.

— FIN-сканування як і SYN-сканування, система, яка надсилає пакети, отримує здебільшого відповідь на пакет TCP FIN. Система, яка надсилає пакет RST, є помилковою тривоною, і користувачам не варто хвилюватися.

— Сканування NULL - це сканування є корисним для систем, відмінних від Windows, які можуть легко виявляти типи пакетів і реагувати відповідями TCP або NULL. Windows не може використовувати сканування NULL, оскільки вони не завжди працюють.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

В той час як ike-scan є сканером і тестовим інструментом безпосередньо для IPSec VPN який виявляє відбитки пальців і тестування систем IPSec VPN. Він створює та надсилає пакети IKE Phase-1 на вказані хости та відображає отримані відповіді. Програма надсилає запити IKE першої фази (основний режим або агресивний режим) на вказані хости та відображає всі отримані відповіді. Він обробляє повторні спроби та повторну передачу з відстрочкою, щоб впоратися з втратою пакетів. Це також обмежує пропускну здатність, яку використовують вихідні пакети IKE. ike-scan може виконувати такі функції:

— Виявлення, на якому з хостах у заданому діапазоні IP запущено IKE. Це робиться шляхом відображення тих хостів, які відповідають на надіслані запити IKE.

— Відбитки пальців визначає, яку реалізацію IKE використовують хости, і в деяких випадках визначте версію програмного забезпечення, яке вони використовують. Це робиться двома способами. По-перше, за допомогою UDP backoff fingerprinting, який передбачає запис часу пакетів відповіді IKE від цільових хостів і порівняння спостережуваного шаблону відстрочки повторної передачі з відомими шаблонами. По-друге, за допомогою відбитків пальців ідентифікатора постачальника, які порівнюють корисне навантаження ідентифікатора постачальника з серверів VPN із відомими шаблонами ідентифікатора постачальника.

— Перерахування перетворень знаходять, які атрибути перетворення підтримуються сервером VPN для IKE Phase-1 (наприклад, алгоритм шифрування, алгоритм гешування тощо).

— Перелік користувачів для деяких систем VPN знаходять дійсні логіни користувачів VPN.

— Злом попереднього спільного ключа виконує офлайн-словник або злом паролів грубою форсою для агресивного режиму IKE із автентифікацією попереднього спільного ключа. Тут використовується інструмент для отримання

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

хешу та інших параметрів, а також psk-crack (який є частиною пакета) для виконання злому.

Для виконання MitM-атаки можна використати безліч утиліт але нажаль безліч з них застайлі але утиліта Ettercap все ще отримує оновлення та нові функції.

Ettercap, інструмент створений Альберто Орнагі (ALoR) і Марко Валлері (NaGA), і в основному це пакет для атак людини посередині в локальній мережі. Він підтримує активну та пасивну дисекцію багатьох протоколів і містить багато функцій для аналізу мережі та хосту. Він здатний перехоплювати трафік у сегменті мережі, перехоплювати паролі та проводити активне підслуховування низки поширених протоколів. Ettercap використовує чотири моделі:

- IP пакети фільтруються на основі джерела та призначення;
- Фільтрація пакетів на основі MAC-адреси;
- Отруєння ARP використовується для перехоплення комутованих з'єднань локальної мережі (повний дуплекс). Загальнодоступний;
- Отруєння ARP використовується, щоб дозволити перехопити один хост будь-яким іншим хостом.

Експериментальний змішаний пакетний інжектор T50 (відомий також як F22 Raptor) — це інструмент, розроблений для виконання «стрес-тестування». Концепція почалася в 2001 році, відразу після випуску 'nb-isakmp.c', і головною метою було: - Наявність інструменту для виконання фаззера протоколу TCP/IP, що охоплює загальні регулярні протоколи, такі як: ICMP, TCP і UDP. Ситуація змінилася, і T50 став хорошим унікальним ресурсом, здатним проводити «Стрес-тестування» [19]. T50 був розроблений для виконання «Стрес-тестування» на різноманітних мережевих пристроях інфраструктури, використовуючи широко реалізовані протоколи, і після деяких запитів його було перероблено, щоб розширити тести (починаючи з версії 5.3), охоплюючи деякі звичайні протоколи (ICMP, TCP і UDP), деякі специфічні для інфраструктури протоколи (GRE, IPSec і RSVP) і деякі протоколи маршрутизації (RIP, EIGRP і OSPF).

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Висновки до розділу 2.

В другому розділі було спроектовано мережну інфраструктуру де ми розробили топологію мережі та розглянули кожну з підмереж. Також було спроектований план тестування безпеки мережі де ми розглянули різні етапи тестування та чотири сценарії тестування, а саме спробувати використати вразливість у механізмах PSK, спробувати виконати MitM-атаку зрадаи того щоб перенаправити трафік через машину хакера, влаштувати збій в мережі за допомогою DOS або DDOS атаки. В останньому підрозділі розглянули засоби тестування а саме Nmap, Ike-scan, Ettercap, T50.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДСИСТЕМИ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ

3.1 Налагодження віддаленого доступу.

Звернімо увагу на маршрутизатор ISP, який відіграє роль глобальної мережі задля економії ресурсів, Саме там якщо розширити її трохи більше буде знаходитись наш “герой”.

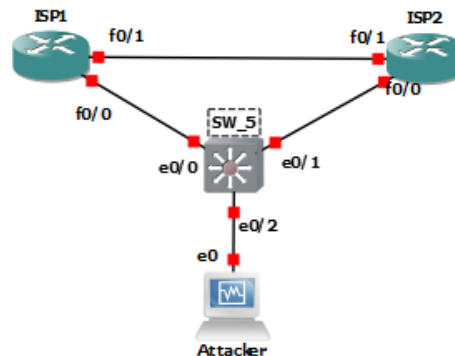


Рисунок 3.1 – Розширена топологія мережі ISP

З початку зловмисник розвідує топологію мережі за допомогою сканера Ike-scan. Під час сканування ми можемо отримати

```
(kali@kali)-[~]
$ sudo ike-scan -M -A 104.1.1.2
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
104.1.1.2    Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=8661bfed2b777852)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.383 seconds (2.61 hosts/sec). 0 returned handshake; 1 returned notify

(kali@kali)-[~]
$ sudo ike-scan -M -A 102.1.1.1
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
102.1.1.1    Notify message 14 (NO-PROPOSAL-CHOSEN)
HDR=(CKY-R=1f058aa8cff01d83)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.155 seconds (6.44 hosts/sec). 0 returned handshake; 1 returned notify
```

Рисунок 3.2 – сканування за допомогою ike-scan.

Під час сканування ми можемо отримати такий результат - “0 returned handshake; 1 returned notify” з чого можемо зробити висновок, що шлюзи VPN відповідають на нашій запит але жодне з них не прийняте. Так як наші запити не прийнятні, у такому випадку слід спробувати провести подальший аналіз і перебрати налаштування

наших повідомлень до серверу або клієнту. Перш за все вам потрібно створити всі можливі варіанти налаштування:

```
(kali@kali)-[~]
$ for ENC in 1 2 3 4 5 6 7/128 7/192 7/256 8; do for HASH in 1 2 3 4 5 6; do for AUTH in 1 2 3 4 5 6 7 8 64221 64222 64223 64224 65001 65002 65003 65004 65005 65006 65007 65008 65009 65010; do for GROUP in 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18; do echo "--trans=$ENC,$HASH,$AUTH,$GROUP" >> ike-dict.txt ;done ;done ;done ;done
```

Рисунок 3.3 – Створення скрипта для перебору всіх можливих трансформацій (налаштувань)

Після чого ми пишемо скрипт для брутфорсу, запускаємо його і чекаємо на результат що показаний на нище.

```
(kali@kali)-[~]
$ while read line; do (echo "Valid trans found: $line" && sudo ike-scan -M $line 104.1.1.2) | grep -B14 "1 returned handshake" | grep "Valid trans found" ; done < ike-dict.txt

Valid trans found: --trans=7/128,2,1,5
```

Рисунок 3.4 – Створення та запуск скрипта.

З новими даними ми можемо спробувати дізнатись трохи більше про нашу ціль а саме про обладнання, версію її ОС для того щоб скоригувати атаку або ж перевірити про наявні бекдори в данному ОС та самому обладнанню. Але через те що дана атака проводилась в емуляторі GNS3 та через особливість даного додатку результат не видав бажаного результату.

```
$ sudo ike-scan -M --trans=7/128,2,1,5 --showbackoff 104.1.1.2

Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
104.1.1.2 Main Mode Handshake returned
HDR=(CKY-R=afe4c24e09653f0e)
SA=(Enc=AES KeyLength=128 Hash=SHA1 Group=5:modp1536 Auth=PSK LifeType=Seconds LifeDuration=28800)

IKE Backoff Patterns:

IP Address      No.      Recv time      Delta Time
104.1.1.2       1        1663785745.899596  0.000000
104.1.1.2       2        1663785757.006450  11.106854
104.1.1.2       3        1663785768.115663  11.109213
104.1.1.2       4        1663785779.234993  11.119330
104.1.1.2       5        1663785790.346423  11.111430
104.1.1.2       6        1663785801.459120  11.112697
104.1.1.2       Implementation guess: UNKNOWN

Some IKE implementations found have unknown backoff fingerprints
If you know the implementation name, and the pattern is reproducible, you
are encouraged to submit the pattern and implementation details
through the github repository at https://github.com/royhills/ike-scan
Ending ike-scan 1.9.5: 1 hosts scanned in 115.686 seconds (0.01 hosts/sec). 1 returned handshake; 0 returned notify
```

Рисунок 3.5 – Створення та запуск скрипта.

На даному моменті зловмисник вже отримав певну інформацію про нашу мережу та буде логічно якщо він спробує захопити PSK (Pre-shared key) для того щоб оффлайн зламати його за допомогою інших утиліт. Та вінзнає невдачі адже в мережі протокол IPsec працює в головному режимі не в агресивному.

Після розвідки можна розглянути приклади вразливостей які були зазначені у попередньому розділі. Спочатку хакер спробує використати одну з вразливостей та спробувати перенаправити весь трафік через свій ПК для цього він може використати атаки типу ARP Poisoning або ICMP Redirect. Для даної атаки існує безліч утиліт таких як: Arp-sk, Scrapy, Ettercap та інші. В даному випадку я використаю утиліту Ettercap-graphical. Для початку ми знову скануємо нашу мережу та вибираємо маршрутизатори до яких під'єднані хаб та клієнське обладнання для проведення Mitm-атаки.

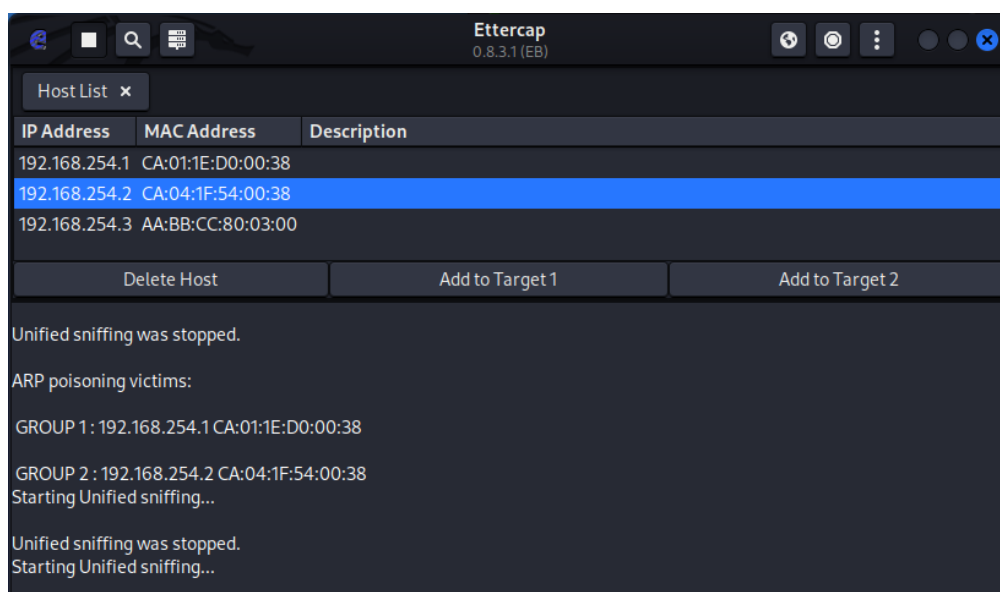


Рисунок 3.6 – Сканування мережі, вибір жерт та запуск атаки

Під час атаки йде перехоплення всього трафіку від наших жертв та блокування його для подальшого відправлення до пункту призначення. Перевіримо чи працює весь трафік від наших жертв до рук хакера для цього спробуємо пропінгувати робочу станцію із нашим VPN хабом.

```

Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\admin>ping 172.10.100.11

Обмен пакетами с 172.10.100.11 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 172.10.100.11:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\admin>

```

Рисунок 3.7 – Пінгування головний хаб DMVPN з робочої станції клієнта.

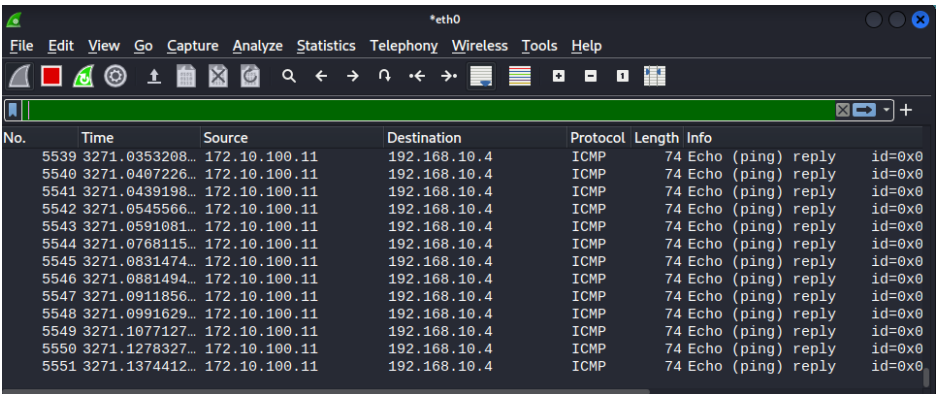


Рисунок 3.8 – Перевірка вдалого перехоплення трафіку.

Впевнившись що ми вдало скористались вразливістю можна почати моніторити перехоплення пакетів від протоколів ESP та ISAKMP для подальшого розшифрування його. Зловмисник може скористатися для розшифрування трафіка як утилітою Wireshark так і іншими додадками.

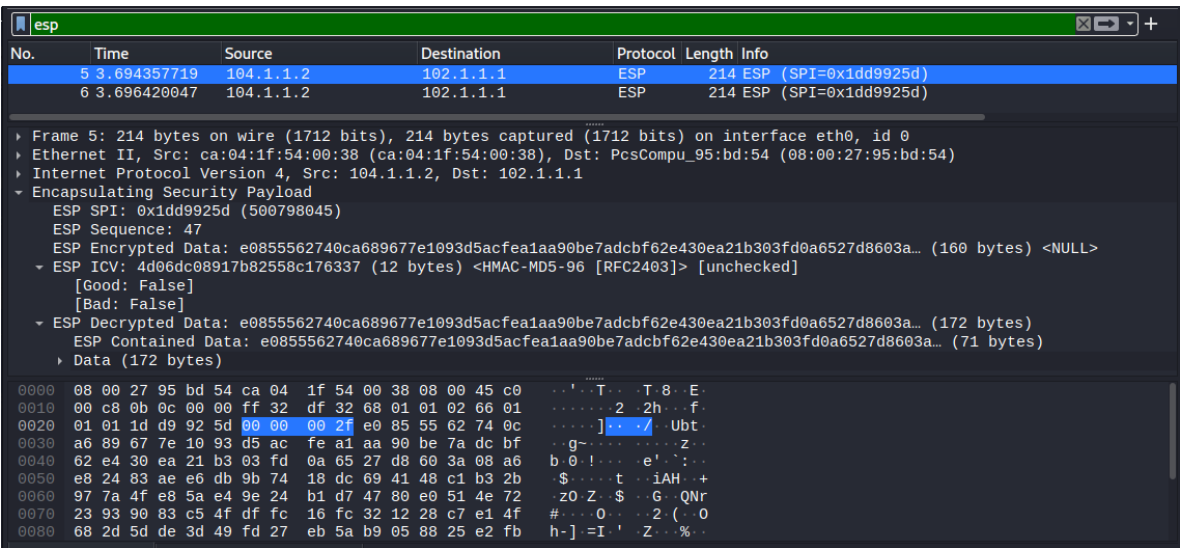


Рисунок 3.9 – Відсортування пакетів та спроба розшифрувати їх.

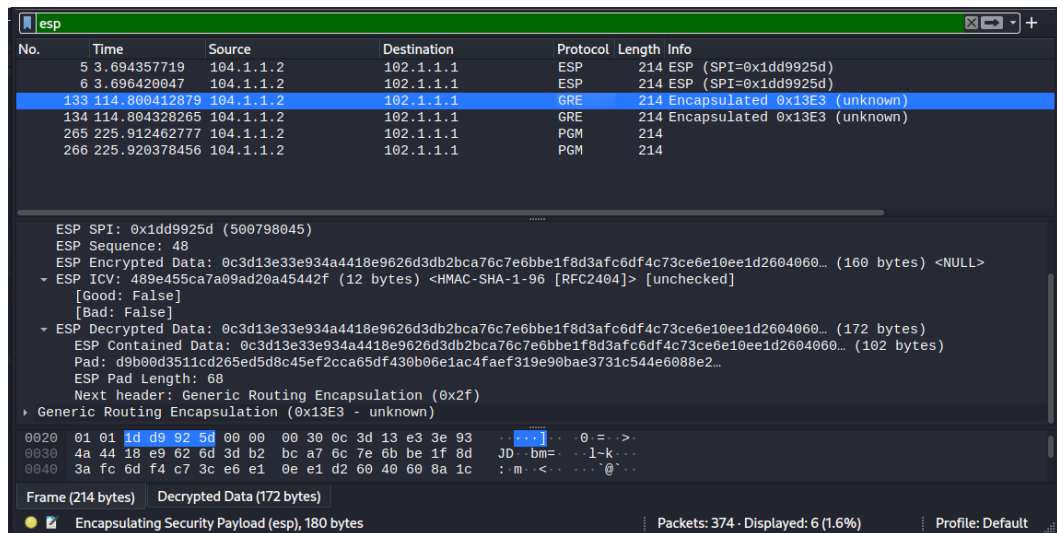


Рисунок 3.10 – Вдала спроба розшифрувати повідомлення.

Також потрібно зазначити що якщо не використовувати протокол для шифрування трафіку то порушник з легкістю отримає дані для аунтифікації до приватної віртуальної мережі як показано на наступному зображенні.

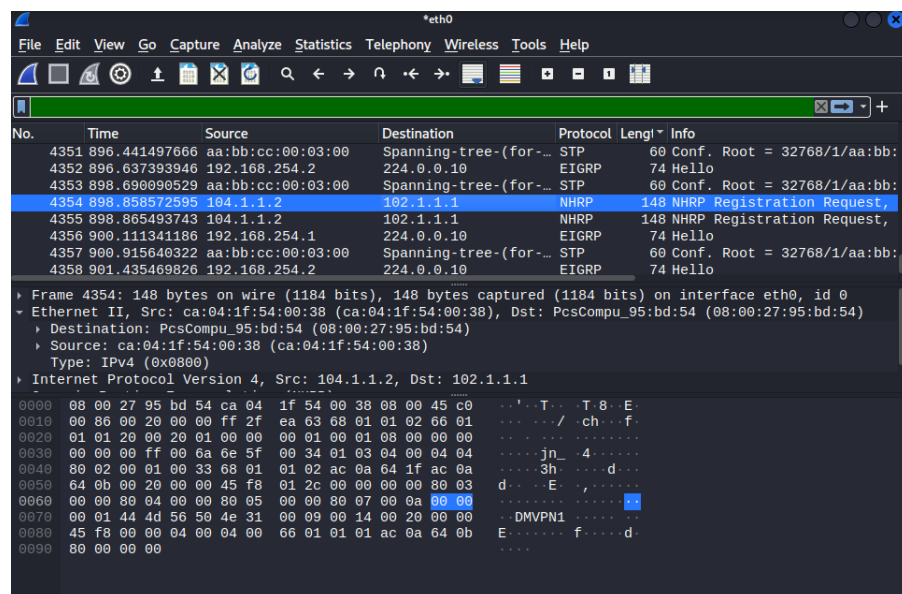


Рисунок 3.11 – Перехоплення відкритого пакету NHRP для реєстрації в мережі DMVPN

Потрібно не забувати й про вразливість більшості мереж до DOS та DDOS атак яка по суті є одними з найлегших але в той же час найруйнівнішим типом атак. Щоб продемонструвати даний тип атак використаю потужну утиліту для стресс тестувань T50.

```

(kali@kali)-[~]
└─$ sudo t50 104.1.1.2 --flood -S --turbo
T50 Experimental Mixed Packet Injector Tool v5.8.7b
Originally created by Nelson Brito <nbrito@sekure.org>
Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

[INFO] Entering flood mode ... [INFO] Turbo mode active ...
[INFO] Performing stress testing ...
[INFO] Hit Ctrl+C to stop ...
[INFO] PID=37979
[INFO] t50 5.8.7b successfully launched at Sun Nov 13 11:49:26 2022
[INFO] PID=37980

```

Рисунок 3.12 – Запуск DOS атаки на Branch1.

```

Branch1#ping 102.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.1.1.1, timeout is 2 seconds:
!..

```

Рисунок 3.13 – Перевірка вдалості атаки.

3.2 Перевірка роботи та дослідження видаленого доступу.

Після тестування оцінки безпеки мережі та розуміння вразливостей нашої мережі потрібно провести покращення безпеки нашої мережі.

Для початку потрібно налаштувати Static ARP маршрут для того щоб унеможливити MitM-атаку (ARP Poisoning) яка націлена на перехоплення трафіку. Протокол ARP дозволяє визначити статичний запис ARP для IP-адреси та заборонити пристроям прослуховувати відповіді ARP для цієї адреси. Наприклад, якщо робоча станція завжди підключається до того самого маршрутизатора, ви можете визначити статичний запис ARP для цього маршрутизатора, запобігаючи атаці.

```

Branch1#sh arp
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 104.1.1.1          9          c407.092c.0010 ARPA    FastEthernet0/0
Internet 104.1.1.2          -          ca04.1f54.0000 ARPA    FastEthernet0/0
Internet 192.168.10.1       -          ca04.1f54.001c ARPA    FastEthernet1/0
Internet 192.168.200.2     -          ca04.1f54.0038 ARPA    FastEthernet2/0
Branch1#

```

Рисунок 3.14 – Перевірка мапи arp на Branch1.

```

Primary_Hub#sh arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 102.1.1.1 - ca01.1ed0.0000 ARPA FastEthernet0/0
Internet 102.1.1.2 23 c406.0971.0010 ARPA FastEthernet0/0
Internet 192.168.100.1 - ca01.1ed0.001c ARPA FastEthernet1/0
Primary_Hub#

```

Рисунок 3.15 – Перевірка мапи arp на головному сервері.

Спочатку потрібно очистити ARP кеш, очищення кешу arp змушує конкретний пристрій надсилати необов'язкову відповідь ARP щодо своєї власної адреси та якщо пристрій працює то відновлює роботу в іншому випадку видаляє з arp мапи. Подальші приклади налаштування будуть показані на маршрутизаторі Branch1, налаштування на інших пристроях аналогічні.

```

Branch1#debug arp
ARP packet debugging is on
Branch1#clear arp-cache
Branch1#
*Nov 17 12:53:42.203: ARP: flushing ARP entries for all interfaces
*Nov 17 12:53:42.215: IP ARP: sent rep src 104.1.1.2 ca04.1f54.0000,
dst 104.1.1.2 ffff.ffff.ffff FastEthernet0/0
*Nov 17 12:53:42.219: IP ARP: sent rep src 192.168.10.1 ca04.1f54.001c,
dst 192.168.10.1 ffff.ffff.ffff FastEthernet1/0
*Nov 17 12:53:42.223: IP ARP: sent rep src 192.168.200.2 ca04.1f54.0038,
dst 192.168.200.2 ffff.ffff.ffff FastEthernet2/0
*Nov 17 12:53:42.223: IP ARP: sent req src 104.1.1.2 ca04.1f54.0000,
dst 104.1.1.1 c407.092c.0010 FastEthernet0/0
Branch1#
*Nov 17 12:53:42.255: IP ARP: rcvd rep src 104.1.1.1 c407.092c.0010, dst 104.1.1.2 FastEthernet0/0
Branch1#clear arp 192.168.200.2
Branch1#
*Nov 17 12:54:10.359: IP ARP: sent rep src 104.1.1.2 ca04.1f54.0000,
dst 104.1.1.2 ffff.ffff.ffff FastEthernet0/0
*Nov 17 12:54:10.359: IP ARP: sent rep src 192.168.10.1 ca04.1f54.001c,
dst 192.168.10.1 ffff.ffff.ffff FastEthernet1/0
*Nov 17 12:54:10.363: IP ARP: sent rep src 192.168.200.2 ca04.1f54.0038,
dst 192.168.200.2 ffff.ffff.ffff FastEthernet2/0
Branch1#

```

Рисунок 3.16 – очищення кешу та пам'яті arp на Branch1.

Коли вже очистили кеш та наш пристрій видалив непотрібні нам пристрої то тепер додаємо статичні arp маршрути.

```

Branch1(config)#arp 192.168.254.2 ca04.1f54.0038 arpa
Branch1(config)#arp 104.1.1.1 c407.092c.0010 arpa
Branch1(config)#arp 192.168.10.1 ca04.1f54.001c arpa
Branch1(config)#end
Branch1#sh arp
*Nov 17 13:13:09.843: %SYS-5-CONFIG_I: Configured from console by console
Branch1#sh arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 104.1.1.1 - c407.092c.0010 ARPA
Internet 104.1.1.2 - ca04.1f54.0000 ARPA FastEthernet0/0
Internet 192.168.10.1 - ca04.1f54.001c ARPA
Internet 192.168.200.2 - ca04.1f54.0038 ARPA FastEthernet2/0
Internet 192.168.254.2 - ca04.1f54.0038 ARPA

```

Рисунок 3.17 – Створення статичних маршрутів.

На наступному етапі знову протестуємо безпеку за допомогою MitM-атаки та перевіримо чи зможе порушник провести атаку.

```

Prymary_Hub#ping 104.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 104.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/50/60 ms
Prymary_Hub#

```

Рисунок 3.18 – Перевірка зв'язку головного сервера з клієнтом.

```

Branch1#ping 102.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 102.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/68/116 ms
Branch1#

```

Рисунок 3.19 – Перевірка зв'язку Branch1 з Prymary_Hub.

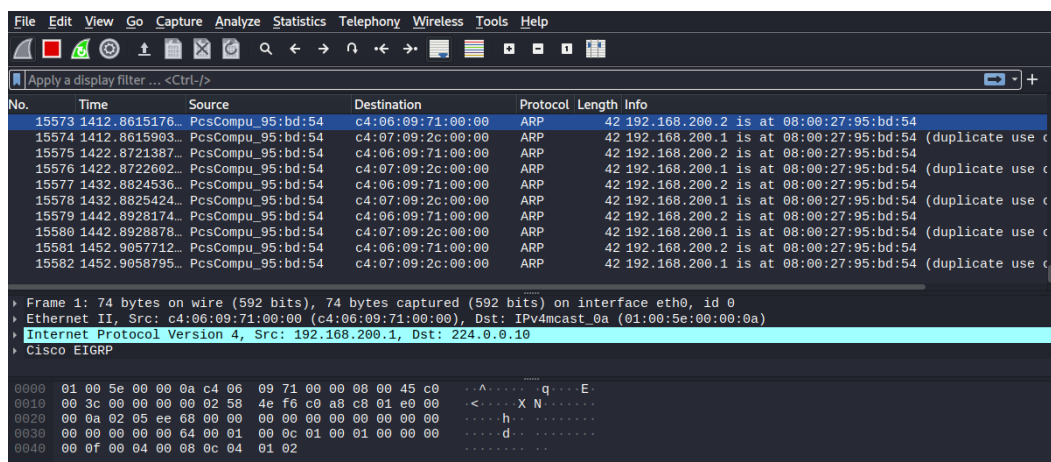


Рисунок 3.20 – Перевірка перехоплення трафіку.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Хоча хакер надсилає про перенаправлення трафіку на його пристрій але трафік не переадресовується через його пристрій як видно на зображенні вище. З чого можна зробити висновок що з цим нам вдалось трохи захистити свою мережу.

