

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

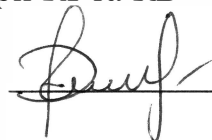
на тему:

«Проект підсистеми захисту мережної інфраструктури
на базі Network Based IPS»

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

 Жданюк Є.В.

Керівник ст. викладач кафедри КІ та КБ

 Байлюк Є.М.

Рецензент, ст. викладач кафедри КІ та КБ

 Покотило О.А.

Житомир – 2023

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Жданюк Євгеній Вадимович

Тема роботи: «Проект підсистеми захисту мережної інфраструктури на базі Network Based IPS»

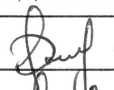
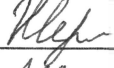
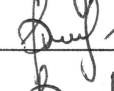
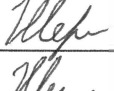
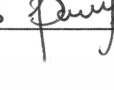
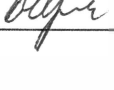
затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 19 червня 2023 р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Комутатори Cisco
5. Операційні системи Cisco IOS, Windows 10
6. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є.М.	23.03.2023 	23.03.2023 
2	Байлюк Є.М.	16.04.2023 	16.04.2023 
3	Байлюк Є.М.	21.05.2023 	21.05.2023 

Студент Жданюк Є.В.
Керівник Байлюк Є.М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20 березня 2023	Виконано
2	Пошук та аналіз джерел	29 квітня 2023 – 9 травня 2023	Виконано
3	Пошук та аналіз моделей маршрутизаторів	10 травня 2023 – 17 травня 2023	Виконано
4	Розробка топології мережі	18 травня 2023 – 19 травня 2023	Виконано
5	Проектування та вибір обладнання для реалізації	20 травня 2023 – 27 травня 2023	Виконано
6	Налагодження пристроїв мережі	28 травня 2023 – 8 червня 2023	Виконано
7	Аналіз працездатності мережі	9 червня 2023 – 11 червня 2023	Виконано
8	Написання пояснювальної записки	12 червня 2023 – 17 червня 2023	Виконано
9	Підготовка презентації	18 червня 2023	Виконано
10	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	19 червня 2023	Виконано
11	Захист		Виконано

Студент Жданюк Є.В.
Керівник Байлюк Є.М.

АНОТАЦІЯ

Кваліфікаційна робота складається з проєкту підсистеми захисту мережевої інфраструктури на базі Network-based IPS. Пояснювальна записка містить 44 сторінки, 31 рисунок та 2 таблиці.

Кваліфікаційна робота присвячена розробці проєкту підсистеми захисту мережевої інфраструктури на базі Network-based IPS. Метою проєкту є масштабованість та захищеність мережі. Мережа повинна забезпечити надійний та безперебійний обмін даними. Для віддаленого та захищеного доступу до мережевих пристроїв було створено користувачів.

Кваліфікаційна робота складатиметься з трьох розділів, в яких буде описано та продемонстровано розробку топології мережі, ПЗ та обрані рішення на основі пристроїв, конфігурація. В додатках буде вказано конфігурації маршрутизатора зі встановленим IPS та комутаторів мережі.

Ключові слова: IPS, МЕРЕЖЕВА ІНФРАСТРУКТУРА, ЗАХИСТ, CISCO, КОМП'ЮТЕРНА МЕРЕЖА, ACTIVE DIRECTORY.

					КІК.КР.Б – 123 – 05 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту мережевої інфраструктури на базі Network-based IPS	Літ.	Арк.	Аркушів
Розроб.		Жданюк Є.В.		20.06.23				
Керівник		Байлюк Є.М.		20.06.23			4	48
Реценз.		Поктило О.		20.06.23				
Затверд.		Єфіменко А.А.		20.06.23		ФІКТ, Гр. КІ-19-1		

ANNOTATION

The qualification work consists of a project of a network infrastructure protection subsystem based on Network-based IPS. The explanatory note contains 41 pages, 31 figures, and 2 tables.

The qualification work is dedicated to the development of a network infrastructure protection subsystem project based on Network-based IPS. The project aims to achieve scalability and security of the network. The network should ensure reliable and uninterrupted data exchange. Users have been created to enable remote and secure access to network devices.

The qualification work will consist of three sections, which will describe and demonstrate the development of the network topology, software, and selected solutions based on devices, configuration. The appendices will specify the configuration of the router with installed IPS and network switches.

Keywords: IPS, NETWORK INFRASTRUCTURE, PROTECTION, CISCO, COMPUTER NETWORK, ACTIVE DIRECTORY.

		Жданюк Є.В.			KIK.KP.B – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРОЄКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ ТА ПІДСИСТЕМА ЗАХИСТУ IPS	10
1.1 Корпоративна мережа та вимоги	10
1.2 Модуль підключення до мережі Інтернет.....	12
1.3 Сервери мережі.....	13
1.4 Теоретичні відомості IPS.....	16
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	21
2.1 Проектування підсистеми захисту та комп'ютерної мережі	21
2.2 Аналіз структурної складової мережі	24
РОЗДІЛ 3 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ	27
3.1 Вибір обладнання для побудованої мережі.....	27
3.2 Налагодження обладнання мережі.	30
3.3 Тестування працездатності мережі.....	39
ВИСНОВКИ.....	41
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	42
ДОДАТКИ.....	44

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

IPS – Intrusion Prevention System

ПК – персональний комп'ютер

GNS3 – Graphical Network Simulator-3

DHCP – Dynamic Host Configuration Protocol

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі Інтернет став важливою частиною нашого життя. Інтернет використовується в багатьох сферах, включаючи бізнес, медицину, науку та інформаційні технології. З одного боку, мережі можуть швидко й ефективно здійснювати обмін інформацією, з іншого боку, вони є причиною для багатьох проблем безпеки.

Останніми роками захистити мережі від кібератак стало складніше, що завдає шкоди підприємствам, компаніям і користувачам. Кіберзлочинці використовують багато методів і технік для проникнення в мережі, такі як віруси, злом, фішинг, соціальна інженерія тощо. Ці атаки можуть призвести до розкриття конфіденційної інформації, втрати даних і зниження продуктивності.

Для запобігання цим атакам фахівці компанії можуть використовувати Intrusion Prevention System (IPS). Технологія здатна виявляти та блокувати шкідливий мережевий трафік.

Network-based IPS використовується для виявлення різної аномальної активності в мережі. Ця технологія запобігає наступним типам атак: DoS (Denial of Service), DDoS (Distributed Denial of Service), SQL Injection, Cross-site scripting та інші. Network-based IPS у мережі може виявляти та зупиняти ці атаки до того, як мережа буде пошкоджена або звести до мінімуму втрати.

Здатність працювати на рівні мережі – є перевагою Network-based IPS, тобто не потребує встановлення спеціального програмного забезпечення на кожен комп'ютер у мережі. Це означає, що Network-based IPS може захистити всі пристрої в мережі від кібератак, включаючи сервери, маршрутизатори, комутатори тощо.

Слід також зазначити, що Network-based IPS не є універсальним засобом захисту мережі. Деякі види атак можна виявити та нейтралізувати, але не всі. Network-based IPS може бути неефективним, якщо кіберзлочинці використовують нові вразливості, які ще не були включені до бази даних захисних систем, то Network-based IPS може бути неефективним.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Хоча Network-based IPS має багато переваг, які можуть допомогти захистити мережу, вона також має деякі недоліки та проблеми, про які слід знати. Важливо розуміти, що безпека мережі є складною темою, і існує багато рівнів, задіяних у забезпеченні безпеки. У більшості випадків Network-based IPS налаштовується як частина стратегії безпеки мережі.

Моделювання підсистеми буде відбуватися у симуляторі GNS3.

Метою кваліфікаційної роботи є розробка підсистеми захисту мережної інфраструктури на базі Network Based IPS.

Визначена мета обумовлює наступні завдання:

- Аналіз наявних приладів;
- Вибір структури мережі;
- Вибір ПЗ для реалізації мережі;
- Реалізація підсистеми захисту;

Об’єктом дослідження є процес налаштування мережевої системи захисту комп’ютерної мережі від кіберзлочинців.

Предметом дослідження є методи і засоби захисту мережі організації за допомогою IPS (Intrusion Prevention System).

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРОЄКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ ТА ПІДСИСТЕМА ЗАХИСТУ IPS

1.1 Корпоративна мережа та вимоги

Корпоративна мережа — це логічно відокремлена група комп'ютерів, маршрутизаторів та інших частин IT-інфраструктури, які функціонують поза традиційними межами Інтернету. Її часто називають інтранет. Термін інтранет описує мережу, яка, на відміну від Інтернету, призначена для доступу лише певної групи людей [1].

Основною метою створення корпоративних мереж є забезпечення безпеки та надійності інформаційної системи управління компанією, системи обробки даних, передачі даних та зв'язку - співробітникам може не виникнути потреби використовувати програмне забезпечення з обмеженими даними, коли вони знаходяться поза робочим місцем. Крім того, розміщення додатків, актуальних лише для членів компанії виключно в корпоративних мережах, може бути набагато менш складним. Корпоративні мережі використовують різні типи пристроїв LAN та WAN, а також широко доступні протоколи та стандарти зв'язку для надання таких функцій [10].

