

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

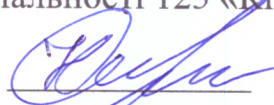
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ
МЕРЕЖІ НА БАЗІ РІШЕНЬ CISCO ASA»

Виконав:

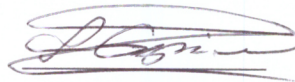
студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»



Назар ЛЯШЕНКО

Керівник:

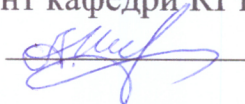
завідувач кафедри КІ та КБ, к.т.н., доцент



Андрій ЄФІМЕНКО

Рецензент:

доцент кафедри КІ та КБ, к.т.н.



Олексій ШЕЛУХА

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

Андрій ЄФІМЕНКО

5 березня 2024 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу бакалавра

Студент: Ляшенко Назар Борисович

Тема роботи: «Проект підсистеми захисту корпоративної мережі на базі рішень Cisco ASA»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

- Захист мережі.
- Набір протоколів IP Security.

Обладнання та програмне забезпечення:

- Маршрутизатор Cisco 7200 Series VRX
- Комутатор Cisco Catalyst WS-C2960-24TT-L
- Міжмережевий екран ASA 5500
- Операційна система Windows 7

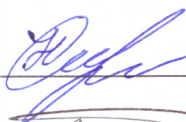
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	5.03.24	05.03.2024
2	Єфіменко А.А.	5.03.24	05.03.2024
3	Єфіменко А.А.	5.03.24	05.03.2024

Студент Назар ЛЯШЕНКО
Керівник Андрій ЄФІМЕНКО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 квітня 2024	Виконано
2	Аналіз технологій, що стосуються захисту комп'ютерних мереж	2 квітня 2024 – 7 квітня 2024	Виконано
3	Проектування загальної топології	8 квітня 2024 – 17 квітня 2024	Виконано
4	Вибір обладнання та розробка IP—адресації	18 квітня 2024 – 28 квітня 2024	Виконано
5	Налаштування пристроїв мережі	29 квітня 2024 – 8 травня 2024	Виконано
6	Тестування налаштованої мережі	9 травня 2024 – 12 травня 2024	Виконано
7	Додаткові налаштування мережі, пов'язані з безпекою	13 травня 2024 – 23 травня 2024	Виконано
8	Написання пояснювальної записки	24 травня 2024 – 6 червня 2024	Виконано
9	Підготовка додаткових матеріалів	7 червня 2024 – 16 червня 2024	Виконано
10	Отримання відгуку та рецензії на кваліфікаційну роботу	16 червня 2024 – 25 червня 2024	Виконано
11	Захист кваліфікаційної роботи	26 червня 2024	Виконано

Студент  Назар ЛЯШЕНКО
Керівник  Андрій ЄФІМЕНКО

АНОТАЦІЯ

Кваліфікаційна робота містить опис проектування, розробки та налаштування проекту підсистеми захисту мережі з використанням Cisco ASA. Пояснювальна записка складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 72 сторінках друкованого тексту.

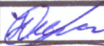
Пояснювальна записка містить 14 сторінок додатків. Список використаних джерел містить 21 найменування і займає 2 сторінки. В роботі наведено 80 рисунків та 2 таблиці. Загальний обсяг роботи 93 сторінки.

У кваліфікаційній роботі проаналізовано практичний приклад налаштування підмережі захисту корпоративної мережі на основі рішень Cisco ASA, порівняно різні протоколи маршрутизації, розглянуто певні аспекти налаштування безпечних функцій мережевих пристроїв з метою додаткового захисту мережі. Спроектовано загальну топологію мережі, обрано обладнання, що найкраще підходить для налаштування топології мережі. Налаштовано комп'ютерну мережу у відповідності до плану та перевірено працездатність мережі, правильність функціонування всіх протоколів.

Метою кваліфікаційної роботи є розробка та налаштування проекту підсистеми захисту корпоративної мережі з використанням рішень Cisco ASA.

В результаті виконання кваліфікаційної роботи досліджено методики та способи побудови підсистем захисту корпоративних мереж, розроблено власну підсистему захисту, наведено результати дослідження роботоздатності побудованої мережі.

КЛЮЧОВІ СЛОВА: КОМП'ЮТЕРНА МЕРЕЖА, ЗАХИСТ, ASA, OSPF, VLAN, VPN, ACL, VPN L2TP, IPSEC, КОРПОРАТИВНА МЕРЕЖА, КОМУТАТОР, МАРШРУТИЗАТОР, БРАНДМАУЕР, МІЖМЕРЕЖЕВИЙ ЕКРАН.

					ККІКБ.КР.Б – 125 – 14 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту корпоративної мережі на базі рішень Cisco ASA	Лім.	Арк.	Аркуші
Розроб.		Ляшенко Н.Б.		25.06.24				
Керівник		Єфіменко А.А.		25.06.24			4	93
Реценз.		Шелуха О.О.		25.06.24				
Н. контр.		Єфіменко А.А.		25.06.24				
Затверд.		Єфіменко А.А.		25.06.24		ФІКТ, Гр. КБ-20-1		

ANNOTATION

The qualification work contains a description of the design, development and configuration of a network security subsystem project using Cisco ASA. The explanatory note consists of a list of abbreviations, introduction, three chapters, conclusions, references and appendices.

The text part is presented on 72 pages of printed text.

The explanatory note contains 14 pages of appendices. The list of references includes 21 titles and occupies 2 pages. The work contains 80 figures and 2 tables. The total volume of the work is 93 pages.

The qualification paper analyzes a practical example of setting up a corporate network security subnet based on Cisco ASA solutions, compares different routing protocols, and considers certain aspects of setting up security functions of network devices for additional network protection. The general network topology is designed, and the equipment that is best suited for configuring the network topology is selected. Set up a computer network in accordance with the plan and checked the network performance, the correct functioning of all protocols.

The purpose of the qualification work is to develop and configure a project of a corporate network security subsystem using Cisco ASA solutions.

As a result of the qualification work, the methods and methods of building corporate network security subsystems were investigated, the own security subsystem was developed, and the results of the study of the built network performance were presented.

KEYWORDS: COMPUTER NETWORK, PROTECTION, ASA, OSPF, VLAN, VPN, ACL, VPN L2TP, IPSEC, CORPORATE NETWORK, SWITCH, ROUTER, FIREWALL, INTERCONNECTION SCREEN.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	5
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ І. ПРИНЦИПИ ТА ТЕХНОЛОГІЇ ПОБУДОВИ ПІДСИСТЕМ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ.....	9
1.1. Загальні підходи до побудови підсистем захисту корпоративних мереж.	9
1.2. Периметровий захист як основа побудови систем захисту корпоративних мереж.	13
1.3. Забезпечення захищеного обміну даними на базі VPN в корпоративних мережах.	17
1.4. Аналіз комплексних рішень для побудови систем захисту корпоративних мереж.....	24
РОЗДІЛ ІІ. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ.....	30
2.1. Проектування політик безпеки корпоративної мережі.	30
2.2. Проектування загальної структури підсистеми захисту корпоративної мережі.	34
2.3. Проектування основних елементів підсистеми захисту корпоративної мережі.	40
РОЗДІЛ ІІІ. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ.	45
3.1. Обґрунтування вибору обладнання та програмного забезпечення для побудови підсистеми захисту.....	45
3.2. Налаштування підсистеми захисту корпоративної мережі.	53
3.3. Тестування функціоналу підсистеми захисту.	64
ВИСНОВКИ	77
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	78
ДОДАТКИ	80

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	6
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІКС — Інформаційно-комунікаційна система.

ЛКМ — