

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

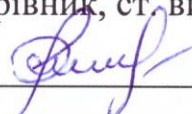
на тему:

«Проект підсистеми периметрового захисту корпоративної
мережі організації»

Виконав студент 4-го курсу, групи КБ-2
спеціальності 125 «Кібербезпека»

 Фальковський Б.С.

Керівник, ст. викладач кафедри КІ та КБ

 Байлюк Є.М.

Рецензент, ст. викладач кафедри КІ та КБ

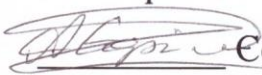
 Покотило О.А.

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

 Сфіменко А. А.

1 березня 2022р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу

Студента **Фальковського Богдана Сергійовича**

Тема роботи: Проект підсистеми периметрового захисту корпоративної мережі організації

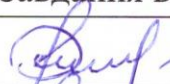
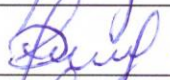
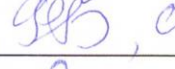
затверджена Наказом по університету від 1 березня 2022 р. № 128/с

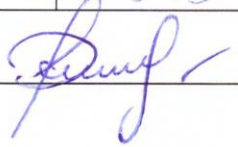
Термін здачі студентом закінченої роботи – 10 червня 2022р.

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, TacacsGUI
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.	 06.03.22	 07.03.22
2	Байлюк Є.М.	 06.03.22	 07.03.22
3	Байлюк Є.М.	 06.03.22	 07.03.22

Керівник  Байлюк Є.М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2022 – 7 березня 2022	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації периметрового захисту мережі	8 березня 2022 – 11 березня 2022	Виконано
3	Аналіз технологій периметрового захисту на основі міжмережного екрану	12 березня 2022 – 16 березня 2022	Виконано
4	Аналіз можливостей мережного обладнання Cisco для гетерогенності мережі	17 березня 2022 – 19 березня 2022	Виконано
5	Розробка загального проекту мережі організації	20 березня 2022– 24 березня 2022	Виконано
6	Проектування мережі та вибір обладнання для її реалізації	25 березня 2022 – 30 березня 2022	Виконано
7	Проектування таблиці маршрутизації	1 квітня 2022 – 4 квітня 2022	Виконано
8	Проектування сценарію тестування мережі	5 квітня 2022– 9 квітня 2022	Виконано
9	Базове налагодження пристроїв мережі	10 квітня 2022– 13 квітня 2022	Виконано
10	Налагодження гетерогенної мережі	14 квітня 2022– 18 квітня 2022	Виконано
11	Тестування роботи гетерогенної мережі	19 квітня 2022– 22 квітня 2022	Виконано
12	Аналіз результатів тестування	23 квітня 2022– 24 квітня 2022	Виконано
13	Написання пояснювальної записки	25 квітня 2022– 29 квітня 2022	Виконано
14	Підготовка презентації та виступу	12 травня 2022	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	13 травня 2022	Виконано
16	Захист	25 травня 2022	Виконано

Студент  Фальковський Б.С.

Керівник  Байлюк Є.М.

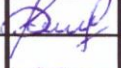
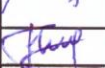
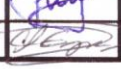
РЕФЕРАТ

Кваліфікаційна робота складається з проєкту підсистеми периметрового захисту корпоративної мережі організації. Пояснювальна записка містить 58 сторінок, 49 ілюстрацій та 9 таблиць.

Дипломний проєкт присвячений розробці проєкту підсистеми периметрового захисту корпоративної мережі організації. Метою проєкту буде надійність, можливість масштабованості та захищеність. Мережа повинна забезпечувати надійний та безперебійний обмін даними. Також для захисту пристроїв у разі стороннього доступу було створено користувачів для віддаленого та фізичного доступу.

Дипломний проєкт складатиметься з трьох розділів, в яких буде продемонстровано розробку логічної та фізичної структури мережі, вибір обладнання та ПЗ, конфігурація пристроїв. В додатках буде вказано конфігурації ASA-971, маршрутизаторів та комутаторів мережі.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, КОРПОРАТИВНА МЕРЕЖА ОРГАНІЗАЦІЇ, ASA, TACACS, CISCO.

					КБ.КВ.Б – 125 -22 -ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проєкт підсистеми периметрового захисту корпоративної мережі організації	Літ.	Арк.	Аркушів
Розроб.		Фальковський Б.С.		16.06				
Керівник		Байлюк Є.М.		16.06			4	70
Рецензент.		Покотило О.А.		16.06		Державний університет «Житомирська політехніка», група КБ-2		
Зав. каф.		Єфіменко А. А.		16.06.22				

ABSTRACT

Qualification work consists of a project of the subsystem of perimeter protection of the corporate network of the organization. The explanatory note contains 58 pages, 49 illustrations and 9 tables.

The thesis project is devoted to the development of the subsystem of perimeter protection of the corporate network of the organization. The aim of the project will be reliability, scalability and security. The network must ensure reliable and uninterrupted data exchange. Users for remote and physical access have also been created to protect devices in the event of third-party access.

The graduation project will consist of three sections, which will demonstrate the development of logical and physical structure of the network, the choice of equipment and software, device configuration. The appendices will list the configurations of the ASA-971, routers, and network switches.

KEY WORDS: PROTECTION, COMPUTER NETWORK, CORPORATE ORGANIZATION NETWORK, ASA, TACACS, CISCO.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ	4
ABSTRACT	5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ КОРПОРАТИВНОЇ ОСНОВИ ЇЇ ДИЗАЙНУ ТА ВИМОГИ ДО НЕЇ	10
1.1 Особливості побудови корпоративної мережі	10
1.2 Ієрархічна модель мережі	11
1.3 Інтернет модуль	13
РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З ПІДСИСТЕМОЮ ПЕРИМЕТРОВОГО ЗАХИСТУ	21
2.1 Принципи роботи мережі	21
2.2 Розробка логічної структури мережі	25
2.3 Вибір обладнання та програмного забезпечення	29
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	35
3.1 Налаштування мережі	35
3.2 Тестування підсистеми периметрового захисту корпоративної мережі організації.	50
3.3 Аналіз результатів тестування	53
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	56
ДОДАТКИ	58

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

ASA – міжмережний екран

GNS3 – Graphical Network Simulator-3

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Інформаційна безпека (ІБ) – це стан захищеності системи, при якому забезпечується конфіденційність, доступність і цілісність інформації. [2] Але ця поняття майже завжди асоціюється з чимось складним, незрозумілим або навіть дратівливим. Деякі користувачі просто ненавидять ту саму безпеку, особливо коли їм раптово відмовляють у доступі до улюблених веб-сайтів або їхні дозволи на зберігання файлів обмежені. Більшість людей думають, що ІБ — це міф, доки самі не потраплять у біду. Враховуючи останні тенденції комп'ютеризації, можливостей для зловмисників стає все більше, а ми стаємо все більш вразливими.

Багато людей часто використовують термін «кібербезпека» як синонім «інформаційної безпеки». Це просто неправда. Під кібербезпекою ми маємо на увазі захист нашої ІТ-інфраструктури від зловмисників (зовнішніх і внутрішніх), а також запобігання випадковим помилкам співробітників. Правильно, небезпека не тільки від хакерів. Наші власні користувачі так само небезпечні, як і хакери, навіть не підозрюючи про це.

Захист інформації схожий на гонку озброєнь, за винятком того, що хакери завжди на крок попереду. Завжди буде перша жертва, а потім описи цих вразливостей, різні виправлення та оновлення захисту. Серйозні структури, такі як ФБР, Пентагон та Служба безпеки України, регулярно руйнуються, а бюджет ІД, який оцінюється в мільярд доларів, є найкращою роботою в службі безпеки. Але коли просунуті хакери ретельно намагаються знайти ключі до найсучаснішого захисту, навіть вони не можуть захиститися від цілеспрямованих атак. Як би божевільним це не звучало, навіть повністю ізольована мережа (відключена від Інтернету) вразлива для успішної атаки. Сучасні віруси здатні проникати в закриту мережу через флешку співробітника, збирати необхідну інформацію і терпляче чекати, коли зможуть вирватися через ту ж флешку.

Але якщо все так погано, навіщо захищатися? Але на перший погляд все виглядає погано. Відсоток таких цілеспрямованих атак мізерно малий у

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

порівнянні з «німими» атаками. Переважна більшість вторгнень у мережі здійснюється за допомогою найпростіших і відомих методик. Вам не потрібно бути експертом-хакером, щоб повторити цей тип атаки. Просто завантажте спеціалізований дистрибутив (наприклад, Kali Linux[9]) і скористайтесь готовими хакерськими програмами. Вам не потрібне глибоке розуміння стеку TCP/IP, навички програмування чи сучасні інструменти безпеки. Просто завантажте дистрибутив, натисніть кілька кнопок і готово. Ви навіть можете завантажити готові віруси/трояни і відправити їх поштою.

Крім того, як зазначалося раніше, під загрозою не лише зовнішні «вороги», а й внутрішні користувачі. Необережна поведінка може призвести до тривалого простою мережі або відкрити вікно для зовнішніх зловмисників. Тому не варто скаржитися на відсутність захисту і забути внести належні налаштування основного мережевого обладнання. Навіть на рівні комутатора та маршрутизатора переважну більшість кіберзагроз можна усунути.

Для реалізації підсистеми буде використовуватися графічний симулятор GNS3.

Метою кваліфікаційної роботи є розробка підсистеми периметрового захисту корпоративної мережі організації.

Встановлена мета створює наступні завдання:

- аналіз сучасних приладів;
- вибір структури мережі;
- вибір ПЗ для реалізації мережі;
- реалізація підсистеми захисту;

Об'єктом дослідження є процес налаштування захисту комп'ютерної мережі від зловмисників.

Предметом дослідження методи і засоби захисту корпоративної мережі за допомогою Cisco ASA.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ КОРПОРАТИВНОЇ ОСНОВИ ЇЇ ДИЗАЙНУ ТА ВИМОГИ ДО НЕЇ

1.1 Особливості побудови корпоративної мережі

Корпоративна мережа – це мережа, головною функцією якої є підтримка роботи підприємства, що володіє даною мережею. Користувачами мережі є тільки співробітники даного підприємства. [1]

Простіше кажучи, корпоративна мережа – це досить закрита для зовнішнього світу мережа, яка забезпечує надійний захист від вторгнень, а також вирішення всіх завдань, які можуть бути поставлені перед підприємством.

Основними характеристиками корпоративної мережі є:

- Операційні можливості – це перелік основних дій по обробці та збереженню даних;
- Час доставки повідомлень – середньо статистичний час від моменту передачі повідомлення до моменту отримання повідомлення адресатом;
- Продуктивність мережі – сумарна продуктивність серверів мережі, які приймають участь в інформаційному обміні;
- Вартість обробки даних – формується з врахуванням вартості засобів, які використовуються для вводу-виводу, передачі, обробки та збереження даних.

Важливо відмітити, що характеристики корпоративної мережі також залежать від її архітектури, тобто це має бути комплекс, який має все необхідне для захисту мережі, достатньо стабільний, а якщо потрібно розширити мережу, то це не повинно бути проблемою.

Головними цілями такої архітектури мають бути:

- Простота впровадження – розгортання в найкоротші терміни;
- Гнучкість і масштабованість – модульна архітектура має дозволяти вносити в мережу тільки ті зміни, які необхідні на даний момент, з можливістю подальшого зростання інформаційно інфраструктури;

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

- Відмовостійкість і безпека – захисти трафіку користувачів у мережі та гарантія стабільної роботи мережі навіть під час атак;
- Простота управління – централізація управління усією мережевою інфраструктурою;
- Готовність до нових технологій – наявна можливість для легкого впровадження нових технологій та сервісів.

Також необхідний принцип модульності мережі. Розбиття архітектури мережі на модулі допоможе зосередитися на налаштуваннях і функціях кожного модуля окремо, що значно спрощує проектування, впровадження нововведень та керування мережею. Модулі, як частина конструктора, з якого можна створити мережу в залежності від поставленого завдання. Ці ж деталі можна використовувати повторно, тобто дублювати, що заощадить час на проектування мережі. Також така практика значно спрощує масштабованість мережі та її розгортання. На рис. 1.1. продемонстровано процес модернізації мережі і можна побачити, що розширення зводиться до звичайного додавання нових модулів.

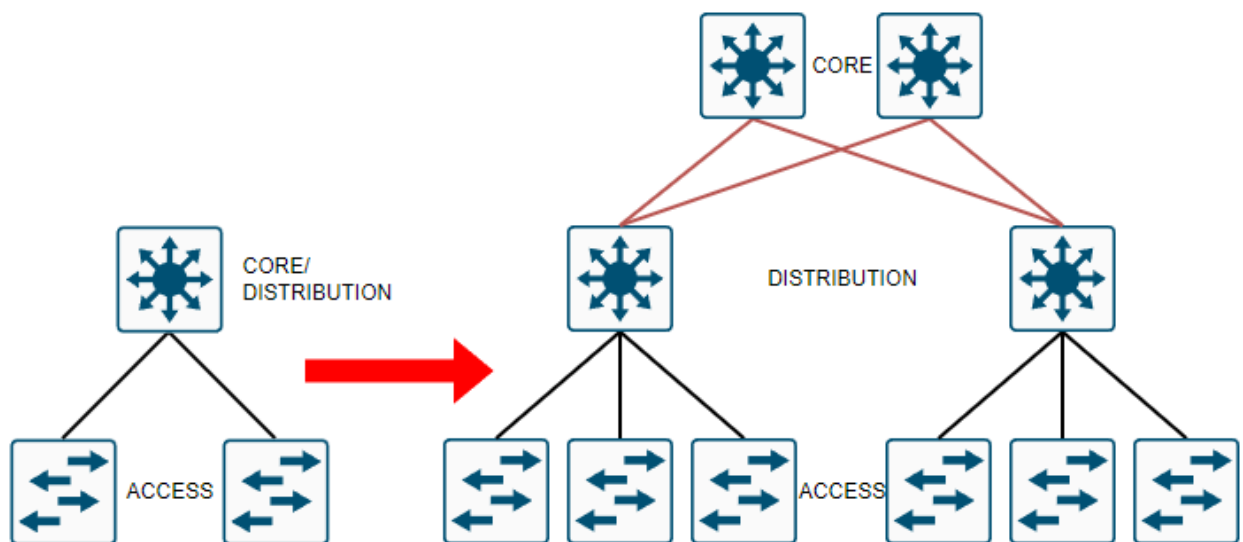


Рис. 1.1. Приклад модернізації мережі

1.2 Ієрархічна модель мережі

Ієрархічна модель розроблена для створення надійних, масштабованих та ефективних мереж. Цей підхід забезпечує економічний, модульний, структурований і простий спосіб задовольнити існуючі та майбутні потреби

зростання мережі. Кожен з цих рівнів має свої особливості та функції, що ще більше спрощує побудову мережі.

Ієрархічна модель ділить мережу на три основних рівня[15]:

1. Рівень доступу – надає користувачам і пристроєм доступ до мережі. Включає в себе комутатори 2 рівня і точки доступу, що забезпечують підключення до робочих станцій і серверів;

Основні функції:

- Комутація 2 рівня;
- Висока доступність;
- Безпека портів;
- Класифікація та маркування;
- Кордони довіри;
- Списки контролю доступу(ACL);
- Кістяк.

2. Рівень розподілу – об'єднує рівні доступу, а також надає доступ до різних сервісів організації. Розташований між рівнями доступу та ядра, основною функцією є забезпечення маршрутизації і фільтрації, а також створює зв'язок між рівнями доступу та ядра;

Основні функції:

- Акумуляування каналів LAN/WAN;
- Контроль доступу та фільтрація;
- Маршрутизація між локальними мережами;
- Балансування навантаження;
- Агрегування маршрутів на кордонах/до рівня ядра;
- Управління широкомовним доменом.

3. Рівень ядра - об'єднує рівні розподілу в великих мережах. Магістральний рівень, відповідає за забезпечення швидкого трафіку між розподільними комутаторами в межах кампусу організації.

Основні функції:

- Висока продуктивність і наскрізна комутація;

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

- Забезпечення надійності та відмовостійкості;
- Масштабованість.

1.3 Інтернет модуль

Уявити сучасну компанію без доступу до Інтернету просто неможливо. Сьогодні велика кількість бізнес-процесів пов'язана з використанням Інтернет-ресурсів, тобто веб-сайтів, електронної пошти тощо. Доступ до Інтернету має бути стабільним і безпечним. Необхідно забезпечити високошвидкісний доступ до Інтернету для працівників підприємства та забезпечити надійний захист від зовнішніх перешкод. Тому в мережі має бути Internet Edge (Internet Edge).

Internet Edge, у свою чергу, розділений на кілька блоків, кожен з яких виконує свої функції та надає необхідні послуги. Розбиття на кілька модулів полегшує масштабування, керування та налагодження, тобто організації зможуть впроваджувати нову функціональність на основі своїх можливостей та потреб, тож ви можете використовувати лише ті модулі, які вам потрібні.

Інтернет-модуль - це частина мережі, яка з'єднує локальну мережу з глобальною мережею. Коротше кажучи, це як межа між загальнодоступною мережею компанії та приватними ресурсами, і саме тут розташований брандмауер, який захищає мережу від зовнішніх загроз, таких як віруси, атаки та шкідливе програмне забезпечення, фільтруючи небажаний і небажаний трафік.

Інтернет модуль включає в себе такі модулі:

- Міжмережний екран – дозволяє або забороняє доступ в середину мережі(списки доступу), надає такий функціонал, як NAT і DMZ.

В якості міжмережного екрану під час написання дипломної роботи в побудованій віртуальній мережі використовувався Cisco ASA (971 версії). Це найбільш сучасна серія міжмережних екранів. Адже будь-якому замовнику, який використовує мережу, необхідний надійний захист. Системи захисту ASA гарантують найвищий рівень безпеки з достатнім рівнем гнучкості, який

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

буде оптимальним для мережі будь-якого розміру. Мережа з надійним захистом, означає безперебійність бізнесу для компанії.

Основні функції Cisco ASA:

- Конфігурація – дозволяє налаштувати безпеку відповідно до потреб і політик компанії;
- Гнучкість – в процесі розвитку бізнесу, завжди є необхідність поповнювати набір функцій і оновлень мережі.
- Розширені можливості безпеки – новітні технології забезпечення безпеки, шифрування, автентифікації, авторизації і попередження вторгнень;
- Простота застосування – легко встановлювати, адмініструвати і контролювати;
- Потужні мережеві можливості – налаштування віртуальних приватних мереж забезпечує для віддалених співробітників безпечний доступ до ресурсів компанії.

Системи серії Cisco ASA допомагають захищати корпоративну мережу від інтернет-зловмисників, крадіжки даних та мережевих атак, збільшують капіталізацію підприємства за рахунок підвищення ефективності та продуктивності, працюють у поєднанні з маршрутизаторами Cisco з інтегрованими сервісами, прості у використанні та управлінні.

- IPS – інспектує трафік у випадку підозрілої активності.

IPS (система попередження вторгнень) – програмна або апаратна система мережевої і комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки та автоматично захищає від них. Виступає в якості додаткового захисту корпоративної мережі від вірусів і шкідливих програм, які уже проникли в мережу, на відміну від міжмережного екрану, який захищає тільки від проникнення в локальну мережу із зовні.

- Віддалений доступ – надання безпечного віддаленого доступу до локальної мережі корпорації.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

Необхідність віддаленого доступу виникає практично в кожній мережі організації, тому всім завжди необхідне захищене підключення до внутрішніх інформаційних ресурсів компанії.

– Захист електронної пошти – захист від спаму.

Електронна пошта є одним із найважливіших функціоналів в більшості організацій, відсутність захисту в цьому модулі може призвести до втрати даних або до втручання із зовні, основними загрозами є: спам – отримання небажаної пошти і шкідливі листи із різним програмним забезпеченням, яке може зашкодити стабільній роботі мережі.

1.4 Серверний модуль

Сервер – це виділений або спеціалізований комп’ютер із групи персональних комп’ютерів для виконання сервісних задач без безпосередньої участі людини у цьому. Сервер і робоча станція можуть мати однакову апаратну конфігурацію, єдина відмінність між ними у участі в роботі людини за консоллю.

Деякі сервісні завдання можуть виконуватися на робочій станції паралельно з роботою користувача, таку робочу станцію умовно називають невиділеним сервером.

Консоль і участь людини необхідні серверу тільки на стадії первинного налаштування, при апаратно-технічному обслуговуванні та управлінні в позаштатних ситуаціях.

В дипломній роботі використовувались DHCP-сервер та TACACS-сервер у якості невиділеного сервера.

DHCP-сервер – необхідний для великих мереж і для комфортної роботи з багатьма робочими станціями у випадку розширення мережі. Головним його завданням виступає, автоматичне налаштування мережевих адаптерів робочих станцій, він може використовуватися, як на базі маршрутизаторів Cisco, так і на базі серверів.

Протокол DHCP працює за схемою клієнт-сервер[6]. Під час запуску робоча станція, яка є клієнтом, відправляє в мережу запит на отримання IP-

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

адреси, сервер у відповідь відправляє основні конфігураційні параметри мережевого адаптера.

DHCP дозволяє автоматично налаштовувати такі основні параметри:

- IP-адресу;
- маску мережі;
- основний шлюз;
- ім'я домену;
- DNS сервер [5].

Розглянемо детальніше процес отримання клієнтом даних від DHCP-серверу. Клієнт котрий потребує адресу, відправляє пакет DHCPDISCOVER у пошуках сервера, потім сервер розглядає цей запит і посилають у відповідь пакет DHCPOFFER, що містить IP-адресу і її час оренди, клієнт обирає адресу і відправляє пакет DHCPREQUEST з адресом вибраного серверу.

Сервер котрого обрав клієнт відправляє пакет підтвердження DHCPACK, на цьому процес надання IP-адреси закінчується. DHCPACK містить адресу та час її оренди, сервер позначає цю адресу, як уже заняту, тобто її уже не зможе отримати інший пристрій, після цього клієнт може почати роботу в мережі.

Варто відмітити що, на пакет DHCPDISCOVER, може відповісти декілька серверів, клієнт обирає одного з них і відправляє DHCPREQUEST, сервери переглядають його, таким чином вони розуміють, що вони були відкинуті і що адреси, які вони пропонують вільні і можуть бути запропоновані іншим клієнтам.

У випадку відмови, він посилає клієнту пакет DHCPACK, що змушує клієнта почати шукати адресу заново. [4] Формат успішного надання IP-адреси DHCP-сервером(рис. 1.2).

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

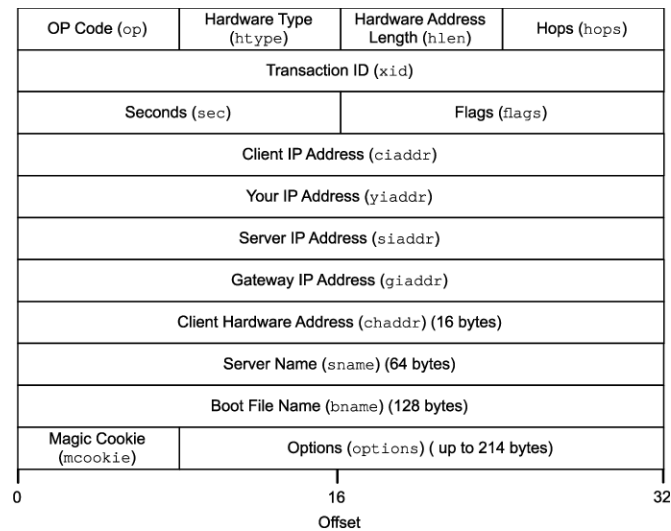


Рис. 1.2 Формат DHCP пакета

Розберемо кожний пункт в цьому пакеті:

- Op – тип повідомлення, може приймати значень BOOTREQUEST(запит) і BOOTREPLY(відповідь).
- Htype – тип адреси.
- hlen – довжина адреси.
- Hops – кількість проміжних маршрутизаторів.
- Xid – унікальний ідентифікатор транзакції, який генерується клієнтом.
- Secs (час операції) – час в секундах, який був витрачений з моменту початку отримання адреси.
- Flags – спеціальні параметри для DHCP.
- Ciaddr – клієнтська IP-адреса.
- Yiaddr – новий IP-адрес клієнта.
- Siaddr – IP-адреса серверу.
- Giaddr – IP-адреса за замовчуванням.
- Chaddr – апаратна адреса.
- Sname – ім'я сервера.
- bname – файл завантаження.
- Options - додаткові налаштування.

DHCP-сервер працює в одному із трьох режимів:

– Статичний розподіл – схожий на введення адреси на кожному комп’ютері вручну. Відмінність в тому, що системний адміністратор задає необхідні відповідності IP для MAC-адрес клієнтів на самому DHCP-сервері.

– Автоматичний розподіл – сервер закріплює IP із області за кожним клієнтом назавжди, тобто термін оренди необмежений.

– Динамічний розподіл – адміністратор присвоює діапазон адресів на сервері і кожен клієнтський комп’ютер повинен запросити IP-адресу окремо.

AAA-сервер дозволяє зберігати облікові записи користувачів мережі, є відмінною альтернативою локальним записам на кожному пристрої окремо.

AAA – використовується для опису процесу надання доступу до комп’ютерної мережі та контролю за ним. Протокол AAA сильно обмежує можливості зломисників у разі доступу до мережі[14].

– Автентифікація вимагає від користувачів, щоб вони надали докази, що вони дійсно є тими, за кого себе видають.

– Авторизація вирішує до яких ресурсів користувач може отримати доступ після автентифікації.

– Облік записує все те що робив користувач під час своєї сесії на пристрої, здійснює аудит для контролю ресурсів мережі.

Переваги AAA-серверу:

– Зручне адміністрування облікових записів.

– Безпека облікових записів, у випадку локальної бази користувачів, при несанкціонованому доступу до пристрою зломисник може отримати доступ до усіх логінів і паролів, які як правило однакові для всіх пристроїв мережі.

– Простота дотримання парольної політики.

Зрозумівши, що таке AAA-сервер, необхідно роздивитися його принцип роботи. Наприклад, припустимо, що у нашій мережі уже є налаштований AAA-сервер з обліковими записами.



Рис. 1.3. Принцип роботи AAA

Розпишемо його принцип роботи поетапно:

1. Користувач підключається до маршрутизатора за допомогою SSH або Telnet.
2. Маршрутизатор надає запит до користувача, щоб він надав логін і пароль.
3. Отримавши дані від користувача клієнт передає їх до серверу.
4. Сервер перевіряє чи є такі дані у базі і вирішує надавати користувачеві доступ до клієнта чи ні та надає користувачеві рівень привілеїв, які закріплені за ним[17].
5. Маршрутизатор отримує заборону або дозвіл для доступу з рівнем привілеїв користувача і відповідно надає доступ до командної лінії.
6. Певна річ, що всі налаштування та дії, які здійснив користувач зберігаються в журналі подій серверу.

Це все відбувається за допомогою AAA-протоколу. В наш час найбільше поширення отримали два протоколи: RADIUS[11] та TACACS+[12].

Оскільки в дипломній роботі використовувався саме TACACS+, через краще шифрування даних, розглянемо тільки його.

TACACS+ – протокол, який приймає рішення, заборонити чи дозволити певному користувачеві в підключенні до пристрою мережі. Є більш покращеним протоколом на відміну від старішого TACACS, у якому не передбачалося жодного збору логів(таким чином від AAA, лишилось тільки AA).

Відмінності TACACS+:

- Транспортний протокол TCP(49 порт);
- Шифруються усі дані між сервером та клієнтом;

- Автентифікація та авторизація повністю незалежні, тобто це дозволяє збирати логи всіх налаштувань, які проводить користувач;
- Протокол є пропрієтарним.

Таблиця 1.2

TACACS+ або RADIUS

	TACACS+	RADIUS
Транспортний протокол	TCP	UDP
Шифрування	Шифрується трафік між клієнтом і сервером	Шифрується тільки пароль, при передачі від RADIUS – клієнта сервера
Підтримка AAA	Підтримує автентифікацію, авторизацію і аудит	Тільки автентифікація і авторизація
Підтримка протоколів	Підтримує протоколи, такі як AppleTalk, NetDIOS b IPX	Працює через з'єднання PPP
Відповіді	Використовує безліч запитів-відповідей для кожного процесу AAA	Використовує запит-відповідь при автентифікації користувача

Висновки до 1-го розділу:

В результаті аналізу корпоративної мережі, було розглянуто та визначено основи її побудови, дизайну та вимог до неї. Також було продумано, яким чином має бути побудований інтернет модуль, враховуючи ті можливості, які надає симулятор віртуальних мереж GNS3.

Було розглянуто можливість налаштування DHCP-серверу, задля забезпечення швидкого надання IP-адрес робочим станція, або у випадку розширення мережі.

Крім цього, обрано протокол AAA та TACACS-сервер для забезпечення процесу надання доступу до пристроїв мережі та збору логів.

З обладнання будемо використовувати провідного виробника – CISCO, так як на пристроях даної фірми можна налаштувати всі обрані протоколи та технології. Для створення саме гетерогенної мережі буде задіяний симулятор GNS3, який дозволить забезпечити взаємодію комунікаційних пристроїв та віртуальних машин з обраними операційними системами.

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З ПІДСИСТЕМОЮ ПЕРИМЕТРОВОГО ЗАХИСТУ

2.1 Принципи роботи мережі

При розробці мережі спершу необхідно розбити її на модулі, як це було описано у попередньому розділі, щоб у подальшому була можливість її легко розширити у разі потреби та логічно її сконструювати задля легкого налаштування та роботи з нею.

Дана мережі буде складатися з трьох модулів: інтернет модуля з налаштованим NAT[13], який буде надавати надійний доступ до мережі інтернет і хмара, яка буде емулювати підключення до інтернет провайдера, а також Cisco ASA для забезпечення надійного захисту, ядра з DHCP-сервером, так як при проектуванні схеми буде використовуватися досить багато різних робочих станцій з різними ОС, то при розробці мережі потрібно брати до уваги наявність великої кількості IP-адрес, тому потрібно забезпечити налаштування протоколу DHCP для автоматизації процесу IP-адресації, а також рівні розподілу і доступу з налаштованими LAN, рівня розподілу, який буде забезпечувати зв'язок між ядром та робочими станціями, які будуть розташовані на рівні доступу.

Розподіл на підмережі буде здійснений за допомогою DHCP-серверу на базі маршрутизатору. Для забезпечення зв'язку та надання IP-адрес буде налаштовано DHCP-relay на рівні розподілу. Окремі підмережі будуть налаштовані для зв'язку між комутаторами рівня ядра та інтернет модулем. Для цього будуть розроблені підмережі з робочими станціями (табл. 2.1).

Також потрібно розробити IP-топологію мережі. Оскільки в схемі буде досить багато підмереж, внутрішню адресацію забезпечуватиме OSPF протокол[3]. Детальні параметри адресації наведено в табл. 2.2

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						21
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN 110	2 робочі станції, одна з яких невиділений сервер (Можливість додавання робочих станцій)	Маршрутизатор
LAN 120	1 робоча станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN 140	1 робоча станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN 150	1 робоча станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN 170	1 робоча станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN 180	1 робоча станції (Можливість додавання робочих станцій)	Маршрутизатор

Таблиця 2.2

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Підмережа А	-	192.168.1.0	255.255.255.0	/24
Підмережа В	-	192.168.2.0	255.255.255.0	/24
Підмережа С	-	192.168.3.0	255.255.255.0	/24
Підмережа D	-	192.168.4.0	255.255.255.0	/24
Підмережа Е	-	192.168.5.0	255.255.255.0	/24
Підмережа F	-	192.168.6.0	255.255.255.0	/24
Підмережа G	-	192.168.7.0	255.255.255.0	/24
Підмережа H	-	192.168.8.0	255.255.255.0	/24

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Підмережа І	-	192.168.9.0	255.255.255.0	/24
Підмережа J	-	192.168.10.0	255.255.255.0	/24
Підмережа К	-	192.168.11.0	255.255.255.0	/24
Підмережа 100	-	192.168.100.0	255.255.255.0	/24
Підмережа 110	-	192.168.110.0	255.255.255.0	/24
Підмережа 120	-	192.168.120.0	255.255.255.0	/24
Підмережа 130	-	192.168.130.0	255.255.255.0	/24
Підмережа 140	-	192.168.140.0	255.255.255.0	/24
Підмережа 150	-	192.168.150.0	255.255.255.0	/24
Підмережа 160	-	192.168.160.0	255.255.255.0	/24
Підмережа 170	-	192.168.170.0	255.255.255.0	/24
Підмережа 180	-	192.168.180.0	255.255.255.0	/24
Інтернет модуль				
Маршрутизатор 7200_Edge_Router1	int g0/0	192.168.1.100	255.255.255.0	/24
	int e1/1	192.168.2.1	255.255.255.0	/24
Маршрутизатор 7200_Edge_Router1	int e1/1	192.168.2.1	255.255.255.0	/24
	int g0/0	192.168.3.1	255.255.255.0	/24
Мережевий екран ASA-971	int m0/0	192.168.3.2	255.255.255.0	/24
	int g0/0	192.168.4.1	255.255.255.0	/24
	int g0/1	192.168.5.1	255.255.255.0	/24
Ядро				
Комутатор L3_CORE_Switch1	int e0/0	192.168.4.2	255.255.255.0	/24
	int e1/0	192.168.6.1	255.255.255.0	/24
	int e1/1	192.168.8.1	255.255.255.0	/24
	int e1/2	192.168.7.1	255.255.255.0	/24
Комутатор L3_CORE_Switch1	int e0/1	192.168.5.2	255.255.255.0	/24
	int e2/0	192.168.9.1	255.255.255.0	/24
	int e2/1	192.168.10.1	255.255.255.0	/24
	int e2/2	192.168.11.1	255.255.255.0	/24
Маршрутизатор DHCP_Server	int e3/0	192.168.100.1	255.255.255.0	/24
	int e3/1	192.168.130.1	255.255.255.0	/24
	int e3/2	192.168.160.1	255.255.255.0	/24

Параметри адресації мережі

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Рівень розподілу				
Комутатор L3_DL_Switch1	int e1/0	192.168.6.2	255.255.255.0	/24
	int e2/0	192.168.9.2	255.255.255.0	/24
	int e3/0	192.168.100.2	255.255.255.0	/24
	int e0/0	192.168.110.1	255.255.255.0	/24
	int e0/1	192.168.120.1	255.255.255.0	/24
Комутатор L3_DL_Switch1	int e1/1	192.168.8.2	255.255.255.0	/24
	int e2/1	192.168.10.2	255.255.255.0	/24
	int e3/1	192.168.130.2	255.255.255.0	/24
	int e0/0	192.168.140.2	255.255.255.0	/24
	int e0/1	192.168.150.2	255.255.255.0	/24
Комутатор L3_DL_Switch1	int e1/2	192.168.7.2	255.255.255.0	/24
	int e2/2	192.168.11.2	255.255.255.0	/24
	int e3/2	192.168.160.2	255.255.255.0	/24
	int e0/0	192.168.170.2	255.255.255.0	/24
	int e0/1	192.168.180.2	255.255.255.0	/24
Рівень доступу				
Комутатор L2_AL_Switch1	Vlan 110	192.168.110.2	255.255.255.0	/24
Робоча станція Windows 10	int e0	192.168.110.4	255.255.255.0	/24
Робоча станція TacsGui	int e0	192.168.110.3	255.255.255.0	/24
Комутатор L2_AL_Switch2	Vlan 120	192.168.120.2	255.255.255.0	/24
Робоча станція PC1	int e0	DHCP		
Комутатор L2_AL_Switch3	Vlan 140	192.168.140.1	255.255.255.0	/24
Робоча станція PC2	int e0	DHCP		
Комутатор L2_AL_Switch4	Vlan 150	192.168.150.1	255.255.255.0	/24
Робоча станція PC3	int e0	DHCP		
Комутатор L2_AL_Switch5	Vlan 170	192.168.170.1	255.255.255.0	/24
Робоча станція PC4	int e0	DHCP		
Комутатор L2_AL_Switch6	Vlan 180	192.168.180.1	255.255.255.0	/24
Робоча станція PC5	int e0	DHCP		

2.2 Розробка логічної структури мережі

В даній мережі використовувалася трирівнева модель, оскільки вона забезпечує надійність, масштабованість і високопродуктивність побудованої мережі. Вона буде складатися з 3-х рівнів: ядра, розподілу та доступу, а також буде включати інтернет модуль.

Розберемо кожен з рівнів окремо. Рівень ядра відповідає за швидке транспортування між пристроями рівня розподілу, тобто між комутаторами мережі, а також буде налаштовано DHCP-сервер. На рівні ядра були застосовані комутатори L3.

Рівень розподілу знаходиться посередині між рівнем ядра та доступу. Завдання даного рівня - забезпечувати маршрутизацію мережі, а також зв'язувати рівень ядра та доступу. На цьому рівні було налаштовано DTP протокол для зручної передачі VLAN-ів між ними. Окрім цього комутатори будуть виступати у якості DHCP-relay для розподілу IP-адрес між VLAN.

Рівень розподілу буде включати в себе комутатори L2 та робочі станції, а також один не виділений сервер TACACS+ і Log-server, для моніторингу та зручної роботи з мережею.

Загальний вигляд розробленої схеми разом із зазначенням вищевказаних рівнів наведено на рисунку 2.1.

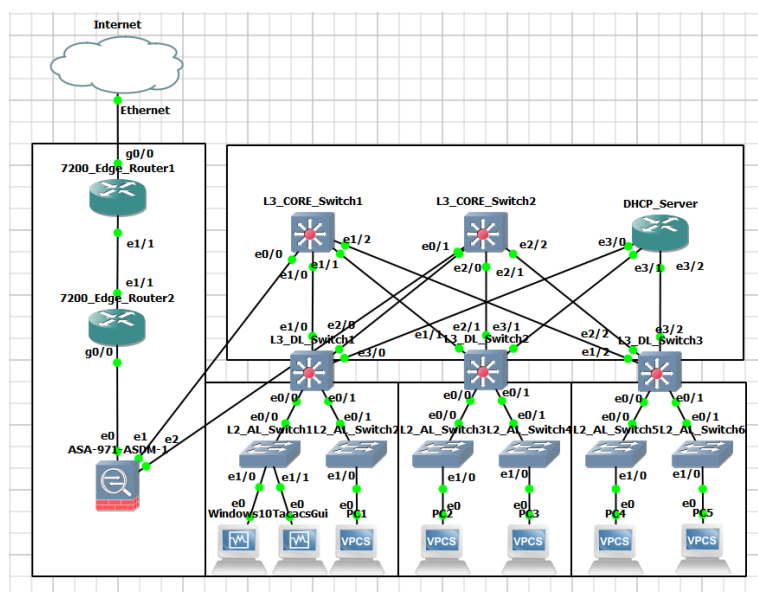


Рис.2.1. Трирівнева ієрархічна модель мережі

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

Детально розглянемо кожну з підмереж окремо. Зовнішній вигляд всіх LAN наведено на рисунках 2.2-2.7, пристрої, що входять до складу підмереж, зазначені в табл. 2.4-2.9.

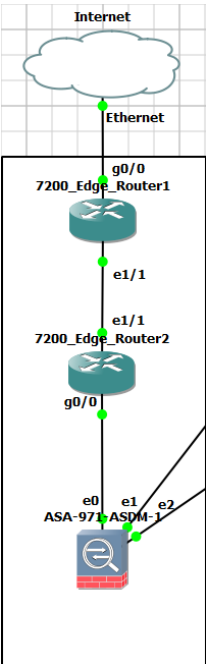


Рис. 2.2. Інтернет модуль

Таблиця 2.3

Інтернет модуль

Маршрутизатори	7200_Edge_Router1 і 7200_Edge_Router2(образ с7200- adventerprisek9_sna-mz.150-1.M3.image)
Мережевий екран	ASA-971(образ asav971-full.qcow2)

Задля забезпечення надійної безпеки мережі в інтернет модулі був встановлений Cisco ASA[10].

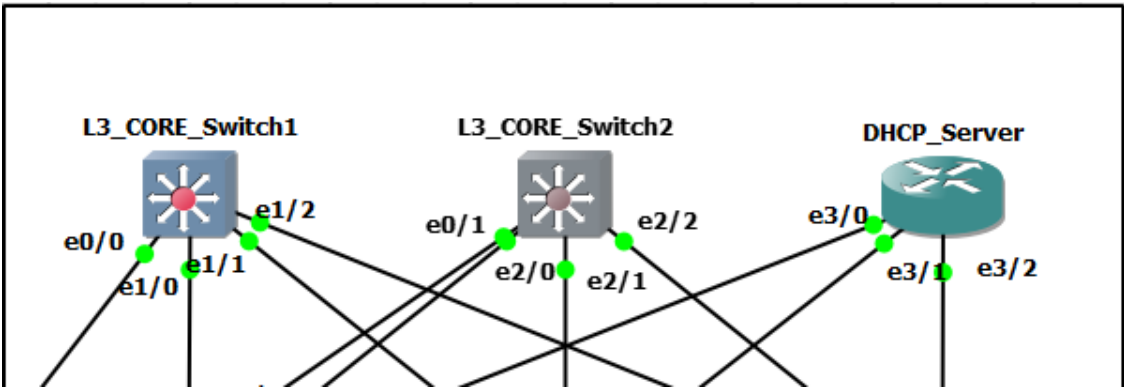


Рис. 2.3 Ядро з DHCP-сервером

Ядро з DHCP-сервером

Маршрутизатор	DHCP-сервер(образ c7200-adventerprisek9_sna-mz.150-1.M3.image)
Комутатори	L3_CORE_Switch1 і L3_CORE_Switch2(образ i86bi-linux-l3-adventerprisek9-15.4.2T4.bin)

Модуль ядра створюється задля того, щоб забезпечити маскимальну працездатність мережі. Для того щоб спростити процес налагодження мережесих адаптерів робочих станцій, у мережу був імплементований DHCP-сервер.

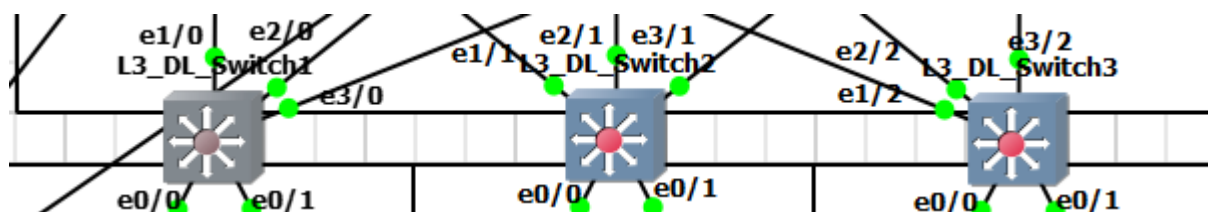


Рис. 2.4. Рівень розподілу, який також виступає у ролі DHCP-relay

Рівень розподілу

Комутатори	L3_DL_Switch1, L3_DL_Switch2 та L3_DL_Switch3(образ i86bi-linux-l3-adventerprisek9-15.4.2T4.bin)
------------	---

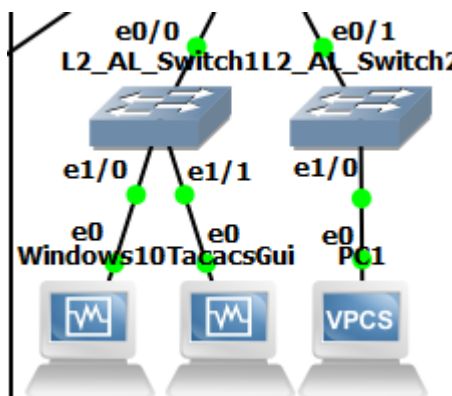


Рис. 2.5. Рівень доступу з робочими станціями

У адміністративному VLAN 110, були встановлені дві робочі станції Windows10 з встановленим Log-сервером та TacacsGui[8] у якості невиділеного серверу.

Таблиця 2.6

Рівень доступу

Комутатори	L2_AL_Switch1 та L2_AL_Switch2(образ i86bi-linux-l2-adventerprisek9-15.1a.bin)
Робочі станції	Windows10, TacacsGui і PC1

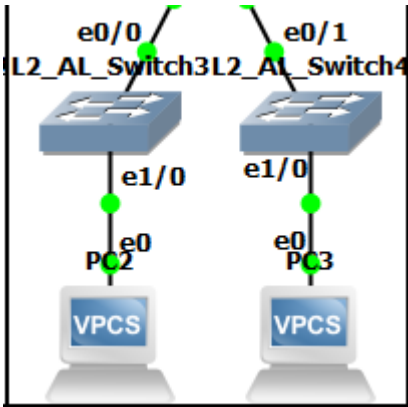


Рис. 2.6. Рівень доступу з робочими станціями

Таблиця 2.7

Рівень доступу

Комутатори	L2_AL_Switch3 та L2_AL_Switch4(образ i86bi-linux-l2-adventerprisek9-15.1a.bin)
Робочі станції	PC2 і PC3

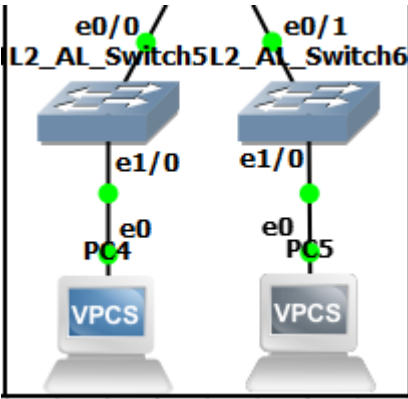


Рис. 2.7. Рівень доступу з робочими станціями

Рівень доступу

Комутатори	L2_AL_Switch5 та L2_AL_Switch6(образ i86bi-linux-l2-adventerprisek9-15.1a.bin)
Робочі станції	PC4 і PC5

Для забезпечення зв'язку між мережами всієї мережі було використано протокол OSPF.

2.3 Вибір обладнання та програмного забезпечення.

Відповідно до потреб, що зазначені вище, сформовано такі вимоги до програмно-апаратного забезпечення:

1. Використання Windows 10[7] у якості Log-серверу.
2. Невиділений сервер TACACS+.
3. Налаштування DHCP-серверу.
4. Наявність віддаленого доступу до робочих станцій.
5. Наявність віддаленого захищеного доступу до пристроїв за допомогою SSH[16].
6. Створення списків доступу.
7. Налаштування Cisco ASA, задля забезпечення надійного захисту мережі.

Захищеність мережі буде забезпечуватися: паролем доступом до пристроїв мережі, створення користувачів з привілеями за допомогою TACACS+, створенням списків доступу, налаштуванням Cisco ASA.

Для реалізації схеми будемо використовувати обладнання фірми CISCO. Основними перевагами CISCO перед іншими компаніями є:

1. Cisco є лідером на ринку продажів пристроїв для побудови мереж.
2. Cisco лідирує в кількості приладів, які доступні для дротових та бездротових мереж корпорацій будь-яких масштабів.

3. Понад два десятиліття вводить інновації у сфері нових технологій. Багато IEEE стандартів засновані саме Cisco.

4. Пристрої Cisco мають функції резервування даних та стійкості у разі атак для забезпечення надійної роботи, також пропонується можливість дистанційного усунення несправностей, щоб запобігти відключенням.

5. Прихильність до малого і середнього бізнесу, Cisco пропонує набір простих, безпечних і з розумною ціною рішень для побудови цифрових мереж.

6. Пристрої Cisco мають вбудований захист, виявлення атак та моніторинг тих хто потрапляє в мережу. Пропонується комплексний захист від загроз і підтримка сегментації мережі.

7. Пристрої Cisco прості у розгортанні та керуванні. Всі пристрої доступні для налаштування на основі графічного інтерфейсу, можливе централізоване управління для налаштування декількох пристроїв одночасно.

8. Пристрої Cisco розроблені для оптимізації роботи з додатками, пропонується можливість для оцифрування аудіо-відео мереж для покращення якості досвіду.

9. Деякі пристрої оснащені живленням через Ethernet інтерфейс, це суттєво може зменшити витрати на прокладку кабелів та на електроенергію, наявні тихі, безвентиляторні моделі для відкритого робочого простору.

10. Cisco має найбільш повну допомогу для допомоги клієнтам у підключенні, співпрацюванні та обчислюванні.

З цього, виходить висновок, прилади Cisco є найкращими у сферах захисту, налаштувань та надійності. У ході роботи будуть використовуватися образи маршрутизаторів серії 7200(рис.2.8)[18], комутаторів 2 і 3 рівня з образами i86bi-l2 і i86bi-l3 відповідно, Cisco ASA(рис. 2.9).

Для створення моделі підсистеми периметрового захисту корпоративної мережі організації будемо використовувати програму GNS3[19]. Для віртуалізації робочих станцій буде використовуватися VirtualBox[20], а також Wireshark для перевірки трафіку та вразливостей в мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис.2.8. Маршрутизатор останньої серії (Cisco 7200 Series Integrated Services Routers)

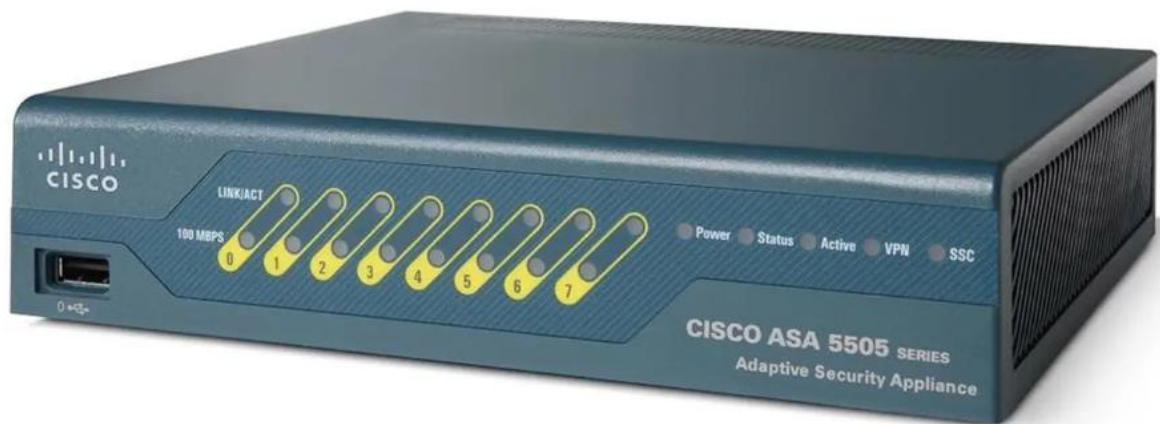


Рис.2.9. Мережевий екран (Cisco ASA)

GNS3 – це графічний симулятор мережі, який дозволяє емуляцію складних мереж. Можливо ви знайомі з VMWare або VirtualBox, які використовуються для емуляції різних операційних систем у навколишнє середовище. Ці програми дозволяють запускати операційні системи у віртуальному середовищі фізичного комп'ютера. GNS3 допускає той самий

тип емуляції за допомогою операційних систем Cisco Internetwork. Це дозволяє запустити Cisco IOS у віртуальному середовищі на вашому комп'ютері.

GNS3 дозволяє емуляцію Cisco IOS на базі Windows або Linux. Емуляція можлива для довгого списку платформ, маршрутизаторів і PIX брандмауерів. GNS3 є безцінним інструментом для підготовки до сертифікації Cisco, наприклад CCNA і CCNP. Існує ряд симуляторів на ринку, але вони обмежуються командами, які розробник вирішив включити. Майже завжди є команди або параметри, які не підтримуються при роботі в практичній лабораторії. У цих симуляторах ви бачите лише відображення результату. Точність такого представлення настільки висока, наскільки це робить розробник. З GNS3 ви використовуєте реальну Cisco IOS, тож ви точно побачите, як працює IOS, і матимете доступ до будь-якої команди або параметру, що підтримується IOS. Крім того, GNS3 — це безкоштовна програма з відкритим вихідним кодом використання. Однак через обмеження ліцензування вам доведеться надати власні Cisco IOS для використання з GNS3. Крім того, GNS3 забезпечить пропускну здатність близько 1000 пакетів в секунду у віртуальному середовищі. Нормальний роутер забезпечить у сто до тисячі разів більшу пропускну здатність. GNS3 не являється справжнім маршрутизатором, але покликаний бути інструментом для навчання та тестування в лабораторних умовах.

Розібравшись з емулятором комп'ютерних мереж, необхідно обрати програму для віртуалізації різних операційних мереж, у дипломній роботі буде використовуватися VirtualBox.

VirtualBox – програма віртуалізації для операційних систем, встановлюється на наявну операційну систему, яка називається хостовою, усередину цієї програми встановлюється інша операційна система, яку називають гостьовою операційною системою.

VirtualBox по праву вважається потужним інструментом управління віртуальними машинами на персональних комп'ютерах, серверах підприємства та системах, що вбудовуються. Можна запускати різні види

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

операційні системи - включаючи все програмне забезпечення, що працює в них, безпосередньо у вашій робочій операційній системі, в спеціальному середовищі, що називається 'віртуальна машина'. З VirtualBox ви можете запускати різні види операційні системи - включаючи все програмне забезпечення, що працює в них, безпосередньо у вашій робочій операційній системі, у спеціальному середовищі, що називається 'віртуальна машина'. Ваш фізичний комп'ютер зазвичай називають 'головний комп'ютер' або 'хост'(host), тоді як віртуальну машину часто називають 'гостем' або 'гостьової ОС'(guest). брандмауер - це не просто маршрутизатор, хост або група систем, що забезпечують безпеку мережі. Швидше, брандмауер – це підхід до безпеки; він допомагає реалізувати політику безпеки, яка визначає дозволені служби та типи доступу до них, і є реалізацією цієї політики у термінах мережевої конфігурації, кількох хостів та маршрутизаторів, та інших заходів захисту, таких як посиленна автентифікація замість статичних паролів. Основна мета системи брандмауера - управління доступом До або З мережі, що захищається. Він реалізує політику мережного доступу, змушуючи проходити всі з'єднання з мережею через брандмауер, де можуть бути проаналізовані і дозволені чи відкинуті.

Основні функції VirtualBox:

- робота на декількох віртуальних машинах відразу;
- наявність налаштувань для виділення фізичних ресурсів хоста для кожної віртуальної машини окремо;
- експорт та імпорт вже образів віртуальних машин;
- можливість збереження стану віртуальної машини задля збереження ресурсів хоста;
- можливість створення спільних папок між хостом та віртуальною машиною;
- можливість робити скріншоти та захват відео з екрану віртуальних машин.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

Wireshark - програма-аналізатор трафіку для комп'ютерних мереж Ethernet та деяких інших. Має графічний інтерфейс користувача. Спочатку проект називався Ethereal, але через проблеми з торговою маркою у червні 2006 року проект був перейменований на Wireshark[21].

Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і набагато більше можливостей по сортуванню та фільтрації інформації. Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу, переводячи мережеву карту в нерозбірливий режим.

Wireshark— це програма, яка «знає» структуру різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних лише з тих мереж, які підтримуються бібліотекою. Тим не менш, Wireshark вміє працювати з безліччю форматів вхідних даних, відповідно можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

Висновки до 2-го розділу:

Створено підсистему, яка буде складатися з інтернет модуля з Cisco ASA, рівнів ядра з DHCP-сервером, розподілу і доступу, на прикладі трирівневої ієрархічної моделі. Сформовано таблиці з параметрами мереж та мережевих інтерфейсів пристроїв мережі.

Окрім цього, було обрано пристрої, які будуть використовуватися при побудові мережі, описано їх можливості та завдання, які будуть перед ними поставлені, обґрунтовано вибір емулятора комп'ютерних мереж та операційних систем, за допомогою яких буде створена мережа.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ПЕРИМЕТРОВОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.

3.1 Налаштування мережі

В даному пункті буде розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (рис.3.1).

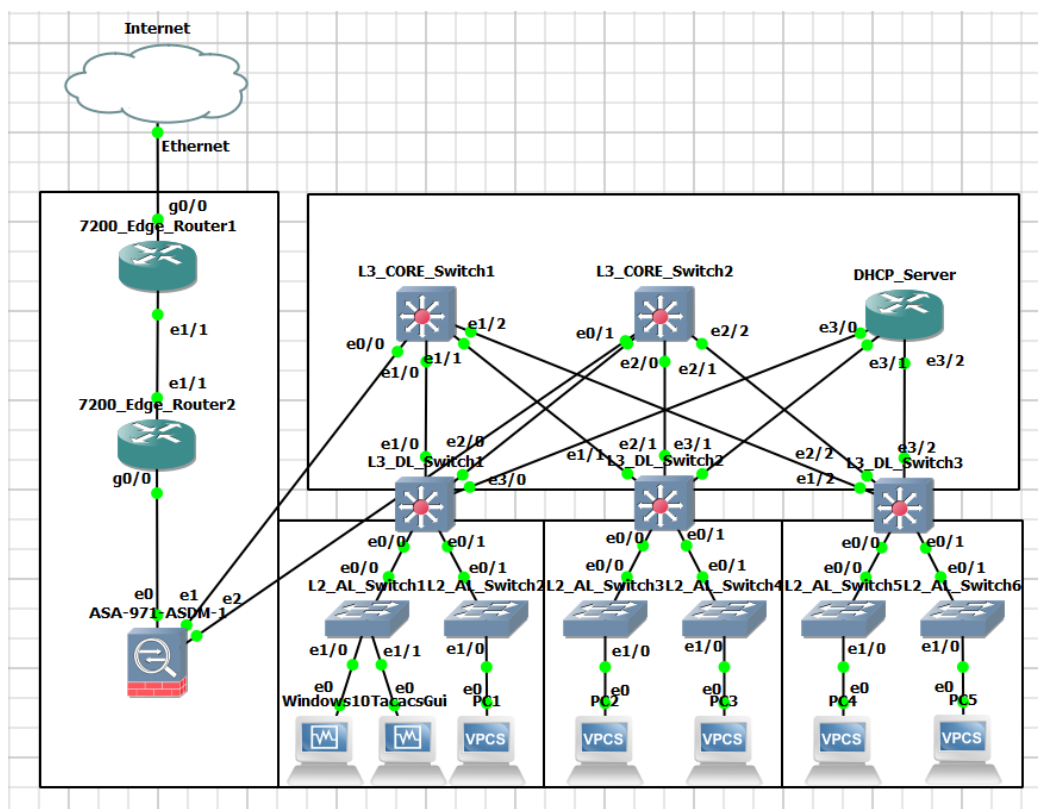


Рис. 3.1 Повна схема мережі

Перш за все, перед початком основних налаштувань, необхідно забезпечити надійний захист пристроїв, як від віддаленого доступу так і фізичного. Оскільки для входу на пристрій Cisco IOS, існує два варіанти через консоль або віддалено через ssh чи telnet, тому необхідно, щоб кожен із цих способів був надійно захищений, без цього зловмисник за допомогою декількох команд, зможе зібрати достатньо інформації про мережу і тип самим знайти її слабкості(рис.3.2).

```

L2_AL_Switch1 - PuTTY
L2_AL_Switch1#sh cdp neighbors detail
-----
Device ID: L3_DL_Switch1.bogdancheg.net
Entry address(es):
  IP address: 192.168.6.2
Platform: Linux Unix, Capabilities: Router Switch IGMP
Interface: Ethernet0/0, Port ID (outgoing port): Ethernet0/0
Holdtime : 154 sec

Version :
Cisco IOS Software, Solaris Software (I86BI_LINUXL2-ADVENTERPRISEK9-M), Experimental Version 15.1(20130726:213425) [dstivers-july26-2013-team_track 104]
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 26-Jul-13 15:56 by dstivers

advertisement version: 2
VTP Management Domain: ''
Native VLAN: 1
Duplex: half
Management address(es):
  IP address: 192.168.6.2
L2_AL_Switch1#

```

Рис.3.2 Виконання команди show cdp neighbors detail

Як можна побачити зловмисник може дізнати IP-адреси мережевих адаптерів, версії приладів, саме тому необхідно забороняти доступ до консолі навіть для користувацького режиму. Щож, приступимо до налаштувань.

```

L2_AL_Switch1 - PuTTY
L2_AL_Switch1(config)#enable secret brisk7833122
L2_AL_Switch1(config)#username bogdancheg privilege 15 secret mandarin7901198
L2_AL_Switch1(config)#service password-encryption
L2_AL_Switch1(config)#banner exec c
Enter TEXT message. End with the character 'c'.
L2_AL_Switch1(config)#ip domain-name bogdancheg.net
L2_AL_Switch1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: L2_AL_Switch1.bogdancheg.net

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

L2_AL_Switch1(config)#ip ssh version 2
L2_AL_Switch1(config)#ip ssh time-out 15
L2_AL_Switch1(config)#ip ssh logging events
L2_AL_Switch1(config)#line vty 0 4
L2_AL_Switch1(config-line)#transport input ssh
L2_AL_Switch1(config-line)#transport output ssh
L2_AL_Switch1(config-line)#logging synchronous
L2_AL_Switch1(config-line)#login local
L2_AL_Switch1(config-line)#exec-timeout 5 0
L2_AL_Switch1(config-line)#exit

```

Рис.3.3 Налаштування доступу по консолі, віддаленого доступу та користувача

Тепер необхідно пояснити, чому в ході налаштувань використовувався SSH, а не Telnet, покажемо це все на прикладі. Спершу побудуємо просту мережу(рис. 3.4).

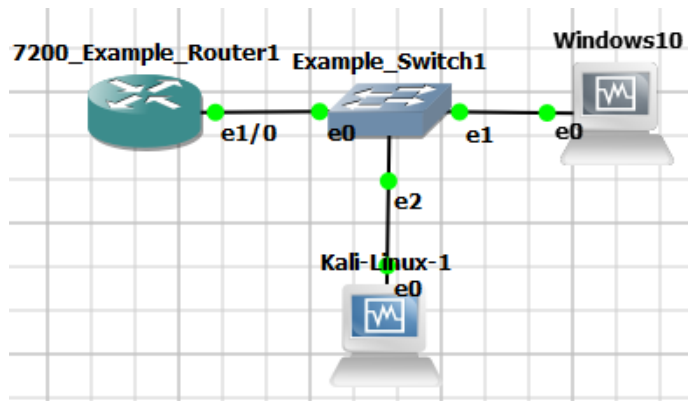


Рис. 3.4 Приклад мережі

Припустимо, що зломисник підключився до нашої мережі, а адміністратор нічого про це не знає і підключається по Telnet до маршрутизатора. В цей час зломисник перехоплює увесь цей трафік.

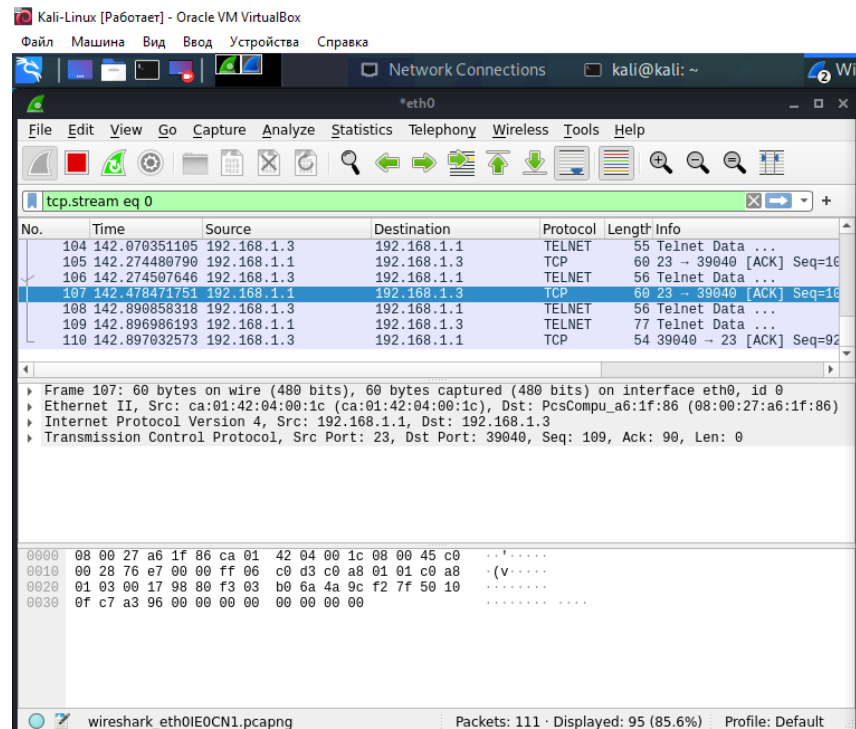


Рис. 3.5 Потік пакетів через інтерфейс

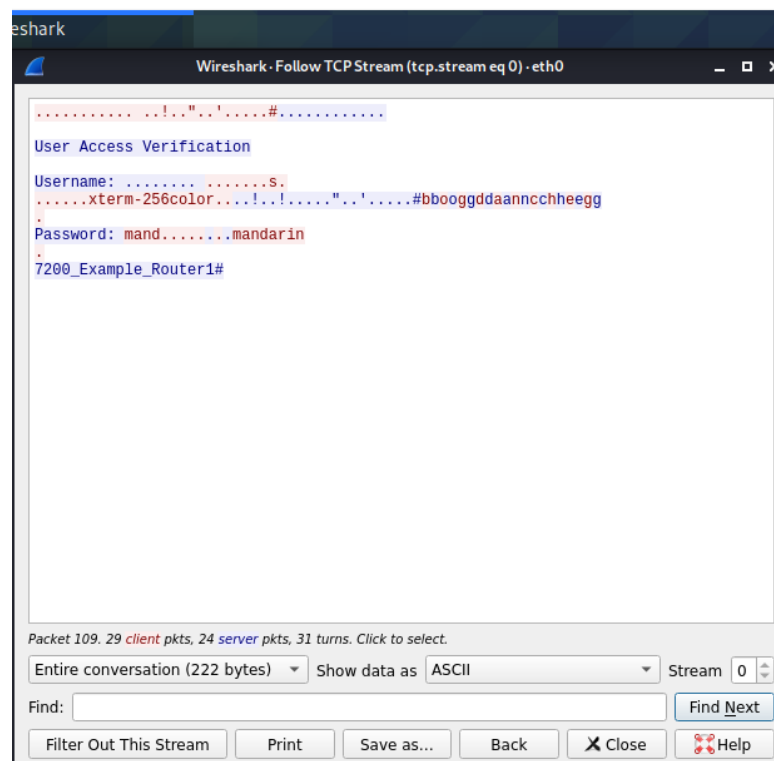


Рис 3.6 Перехоплений пакет

Як можна побачити (на рис.3.5 і 3.6) перехопивши пакет зловмисник дізнався логін і пароль. Саме тому в ході налаштувань мережі використовувався більш захищений протокол SSH, оскільки він створює захищений канал між двома пристроями. Пристрій до якого ми намагаємося підключитися виступає у вигляді SSH-серверу, а наш комп'ютер з якого ми починаємо сесію є SSH-клінтом. Створимо ту саму ситуацію, але уже на прикладі реальної мережі(Рис 3.7-9).

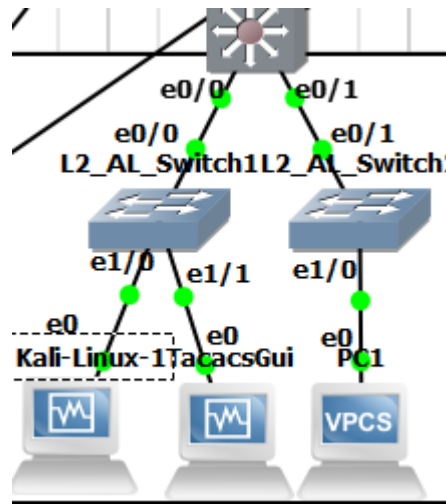


Рис. 3.7 Налаштована мережа

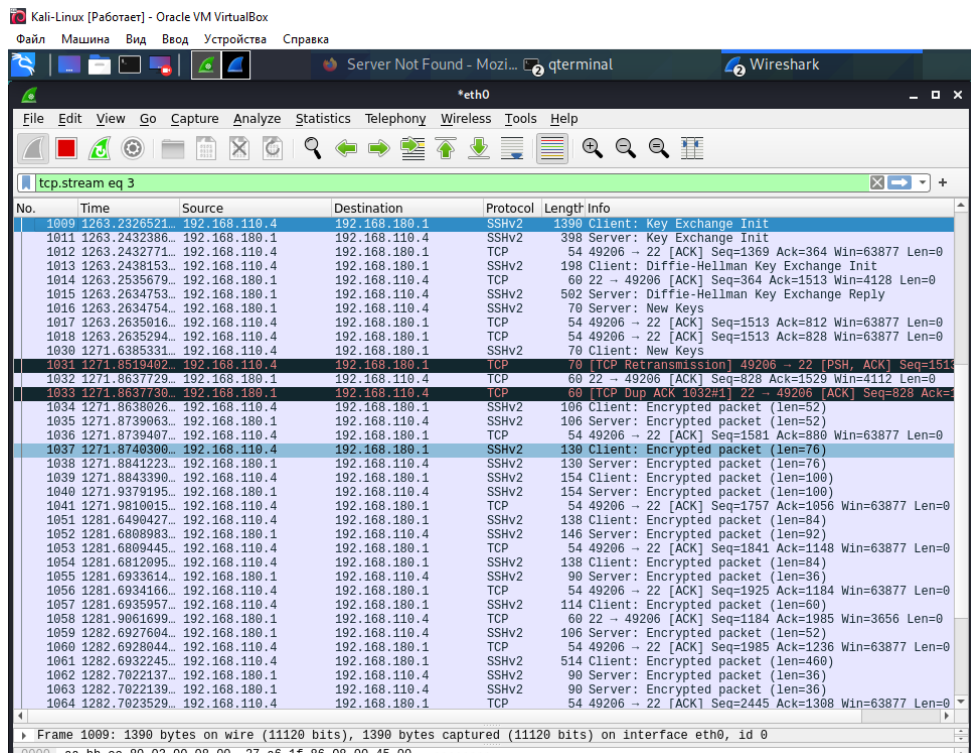


Рис. 3.8 Перехоплені пакети

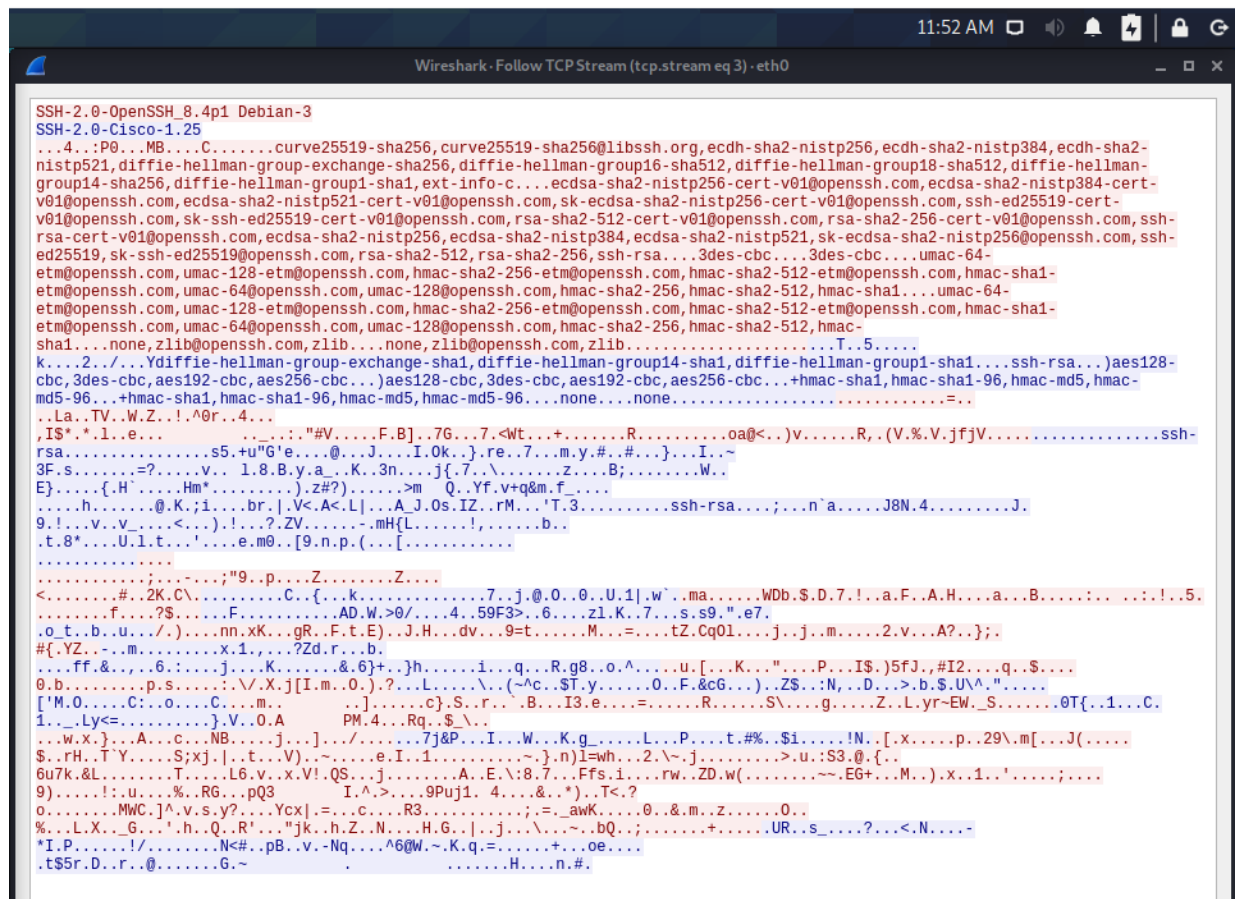


Рис. 3.9 Защищенный протокол SSHv2

У даному випадку зломисник уже не зможе побачити логін і пароль, це робить перехоплення SSH трафіку не ефективним.

Тепер розібравшись з віддаленим доступом до пристроїв необхідно налаштувати, списки доступу до пристроїв та захист від brute force, щоб звичайний користувач мережі не міг втрутитися у конфігурацію пристрою і зашкодити роботі мережі.

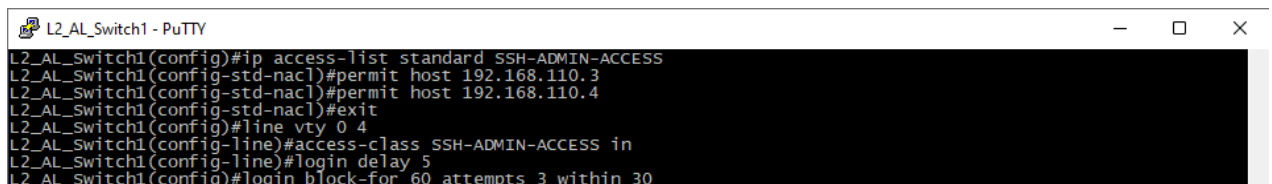


Рис. 3.10 Налаштування списків доступу та захисту від brute force

Далі перейдемо до налаштування AAA-серверу, хоч і можна зберігати та створювати користувачів на кожному із пристроїв окремо, але зберігати їх централізовано, набагато зручніше саме на сервері.

```
L2_AL_Switch1 - PuTTY
L2_AL_Switch1(config)#aaa new-model
L2_AL_Switch1(config)#tacacs-server host 192.168.110.3
warning: The cli will be deprecated soon
tacacs-server host 192.168.110.3
Please move to 'tacacs server <name>' CLI
L2_AL_Switch1(config)#tacacs-server key nvutmrzvhæud
L2_AL_Switch1(config)#aaa authentication login default group tacacs+ local
L2_AL_Switch1(config)#aaa authorization exec default group tacacs+ local
L2_AL_Switch1(config)#aaa authorization config-command
L2_AL_Switch1(config)#$zation commands 1 default group tacacs+ local
L2_AL_Switch1(config)#$zation commands 15 default group tacacs+ local
L2_AL_Switch1(config)#aaa authorization console
L2_AL_Switch1(config)#aaa accounting exec default start-stop group tacacs+
L2_AL_Switch1(config)#$ing commands 1 default start-stop group tacacs+
L2_AL_Switch1(config)#$ing commands 15 default start-stop group tacacs+
L2_AL_Switch1(config)#logging on
L2_AL_Switch1(config)#logging buffered 32768
L2_AL_Switch1(config)#logging buffered informational
L2_AL_Switch1(config)#logging host 192.168.110.4
L2_AL_Switch1(config)#logging trap informational
L2_AL_Switch1(config)#logging rate-limit all 50
L2_AL_Switch1(config)#
```

Рис. 3.11 Налаштування AAA та Log серверів

Тепер перейдемо безпосередньо до налаштування TacacsGUI.

Sign In

Username

tacgui

Password

.....

Sign In

Рис. 3.12 Вхід до TacacsGUI

Після успішного входу, необхідно додати пристрій який ми щойно налаштували. Як показано на рис.3.13 та рис.3.14, при додаванні нового пристрою, необхідно вказати назву, групу до якої він входить, вказуємо його IP-адресу і Tacacs ключ, за допомогою якого відбувається процес шифрування між кінцевим пристроєм і AAA-сервером.

Edit Device

Name

L2_AL_Switch1

It should be unique, but you can change it later

Device Group

defaultGroup

Address

L2_AL_Switch1

Tacacs Key

nvutmrzvhæud

Enable Password

\$!\$Uy2oKlv\$eZuUuQqCtEVGTCT0yYw.

Type of storing

MD5

Banners

>

Access

>

Info

>

Manual Configuration

>

Disabled

☐

Save

Cancel

Рис. 3.13 Додавання нового пристрою

Edit Address

Item Name

it should be unique, but you can change it later

Type

IPv4
▼

Network Address

e.g., 10.6.20.10 or 10.6.20.10/32

Created: 2022-05-26 07:26:17

Save
Cancel

Рис. 3.14 Додавання IP-адреси

Після успішного додавання, можна переглянути увесь список пристроїв мережі(рис. 3.15).

Tacacs Devices		tacacs device list	
+ Add	Search for..	Actions	More Columns
Item Name	Address	Group	Action
+ DHCP_Server	192.168.100.1	defaultGroup	↗ 🗑
+ L2_AL_Switch1	192.168.110.2/24	defaultGroup	↗ 🗑
+ L2_AL_Switch2	192.168.120.2/24	defaultGroup	↗ 🗑
+ L2_AL_Switch3	192.168.140.1/24	defaultGroup	↗ 🗑
+ L2_AL_Switch4	192.168.150.1/24	defaultGroup	↗ 🗑
+ L2_AL_Switch5	192.168.170.1/24	defaultGroup	↗ 🗑
+ L2_AL_Switch6	192.168.180.1/24	defaultGroup	↗ 🗑
+ L3_CORE_Switch1	192.168.6.1/24	defaultGroup	↗ 🗑
+ L3_CORE_Switch2	192.168.9.1/24	defaultGroup	↗ 🗑
+ L3_DL_Switch2	192.168.8.2/24	defaultGroup	↗ 🗑
+ L3_DL_Switch3	192.168.7.2/24	defaultGroup	↗ 🗑

Рис. 3.15 Перегляд доданих пристроїв

Після того, як ми додали новий пристрій до TacacsGUI, можна перейти до додавання нового користувача(рис. 3.16), в прикладі наведеному нижче створений користувач adminer з паролем в MD5 хешуванні, також можна переглянути увесь список користувачів(рис. 3.17).

Add New User

Username

bogdancheg

Default User Group

+

- default group for that user

Login Password

.....

Type

Local Database (MAVIS)

Enable Password

.....

Type

MD5

Service

+

Access Control List

+

☒
Default Service Permit

Message

>

Access Control

>

Extra Options

>

Manual Configuration

>

Valid From

Valid Until

Рис. 3.16 Додавання нового користувача

Tacacs Users

tacacs user list

+ Add

Search for_

Actions

More Columns

⌵ Username

+ admin

+ bogdancheg

Action

Рис. 3.17 Перегляд списку користувачів

Після того, як ми провели налаштування вказані вище, необхідно це все зберегти.

Tacacs Configuration File
here you can see configuration file, test and apply configuration

Test

Apply

☒
Make backup after applying

No Changes Detected

Test Configuration

Success

Apply Configuration

Daemon was Reloaded. Success. Active: active (running) since Fri 2022-05-27 11:02:46 UTC; 129ms ago

Рис. 3.18 Збереження конфігурації

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

Також TascacsGUI надає зручний та повний перегляд логів автентифікації, авторизації та обліку наведений нижче(рис. 3.19-3.22).

Authentication Report					
More Columns					
Add Query					
IF Date	Server	Nas	Username	Nac	Action
2022-06-02 12:50:38	localhost	192.168.9.1	bogdancheg	192.168.110.4	shell login succeeded
2022-06-02 12:46:00	localhost	192.168.9.1	bogdancheg	192.168.110.4	shell login succeeded
2022-06-02 12:45:52	localhost	192.168.9.1	bogdancheg	192.168.110.4	shell login failed
2022-06-02 12:44:44	localhost	192.168.9.1	bogdancheg	192.168.110.4	shell login succeeded
2022-06-02 12:44:39	localhost	192.168.9.1	bogdancheg	192.168.110.4	shell login failed
2022-06-02 12:42:38	localhost	192.168.9.1	bogdancheg	async	shell login succeeded
2022-06-01 17:54:00	localhost	192.168.110.2	bogdancheg	192.168.110.4	shell login succeeded
2022-06-01 15:51:21	localhost	192.168.180.1	bogdancheg	192.168.110.4	shell login succeeded
2022-06-01 12:51:51	localhost	192.168.110.1	bogdancheg	async	shell login succeeded
2022-06-01 09:10:54	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-31 09:02:00	localhost	192.168.6.1	bogdancheg	async	shell login succeeded
2022-05-31 09:01:30	localhost	192.168.9.1	bogdancheg	async	shell login succeeded
2022-05-27 11:09:34	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-27 08:19:05	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-27 08:18:25	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-26 16:37:25	localhost	192.168.180.1	bogdancheg	async	shell login succeeded
2022-05-26 16:37:07	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-26 11:02:17	localhost	192.168.100.1	bogdancheg	async	shell login succeeded
2022-05-26 10:55:07	localhost	192.168.120.2	bogdancheg	async	shell login succeeded
2022-05-26 10:55:00	localhost	192.168.110.2	bogdancheg	async	shell login succeeded
2022-05-26 10:54:53	localhost	192.168.110.1	bogdancheg	async	shell login succeeded
2022-05-26 08:51:07	localhost	192.168.100.1	bogdancheg	async	shell login succeeded
2022-05-26 08:41:28	localhost	192.168.180.1	bogdancheg	async	shell login succeeded
Total: 187					

Рис. 3.19 Перегляд логів Authentication

Authorization Report						
More Columns						
Add Query						
IF Date	Server	Nas	Username	Nac	Action	Command
2022-06-02 12:55:03	localhost	192.168.9.1	bogdancheg	async	permit	ssh -l bogdancheg 192.168.6.1
2022-06-01 17:55:15	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	ping 192.168.110.2
2022-06-01 17:55:14	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	ping 192.168.110.1
2022-06-01 17:55:02	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	show cdp neighbors
2022-06-01 17:54:54	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	show cdp
2022-06-01 17:54:50	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	show version
2022-06-01 17:54:35	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	show running-config
2022-06-01 17:54:12	localhost	192.168.110.2	bogdancheg	192.168.110.4	permit	show running-config
2022-06-01 14:51:48	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.4
2022-06-01 14:51:03	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.4
2022-06-01 14:51:01	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.3
2022-06-01 14:51:00	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.2
2022-06-01 14:50:58	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.1
2022-06-01 14:50:46	localhost	192.168.110.2	bogdancheg	async	permit	ping 192.168.110.4
2022-06-01 13:33:57	localhost	192.168.110.2	bogdancheg	async	permit	show cdp neighbors detail
2022-06-01 13:32:59	localhost	192.168.110.1	bogdancheg	async	permit	show cdp neighbors detail
2022-06-01 12:52:05	localhost	192.168.110.1	bogdancheg	async	permit	show cdp neighbors detail
2022-06-01 09:10:58	localhost	192.168.110.2	bogdancheg	async	permit	show version
2022-05-31 09:02:02	localhost	192.168.6.1	bogdancheg	async	permit	show running-config
2022-05-31 09:01:33	localhost	192.168.9.1	bogdancheg	async	permit	show running-config
2022-05-27 11:32:21	localhost	192.168.110.2	bogdancheg	async	permit	show arp
2022-05-27 11:32:01	localhost	192.168.110.2	bogdancheg	async	permit	show aaa clients
2022-05-27 11:31:31	localhost	192.168.110.2	bogdancheg	async	permit	show running-config
Total: 1259						

Рис. 3.20 Перегляд логів Authorization

Accounting Report						
More Columns						
Add Query						
IF Date	Server	Nas	Username	Nac	Action	Command
2022-06-02 12:55:50	localhost	192.168.9.1	bogdancheg	192.168.110.4	stop	
2022-06-02 12:55:04	localhost	192.168.9.1	bogdancheg	async	stop	ssh -l bogdancheg 192.168.6.1
2022-06-02 12:51:15	localhost	192.168.9.1	bogdancheg	192.168.110.4	stop	
2022-06-02 12:50:43	localhost	192.168.9.1	bogdancheg	192.168.110.4	start	
2022-06-02 12:46:05	localhost	192.168.9.1	bogdancheg	192.168.110.4	start	
2022-06-02 12:44:52	localhost	192.168.9.1	bogdancheg	192.168.110.4	stop	
2022-06-02 12:44:49	localhost	192.168.9.1	bogdancheg	192.168.110.4	start	
2022-06-02 12:42:38	localhost	192.168.9.1	bogdancheg	async	start	
2022-06-01 18:00:16	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	
2022-06-01 17:55:15	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	ping 192.168.110.2
2022-06-01 17:55:14	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	ping 192.168.110.1
2022-06-01 17:55:02	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	show cdp neighbors
2022-06-01 17:54:54	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	show cdp
2022-06-01 17:54:50	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	show version
2022-06-01 17:54:35	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	show running-config
2022-06-01 17:54:12	localhost	192.168.110.2	bogdancheg	192.168.110.4	stop	show running-config
2022-06-01 17:54:01	localhost	192.168.110.2	bogdancheg	192.168.110.4	start	
2022-06-01 15:56:22	localhost	192.168.180.1	bogdancheg	192.168.110.4	stop	
2022-06-01 15:51:22	localhost	192.168.180.1	bogdancheg	192.168.110.4	start	
2022-06-01 14:51:48	localhost	192.168.110.2	bogdancheg	async	stop	ping 192.168.110.4
2022-06-01 14:51:03	localhost	192.168.110.2	bogdancheg	async	stop	ping 192.168.110.4
2022-06-01 14:51:01	localhost	192.168.110.2	bogdancheg	async	stop	ping 192.168.110.3
2022-06-01 14:51:00	localhost	192.168.110.2	bogdancheg	async	stop	ping 192.168.110.2
Total: 1255						

Рис. 3.21 Перегляд логів Accounting

GUI Report						
api event log						
Search for... More Columns						
IF Date	Username	IP Address	Section	Object Name	Action	Message
2022-06-09 10:42:37	taogui	192.168.110.4	api auth		Signin	Sign in successfully
2022-06-01 17:11:56	taogui	192.168.110.4	api auth		Signin	Sign in successfully
2022-05-27 11:02:46	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs apply conf	Tacacs configuration was applied successfully
2022-05-27 11:02:40	taogui	192.168.110.4	api backup	tcfg	add	Backup was added successfully
2022-05-27 11:02:39	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 11:02:39	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 11:02:38	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 11:02:24	taogui	192.168.110.4	tacacs device groups	tacacs+	delete	Device group was deleted
2022-05-27 11:01:00	taogui	192.168.110.4	api auth		Signin	Sign in successfully
2022-05-27 08:18:51	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:18:51	taogui	192.168.110.4	api backup	tcfg	add	Backup was added successfully
2022-05-27 08:18:51	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs apply conf	Tacacs configuration was applied successfully
2022-05-27 08:18:50	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:18:50	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:18:47	taogui	192.168.110.4	tacacs devices	L2_AL_Switch1	edit	Device was edited
2022-05-27 08:17:53	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs apply conf	Tacacs configuration was applied successfully
2022-05-27 08:17:48	taogui	192.168.110.4	api backup	tcfg	add	Backup was added successfully
2022-05-27 08:17:47	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:17:47	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:17:46	taogui	192.168.110.4	tacacs configuration	tacacs configuration	tacacs test conf	Tacacs configuration was tested successfully
2022-05-27 08:17:42	taogui	192.168.110.4	tacacs devices	L2_AL_Switch1	edit	Device was edited
2022-05-27 08:15:59	taogui	192.168.110.4	api auth		Signin	Sign in successfully
Total: 471						

Рис. 3.22 Перегляд Gui log

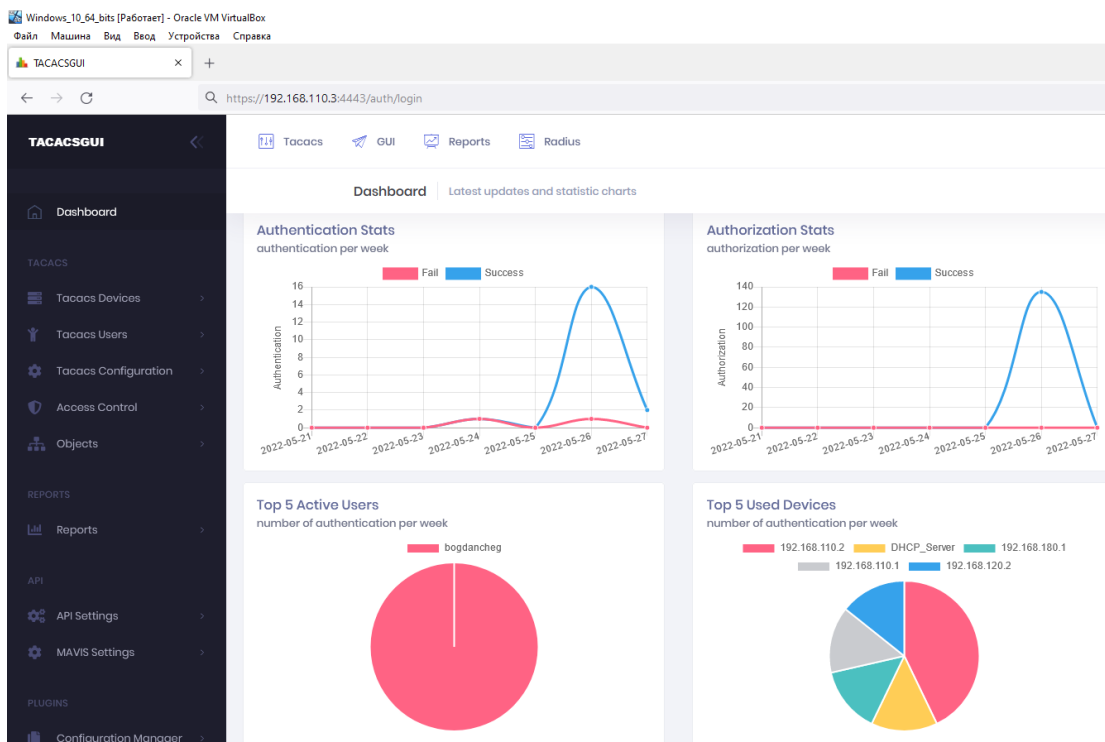


Рис. 3.22 Перегляд графіків активності на пристроях

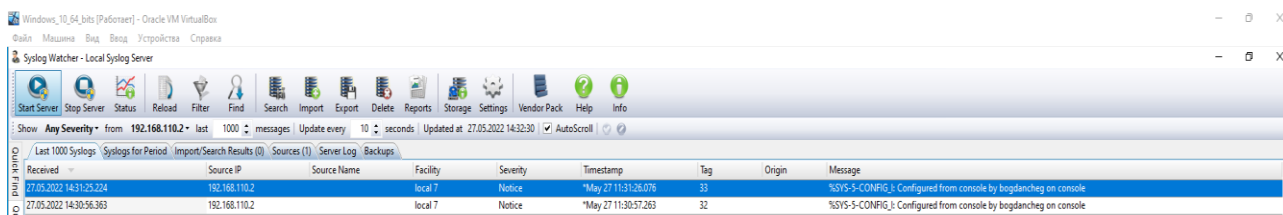


Рис. 3.23 Інтерфейс Syslog Watcher

Далі налаштуємо DHCP-сервер на базі маршрутизатора Cisco 7200.(рис.3.24-3.25).

```

DHCP_Server
DHCP_Server#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DHCP_Server(config)#int eth3/0
DHCP_Server(config-if)#ip add 192.168.100.1 255.255.255.0
DHCP_Server(config-if)#no shut
DHCP_Server(config-if)#exit
DHCP_Server(config)#int eth3/1
DHCP_Server(config-if)#ip add 192.168.130.1 255.255.255.0
DHCP_Server(config-if)#no shut
DHCP_Server(config-if)#exit
DHCP_Server(config)#int eth3/2
DHCP_Server(config-if)#ip add 192.168.160.1 255.255.255.0
DHCP_Server(config-if)#no shut
DHCP_Server(config-if)#exit
DHCP_Server(config)#router ospf
DHCP_Server(config)#router ospf 1
DHCP_Server(config-router)#network 192.168.100.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.110.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.120.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.130.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.140.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.150.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.160.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.170.0 0.0.0.255 area 0
DHCP_Server(config-router)#network 192.168.180.0 0.0.0.255 area 0
DHCP_Server(config-router)#exit
DHCP_Server(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
DHCP_Server(config)#ip route 0.0.0.0 0.0.0.0 192.168.130.2
DHCP_Server(config)#ip route 0.0.0.0 0.0.0.0 192.168.160.2

```

Рис. 3.24 Налаштування IP-адресації на DHCP_Server

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

```

DHCP_Server(config)#ip dhcp pool ADMS
DHCP_Server(dhcp-config)#network 192.168.110.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.110.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp pool office2
DHCP_Server(dhcp-config)#network 192.168.120.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.120.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp pool office3
DHCP_Server(dhcp-config)#network 192.168.140.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.140.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp pool office4
DHCP_Server(dhcp-config)#network 192.168.150.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.150.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp pool office5
DHCP_Server(dhcp-config)#network 192.168.170.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.170.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp pool office6
DHCP_Server(dhcp-config)#network 192.168.180.0 255.255.255.0
DHCP_Server(dhcp-config)#default-router 192.168.180.1
DHCP_Server(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCP_Server(dhcp-config)#exit
DHCP_Server(config)#ip dhcp excluded-address 192.168.110.1 192.168.110.10
DHCP_Server(config)#ip dhcp excluded-address 192.168.120.1 192.168.120.10
DHCP_Server(config)#ip dhcp excluded-address 192.168.140.1 192.168.140.10
DHCP_Server(config)#ip dhcp excluded-address 192.168.150.1 192.168.150.10
DHCP_Server(config)#ip dhcp excluded-address 192.168.170.1 192.168.170.10
DHCP_Server(config)#ip dhcp excluded-address 192.168.180.1 192.168.180.10

```

Рис. 3.25 Налаштування pool і excluded-address на кожен Vlan окремо

Після налаштування DHCP_Server, налаштовуємо IP-адресацію, а також DHCP-relay на решті пристроїв мережі, окрім цього налаштуємо DTP, а точніше переведемо trunk порти в стан Access, це необхідно оскільки trunk налаштований за замовчуванням, можна відключити порти, які не використовуються, однак цього не достатньо, адже зломисник може просто перемкнути порти і вже після цього перетягнути всі Vlan з нашого пристрою, саме тому необхідно перемикати порти в стан Access, процес налаштувань продемонстровано на рис. 3.26.

```

L3_CORE_Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
L3_CORE_Switch1(config)#int eth0/0
L3_CORE_Switch1(config-if)#ip add 192.168.4.2 255.255.255.0
L3_CORE_Switch1(config-if)#no shut
L3_CORE_Switch1(config-if)#exit
L3_CORE_Switch1(config)#int eth1/0
L3_CORE_Switch1(config-if)#ip add 192.168.6.1 255.255.255.0
L3_CORE_Switch1(config-if)#no shut
L3_CORE_Switch1(config-if)#exit
L3_CORE_Switch1(config)#int eth1/1
L3_CORE_Switch1(config-if)#ip add 192.168.8.1 255.255.255.0
L3_CORE_Switch1(config-if)#no shut
L3_CORE_Switch1(config-if)#exit
L3_CORE_Switch1(config)#int eth1/2
L3_CORE_Switch1(config-if)#ip add 192.168.7.1 255.255.255.0
L3_CORE_Switch1(config-if)#no shut
L3_CORE_Switch1(config-if)#exit

```

Рис. 3.26 Налаштування IP-адресації на L3_CORE_Switch1

```

L3_DL_Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
L3_DL_Switch1(config)#vlan 2
L3_DL_Switch1(config-vlan)#exit
L3_DL_Switch1(config)#vlan 3
L3_DL_Switch1(config-vlan)#exit
L3_DL_Switch1(config)#vlan 100
L3_DL_Switch1(config-vlan)#name DHCP-Server
L3_DL_Switch1(config-vlan)#exit
L3_DL_Switch1(config)#vlan 110
L3_DL_Switch1(config-vlan)#name ADMINS
L3_DL_Switch1(config-vlan)#exit
L3_DL_Switch1(config)#vlan 120
L3_DL_Switch1(config-vlan)#name Office2
L3_DL_Switch1(config-vlan)#exit
L3_DL_Switch1(config)#int vlan 2
L3_DL_Switch1(config-if)#ip add 192.168.6.2 255.255.255.0
L3_DL_Switch1(config-if)#no shut
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int vlan 3
L3_DL_Switch1(config-if)#ip add 192.168.9.2 255.255.255.0
L3_DL_Switch1(config-if)#no shut
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int vlan 100
L3_DL_Switch1(config-if)#ip add 192.168.100.2 255.255.255.0
L3_DL_Switch1(config-if)#no shut
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int vlan 110
L3_DL_Switch1(config-if)#ip add 192.168.110.1 255.255.255.0
L3_DL_Switch1(config-if)#no shut
L3_DL_Switch1(config-if)#ip helper-address 192.168.100.1
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int vlan 120
L3_DL_Switch1(config-if)#ip add 192.168.120.1 255.255.255.0
L3_DL_Switch1(config-if)#no shut
L3_DL_Switch1(config-if)#ip helper-address 192.168.100.1
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int eth3/0
L3_DL_Switch1(config-if)#switchport mode access
L3_DL_Switch1(config-if)#switchport access vlan 100
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int eth1/0
L3_DL_Switch1(config-if)#switchport access vlan 2
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int eth2/0
L3_DL_Switch1(config-if)#switchport access vlan 3
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int eth0/0
L3_DL_Switch1(config-if)#switchport trunk encapsulation dot1q
L3_DL_Switch1(config-if)#switchport mode trunk
L3_DL_Switch1(config-if)#switchport trunk allowed vlan 110,120
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#int eth0/1
L3_DL_Switch1(config-if)#switchport trunk encapsulation dot1q
L3_DL_Switch1(config-if)#switchport mode trunk
L3_DL_Switch1(config-if)#switchport trunk allowed vlan 110,120
L3_DL_Switch1(config-if)#exit
L3_DL_Switch1(config)#router ospf 1
L3_DL_Switch1(config-router)#network 192.168.6.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.7.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.8.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.9.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.10.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.11.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#exit

```

Рис. 3.26 Налаштування IP-адресації, DTP та Trunk-портів

Тепер для зв'язку між маршрутизаторами, комутаторами та іншими приладами налаштуємо протокол маршрутизації. В нашому випадку це протокол OSPF (рис.3.27)

```

L3_DL_Switch1(config)#router ospf 1
L3_DL_Switch1(config-router)#network 192.168.6.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.7.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.8.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.9.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.10.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#network 192.168.11.0 0.0.0.255 area 0
L3_DL_Switch1(config-router)#exit

```

Рис. 3.27 Налаштування протоколу маршрутизації OSPF

Тепер перейдемо до налаштування інтернет модуля, необхідно налагодити функціонування протоколу NAT(рис. 3.28), а також забезпечити захист від зовнішніх втручань за допомогою Cisco ASA.

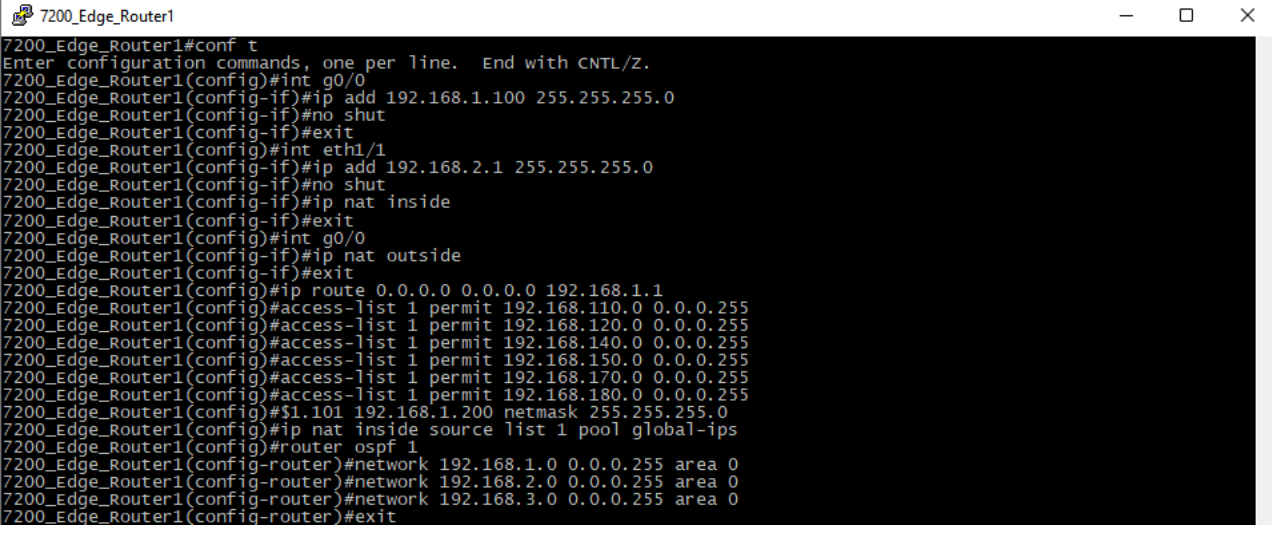
Приступимо до налагодження, інтерфейси які з'єднують ASA з ядром, налаштовані з іменами інтерфейсів INSIDE1 і INSIDE2, їм буде призначено

рівень безпеки 100. З'єднання, яке іде до маршрутизатора 7200_Edge_Router1, налаштоване з іменем інтерфейсу OUTSIDE і йому призначено рівень безпеки 0.

Завдяки концепції рівнів безпеки трафік TCP і UDP від хостів, підключених до внутрішніх інтерфейсів (рівень 100), може досягати хостів в Інтернеті за зовнішнім інтерфейсом (рівень 0) . У цьому випадку мережевий трафік проходить шлях від інтерфейсів ядра (рівень 100) до зовнішнього (рівень 0) інтерфейсу і назад.

Простими словами, трафік який ініціалізований з інтерфейсу з вищим рівнем безпеки, дозволяється входити в інтерфейс з нищим рівнем безпеки і назад. Однак трафік з інтерфейсу з нищим рівнем безпеки не передається до інтерфейсу з вищим рівнем безпеки, тому якщо необхідно дозволити трафіку із зовнішнього інтерфейсу потрапляти до внутрішнього, необхідно налагодити списки доступу(ACL).

Окрім цього потрібно налаштувати статичний маршрут за замовчуванням, щоб дістатися до хостів в Інтернеті. Пізніше цей маршрут буде налаштовано за допомогою протоколу OSPF.



```
7200_Edge_Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
7200_Edge_Router1(config)#int g0/0
7200_Edge_Router1(config-if)#ip add 192.168.1.100 255.255.255.0
7200_Edge_Router1(config-if)#no shut
7200_Edge_Router1(config-if)#exit
7200_Edge_Router1(config)#int eth1/1
7200_Edge_Router1(config-if)#ip add 192.168.2.1 255.255.255.0
7200_Edge_Router1(config-if)#no shut
7200_Edge_Router1(config-if)#ip nat inside
7200_Edge_Router1(config-if)#exit
7200_Edge_Router1(config)#int g0/0
7200_Edge_Router1(config-if)#ip nat outside
7200_Edge_Router1(config-if)#exit
7200_Edge_Router1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
7200_Edge_Router1(config)#access-list 1 permit 192.168.110.0 0.0.0.255
7200_Edge_Router1(config)#access-list 1 permit 192.168.120.0 0.0.0.255
7200_Edge_Router1(config)#access-list 1 permit 192.168.140.0 0.0.0.255
7200_Edge_Router1(config)#access-list 1 permit 192.168.150.0 0.0.0.255
7200_Edge_Router1(config)#access-list 1 permit 192.168.170.0 0.0.0.255
7200_Edge_Router1(config)#access-list 1 permit 192.168.180.0 0.0.0.255
7200_Edge_Router1(config)#$1.101 192.168.1.200 netmask 255.255.255.0
7200_Edge_Router1(config)#ip nat inside source list 1 pool global-ips
7200_Edge_Router1(config)#router ospf 1
7200_Edge_Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
7200_Edge_Router1(config-router)#network 192.168.2.0 0.0.0.255 area 0
7200_Edge_Router1(config-router)#network 192.168.3.0 0.0.0.255 area 0
7200_Edge_Router1(config-router)#exit
```

Рис. 3.28 Налаштування NAT, списків доступу на 7200_Edge_Router1

```

ASA-971-ASDM-1 - PuTTY
ciscoasa# conf t
ciscoasa(config)# zone inside_zone
ciscoasa(config)# int g0/0
ciscoasa(config-if)# des CORE1
ciscoasa(config-if)# nameif INSIDE1
INFO: Security level for "INSIDE1" set to 0 by default.
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip add 192.168.4.1 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# zone-member inside_zone
ciscoasa(config-if)# exit
ciscoasa(config)# int g0/1
ciscoasa(config-if)# des CORE2
ciscoasa(config-if)# nameif INSIDE2
INFO: Security level for "INSIDE2" set to 0 by default.
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip add 192.168.5.1 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# zone-member inside_zone
ciscoasa(config-if)# exit
ciscoasa(config)# int management 0/0
ciscoasa(config-if)# des EDGE
ciscoasa(config-if)# nameif OUTSIDE
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip add 192.168.3.2 255.255.255.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)# route OUTSIDE 0.0.0.0 0.0.0.0 192.168.3.1

```

Рис. 3.29 Налаштування інтерфейсів, рівнів безпеки та статичного маршруту

Задля забезпечення простішого налаштування, були створені об'єкти та групи об'єктів, які будуть допомагати підтримувати конфігурацію, тобто за допомогою об'єктів ми зможемо налаштовувати всі посилання, які прив'язані до нього.

```

ASA-971-ASDM-1 - PuTTY
ciscoasa(config)# object network vlan120_192.168.120
ciscoasa(config-network-object)# subnet 192.168.120.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network vlan140_192.168.140
ciscoasa(config-network-object)# subnet 192.168.140.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network vlan150_192.168.150
ciscoasa(config-network-object)# subnet 192.168.150.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network vlan170_192.168.170
ciscoasa(config-network-object)# subnet 192.168.170.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network vlan180_192.168.180
ciscoasa(config-network-object)# subnet 192.168.180.0 255.255.255.0
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network google_dns1
ciscoasa(config-network-object)# host 8.8.8.8
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network google_dns2
ciscoasa(config-network-object)# host 8.8.4.4
ciscoasa(config-network-object)# exit
ciscoasa(config)# object-group network MGMT
ciscoasa(config-network-object-group)# network-object object vlan110_192.168.15
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network OFFICES
ciscoasa(config-network-object-group)# network-object object vlan110_192.168.15
ciscoasa(config-network-object-group)# network-object object vlan120_192.168.15
ciscoasa(config-network-object-group)# network-object object vlan140_192.168.15
ciscoasa(config-network-object-group)# network-object object vlan150_192.168.15
ciscoasa(config-network-object-group)# network-object object vlan170_192.168.15
ciscoasa(config-network-object-group)# network-object object vlan180_192.168.15
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network google_dns
ciscoasa(config-network-object-group)# network-object object google_dns1
ciscoasa(config-network-object-group)# network-object object google_dns2
ciscoasa(config-network-object-group)# exit

```

Рис. 3.30 Налаштування об'єктів та груп об'єктів

Створення ICMP ECHO Request та Echo Reply(рис. 3.31) на внутрішніх інтерфейсах, надання дозволів підмережам (192.168.110-180), здійснювати ping зовнішніх інтерфейсів ASA.

Рис. 3.31 Налаштування ICMP ECHO Request та Echo Reply

OSPF протокол, забезпечує з'єднання між робочими станціями та хостами які знаходяться в Інтернеті. Статичний маршрут за замовчуванням, що вказує на 7200_Edge_Router1, перерозподіляється на процес OSPF.

Рис. 3.32 Налаштування OSPF на Cisco ASA

Списки доступу дозволення пакетам із вихідною адресою 8.8.8.8 та 8.8.4.4 до підмереж кінцевого користувача. ACL дозволяє користувачам перевірити підключення до загальнодоступного DNS Google за допомогою команди ping. Без списків доступу vASA не передаватиме пакети із зовнішнього інтерфейсу до інтерфейсу всередині(рис. 3.33).

Рис. 3.33 Створення списків доступу

3.2 Тестування підсистеми периметрового захисту корпоративної мережі організації.

Тестування підсистеми периметрового захисту корпоративної мережі організації проводиться з метою перевірки налаштувань на відповідність поставленим завданням.

Для початку перевіримо налаштування DHCP-серверу та наявність зв'язку пристроями мережі (рис.3.34-3.26).

```

DHCP_Server
DHCP_Server#show ip dhcp pool

Pool ADMINS :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 0
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.110.1 192.168.110.1 - 192.168.110.254 0

Pool Office2 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.120.12 192.168.120.1 - 192.168.120.254 1

Pool Office3 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.140.12 192.168.140.1 - 192.168.140.254 1

Pool Office4 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.150.12 192.168.150.1 - 192.168.150.254 1

Pool Office5 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.170.12 192.168.170.1 - 192.168.170.254 1

Pool Office6 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.180.12 192.168.180.1 - 192.168.180.254 1

```

Рис. 3.34 Виконання команди show ip dhcp pool

```

DHCP_Server
DHCP_Server#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type
Hardware address/
User name
192.168.120.11   0100.5079.6668.00 Jun 03 2022 12:14 PM Automatic
192.168.140.11   0100.5079.6668.01 Jun 03 2022 11:51 AM Automatic
192.168.150.11   0100.5079.6668.02 Jun 03 2022 12:14 PM Automatic
192.168.170.11   0100.5079.6668.03 Jun 03 2022 12:14 PM Automatic
192.168.180.11   0100.5079.6668.04 Jun 03 2022 12:14 PM Automatic

```

Рис. 3.35 Виконання команди show ip dhcp binding

```

PC4 - PuTTY
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
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" licence.
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

PC4> ip dhcp
DDORA IP 192.168.170.11/24 GW 192.168.170.1
PC4>

```

Рис. 3.36 Перевірка видання IP-адреси сервером

```

TascasGui [Роботає] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=1 ttl=115 time=83.2 ms
--- www.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 83.239/83.239/83.239/0.000 ms
tacgui@tacgui:~$ ping 192.168.120.11
PING 192.168.120.11 (192.168.120.11) 56(84) bytes of data.
64 bytes from 192.168.120.11: icmp_seq=1 ttl=63 time=3008 ms
64 bytes from 192.168.120.11: icmp_seq=2 ttl=63 time=1996 ms
64 bytes from 192.168.120.11: icmp_seq=3 ttl=63 time=972 ms
64 bytes from 192.168.120.11: icmp_seq=4 ttl=63 time=7.05 ms
--- 192.168.120.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3037ms
rtt min/avg/max/mdev = 7.057/1495.973/3008.255/1121.212 ms, pipe 3
tacgui@tacgui:~$ ping 192.168.140.11
PING 192.168.140.11 (192.168.140.11) 56(84) bytes of data.
64 bytes from 192.168.140.11: icmp_seq=1 ttl=60 time=13.6 ms
64 bytes from 192.168.140.11: icmp_seq=2 ttl=60 time=11.3 ms
64 bytes from 192.168.140.11: icmp_seq=3 ttl=60 time=13.1 ms
64 bytes from 192.168.140.11: icmp_seq=4 ttl=60 time=14.3 ms
--- 192.168.140.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 11.375/13.130/14.365/1.116 ms
tacgui@tacgui:~$ ping www.google.com
PING www.google.com (216.58.209.4) 56(84) bytes of data.
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=1 ttl=115 time=76.0 ms
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=2 ttl=115 time=83.7 ms
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=3 ttl=115 time=78.8 ms
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=4 ttl=115 time=76.9 ms
64 bytes from uaw02s18-in-f4.1e100.net (216.58.209.4): icmp_seq=5 ttl=115 time=68.1 ms
--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 68.106/76.713/83.722/5.076 ms
tacgui@tacgui:~$

```

Рис. 3.37 Перевірка зв'язку з робочих станцій

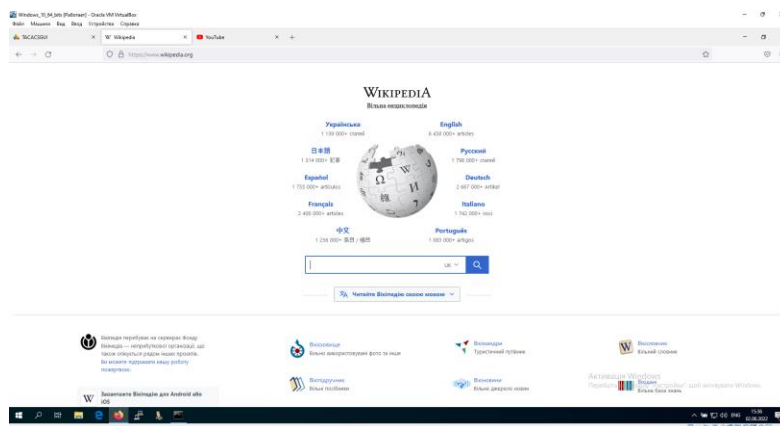


Рис.3.38 Перевірка наявності зв'язку до мережі Інтернет

Тепер спробуємо зайти під користувачем bogdancheg на маршрутизаторі L3_CORE_Switch2, тим самим перевіримо правильність налаштування SSH(рис.3.39).

```

192.168.9.1 - PuTTY
login as: bogdancheg
Keyboard-interactive authentication prompts from server:
| Unauthorized access is prohibited!
| Password:
| Today is a perfect day! Have a nice day!
End of keyboard-interactive prompts from server

L3_CORE_Swit
L3_CORE_Switch2>en
Password:
L3_CORE_Switch2#

```

Рис. 3.39. Перевірка налаштувань користувачів та SSH

3.3 Аналіз результатів тестування

Як і планувалося, всі вимоги, які ставились раніше, були успішно виконані. В майбутньому дана мережа може бути збільшена та покращена під якісь певні завдання. Для цього є всі можливості. DHCP допоможе при встановленні нових робочих станцій та пристроїв, сервер - для налаштування нових приладів та моніторингу за ними, а рівень ядра, так як використовуються маршрутизатори фірми CISCO, є досить гнучкий для майбутніх налаштувань.

Ще одна перевага мережі в тому, що на рівні ядра є 2 маршрутизатори, які з'єднані між собою і якщо один з них виходить з ладу, то за допомогою протоколу OSPF досить швидко знаходиться новий маршрут до потрібної мережі.

Був встановлений Cisco ASA в інтернет модулі, що забезпечить надійний захист мережі від втручання зломисників із мережі інтернет.

Щодо недоліків даної мережі, чим більш професійне та якісне обладнання, тим воно буде дорожче. Тобто комутатори та маршрутизатори від компанії CISCO є досить дорогими через їх надійність, якість, гарантію на заміну пристрою чи його компонентів при неполадках в малі строки, що досить вигідно великим компаніям, коли кожна хвилина коштує грошей.

Висновки до 3-го розділу:

В даному розділі було описано базові налаштування всіх пристроїв даної мережі. Була налаштована статична та динамічна (DHCP) маршрутизація. Для зручності використання та налаштування пристроїв було надано кожному особисту назву.

На всіх пристроях мережі було налаштовано протокол SSH для віддаленого підключення до них. Також налаштовано Tacs-сервер для збереження усіх локальних записів. Для зв'язку між всіма підмережами налаштовано протокол маршрутизації OSPF.

Було проведено аналіз тестування та описано можливості масштабування та покращення мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У дипломному проекті була спроектована ієрархічна модель підсистеми периметрового захисту корпоративної мережі організації. Для побудови мережі використовувалися технології від компанії CISCO.

Для початку було проведено аналіз та вибір існуючих технологій побудови сучасних гетерогенних мереж. Зокрема було обрано графічний симулятор GNS3, ОС Windows, TacacsGUI, протокол маршрутизації OSPF, а також технології прикладного рівня SSH та DHCP.

На етапі розробки мережі було визначено, що комп'ютерна мережа міститиме інтернет модуль, рівень ядра з сервером, розподілу та доступу з робочими станціями та невиділеним сервером. Щоб спростити у разі росту мережі налаштування IP-адресації пристроїв було використано DHCP-сервер. Для можливості віддаленого досупу використовувався захищений протокол SSHv2.

Було спроектовано трирівневу ієрархічну модель комп'ютерної мережі.

Далі було спроектовано логічну ієрархічну модель комп'ютерної мережі трьох рівнів, яка складається з рівнів ядра, розподілу і доступу.

Це дозволяє забезпечити зміни мережі в майбутньому – масштабованість та надійність роботи. Комп'ютерна мережі має в собі сім робочих станцій, дві з яких невиділені сервери.

Для масштабованості мережі в майбутньому використовувалися образи комутатора другого рівня з шістнадцятьма портами (образ i86bi-linux-l2-adventerprisek9-15.1a.bin), адже звичайний комутатор, який знаходиться в GNS3, неможливо налаштувати необхідним нам чином. Для ядра мережі використовувалися образи досить потужних та гнучких в налаштуванні маршрутизаторів третього рівня фірми CISCO (образ i86bi-linux-l3-adventerprisek9-15.4.2T4.bin). Для серверу було обрано маршрутизатор Cisco 7200(образ c7200-adventerprisek9_sna-mz.150-1.M3.image). Сервер також дає змогу зазначати орендовані адреси та назви комп'ютерів і пристроїв, які орендували їх. Також можна продивитися заборонені IP-адреси.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

В інтернет модулі було встановлено Cisco ASA і в ході налаштувань пояснювалася конфігурація пристрою ASA-971. Пристрій являє собою віртуальний пристрій Cisco Adaptive Security Virtual Appliance, встановлений на диску qcow2. ASA-971 надає послуги фільтрації та перевірки трафіку для мережі. Він також з'єднує робочу мережу до інтернет модуля.

В третьому розділі було обрано обладнання на програмне забезпечення. Образи маршрутизаторів та комутаторів обрані від компанії CISCO через їх надійність на гнучкість в налаштуваннях. Це ще раз доводить те, що система буде досить надійною. Програма, в якій виконувався дипломний проект (GNS3) була обрана через, те що вона дозволяє створити саме гетерогенну мережу за допомогою VirtualBox, яка в свою чергу, дозволяє використовувати різні операційні системи, зокрема Windows.

Проведено налаштування пристроїв та аналіз результатів, сформовано висновки стосовно модернізації та вдосконалення роботи. Реалізована мережа є готовим макетом реальної реалізації проекту, а конфігурації можуть застосовуватися для реального обладнання.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корпоративна мережа [Електронний ресурс] – https://uk.wikipedia.org/wiki/Корпоративна_мережа
2. Інформаційна безпека [Електронний ресурс] – https://uk.wikipedia.org/wiki/Інформаційна_безпека
3. Протокол OSPF [Електронний ресурс] – <https://habr.com/ru/post/418391/>
4. Налаштування CISCO DHCP [Електронний ресурс] – https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html
5. DNC сервер [Електронний ресурс] – <https://ru.wikipedia.org/wiki/DNS>
6. DHCP relay [Електронний ресурс] – <https://ixnfo.com/dhcp-relay-cisco.html>
7. Windows 10 [Електронний ресурс] – <https://www.microsoft.com/uk-ua/software-download/windows10>
8. TacacsGUI [Електронний ресурс] – <https://tacacsgui.com>
9. Kali Linux [Електронний ресурс] – <https://www.kali.org/get-kali/#kali-virtual-machines>
10. Cisco ASA v [Електронний ресурс] – <https://docs.gns3.com/docs/how-to-guides/cisco-asa/>
11. RADIUS [Електронний ресурс] – <https://uk.wikipedia.org/wiki/RADIUS>
12. TACACS+ [Електронний ресурс] – <https://ru.wikipedia.org/wiki/TACACS%2B>
13. Налаштування NAT [Електронний ресурс] – <http://commonerrors.blogspot.com/2011/07/nat-configuration-on-gns3.html>
14. Протокол AAA [Електронний ресурс] – https://uk.wikipedia.org/wiki/Протокол_AAA
15. Ієрархічна модель мережі від Cisco [Електронний ресурс] – <http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
16. Протокол SSH [Електронний ресурс] – <https://uk.wikipedia.org/wiki/SSH>

17. Cisco IOS – Privilege Levels [Електронний ресурс] -
<https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>
18. Cisco 7200 - [Електронний ресурс] –
<https://www.cisco.com/c/en/us/support/routers/7200-series-routers/series.html>
19. GNS3 [Електронний ресурс] - <https://habr.com/ru/post/266503/>
20. VirtualBox [Електронний ресурс] - <https://www.virtualbox.org/>
21. Wireshark [Електронний ресурс] –
https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

Міжмережний екран

ASA-971

ciscoasa# show running-config

: Saved

:

: Serial Number: 9A7HTE9H6S7

: Hardware: ASAv, 2048 MB RAM, CPU Pentium II 2496 MHz

:

ASA Version 9.7(1)

!

hostname ciscoasa

enable password \$sha512\$5000\$krVaOasANfdkv8Hw+ySViA==\$NNcmfNSS+58bUvTne/JkA== 2

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

names

zone inside_zone

!

interface GigabitEthernet0/0

nameif INSIDE1

security-level 100

zone-member inside_zone

ip address 192.168.4.1 255.255.255.0

!

interface GigabitEthernet0/1

nameif INSIDE2

security-level 100

zone-member inside_zone

ip address 192.168.5.1 255.255.255.0

!

interface GigabitEthernet0/2

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/3

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/4

shutdown

no nameif

no security-level

no ip address

!

interface Management0/0

nameif OUTSIDE

security-level 0	network-object object google_dns2
ip address 192.168.3.2 255.255.255.0	access-list out-to-ins extended permit icmp any object-group MGMT echo-reply
!	
ftp mode passive	access-list out-to-ins extended permit icmp any object-group OFFICES echo-reply
object network vlan110_192.168.110	access-list out-to-ins extended permit icmp object-group google_dns object-group
subnet 192.168.110.0 255.255.255.0	
object network vlan120_192.168.120	pager lines 23
subnet 192.168.120.0 255.255.255.0	mtu INSIDE1 1500
object network vlan140_192.168.140	mtu INSIDE2 1500
subnet 192.168.140.0 255.255.255.0	mtu OUTSIDE 1500
object network vlan150_192.168.150	no failover
subnet 192.168.150.0 255.255.255.0	no monitor-interface service-module
object network vlan170_192.168.170	icmp unreachable rate-limit 1 burst-size 1
subnet 192.168.170.0 255.255.255.0	icmp permit 192.168.110.0 255.255.255.0 INSIDE1
object network vlan180_192.168.180	icmp permit 192.168.4.0 255.255.255.0 INSIDE1
subnet 192.168.180.0 255.255.255.0	icmp permit 192.168.5.0 255.255.255.0 INSIDE1
object network google_dns1	icmp permit 192.168.120.0 255.255.255.0 INSIDE1
host 8.8.8.8	icmp permit 192.168.140.0 255.255.255.0 INSIDE1
object network google_dns2	icmp permit 192.168.150.0 255.255.255.0 INSIDE1
host 8.8.4.4	icmp permit 192.168.170.0 255.255.255.0 INSIDE1
object-group network MGMT	icmp permit 192.168.180.0 255.255.255.0 INSIDE1
network-object object vlan110_192.168.110	icmp permit 192.168.110.0 255.255.255.0 INSIDE2
object-group network OFFICES	icmp permit 192.168.4.0 255.255.255.0 INSIDE2
network-object object vlan110_192.168.110	icmp permit 192.168.5.0 255.255.255.0 INSIDE2
network-object object vlan120_192.168.120	icmp permit 192.168.120.0 255.255.255.0 INSIDE2
network-object object vlan140_192.168.140	icmp permit 192.168.140.0 255.255.255.0 INSIDE2
network-object object vlan150_192.168.150	icmp permit 192.168.150.0 255.255.255.0 INSIDE2
network-object object vlan170_192.168.170	icmp permit 192.168.170.0 255.255.255.0 INSIDE2
network-object object vlan180_192.168.180	icmp permit 192.168.180.0 255.255.255.0 INSIDE2
object-group network google_dns	no asdm history enable
network-object object google_dns1	arp timeout 14400

no arp permit-nonconnected	auto-import
arp rate-limit 8192	crypto ca certificate chain _SmartCallHome_ServerCA
access-group out-to-ins in interface OUTSIDE	certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
router ospf 1	308204d3 308203bb a0030201 02021018 dad19e26
network 192.168.3.0 255.255.255.0 area 0	7de8bb4a 2158cdcc 6b3b4a30
network 192.168.4.0 255.255.255.0 area 0	0d06092a 864886f7 0d010105 05003081 ca310b30
network 192.168.5.0 255.255.255.0 area 0	09060355 04061302 55533117
log-adj-changes	30150603 55040a13 0e566572 69536967 6e2c2049
!	6e632e31 1f301d06 0355040b
route OUTSIDE 0.0.0.0 0.0.0.0 192.168.3.1 1	13165665 72695369 676e2054 72757374 204e6574
timeout xlate 3:00:00	776f726b 313a3038 06035504
timeout pat-xlate 0:00:30	0b133128 63292032 30303620 56657269 5369676e
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp	2c20496e 632e202d 20466f72
0:02:00 icmp 0:00:02	20617574 686f7269 7a656420 75736520 6f6e6c79
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp	31453043 06035504 03133c56
0:05:00 mgcp-pat 0:05:00	65726953 69676e20 436c6173 73203320 5075626c
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00	69632050 72696d61 72792043
sip-disconnect 0:02:00	65727469 66696361 74696f6e 20417574 686f7269
timeout sip-provisional-media 0:02:00 uauth 0:05:00	7479202d 20473530 1e170d30
absolute	36313130 38303030 3030305a 170d3336 30373136
timeout tcp-proxy-reassembly 0:01:00	32333539 35395a30 81ca310b
timeout floating-conn 0:00:00	30090603 55040613 02555331 17301506 0355040a
timeout conn-holddown 0:00:15	130e5665 72695369 676e2c20
timeout igp stale-route 0:01:10	496e632e 311f301d 06035504 0b131656 65726953
user-identity default-domain LOCAL	69676e20 54727573 74204e65
no snmp-server location	74776f72 6b313a30 38060355 040b1331 28632920
no snmp-server contact	32303036 20566572 69536967
crypto ipsec security-association pmtu-aging infinite	6e2c2049 6e632e20 2d20466f 72206175 74686f72
crypto ca trustpoint _SmartCallHome_ServerCA	697a6564 20757365 206f6e6c
no validation-usage	79314530 43060355 0403133c 56657269
crl configure	5369676e 20436c61 73732033 20507562
crypto ca trustpool policy	6c696320 5072696d 61727920 43657274 69666963
	6174696f 6e204175 74686f72
	69747920 2d204735 30820122 300d0609 2a864886
	f70d0101 01050003 82010f00
	3082010a 02820101 00af2408 08297a35 9e600caa
	e74b3b4e dc7cbc3c 451cbb2b

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

e0fe2902 f95708a3 64851527 f5f1adc8 31895d22
e82aaaa6 42b38ff8 b955b7b1

b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4
d8def8e0 c362083d 5413eb49

ca595485 26e52b8f 1b9feb5f a191c233 49d84363
6a524bd2 8fe87051 4dd18969

7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0
f4a225f2 af1c9267 18e5f406

04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb
378becf4 d7acf2f6 f03dafdd

75913319 1d1c40cb 74241921 93d914fe ac2a52c7
8fd50449 e48d6347 883c6983

cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314
087ee53f 9f73b833 0acf5d3f

3487968a ee53e825 15020301 0001a381 b23081af
300f0603 551d1301 01ff0405

30030101 ff300e06 03551d0f 0101ff04 04030201
06306d06 082b0601 05050701

0c046130 5fa15da0 5b305930 57305516 09696d61
67652f67 69663021 301f3007

06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf
806ad448 182c7b19 2e302516

23687474 703a2f2f 6c6f676f 2e766572 69736967
6e2e636f 6d2f7673 6c6f676f

2e676966 301d0603 551d0e04 1604147f d365a7c2
ddecbbf0 3009f343 39fa02af

33313330 0d06092a 864886f7 0d010105 05000382
01010093 244a305f 62cfd81a

982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45
7064c5e7 97662d98

097e5faf d6cc2865 f201aa08 1a47def9 f97c925a
0869200d d93e6d6e 3c0d6ed8

e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415
3881c994 eea28429 0b136f8e

db0cdd25 02dba48b 1944d241 7a05694a 584f60ca
7e826a0b 02aa2517 39b5db7f

e784652a 958abd86 de5e8116 832d10cc defda882
2a6d281f 0d0bc4e5 e71a2619

e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef
a57d4540 728eb70e

6b0e06fb 33354871 b89d278b c4655f0d 86769c44
7af6955c f65d3208 33a454b6

183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a

quit

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

ssh key-exchange group dh-group1-sha1

console timeout 0

threat-detection basic-threat

threat-detection statistics access-list

no threat-detection statistics tcp-intercept

dynamic-access-policy-record DfltAccessPolicy

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns migrated_dns_map_1

parameters

message-length maximum client auto

message-length maximum 512

no tcp-inspection

policy-map global_policy

class inspection_default

inspect dns migrated_dns_map_1

inspect ftp

```

inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp

policy-map type inspect dns migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
service-policy global_policy global

prompt hostname context

no call-home reporting anonymous

call-home

profile CiscoTAC-1
no active

destination          address          http
https://tools.cisco.com/its/service/oddce/services/De

destination address email callhome@cisco.com

destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly

subscribe-to-alert-group telemetry periodic daily

profile License

destination          address          http
https://tools.cisco.com/its/service/oddce/services/De

destination transport-method http

Cryptochecksum:d37cfb80e6c873c9528ab9409c4ba20e

: end

ciscoasa#

```

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

L3_CORE_Switch2

L3_CORE_Switch2#show running-config

Building configuration...

Current configuration : 3072 bytes

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname L3_CORE_Switch2

!

boot-start-marker

boot-end-marker

!

!

logging buffered informational

logging rate-limit all 50

enable secret 5 \$1\$ad02\$qcL7Bs.LJ9De71QUrzzXn1

!

aaa new-model

!

!

aaa authentication login default group tacacs+ local

aaa authorization console

aaa authorization config-commands

aaa authorization exec default group tacacs+ local

aaa authorization commands 1 default group tacacs+ local

aaa authorization commands 15 default group tacacs+ local

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 1 default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacacs+

!

aaa session-id common

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

!

no ip domain lookup

ip domain name bogdancheg.net

ip cef

login block-for 60 attempts 3 within 30

login delay 5

no ipv6 cef

!

multilink bundle-name authenticated

!

username bogdancheg privilege 15 secret 5 \$1\$PT3B\$c15dw4k7YG/qcDvBbGlQD/

!

redundancy

!

no cdp log mismatch duplex

!

ip tcp synwait-time 5

ip ssh time-out 15

ip ssh logging events

ip ssh version 2

!

interface Ethernet0/0

no ip address

shutdown

!

interface Ethernet0/1

ip address 192.168.5.2 255.255.255.0

!

interface Ethernet0/2

no ip address

shutdown

!

interface Ethernet0/3

no ip address

shutdown

!

interface Ethernet1/0

no ip address

shutdown

!

interface Ethernet1/1

no ip address

shutdown

!

interface Ethernet1/2

no ip address

shutdown

!

interface Ethernet1/3

no ip address

shutdown

!

interface Ethernet2/0

ip address 192.168.9.1 255.255.255.0

!

interface Ethernet2/1

ip address 192.168.10.1 255.255.255.0

!

interface Ethernet2/2

ip address 192.168.11.1 255.255.255.0

!

interface Ethernet2/3

no ip address

shutdown

!

interface Ethernet3/0

no ip address

shutdown

!

interface Ethernet3/1

no ip address

shutdown

!

interface Ethernet3/2

no ip address

shutdown

!

interface Ethernet3/3

no ip address

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						65
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
!
router ospf 1
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.7.0 0.0.0.255 area 0
network 192.168.9.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.5.1
!
ip access-list standard SSH-ADMIN-ACCESS
permit 192.168.110.4
permit 192.168.110.3
!
!
logging host 192.168.110.4
!
!
tacacs-server host 192.168.110.3
tacacs-server key 7 050513193541541B0F0D16171E08
!
control-plane
!
banner exec ^C

```

```

L3_CORE_Swit^C
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class SSH-ADMIN-ACCESS in
exec-timeout 5 0
logging synchronous
transport input ssh
transport output ssh
!
!
End
L3_CORE_Switch2#

```

Маршрутизатор

DHCP_Server

DHCP_Server#show running-config

Building configuration...

Current configuration : 4044 bytes

!

upgrade fpd auto

version 15.0

service timestamps debug datetime msec

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

service timestamps log datetime msec	group tacacs+
service password-encryption	!
!	!
hostname DHCP_Server	aaa session-id common
!	!
boot-start-marker	!
boot-end-marker	!
!	ip source-route
logging buffered informational	no ip icmp rate-limit unreachable
logging rate-limit all 50	ip cef
enable secret 5 \$1\$cJ7j\$dRqQEnLpWCH9HgR3R7P.D0	!
!	!
aaa new-model	ip dhcp excluded-address 192.168.110.1 192.168.110.10
!	ip dhcp excluded-address 192.168.120.1 192.168.120.10
!	ip dhcp excluded-address 192.168.140.1 192.168.140.10
aaa authentication login default group tacacs+ local	ip dhcp excluded-address 192.168.150.1 192.168.150.10
aaa authorization console	ip dhcp excluded-address 192.168.170.1 192.168.170.10
aaa authorization config-commands	ip dhcp excluded-address 192.168.180.1 192.168.180.10
aaa authorization exec default group tacacs+ local	!
aaa authorization commands 1 default group tacacs+ local	ip dhcp pool ADMINS
aaa authorization commands 15 default group tacacs+ local	network 192.168.110.0 255.255.255.0
aaa accounting exec default	default-router 192.168.110.1
action-type start-stop	dns-server 8.8.8.8 8.8.4.4
group tacacs+	!
!	ip dhcp pool Office2
aaa accounting commands 1 default	network 192.168.120.0 255.255.255.0
action-type start-stop	default-router 192.168.120.1
group tacacs+	dns-server 8.8.8.8 8.8.4.4
!	!
aaa accounting commands 15 default	ip dhcp pool Office3
action-type start-stop	network 192.168.140.0 255.255.255.0

default-router 192.168.140.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	ip tcp synwait-time 5
ip dhcp pool Office4	ip ssh time-out 15
network 192.168.150.0 255.255.255.0	ip ssh logging events
default-router 192.168.150.1	ip ssh version 2
dns-server 8.8.8.8 8.8.4.4	!
!	!
ip dhcp pool Office5	interface Ethernet0/0
network 192.168.170.0 255.255.255.0	no ip address
default-router 192.168.170.1	shutdown
dns-server 8.8.8.8 8.8.4.4	duplex auto
!	!
ip dhcp pool Office6	!
network 192.168.180.0 255.255.255.0	interface GigabitEthernet0/0
default-router 192.168.180.1	no ip address
dns-server 8.8.8.8 8.8.4.4	shutdown
!	duplex full
!	speed 1000
no ip domain lookup	media-type gbic
login block-for 60 attempts 3 within 30	negotiation auto
login delay 5	!
no ipv6 cef	!
!	interface Ethernet3/0
multilink bundle-name authenticated	ip address 192.168.100.1 255.255.255.0
!	duplex half
!	!
username bogdancheg privilege 15 secret 5 \$1\$SDru\$8cuD1lS7OkrkQH9N2o.A4.	!
!	interface Ethernet3/1
redundancy	ip address 192.168.130.1 255.255.255.0
	duplex half

!	ip route 0.0.0.0 0.0.0.0 192.168.100.2
!	ip route 0.0.0.0 0.0.0.0 192.168.130.2
interface Ethernet3/2	ip route 0.0.0.0 0.0.0.0 192.168.160.2
ip address 192.168.160.1 255.255.255.0	!
duplex half	ip access-list standard SSH-ADMIN-ACCESS
!	permit 192.168.110.4
!	permit 192.168.110.3
interface Ethernet3/3	!
no ip address	!
shutdown	logging 192.168.110.4
duplex half	no cdp log mismatch duplex
!	!
!	!
!	tacacs-server host 192.168.110.3
router ospf 1	tacacs-server key 7 04551E101B2C565C1F110412070F
log-adjacency-changes	!
network 192.168.100.0 0.0.0.255 area 0	control-plane
network 192.168.110.0 0.0.0.255 area 0	!
network 192.168.120.0 0.0.0.255 area 0	gatekeeper
network 192.168.130.0 0.0.0.255 area 0	shutdown
network 192.168.140.0 0.0.0.255 area 0	!
network 192.168.150.0 0.0.0.255 area 0	banner exec ^C
network 192.168.160.0 0.0.0.255 area 0	DHCP_Server
network 192.168.170.0 0.0.0.255 area 0	ip domain-name bogdan^C
network 192.168.180.0 0.0.0.255 area 0	!
!	line con 0
ip forward-protocol nd	exec-timeout 0 0
no ip http server	privilege level 15
no ip http secure-server	logging synchronous
!	stopbits 1
!	line aux 0

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

access-class SSH-ADMIN-ACCESS in

exec-timeout 5 0

logging synchronous

transport input ssh

transport output ssh

!

end

DHCP_Server#

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						71
Змн.	Арк.	№ докум.	Підпис	Дата		