Отже, спираючись на вище написане, можна зробити такі висновки: корпоративна мережа – це закрита локальна мережа доступ до якої мають лише працівники компанії, ізолюваність забезпечує інформаційну безпеку даних компанії.

Характеристики, які можуть включати у корпоративні мережі такі:

– Розмір та масштаб: Корпоративні мережі можуть бути розгорнуті в невеликих організаціях з кількома пристроями або великих підприємствах з тисячами комп'ютерів і пристроїв. Розмір мережі визначається обсягом і складністю робочих процесів в організації.

– Топологія: Корпоративна мережа може бути побудована за різними топологіями, такими як старовинна зірка, дерево, меш і т. д. Топологія визначає, як пристрої підключаються один до одного і як формується структура мережі.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

– Засоби зв'язку: Корпоративна мережа використовує різні засоби зв'язку для передачі даних між пристроями. Це можуть бути кабельні підключення, безпроводові технології, оптоволоконні канали тощо. Вибір засобів залежить від потреб організації та характеристик мережі.

– Безпека: Корпоративні мережі часто мають складні системи безпеки для захисту конфіденційності, цілісності та доступності даних. Це можуть бути мережеві брандмауери, віртуальні приватні мережі (VPN), системи аутентифікації та авторизації користувачів, антивірусні програми та інші заходи безпеки.

– Швидкість передачі даних: Корпоративні мережі можуть підтримувати високу швидкість передачі даних, особливо у випадку розгортання широкосмугових технологій, таких як Gigabit Ethernet або краще. Це дозволяє швидкий обмін даними між пристроями та швидку реакцію на вимоги користувачів.

– Централізоване управління: Корпоративні мережі часто мають централізовану систему управління, яка дозволяє адміністраторам мережі контролювати і налаштовувати пристрої, моніторити стан мережі, надавати права доступу користувачам тощо.

– Спільні ресурси: Одні з основних функцій корпоративних мереж - надання спільного доступу до ресурсів, таких як файли, принтери, бази даних тощо. Це сприяє спільній роботі та обміну інформацією між користувачами.

Варто зазначити, що характеристики залежать від розміру та архітектури корпоративної мережі. А отже потрібно мати комплекс рішень, які забезпечать стабільну роботу мережі та, за потреби, можливість впровадження нових пристроїв у мережу.

Основні цілі архітектури корпоративної мережі включають:

– Надійність та доступність: Один з головних аспектів архітектури корпоративної мережі – це забезпечення стабільної роботи та доступності мережевих послуг.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

- Масштабованість: Корпоративні мережі мають тенденцію зростати з часом.
- Безпека: Забезпечення безпеки є важливим аспектом архітектури корпоративної мережі.
- Ефективність та продуктивність: Архітектура мережі повинна бути спроектована з урахуванням ефективного використання ресурсів та максимальної продуктивності.
- Адміністрування: Архітектура мережі повинна спрощувати процес управління та адміністрування.

1.2 Модуль підключення до мережі Інтернет

Інтернет-модуль – це пристрій або компонент, який дозволяє підключати пристрої до Інтернету і забезпечує комунікацію з мережевими сервісами та іншими пристроями через Інтернет. Також інтернет-модуль може включати в себе різні компоненти для бездротового або проводового підключення до Інтернету.

Основні компоненти, які можуть включатися до інтернет-модуля:

- Мережевий адаптер: Інтернет-модуль має вбудований мережевий адаптер, який дозволяє підключатися до мережі Інтернет. Це може бути Wi-Fi-адаптер для бездротового з'єднання або Ethernet-адаптер для фізичного з'єднання.
- Пам'ять: Інтернет-модуль може мати вбудовану пам'ять для збереження програмного забезпечення, налаштувань та даних.
- Програмне забезпечення: Інтернет-модуль має вбудоване програмне забезпечення, яке керує його функціональністю, забезпечує безпеку та забезпечує можливості підключення до мережевих сервісів.
- Міжмережний екран – це пристрій, який на основі заданих налаштувань буде надавати або забороняти доступ до мережі.

Під час написання дипломної роботи в побудованій симуляції мережі використовувався маршрутизатор на який було встановлено IPS. Intrusion Prevention System (IPS) часто включає міжмережний екран як одну зі своїх

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

складових. Міжмережний екран використовується для контролю та фільтрації мережевого трафіку, що входить та виходить з мережі. Він визначає правила доступу, блокує небажаний трафік та допомагає захистити мережу від зовнішніх загроз [12].

Однак, IPS виходить за межі простого міжмережного екрана, оскільки він також виявляє та блокує потенційно шкідливу активність в мережі, таку як атаки на вразливості, спроби вторгнення та інші види загроз безпеці. IPS аналізує мережевий трафік в реальному часі та застосовує набір правил для ідентифікації та блокування підозрілого або шкідливого трафіку.

Основні функції IPS [2] це:

- Виявлення загроз;
- Блокування загроз;
- Моніторинг;
- Захист від вразливостей;
- Аудит подій;

Загалом всі функції зрозумілі, і можна прийти до такого висновку, що IPS виявляє та блокує небажаний трафік та захищає від відомих вразливостей, також ця система може збирати інформацію про потенційні загрози та атаки, що сталися, та відправляти її на сервер, забезпечуючи, тим самим, журналювання подій. Це допомагає у розслідуванні інцидентів безпеки, аналізі причин і наслідків, а також вдосконаленні стратегій безпеки. Отже з попередніх міркування можна зробити висновок, що IPS є досить надійним рішенням безпеки Cisco.

1.3 Сервери мережі

Термін «сервер» має подвійне значення. Сервер – це комп’ютер, який надає доступ до ресурсів через мережу, а також програми, яка виконується на цьому комп’ютері [7]. Тому необхідно мати два різних визначення сервера:

Апаратний сервер – це фізичний пристрій, підключений до комп’ютерної мережі, на якому разом з операційною системою працюють один або кілька

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

програмних серверів. Альтернативним терміном для апаратного сервера є хост. В принципі, будь-який комп'ютер можна використовувати як хост із серверним програмним забезпеченням.

Програмний сервер – це програма, яка пропонує спеціалізований сервіс для використання іншими програмами (відомими як клієнти) локально або через мережу. Пропонована послуга залежить від типу серверного програмного забезпечення. В основі спілкування лежить модель клієнт-сервер. Коли справа доходить до обміну даними, використовуються протоколи зв'язку для певних послуг.

В дипломній роботі використовувались DHCP-сервер та хост зі встановленим ПО Windows Server.

DHCP (Dynamic Host Configuration Protocol) - це протокол мережевої комунікації, який використовується для автоматичного налаштування параметрів мережі для пристроїв, які підключаються до мережі. DHCP визначається у стандарті RFC 2131.

Основна функція DHCP полягає в тому, щоб забезпечити автоматичне призначення IP-адрес, маски підмережі, шлюзу за замовчуванням та інших параметрів мережі для комп'ютерів, принтерів, маршрутизаторів та інших мережевих пристроїв [8].

Основні переваги використання DHCP:

Автоматичне призначення IP-адрес: DHCP дозволяє призначати IP-адреси мережевим пристроям автоматично, що спрощує процес налаштування мережі і уникнення конфліктів IP-адрес.

– Економія часу: DHCP дозволяє автоматично призначати параметри мережі, що зменшує час, необхідний для налаштування кожного пристрою окремо.

– Уникнення конфліктів IP-адрес: DHCP відслідковує призначені IP-адреси і запобігає повторному використанню однакових адрес в мережі, що допомагає уникнути конфліктів IP-адрес та забезпечити їх унікальність.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

– Динамічне оновлення налаштувань: DHCP дозволяє оновлювати налаштування мережі, такі як IP-адреси, без необхідності перезавантаження пристроїв.

Отже з вище перелічених властивостей можна зробити висновок що, DHCP спрощує процес налаштування та управління мережевими пристроями, дозволяючи автоматично призначати та оновлювати параметри мережі.

Перейдімо до етапу коли клієнт робить запит до сервера, щоб отримати IP-адресу. Коли клієнт, що шукає IP-адресу, відправляє широкомовний DHCPDISCOVER пакет, він містить свою апаратну адресу. Сервери DHCP отримують запит і надсилають відповідь у вигляді пакету DHCPOFFER, який містить пропозиції IP-адреси та час оренди.

Клієнт обирає одну з пропозицій з DHCPOFFER пакетів, зазвичай вибираючи адресу з найдовшим часом оренди. Він надсилає пакет DHCPREQUEST з обраною адресою індивідуального сервера.

Вибраний сервер відправляє підтвердження DHCPACK, і процес узгодження завершується. DHCPACK пакет містить призначену адресу та час оренди. Сервер позначає цю адресу як зайняту до закінчення оренди, що запобігає її призначенню іншому клієнту. Клієнт налаштовує свої параметри згідно з отриманими даними і може почати працювати в мережі.

Цей процес може мати кілька серверів, які відповідають на запит DHCPDISCOVER. Клієнт повинен обрати одну з пропозицій і відправити DHCPREQUEST пакет з ідентифікатором вибраного сервера. Інші сервери, яких відкинули, переглядають пакет DHCPREQUEST та знають, що їхні пропозиції відкинуті і їхні IP-адреси можна надати іншим клієнтам.

У випадку, якщо сервер не може підтвердити конфігурацію, він надсилає пакет DHCPNAK, що змушує клієнта розпочати процес узгодження знову.

Windows Server - це операційна система, розроблена компанією Microsoft спеціально для використання на серверах. Вона є варіантом операційної системи Windows, пристосованої для роботи в розподіленому середовищі мережі.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows Server надає набір функцій і можливостей, спеціально розроблених для обробки завдань на серверах. Ця операційна система може використовуватися для різноманітних завдань, таких як керування мережею, зберігання даних, хостинг веб-сайтів, установка програмного забезпечення, віртуалізація та інші.

Windows Server надає багатофункціональність для керування серверами і мережами, такі як Active Directory, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), файлові служби, друковані служби, веб-служби та багато інших. Операційна система має також підтримку для віртуалізації, що дозволяє розгортати віртуальні сервери та керувати ними.

1.4 Теоретичні відомості IPS

Технологія Intrusion Prevention System (IPS) - це комплексна система захисту мереж та комп'ютерних систем, яка забезпечує виявлення та блокування небажаних вторгнень і запобігає потенційним загрозам безпеці [6].

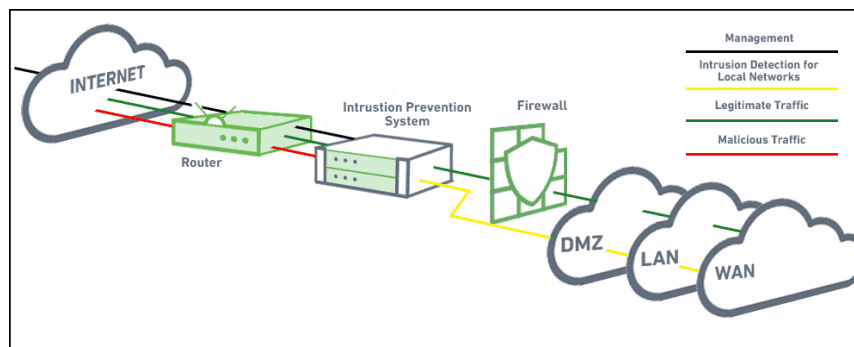


Рис. 1.1 Схема роботи IPS

Одним з головних елементів IPS є сигнатурний аналіз. Він використовує базу даних, що містить зразки відомих шкідливих програм і підозрілу активність. Коли IPS виявляє співпадіння між активністю в мережі та сигнатурами, він активує заходи для блокування цих загроз. Сигнатурний аналіз ефективний для виявлення відомих атак, але не здатний розпізнавати нові типи загроз.

Щоб запобігти новим загрозам, IPS використовує аналіз поведінки. Він стежить за типовими шаблонами активності в мережі та системі, виявляючи аномалії, які можуть свідчити про атаку. Наприклад, якщо система зазвичай не

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

надсилає великий обсяг даних певному користувачу, але раптово ця активність змінюється, IPS спрацьовує і блокує цю ненормальну поведінку [11].

Є ще одна важлива техніка, що використовується в IPS - евристичний аналіз. Вона базується на виявленні певних зразків або властивостей, які можуть вказувати на наявність загрози. Наприклад, евристичний аналіз може виявити невідому шкідливу програму, яка намагається змінити налаштування системи або виконати підозрілі дії.

Інша важлива функція IPS - це захист від вразливостей. IPS аналізує трафік мережі та перевіряє, чи існують відомі вразливості, які можуть бути експлуатовані зловмисниками. Якщо виявляється така вразливість, IPS вживає заходів, наприклад, шляхом блокування атакуючого трафіку або запобіжних заходів на рівні мережі.

Однією з переваг IPS є можливість реагувати в реальному часі. Він працює на принципі неперервного моніторингу трафіку та виявлення небажаної активності миттєво. Це дозволяє швидко реагувати на потенційні загрози та забезпечує ефективний захист мережі та системи [9].

Іншою перевагою IPS є можливість інтеграції з іншими системами безпеки. Він може працювати у взаємодії з мережевими брандмауерами, системами виявлення вторгнень (Intrusion Detection System, IDS), системами управління інцидентами та іншими засобами безпеки, що забезпечує комплексний захист мережі та даних [2].

Проте IPS також має свої недоліки. Перш за все, він може спричиняти помилкові спрацювання, коли легітимний трафік помилково ідентифікується як загроза і блокується. Це може призвести до проблем з функціонуванням системи та спричинити незручності для користувачів.

Крім того, IPS може стати причиною затримки мережевого трафіку через необхідність аналізувати великий обсяг даних. Це може вплинути на продуктивність мережі та завдати шкоди швидкодії передачі даних. Також варто враховувати, що IPS не забезпечує 100% захист від усіх видів атак. Існують

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

випадки, коли нові, раніше не відомі загрози можуть обійти сигнатурний аналіз та евристичні методи IPS. Тому важливо постійно оновлювати бази сигнатур та алгоритми аналізу, щоб впроваджувати нові заходи безпеки.

Ще одним недоліком IPS може бути складність конфігурації та налаштування. Встановлення правильних параметрів може бути складним завданням і вимагати досвіду в галузі безпеки мережі. Неправильна конфігурація може призвести до помилкових спрацювань.

Окрім того, IPS вимагає значних ресурсів для ефективної роботи. Великі мережі з високим обсягом трафіку можуть вимагати потужного обладнання та масштабованості, щоб забезпечити швидку та надійну роботу системи.

Незважаючи на недоліки, використання Intrusion Prevention System є критичним для забезпечення безпеки мереж та комп'ютерних систем. Він допомагає виявляти та блокувати шкідливий трафік, запобігає втраті даних та забезпечує надійність інфраструктури. Важливо розглядати IPS як одну з складових стратегії безпеки, доповнюючи її іншими заходами, такими як брандмауери, антивіруси та регулярне оновлення програмного забезпечення, щоб створити надійний і комплексний захист мережі.

Класифікація Intrusion Prevention System (IPS) зазвичай здійснюється на основі різних критеріїв, таких як методи виявлення та блокування атак, рівень застосування та масштаб системи.

В даній дипломній роботі був використаний сигнатурний IPS, який використовує базу сигнатур для порівняння мережевого трафіку з відомими атаками та шкідливими програмами.

Проте також існують і інші класифікації:

1) За рівнем застосування:

– Network-based IPS: Розташовані на рівні мережевого з'єднання та контролюють вхідний та вихідний трафік мережі.

– Host-based IPS: Розташовані на окремих хост-системах та спостерігають за активністю на самому пристрої.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

– Комбіновані IPS: Поєднують функціональність мережевого та хост-IPS для комплексного захисту мереж та пристроїв.

2) За масштабом системи:

– Відокремлені IPS: Самостійні фізичні пристрої або програмне забезпечення, які встановлюються окремо для захисту конкретних мереж або пристроїв.

– Інтегровані IPS: Інтегровані в існуючі мережеві пристрої, такі як брандмауери, комутатори або маршрутизатори, для забезпечення захисту на рівні мережі.

Ця класифікація допомагає визначити та обрати підходящий тип IPS для конкретної організації або мережевого середовища. Наприклад, для великих корпоративних мереж часто використовуються гібридні IPS, які комбінують сигнатурний аналіз та аналіз поведінки для надійного виявлення різних загроз.

Вибір між мережевим та хост-IPS залежить від потреб організації. Мережеві IPS можуть забезпечувати централізований контроль над усіма трафіком, але вимагають великих обчислювальних ресурсів та фізичного розміщення пристроїв в мережі. Хост-IPS, натомість, можуть забезпечити детальний контроль на рівні окремих пристроїв, але вимагають індивідуального налаштування та підтримки для кожного хосту.

Відокремлені IPS зазвичай використовуються для малих і середніх підприємств або для специфічних застосувань, де потрібна самостійна система захисту. Інтегровані IPS, з іншого боку, можуть бути вигідним вибором для організацій, які вже мають існуючі мережеві пристрої з підтримкою IPS функцій.

Висновки до першого розділу

Після того як було розглянуто особливості корпоративної мережі, було продумано яким чином побудувати мережу, включаючи всі необхідні модулі. Також було досліджено можливості програмного симулятора мереж GNS3 аби забезпечити проєкт необхідним функціоналом.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Було розглянуто сервери локальної мережі. Також розглянули роботу запиту DHCP та особливості програмного сервера Windows server.

Для захисту мережі від вторгнень та небажаного зовнішнього трафіку було обрано IPS. Також передбачена можливість запису логів, які будуть відправлятися на хост зі встановленим програмним сервером.

Мережа буде побудована на базі обладнання компанії Cisco. Для створення мережі буде задіяний симулятор GNS3. За допомогою якого можна забезпечити взаємодію мережевих пристроїв та віртуальних машин.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Проектування підсистеми захисту та комп'ютерної мережі

Для проектування комп'ютерної мережі була використана трьохрівнева модель мережі. Трьох рівнева модель є ієрархічною та передбачає, що кожен рівень мережі будуть залежними один від одного. Складові моделі такі:

- Рівень ядра;
- Рівень розподілу;
- Рівень доступу.

До складової рівня ядра входять 2 маршрутизатори. На одному з маршрутизаторів, який буде межувати з інтернет-модулем та локальною мережею офісу буде встановлено IPS, що в свою чергу передбачає попередження потрапляння небажаного трафіку до мережі офісу. До складової мережі входить досить багато робочих станцій, що тим самим спричиняє зріст кількості використовуваних IP-адрес. Для авоматизації процесу IP-адресації, потрібно налаштувати протокол DHCP. Також для зручності адміністрування мережі передбачено встановлення на одному з хостів Windows Server. Даний сервер буде виконувати функцію DHCP серверу та як складова захисту мережі. На сервері будуть створені облікові записи користувачів, які представлятимуть робітників офісу та налаштована функціональність кожної групи облікового запису. Дана процедура робиться для того, щоб обмежити використання небажаних, з погляду адміністратора, програм та функцій на робочих станціях. Працівники офісу не матимуть доступу до панелі керувань та консолі.

Також однією з задач є розробка IP-топології мережі. Оскільки мережа передбачає наявність кількох підмереж, для забезпечення функціональності та обміну інформації між ними потрібно налаштувати протокол OSPF. Інформацію щодо адресації мережі наведено в табл. 2.1.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Підмережа А	-	195.191.1.0	255.255.255.0	/24
Підмережа В	-	195.191.2.0	255.255.255.0	/24
Підмережа С	-	195.191.3.0	255.255.255.0	/24
Підмережа D	-	195.191.4.0	255.255.255.0	/24
Підмережа Е	-	195.191.5.0	255.255.255.0	/24
Підмережа F	-	195.191.6.0	255.255.255.0	/24
Інтернет модуль				
Маршрутизатор R5	Fa0/0	195.191.2.254	255.255.255.0	/24
	Fa0/1	195.191.1.254	255.255.255.0	/24
Ядро				
Маршрутизатор R1	Fa0/0	195.191.3.253	255.255.255.0	/24
	Fa0/1	195.191.2.253	255.255.255.0	/24
Маршрутизатор IPS	Fa0/0	195.191.3.254	255.255.255.0	/24
	Fa0/1	195.191.4.251	255.255.255.0	/24
	Fa1/0	195.191.5.251	255.255.255.0	/24
	Fa1/1	195.191.6.251	255.255.255.0	/24
Рівень розподілу/доступу				
Комутатор SW-5-1	Vlan1	195.191.5.252	255.255.255.0	/24
Комутатор SW-5-2	Vlan1	195.191.5.253	255.255.255.0	/24
Комутатор SW-5-3	Vlan1	195.191.6.252	255.255.255.0	/24
Комутатор SW-5-4	Vlan1	195.191.6.253	255.255.255.0	/24

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Продовження таблиці 2.1(1)

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Комутатор SW-5-5	Vlan1	195.191.4.252	255.255.255.0	/24
Комутатор SW-5-6	Vlan1	195.191.4.253	255.255.255.0	/24
Робоча станція PC1	Eth0	DHCP		
Робоча станція PC2	Eth0	DHCP		
Робоча станція PC3	Eth0	DHCP		
Робоча станція PC4	Eth0	DHCP		
Робоча станція PC5	Eth0	DHCP		
Робоча станція PC6	Eth0	DHCP		
Робоча станція PC7	Eth0	DHCP		
Робоча станція WS-191-8-5	Eth0	DHCP		
Робоча станція WS-191-8-1	Eth0	DHCP		
Сервер Serv-5-1	Eth0	195.191.5.1	255.255.255.0	/24
Сервер Serv-5-2	Eth0	195.191.5.2	255.255.255.0	/24

2.2 Аналіз структурної складової мережі

Беручи до уваги попередні дані, було обрано трирівневу модель мережі. Перевагами такої моделі є: надійність, масштабованість і продуктивність. Оскільки модель має три рівні, то буде розглянуто кожен рівень окремо з усіма його складовими.

Почнімо з рівня ядра. В даній дипломній роботі в задачі ядра входять швидке транспортування між пристроями, також забезпечення безпеки мережі офісу. Для налаштування безпеки було обрано систему привентизації вторгнень зі встановленими сигнатурами від компанії Cisco [5]. Для забезпечення обміну інформації між підмережами на маршрутизаторах буде налаштовано протокол OSPF.

До рівня розподілу та доступу будуть входити комутатори і робочі станції. На одній з підмереж дві робочі станції будуть налаштовані як сервер та контролер домену. Для автоматизації IP-адресації робочих станцій Windows Server буде виконувати функцію DHCP-сервера, а також для інших функцій адміністрування. Windows Server також матиме функцію Syslog сервера. Події, які записуються на маршрутизаторі з встановленим IPS будуть відправлятися комп'ютер адміністратора [3]. Це потрібно для того, щоб адміністратору було зручно стежити за трафіком та в розслідуванні кібер інцидентів.

Загальний вигляд топології мережі із використанням трьохрівневої моделі наведено на рисунку 2.1.

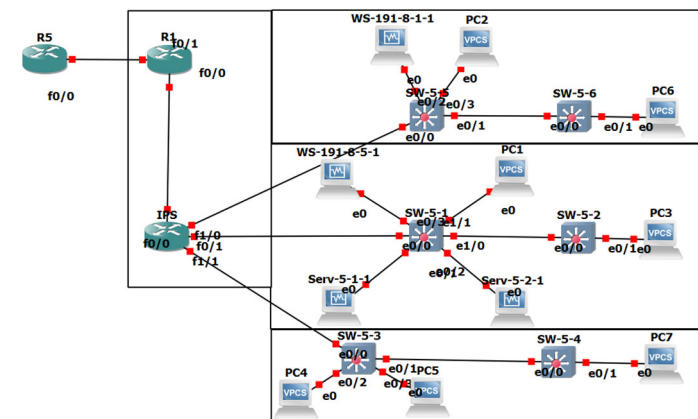


Рис.2.1. Топологія трирівневої мережі

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

Перейдімо до огляду кожної підмережі. Всі підмережі будуть зображені на рисунках 2.2-2.4, пристрої, які є складовою мережі показано в табл. 2.2.

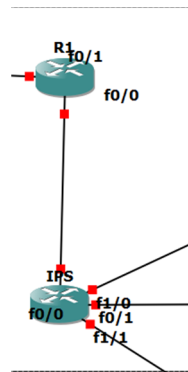


Рис.2.2. Рівень ядра

Таблиця 2.2

Рівень ядра

Маршрутизатори	R1 та IPS (образ c7200-adventerprisek9-mz.152-4.M7.image)
Сигнатури	IOS-S855-CLI.pkg

Для безпеки мережі було встановлено IPS з відповідними сигнатурами. Також на маршрутизаторах налаштований протокол OSPF для зв'язку підмереж.



Рис.2.3. Рівень розподілу

В кваліфікаційній роботі для комутаторів був використаний образ i86bi-linux-l2-ipbasek9-15.1a.bin.

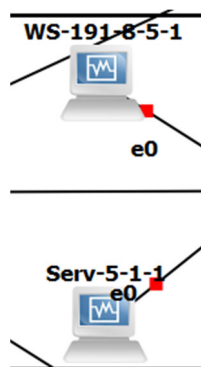


Рис.2.4. Рівень доступу

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

В підмережі 195.191.5.0 встановлено п'ять робочих станцій, дві з яких показано на рисунку 2.4. На рисунку показано робочу станцію з ОС Windows 10(7) та іншу – Windows Server з встановленим Syslog.

Висновки до другого розділу

Розроблено та проаналізовано топологію мережі складовою якої є маршрутизатори, комутатори та робочі станції. На рівні ядра, в маршрутизатор буде встановлено та налаштовано IPS. Розроблено таблицю з параматрами адресації кожного пристрою.

Було розглянуто образи та операційні системи, які будуть використовуватися під час створення мережі.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

РОЗДІЛ 3 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Вибір обладнання для побудованої мережі.

Маршрутизатори працюють на мережевому рівні моделі OSI: можуть пересилати пакети з однієї мережі до іншої. Для того, щоб надіслати пакети в потрібному напрямку, маршрутизатор використовує таблицю маршрутизації, яка зберігається у його пам'яті. Таблиця маршрутизації може складатися засобами статичної або динамічної маршрутизації. На рівні ядра та на рівні розподілу нам потрібний маршрутизатор який би підтримував би технологію FastEthernet, можливість встановлення технології IPS та містив додаткові функції налаштування. Маршрутизатор CiscoSystems CISCO7200, рис 3.1, найбільш оптимальний варіант для великої мережі підприємства чи офісу [15].



Рис. 3.1. Маршрутизатор Cisco 7200

Комутатор працює на каналному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. В моєму курсовому проекті було використано комутатори моделі 2960-24TT.

Fast Ethernet (Швидкий Ethernet) — термін, що описує набір стандартів Ethernet для пакетної передачі даних з номінальною швидкістю 100 Мбіт/с, що в 10 разів швидше за початкову для Ethernet швидкість у 10 Мбіт/с. Він визначений

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

1995 року в документі IEEE 802.3u. На сьогодні існують швидші в 10 (Gigabit Ethernet) і 100 (10 Gigabit Ethernet) разів стандарти технології Ethernet.



Рис. 3.2. Комутатор

Визначившись з обладнанням на основі якого буде побудована мережа, перейдімо до програмно-апаратного забезпечення.

До даного критерію налаштувань належать:

1. Використання ОС таких як Windows 7(10) та Windows Server;
2. Встановлення контролера домена;
3. Встановлення додатку TFTPd32 через який буде завантажено сигнатури на маршрутизатор, а в подальшому виконуватиме роль Syslog серверу.
4. DHCP-сервер;
5. Наявність зв'язку між станціями;
6. Налаштування SSH задля безпечного віддаленого доступу до мережевих пристроїв;
7. Встановлення IPS з відповідними сигнатурами для захисту мережі.

З метою побудувати топологію мережі з підсистемою захисту на базі IPS було застосовано програмний додаток GNS3. VirtualBox був використаний для віртуалізації робочих станцій мережі офісу.

GNS3 (Graphical Network Simulator 3) – це безкоштовний додаток для моделювання мереж, що дозволяє створювати віртуальні мережі з використанням різних пристроїв мережі. Даний інструмент є корисним для

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

інженерів мереж, системних адміністраторів та студентів, які бажають експериментувати, тестувати та вивчати різноманітні аспекти мережевих технологій [13].

Основна мета GNS3 – це забезпечити можливість створення віртуальних мереж, що досить точно відтворює реальні мережеві середовища. Ми маємо можливість розміщувати віртуальні пристрої, такі як маршрутизатори, комутатори, файрволи та інші мережеві пристрої, і з'єднувати їх, налаштовувати, тестувати та аналізувати роботу мережі. Для цього не потрібно фізичного обладнання, так як все відбувається в віртуальному середовищі.

Розглянувши головний інструмент для виконання роботи перейдімо до підрядних.

TFTPD32 - це безкоштовний сервер TFTP (Trivial File Transfer Protocol) для операційних систем Windows. TFTP - це простий протокол передачі файлів, який використовується для віддаленого завантаження файлів між комп'ютерами в мережі. TFTPD32 надає сервер TFTP разом із додатковими функціями, що розширюють його функціональність.

TFTPD32 дає можливість налаштовувати та запускати TFTP сервер, що дозволяє передавати файли між комп'ютерами в мережі. Він особливо корисний для завантаження образів операційних систем або конфігураційних файлів на мережеві пристрої, такі як маршрутизатори або комутатори.

Також додаток містить в собі простий DHCP сервер, який дозволяє автоматично призначати IP-адреси та інші мережеві налаштування комп'ютерам в мережі. Це особливо зручно для тестування та налагодження мережевих пристроїв або для створення локальної мережі без необхідності використовувати додатковий DHCP сервер.

Поміж інших функцій, TFTPD32 включає простий TFTP клієнт, який дозволяє віддалено завантажувати файли з TFTP серверів.

VirtualBox - це безкоштовний гіпервізор, який дозволяє створювати та управляти віртуальними машинами на комп'ютері. Він розроблений компанією

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Oracle і доступний для різних операційних систем, включаючи Windows, macOS, Linux та інші [14].

Основна функція VirtualBox полягає в тому, щоб створювати віртуальну середу, де можна запускати і використовувати інші операційні системи. За допомогою VirtualBox з'являється можливість створити віртуальну машину, що емулює фізичний комп'ютер зі своїм власним процесором, оперативною пам'яттю, жорстким диском, мережевими адаптерами тощо.

Основні призначення VirtualBox:

- Тестування операційних систем. Можна встановити та запустити різні операційні системи віртуально, щоб провести тестування програмного забезпечення, перевірити сумісність, відлагоджувати проблеми та експериментувати з різними конфігураціями.

- Розробка та тестування програмного забезпечення. Розробники можуть використовувати VirtualBox для створення віртуальних машин з різними операційними системами для розробки, тестування та відлагодження своїх програм.

- Віртуалізація серверів. За допомогою цього додатку можна встановити та керувати віртуальними серверами на своєму комп'ютері, що дозволяє ефективно використовувати ресурси та розгортати різні сервіси в окремих віртуальних середовищах.

- Безпечне середовище. Створивши віртуальну машину з окремою операційною системою, щоб виконувати потенційно небезпечні завдання в ізольованому середовищі, може допомогти уникнути можливих загроз безпеці.

3.2 Налаштування обладнання мережі.

Розглянувши та проаналізувавши всі аспекти побудови мережі, переходимо до реалізації. В даному розділі буде розглянуто основні етапи налаштування мережових пристроїв.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-5-1#sh cdp neighbors detail
-----
Device ID: IPS.IPS
Entry address(es):
  IP address: 195.191.5.254
Platform: Cisco 7206VXR, Capabilities: Router
Interface: Ethernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime : 171 sec

Version :
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 25-Sep-14 10:36 by prod_rel_team

advertisement version: 2
Duplex: full
Management address(es):
-----
Device ID: IOU2
Entry address(es):
  IP address: 195.191.5.252
Platform: Linux Unix, Capabilities: Router Switch
Interface: Ethernet1/0, Port ID (outgoing port): Ethernet0/0
Holdtime : 144 sec

Version :
Cisco IOS Software, Solaris Software (I86BI LINUXL2-IPBASEK9-M), Experimental Ve
rsion 15.1(20130124:233217) [dstivers-jan24-2013-team_track 101]
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Thu 24-Jan-13 16:17 by dstivers

advertisement version: 2
VTP Management Domain: ''
Duplex: half
Management address(es):
  IP address: 195.191.5.252

SW-5-1#
SW-5-1#
SW-5-1#

```

Рис. 3.3. Вивід команди show cdp neighbors detail

Зважаючи на дані, які отримали на рис.3.3 маємо висновок, що кожен може, якщо забажає, дізнатися адреси мережевих пристроїв. Аби не допустити цього налаштуємо доступ таким чином, щоб до мережевих пристроїв мав доступ тільки адміністратор.

```

IPS
% Please define a domain-name first.
IPS(config)#ip domain-name IPS
IPS(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: IPS.IPS

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

IPS(config)#
*May 29 13:51:52.910: %SSH-5-ENABLED: SSH 1.99 has been enabled
IPS(config)#username admin01 algorithm-type scrypt secret cisco123
IPS(config)#line console 0
IPS(config-line)#login local
IPS(config-line)#exec-timeout 5 0
IPS(config-line)#logging synchronous
IPS(config-line)#exit
IPS(config)#line vty 0 4
IPS(config-line)#login local
IPS(config-line)#exec-timeout 5 0
IPS(config-line)#transport input ssh
IPS(config-line)#exit
IPS(config)#enable algorithm-type scrypt secret cisco123
IPS(config)#

```

Рис. 3.4. Налаштування доступу до маршрутизатора

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

В ході налаштування було обрано протокол SSH, тому що він шифрує пакети і при перехопленні зломисник не зможе дізнатися логіну та паролю до мережевого пристрою.

Далі задамо адресу серверу та зробимо основні налаштування.

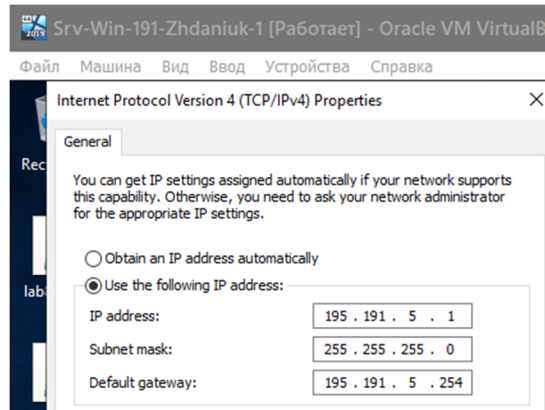


Рис. 3.5. Налаштування адресації на Serv-191-1

На даному сервері створемо домен office.net до якого будуть під'єднуватися робочі станції.

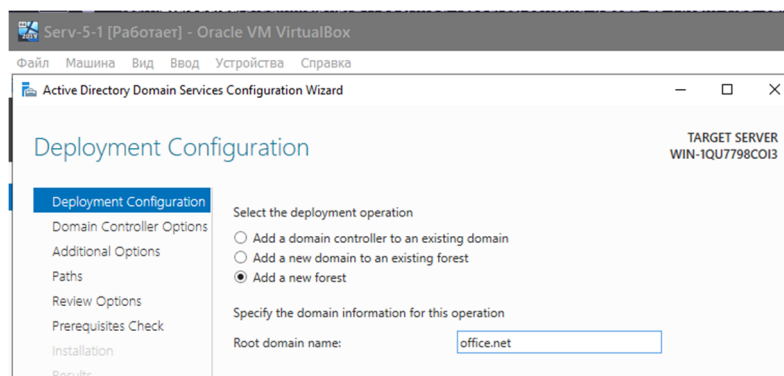


Рис. 3.6. Створення домену office.net

На цьому ж сервері слід створити і налаштувати DHCP сервер, аби робочі станції мали змогу динамічно отримувати адреси. Тому створюю область office_score, рис.3.7 і визначаю діапазон роздачі адрес, рис.3.8.

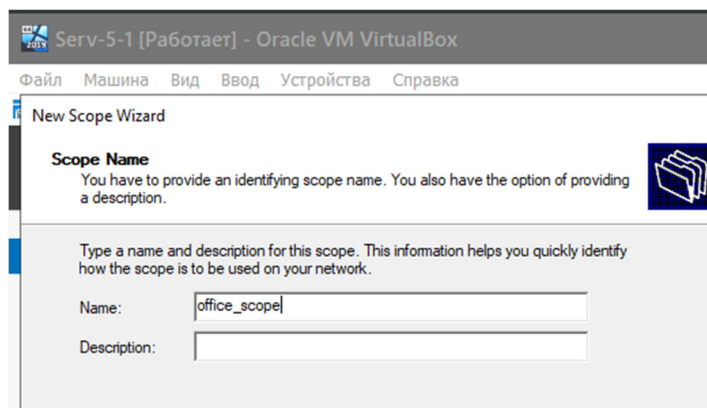


Рис. 3.8. Створення області office_scope

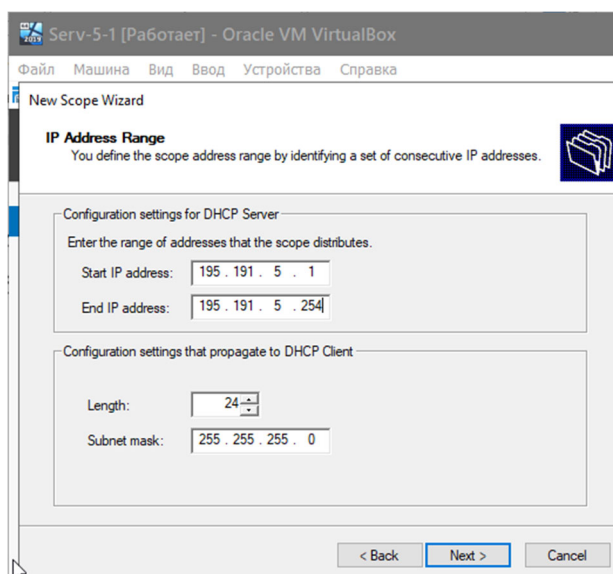


Рис. 3.9. Визначення діапазону роздачі адрес

Тепер визначимо які адреси будуть призначені статично пристоям мережі,
рис. 3.10.

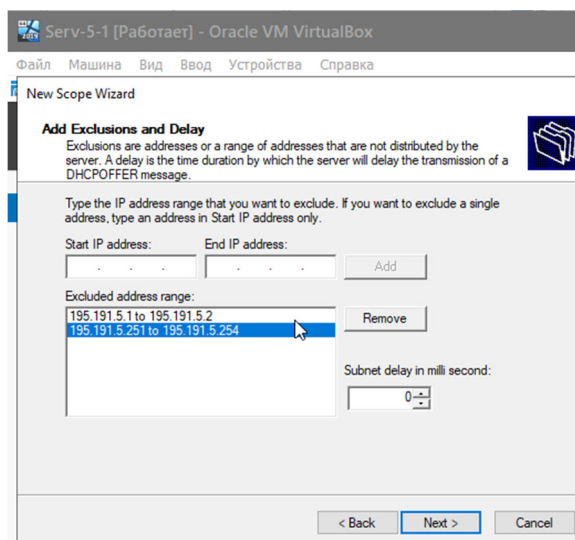


Рис. 3.10. Виключення статичних адрес

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

В налаштуваннях DHCP вказую шлюз за замовчуванням, рис.3.11 та DNS сервер, рис.3.12.

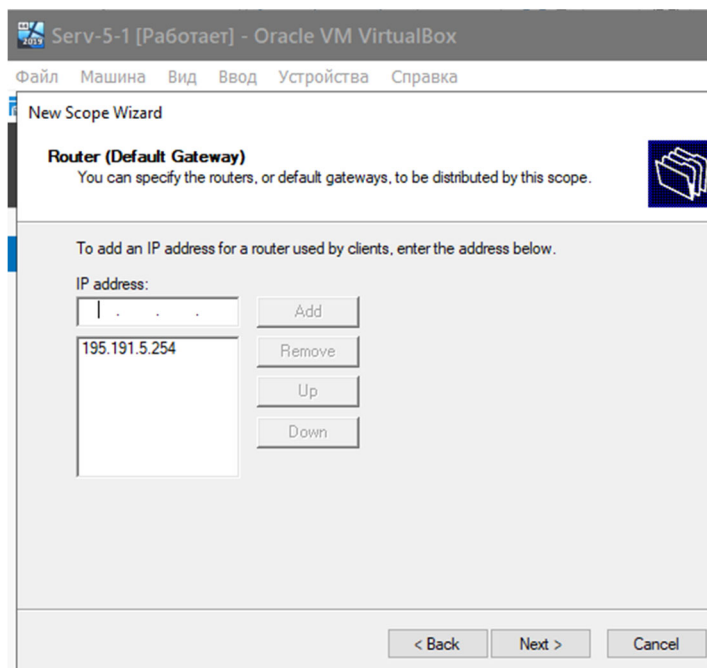


Рис. 3.11. Визначення шлюзу

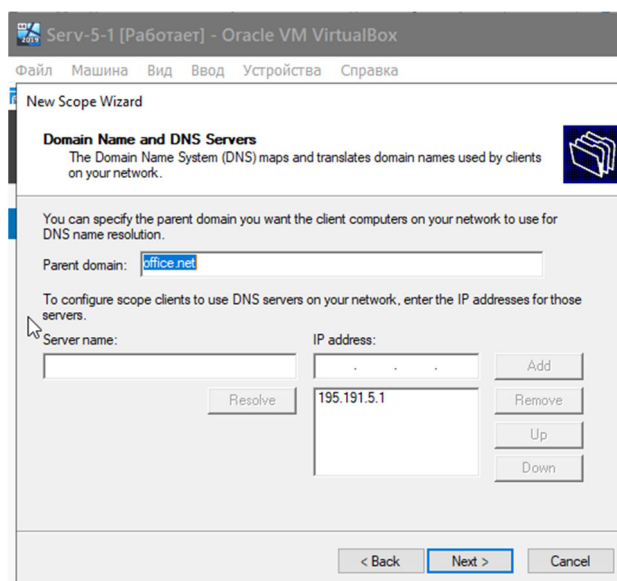


Рис. 3.12. Визначення DNS серверу

Після того як попередні налаштування були зроблені додамо робочу станцію до домену рис.3.13, аби перевірити функціонування мережі та серверу DHCP в цілому.

Оскільки DHCP сервер знаходиться в підмережі 195.191.5.0, то потрібно налаштувати маршрутизатор як агента DHCP-relay рис. 3.14. Маршрутизатор

буде пересилати запити на сервер, а той в свою чергу адресу відповідній підмережі.

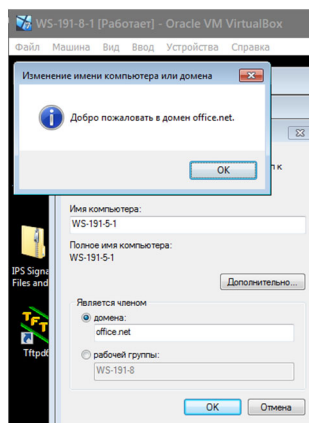


Рис. 3.13. Додавання пристрою WS-191-5-1 до домену office.net

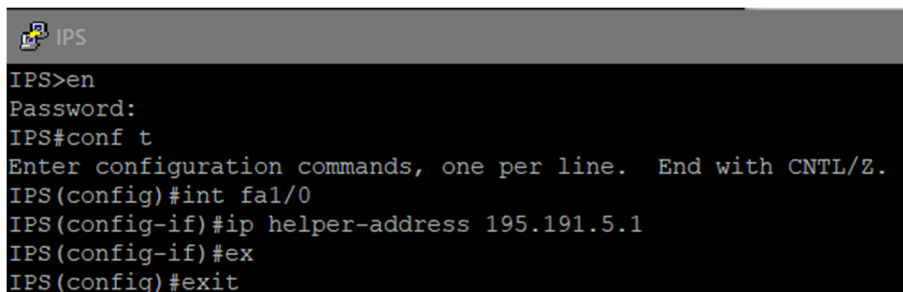


Рис. 3.14. Налаштування DHCP-relay

Наступним етапом буде підготовка маршрутизатора для встановлення IPS. Оскільки сигнатури містять файли яким потрібно десь зберігатися в першу чергу потрібно підготувати пам'ять. Досить важливо також переконатися, що маршрутизатор підтримує функцію IPS. Налаштування відбуватимуться на серії 7200.

Перед встановленням IPS на маршрутизаторі відформатуємо диск 0 та створемо на ньому каталог (рис. 3.15.). Це робиться для того аби підготувати місце на маршрутизаторі під сигнатури, які в свою чергу потрібні для роботи IPS та аналізування трафіку.

```

IPS#format disk0:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "disk0:". Continue? [confirm]
Writing Monlib sectors....
Monlib write complete

Format: All system sectors written. OK...

Format: Total sectors in formatted partition: 1048544
Format: Total bytes in formatted partition: 536854528
Format: Operation completed successfully.