Наступним етапом потрібно захистити мережі від DOS/DDOS атак. Найкращим варіантом було б налаштувати брандмаузер з використанням Cisco ASA але даний варіант дуже фінансово затратний тому використаємо наявні маршрутизатори.

```
Branch1(config)#access-list 103 permit icmp any any
Branch1(config)#ip inspect name firewall tcp
Branch1(config)#ip inspect name firewall tcp
Branch1(config)#
Branch1(config)#ip inspect name firewall udp
Branch1(config)#
Branch1(config)#int f0/0
Branch1(config-if)#ip access-group 103 in
Branch1(config-if)#ip access-group 103 in
Branch1(config-if)#
Branch1(config-if)#ip nat outside
Branch1(config-if)#
Branch1(config-if)#no cdp enable
Branch1(config-if)#
Branch1(config-if)#
Branch1(config-if)#access-list 103 permit udp host 102.1.1.1 any eq isakmp
Branch1(config)#access-list 103 permit udp host 102.1.1.1 eq isakmp any
Branch1(config)#
Branch1(config)#access-list 103 permit esp host 102.1.1.1 any
Branch1(config)#access-list 103 permit icmp any any
```

Рисунок 3.21 – Налаштування простого брандмаузера.

```
Primary_Hub#ping 104.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 104.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/53/64 ms
```

Рисунок 3.22 – Перевірка зв'язку головного сервера з клієнтом.

Останньою порадою буде використовувати більш складніші паролі та ключів. Тому що довжина паролів, ключі і так далі на пряму впливає наскільки більшу безпеку буде забезпечувати система, тому що зловиснику будуть потрібні довші та затратніші (як по часу так і по техніці) зусилля для його злому методом перебору. Це можна представити в термінах очікуваного часу розкриття пароля або очікуваного безпечного часу. Очікуваний безпечний час (T_S) — половина добутку

числа можливих паролів і часу, необхідного для того, щоб спробувати кожен пароль з послідовності запитів. Представимо це у виді формули:

$$T_s = \frac{A^S * t}{2},$$

де t — час, необхідний на спробу введення пароля, рівний E/R , E — число символів у переданому повідомленні при спробі одержати доступ (включаючи пароль і службові символи), R — швидкість передачі (символи/хв) у лінії зв'язку, S — довжина пароля, A — число символів в алфавіті, з яких складається пароль.

Якщо після кожної невдалої спроби підбору автоматично передбачається десятисекундна затримка, то безпечний час різко збільшується. Тому при використанні аутентифікації на основі паролів захищеною системою повинні дотримуватися наступні рекомендації:

- не дозволяються паролі менше 6–8 символів;
- паролі повинні перевірятися відповідними запитами (наприклад Regex);
- кожна вдалий вхід повинен записуватися у логи системи;
- обмежити кількість спроб уведення пароля (наприклад при 3 невдалих спроб робити інетрвал входу від 1хвилини до години або блокувати вхід з даної робочої машини);
- ввести затримку часу при кожній спробі введення пароля;
- паролі повинні зберігатися в пам'яті системи тільки в зашифрованому вигляді у файлах, недоступних користувачам або з певними обмеженням по доступам;
- паролі повинні періодично мінятися, бажано раз в місяць.

3.3 Висновки до розділу 3.

В останньому розділі було налаштовано мережна інфраструктура мережі та розглянуто на практиці сценарії тестування захисту мережі. А саме провели налаштування головного сервера, запасного серверу DMVPN, та налаштували двох клієнтів (branch). Також провели тестування мережі за допомогою MitM-атаки під час якої нам вдалось перехопити трафік та частково розшифрувати його, також

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

розглянули результат в якому дані будуть передаватись без захисту протоколу IPsec, також провели тестування за допомогою DOS-атаки під час якої вдало зірвали передачу повідомлень між сервером та клієнтом. Також враховуючи результати тестування було надані поради щодо покращення безпеки мережі щодо налаштувань брандмаузера та захисту портів щоб зарадити DOS/DDOS атакам, налаштування статичних маршрутів та особливу увагу приділили налаштуванню ключам доступів та паролів адже саме від їх складності залежить весь захист мережі.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

ВИСНОВКИ

Під час виконання випускної роботи бакалавра було спроектовано, реалізовано мережу та тестування безпеки даної мережі на базі технологій DMVPN та було виконано наступні завдання:

Під час написання першого розділу було проведено аналіз теоретичних відомостей які надали характеристики організації приватних віртуальних мереж. Проаналізували основні переваги протоколів на яких на даному моменті працюють технології DMVPN. Під кінець було розглянуто приклади вразливостей безпеки у технології багатоточкових динамічних віртуальних приватних мереж. Також розробили технічне завдання.

В другому розділі було спроектовано мережну інфраструктуру де ми розробили топологію мережі та розглянули кожну з підмереж. Також було спроекторваний план тестування безпеки мережі де ми розглянули різні етапи тестування та чотири сценарії тестування, а саме спробувати використати вразливість у механізмах PSK, спробувати виконати MitM-атаку зрадаи того щоб перенаправити трафік через машину хакера, влаштувати збій в мережі за допомогою DOS або DDOS атаки. В останньому підрозділі розглянули засоби тестування а саме Nmap, Ike-scan, Ettercap, T50.

В останньому розділі було налаштовано мережна інфраструктура мережі та розглянуто на практиці сценарії тестування захисту мережі. А саме провели налаштування головного сервера, запасного серверу DMVPN, та налаштували двох клієнтів (branch). Також провели тестування мережі за допомогою MitM-атаки під час якої нам вдалось перехопити трафік та частково розшифрувати його, також розглянули результат в якому дані будуть передаватись без захисту протоколу IPsec, також провели тестування за допомогою DOS-атаки під час якої вдало зірвали передачу повідомлень між сервером та клієнтом. Також враховуючи результати тестування було надані поради щодо покращення безпеки мережі щодо налаштувань брандмаузера та захисту портів щоб зарадити DOS/DDOS атакам, налаштування статичних маршрутів та особливу увагу приділили кналаштуванню ключам доступів та паролів адже саме від їх складності залежить весь захист мережі.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Реалізована мережа та налаштування сервера може швидко перенестись на реальну топологію мережі завдяки зручному симулятору GNS3 та із-за використання емульованих реальних образів. Також розроблені методи тестування мережі на проникнення можна використовувати до будь якої DMVPN мережі або VPN мережі яка базується на інших технологіях типу site-to-site.

В майбутньому можливо розширити серверну структуру та налаштувати додаткові функції, доповнити методи тестування мережі іншими сценаріями пов'язаними з іншими протоколами та їх вразливостями.