Format of disk0: complete
IPS#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir disk0:/ipsdir
IPS#

```

Рис. 3.15. Створення каталогу в пам'яті маршрутизатора

Далі з завантажених з офіційного сайту cisco сигнатур, потрібно скопіювати криптографічний ключ і ввести його в маршрутизаторі(рис. 3.16.).

```

IPS(config)#crypto key pubkey-chain rsa
IPS(config-pubkey-chain)#named-key realm-cisco.pub signature
Translating "realm-cisco.pub"

IPS(config-pubkey-key)#key-string
Enter a public key as a hexadecimal number ....

IPS(config-pubkey)#$64886 F70D0101 01050003 82010F00 3082010A 02820101
IPS(config-pubkey)#$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
IPS(config-pubkey)#$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
IPS(config-pubkey)#$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
IPS(config-pubkey)#$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
IPS(config-pubkey)#$994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
IPS(config-pubkey)#$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
IPS(config-pubkey)#$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
IPS(config-pubkey)#$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
IPS(config-pubkey)# F3020301 0001
IPS(config-pubkey)#quit
IPS(config-pubkey-key)#

```

Рис. 3.16. Введення криптографічного ключа

Далі нам потрібно ввімкнути сповіщення о подіях та налаштувати syslog для IPS, для журналювання подій. Всі повідомлення будуть надсилатися на комп'ютер адміністратора. На робочій станції адміністратор матиме змогу аналізувати трафік в реальному часі та зберігати логи.

```

IPS(config)#ip ips name iosips
IPS(config)#ip ips config location disk0:ipsdir
IPS(config)#ip http server
IPS(config)#ip ips notify sdee
IPS(config)#ip ips notify log
IPS(config)#clock set 15:36:00 29 may 2023
^
% Invalid input detected at '^' marker.

IPS(config)#ex
% Ambiguous command: "ex"
IPS(config)#exit
IPS#conf t
*May 29 15:13:43.355: %SYS-5-CONFIG_I: Configured from console by admin01 on console
IPS#clock set 15:37:00 29 may 2023
IPS#
*May 29 15:37:00.003: %SYS-6-CLOCKUPDATE: System clock has been updated from 15:14:29 UTC Mon May 29 2023 to 15:37:00 UTC Mon May 29 2023, configured from console by admin01 on console.
IPS#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IPS(config)#service timestamps log datetime msec
IPS(config)#logging 195.191.5.1
IPS(config)#
May 29 15:37:56.395: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 195.191.5.1 port 514 started - CLI initiated
IPS(config)#

```

		Жданюк Є.В.			KIK.KP.B – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Рис. 3.17. Налаштування сповіщення на маршрутизаторі IPS

Далі потрібно відкрити одну з передчасно заданих категорій сигнатур та задати інтерфейси до яких будуть задіяні правила аналізування трафіку.

```
IPS(config)#ip ips signature-category
IPS(config-ips-category)#category all
IPS(config-ips-category-action)#retired true
IPS(config-ips-category-action)#exit
IPS(config-ips-category)#category ios_ips basic
IPS(config-ips-category-action)#retired false
IPS(config-ips-category-action)#exit
IPS(config-ips-category)#exit
Do you want to accept these changes? [confirm]
IPS(config)#
May 29 15:45:57.235: Applying Category configuration to signatures ...
IPS(config)#int fa0/0
IPS(config-if)#ip ips iosips in
IPS(config-if)#
*****
The signature package is missing or was saved by a previous version
IPS Please load a new signature package
*****
May 29 15:47:17.667: %IPS-3-SIG_UPDATE_REQUIRED: IOS IPS requires a signature update
package to be loaded
IPS(config-if)#
```

Рис. 3.18. Налаштування категорії та інтерфейсу який перевірятиметься

За замовчуванням всі echo запити заблокованні. Внесемо зміни в налаштування IPS аби дозволити ці запити, для зручності налаштування мережі.

```
IPS(config)#ip ips signature-definition
IPS(config-sigdef)#signature 2004 0
IPS(config-sigdef-sig)#status
IPS(config-sigdef-sig-status)#retired false
IPS(config-sigdef-sig-status)#enabled true
IPS(config-sigdef-sig-status)#engine
IPS(config-sigdef-sig-engine)#event-action produce-alert
IPS(config-sigdef-sig-engine)#event-action deny-packet-inline
IPS(config-sigdef-sig-engine)#event-action reset-tcp-connection
IPS(config-sigdef-sig-engine)#exit
IPS(config-sigdef-sig)#exit
IPS(config-sigdef)#exit
Do you want to accept these changes? [confirm]
IPS(config)#
```

Рис. 3.19. Ввімкнення echo запитів

Оскільки під час налаштування IPS було повідомлення про відсутність встановлених сигнатур, потрібно під'єднати робочу станцію на яку було завантажено сигнатури. Передача файлів буде відбуватися за допомогою додатку TFTP32.

Для забезпечення зв'язку між маршрутизатором та робочою станцією налаштуємо комутатор.

```
IOU1(config)#ip domain-lookup
IOU1(config)#ip name-server 195.191.5.1
IOU1(config)#ip domain-name office.net
IOU1(config)#ip default-gateway 195.191.5.254
IOU1(config)#
```

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

```

IOU1(config)#int eth0/0
IOU1(config-if)#duplex full
IOU1(config-if)#ex
IOU1(config)#int vlan1
IOU1(config-if)#ip add 195.191.5.251 255.255.255.0
IOU1(config-if)#no sh
IOU1(config-if)#ex
IOU1(config)#hostname SW-5-1
SW-5-1(config)#

```

Рис. 3.20. – 3.21. Базове налаштування комутатора

Після всіх підготовчих робіт можемо приступати безпосередньо до завантаження сигнатур з робочої станції на маршрутизатор.

```

IPS
IPS con0 is now available

Press RETURN to get started.

User Access Verification

Username: admin01
Password:
IPS>en
Password:
IPS#copy tftp://195.191.5.1/IOS-S855-CLI.pkg idconf
Loading IOS-S855-CLI.pkg from 195.191.5.1 (via FastEthernet0/1): !!!!!

```

Рис. 3.22. Початок завантаження сигнатур з серверу

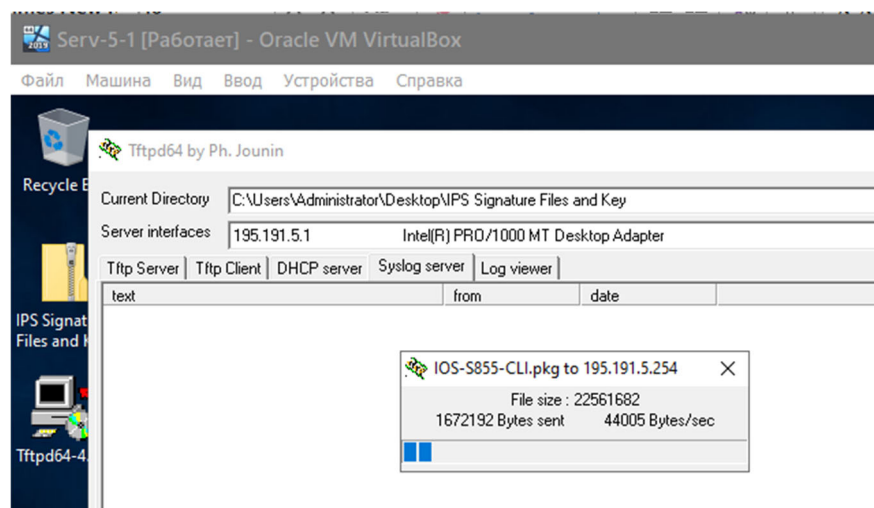


Рис. 3.23. Відображення процесу завантаження на сервері

Аби забезпечити зв'язок між маршрутизаторами було налаштовано протокол OSPF.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 195.191.3.0 0.0.0.255 area 0
R1(config-router)#network 195.191.2.0 0.0.0.255 area 0
R1(config-router)#exit
R1(config)#

```

Рис. 3.24. Налаштування OSPF на маршрутизаторі

3.3 Тестування працездатності мережі.

Проведемо сетування підсистеми захисту мережевої інфраструктури з метою перевірки налаштувань.

Почнімо нашу перевірку з серверу DHCP та його роботи. За проєктом передбачено, що Windows Server повинен роздавати адреси.