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Dynamic Multipoint VPN (DMVPN) [Електронний ресурс] / Rahul Awati,. – Електрон. текст. дані. – Режим доступу: <https://www.techtarget.com/searchnetworking/definition/dynamic-multipoint-VPN-DMVPN>. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
2. Cisco FlexVPN DMVPN, Part 1 – Overview and Design [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: <https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/>. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
3. Cisco IOS FlexVPN Data Sheet [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
4. Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
5. NetEngine AR V300R019 CLI-based Configuration Guide - VPN [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: <https://support.huawei.com/enterprise/en/doc/EDOC1100112360/3ae1a4cf/implementationl>. – Дата останнього доступу: 16.11.2021. – Назва з екрану.
6. Cisco Intelligent WAN (IWAN): Cisc Inte Wide Area Netw [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Dec2016/CVD-IWAN-DIADesignGuide-Dec16.pdf> – Дата останнього доступу: 26.07.2022. – Назва з екрану.
7. Cisco IOS in a Nutshell (A Desktop Quick Reference for IOS on IP Networks) [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу:

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

- <https://vdoc.pub/documents/cisco-ios-in-a-nutshell-5qrqk7vgdh80> – Дата останнього доступу: 26.07.2022. – Назва з екрану.
8. CCNP Security Secure 642-637 Official Cert Guide: CCNP Se Secu 642-637 ePub_1 [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: https://www.academia.edu/4462541/CCNP_Security – Дата останнього доступу: 26.07.2022. – Назва з екрану.
9. NHRP: A Node-centric Hybrid Routing Approach for Ad-hoc Networks pdf [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: <https://apps.dtic.mil/sti/pdfs/ADA461790.pdf> – Дата останнього доступу: 26.07.2022. – Назва з екрану.
10. CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2 [Електронний ресурс] /. – Електрон. текст. дані. – Режим доступу: <https://ptgmedia.pearsoncmg.com/images/9781587144912/samplepages/9781587144912.pdf> – Дата останнього доступу: 26.07.2022. – Назва з екрану.
11. Huaqi Chen - Design and implementation of secure Enterprise Network based on DMVPN/ Huaqi Chen, Guangzhou Guangdong: International Conference on Business Management and Electronic Information (BMEI) China, 2011-511 стр.
12. Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1). URL: <https://community.cisco.com/legacyfs/online/legacy/3/9/5/26593-DMVPNbk.pdf> (дата звернення: 20.07.2022).
13. Route creation influence on DMVPN QoS. URL: https://www.researchgate.net/publication/224574013_Route_creation_influence_on_DMVPN_QoS (дата звернення: 20.07.2022).
14. IPsec Vulnerabilities and Software Security Prediction. URL: <https://www.altsci.com/ipsec/> (дата звернення: 20.07.2022).
15. 500/udp - Pentesting IPsec/IKE VPN Prediction. URL: <https://book.hacktricks.xyz/network-services-pentesting/ipsec-ike-vpn-pentesting> (дата звернення: 20.07.2022).

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

16. IPsec VPN Penetration Testing with BackTrack Tools. URL:

<https://www.opensourceforu.com/2012/01/ipsec-vpn-penetration-testing-backtrack-tools/> (дата звернення: 20.07.2022).

17. Security of Dynamic and Multipoint Virtual Private Network. URL:

https://www.researchgate.net/publication/306278979_Security_of_Dynamic_and_Multipoint_Virtual_Private_Network (дата звернення: 17.11.2022).

18. Ethical Hacking - ARP Poisoning. URL:

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_arp_poisoning.htm (дата звернення: 17.11.2022).

19. T50 Experimental Packet Injector Tool. URL: <https://gitlab.com/fredericopissarra/t50>

(дата звернення: 17.11.2022)

20. Ettercap and middle-attacks tutorial. URL: <https://pentestmag.com/ettercap-tutorial-for-windows/> (дата звернення: 17.11.2022)

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

ДОДАТКИ

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Технічні характеристики пристроїв спроектованої мережі

Таблиця А.1 – Системні характеристики Маршрутизатора Cisco ISR4331/K9

Виробник	Cisco
Ідентифікатор товару	ISR4331/K9
Тип продукту	маршрутизатор
Інтерфейси / порти	
Загальна кількість портів	3
USB	Має
Порт управління	має
Кількість мережевих портів (RJ-45)	2
Розширення вводу-виводу	
Кількість загальних слотів розширення	6
Тип слота розширення	AIM \ PVDM
Network & Communication	
Мережеві технології	10/100/1000Base-T
Технологія Ethernet	Gigabit Ethernet
Пам'ять	
Стандартна пам'ять	4 GB
Максимум пам'яті	16 GB
Технологія пам'яті	DDR3 ECC RAM
Флеш-пам'ять	4 GB
Опис живлення	
Вхідна напруга	120 V AC \ 230 V AC
Фізичні характеристики	
Форм-фактор	Монтаж в стійку
Висота	4.45
Ширина	43.8
Глибина	43.8

Конфігураційні файли пристроїв мережі

Конфігураційний файл Маршрутизаторів Cisco ISR4331/K9

Primary_Hub	multilink bundle-name authenticated
Building configuration...	archive
Current configuration : 1839 bytes	log config
!	hidekeys
upgrade fpd auto	!
version 12.4	crypto isakmp policy 20
service timestamps debug datetime msec	encr aes
service timestamps log datetime msec	authentication pre-share
no service password-encryption	group 5
!	crypto isakmp key dmvpn1 address 0.0.0.0 0.0.0.0
hostname Primary_Hub	!
!	crypto ipsec transform-set dmvpn1 esp-aes esp-sha-hmac
boot-start-marker	!
boot-end-marker	crypto ipsec profile gre_protection
!	set security-association lifetime seconds 86400
logging message-counter syslog	set transform-set dmvpn1
!	!
no aaa new-model	ip tcp synwait-time 5
ip source-route	!
no ip icmp rate-limit unreachable	interface Tunnel1
ip cef	ip address 172.10.100.11 255.255.255.0
!	no ip redirects
no ip domain lookup	ip nhrp authentication DMVPN1
no ipv6 cef	ip nhrp map multicast dynamic
!	ip nhrp network-id 1