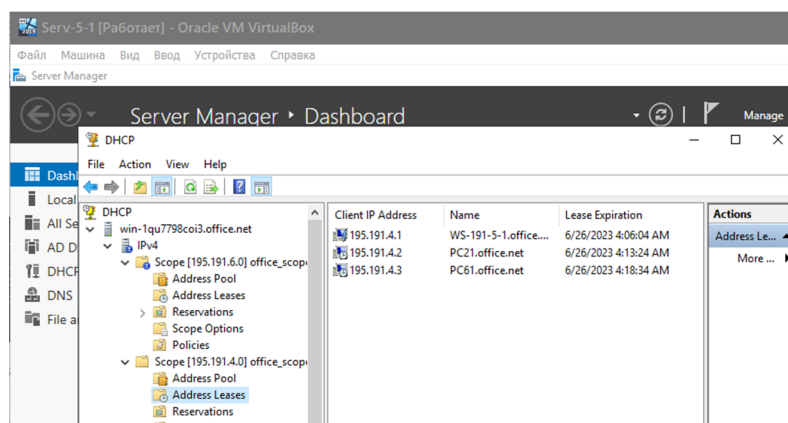


Рис. 3.25. Список виданих адрес в AD

```

PC2 - PuTTY
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" lic
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip dhcp
DORA IP 195.191.4.2/24 GW 195.191.4.254

PC2> ping 195.191.5.1
84 bytes from 195.191.5.1 icmp_seq=1 ttl=127 time=19.619 ms
84 bytes from 195.191.5.1 icmp_seq=2 ttl=127 time=14.906 ms
84 bytes from 195.191.5.1 icmp_seq=3 ttl=127 time=16.419 ms
84 bytes from 195.191.5.1 icmp_seq=4 ttl=127 time=14.972 ms
84 bytes from 195.191.5.1 icmp_seq=5 ttl=127 time=16.932 ms

PC2>

```

Рис. 3.26. Перевірка запиту DHCP та зв'язку мережі

		Жданюк Є.В.			KIK.KP.B – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

В роботі було сказано, що сервер мав отримувати повідомлення про всі події. Перевіримо і це налаштування.

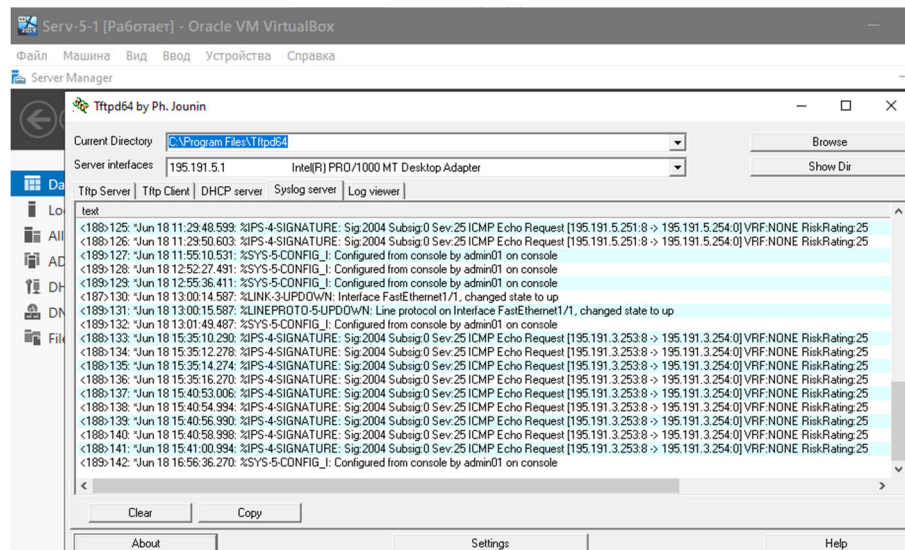


Рис. 3.27. Syslog server та події

Висновки до третього розділу

В третьому розділі було проведено та описано базову конфігурацію пристроїв мережі. Було встановлено та налаштовано домен організації. До якого в свою чергу були під'єднані робочі станції працівників. Динамічна маршрутизація була налаштована як один з інструментів Active Directory. Всі пристрої мережі отримали відповідь під час DHCP запиту, а видані адреси записалися на комп'ютер адміністратора.

Також було встановлено IPS, який збирає та аналізує трафік. Для зв'язку маршрутизаторів було налаштовано протокол OSPF.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В даній кваліфікаційній роботі була створена ієрархічна топологія підсистеми захисту мережевої інфраструктури на базі Network-based IPS. Для реалізації мережі використовувалися образи мережевих пристроїв компанії cisco.

В першому розділі було визначено особливості проектування корпоративних мереж та їх основні функції. Було розглянуто призначення технології IPS, а також існуючі протоколи зазначаючи їх переваги та недоліки. Детально було розглянуто протокол IPS вказавши його переваги та можливості.

В другому розділі було розроблено топологію корпоративної мережі організації. Визначено затребувану кількість мережевого обладнання, робочих станцій. Розроблено схеми адресацій відповідно до кількості девайсів в мережі та належність до домену. Було вирішено, що мережа матиме сервер за допомогою якого буде відбуватися все керування мережі та на який будуть надсилатися повідомлення про трафік мережі. Для зменшення навантаження на маршрутизатор також було прийняте рішення надати Windows серверу роль DHCP серверу.

Також в даному розділі було вирішено, які вимоги ставитимуться до мережевих пристроїв, щоб обрати найбільш оптимальний варіант. Аби задовольнити потреби, які могли виникнути під час реалізації проєкту мережі. В роботі був використаний образ c7200-adventerprisek9-mz.152-4.M7.image. Під час налаштування якого з проблемою несумісності з технологією IPS не зіткнувся. З чого маємо висновок, що завдання з підбором обладнання виконано.

В третьому розділі проаналізувавши вимоги створеної мережі, було обрано моделі маршрутизаторів та комутаторів. Також було розглянуто та коротко описано додатки, які використовувалися під час роботи та їх особливості призначення. В даному розділі було детально описано важливі кроки налаштування мережі такі як: встановлення IPS, створення та налаштування домену та ін. Також були використанні сигнатури, які потім були встановленні в маршрутизатор. Наявність зв'язку між пристроями мережі перевірено.

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж. Навчальний посібник. С. В. Мінухін, С. В. Кавун, С. В. Знахур. – Харків: Вид. ХНЕУ, 2008. – с. (Укр. мов.)
2. Cisco IDS/IPS Fundamentals [Електронний ресурс] – Режим доступу до ресурсу: <https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals>
3. CCNA-Security-Configure-an-Intrusion-Prevention-System-(IPS) [Електронний ресурс] – Режим доступу до ресурсу: [https://education.cisco.org/docs/CCNA-Security-Configure-an-Intrusion-Prevention-System-\(IPS\).pdf](https://education.cisco.org/docs/CCNA-Security-Configure-an-Intrusion-Prevention-System-(IPS).pdf)
4. IPS Security: How Active Security Saves Time and Stops Attacks in their Tracks [Електронний ресурс] – Режим доступу: <https://www.exabeam.com/ueba/ips-security-how-active-security-saves-time-and-stop-attacks-in-their-tracks/>
5. Мережна академія Cisco [Електронний ресурс] – Режим доступу: <https://www.netacad.com/>
6. Intrusion Prevention System (IPS) [Електронний ресурс] – Режим доступу: <https://www.geeksforgeeks.org/intrusion-prevention-system-ips/>
7. Визначення «сервер» [Електронний ресурс] – Режим доступу: <https://www.ionos.com/digitalguide/server/know-how/what-is-a-server-one-term-two-definitions/>
8. DHCP [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/DHCP>
9. Посібник cisco по IPS [Електронний ресурс] – Режим доступу: https://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_fwids.html#wp1112220
10. Визначення корпоративна мережа [Електронний ресурс] – Режим доступу: https://ceopedia.org/index.php/Corporate_network

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

11. Теорія по Intrusion Prevention System [Електронний ресурс] – Режим доступу: <https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html>
12. Що таке IPS/IDS [Електронний ресурс] – Режим доступу: <https://www.cloud4y.ru/blog/ips-and-ids-what-is-it/>
13. GNS3 [Електронний ресурс] – Режим доступу: <https://habr.com/ru/post/266503/>
14. VirtualBox [Електронний ресурс] – Режим доступу: <https://www.virtualbox.org/>
15. Cisco Router 7200 [Електронний ресурс] – Режим доступу: [Cisco 7200 Series Routers - Cisco](#)

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

IPS#show running-config
Building configuration...

Current configuration : 3163 bytes

!

! Last configuration change at 13:01:49 UTC Sun Jun 18 2023 by admin01

upgrade fpd auto

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname IPS

!

boot-start-marker

boot-end-marker

!

!

enable secret 9 \$9\$0wHcMQEX5jNqZx\$BjPxawgjSaijrd.SLIzRfk6BouzoOHSqUHTVUQc0Kbo

!

no aaa new-model

no ip icmp rate-limit unreachable

!

!

!

!

!

!

!

no ip domain lookup

ip domain name IPS

ip ips config location disk0:ipsdir retries 1

ip ips notify SDEE

ip ips name iosips

!

ip ips signature-category

category all

retired true

category ios_ips basic

retired false

!

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

!

!

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

```

!
!
!
!
username admin01 secret 9
$9$QhU.s8oBdodooK$1Qw9HCMfbc4GTJu6tGLjHdcSYRpWm2DjEZ4W
I53ijpA
!
redundancy
!
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 195.191.3.254 255.255.255.0
ip ips iosips in
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 195.191.5.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 195.191.4.254 255.255.255.0
ip helper-address 195.191.5.1

```

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```

duplex auto
speed auto
!
interface FastEthernet1/1
ip address 195.191.6.254 255.255.255.0
ip helper-address 195.191.5.1
duplex auto
speed auto
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet6/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet6/1
no ip address

```

		Жданюк Є.В.			КІК.КР.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

```

shutdown
duplex auto
speed auto
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
!
!
logging host 195.191.5.1
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 5 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
!
!
end

```

		Жданюк Є.В.			KIK.KP.Б – 123 – 05 – ПЗ	Арк.
		Байлюк Є.М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		