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

ip nhrp holdtime 300	no ip http secure-server
ip nhrp redirect	!
ip tcp adjust-mss 1360	no cdp log mismatch duplex
tunnel source FastEthernet0/0	!
tunnel mode gre multipoint	control-plane
tunnel key 1	!
tunnel protection ipsec profile gre_protection	gatekeeper
!	shutdown
interface FastEthernet0/0	!
ip address 102.1.1.1 255.255.255.252	line con 0
duplex half	exec-timeout 0 0
!	privilege level 15
interface FastEthernet1/0	logging synchronous
ip address 192.168.100.1 255.255.255.0	stopbits 1
duplex half	line aux 0
!	exec-timeout 0 0
interface FastEthernet2/0	privilege level 15
ip address 192.168.200.1 255.255.255.0	logging synchronous
shutdown	stopbits 1
duplex half	line vty 0 4
!	login
router eigrp 100	!
network 102.1.1.0 0.0.0.3	end
network 192.168.1.0	
network 192.168.200.0	Second_Hub
auto-summary	Building configuration...
!	Current configuration : 1475 bytes
ip forward-protocol nd	!
no ip http server	upgrade fpd auto

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Second_Hub
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface Tunnel2
ip address 172.10.200.21 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN2
ip nhrp map multicast dynamic
ip nhrp network-id 2
ip nhrp holdtime 300
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 2
!
interface FastEthernet0/0
ip address 101.1.1.1 255.255.255.252
duplex half
!
interface FastEthernet1/0
ip address 192.168.100.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 101.1.1.0 0.0.0.3

```

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

network 192.168.2.0

no auto-summary

!

ip forward-protocol nd

no ip http server

no ip http secure-server

!

no cdp log mismatch duplex

!

control-plane

!

gatekeeper

shutdown

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

!

End

Branch_1

Building configuration...

Current configuration : 2895 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Branch1

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

no ip domain lookup

ip inspect name firewall tcp

ip inspect name firewall udp

no ipv6 cef

!

multilink bundle-name authenticated

!

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

archive
log config
hidekeys
!
crypto isakmp policy 20
encr aes
authentication pre-share
group 5
crypto isakmp key dmvpn1 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set dmvpn1 esp-aes esp-sha-hmac
!
crypto ipsec profile gre_protection
set security-association lifetime seconds 86400
set transform-set dmvpn1
!
ip tcp synwait-time 5
!
interface Tunnel1
ip address 172.10.100.31 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN1
ip nhrp map 172.10.100.11 102.1.1.1
ip nhrp map multicast 102.1.1.1
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 172.10.100.11
ip nhrp shortcut
ip tcp adjust-mss 1360

tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile gre_protection
!
interface Tunnel2
ip address 172.10.200.31 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN2
ip nhrp map 172.10.200.21 101.1.1.1
ip nhrp map multicast 101.1.1.1
ip nhrp network-id 2
ip nhrp holdtime 300
ip nhrp nhs 172.10.200.21
ip nhrp shortcut
ip tcp adjust-mss 1360

tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 2
!
interface FastEthernet0/0
ip address 104.1.1.2 255.255.255.252
ip access-group 103 in
ip nat outside
ip virtual-reassembly
duplex half
no cdp enable
!
interface FastEthernet1/0

```

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 192.168.200.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 104.1.1.0 0.0.0.3
network 192.168.1.0
network 192.168.10.0
network 192.168.200.0
auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
access-list 103 permit udp host 102.1.1.1 any eq isakmp
access-list 103 permit esp host 102.1.1.1 any
access-list 103 permit icmp any any
access-list 103 permit udp host 102.1.1.1 eq isakmp any
no cdp log mismatch duplex
arp 104.1.1.1 c407.092c.0010 ARPA
arp 192.168.10.1 ca04.1f54.001c ARPA
arp 192.168.254.2 ca04.1f54.0038 ARPA
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login

```

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

```

!
End

Branch_2

Building configuration...

Current configuration : 1866 bytes
!
upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Branch2

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

```

```

!

archive

log config

hidekeys

!

ip tcp synwait-time 5

!

interface Tunnel1

ip address 172.10.100.41 255.255.255.0

no ip redirects

ip nhrp authentication DMVPN1

ip nhrp map 172.10.100.11 102.1.1.1

ip nhrp map multicast 102.1.1.1

ip nhrp network-id 1

ip nhrp holdtime 300

ip nhrp nhs 172.10.100.11

ip nhrp shortcut

ip tcp adjust-mss 1360

tunnel source FastEthernet0/0

tunnel mode gre multipoint

tunnel key 1

!

interface Tunnel2

ip address 172.10.200.41 255.255.255.0

no ip redirects

ip nhrp authentication DMVPN2

ip nhrp map 172.10.200.21 101.1.1.1

ip nhrp map multicast 101.1.1.1

ip nhrp network-id 2

```

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

```

ip nhrp holdtime 300
!
ip nhrp nhs 172.10.200.21
ip forward-protocol nd
ip nhrp shortcut
no ip http server
ip tcp adjust-mss 1360
no ip http secure-server
tunnel source FastEthernet0/0
!
tunnel mode gre multipoint
no cdp log mismatch duplex
tunnel key 2
!
!
control-plane
interface FastEthernet0/0
!
ip address 103.1.1.2 255.255.255.252
gatekeeper
duplex half
shutdown
!
!
interface FastEthernet1/0
line con 0
no ip address
exec-timeout 0 0
shutdown
privilege level 15
duplex auto
logging synchronous
speed auto
stopbits 1
!
line aux 0
interface FastEthernet1/1
exec-timeout 0 0
no ip address
privilege level 15
shutdown
logging synchronous
duplex auto
stopbits 1
speed auto
line vty 0 4
!
login
router eigrp 100
!
network 103.1.1.0 0.0.0.3
end
no auto-summary

```

		Волинець Б.О.			Житомирська політехніка.22.125.03.001	Арк.
		Марцева Л.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72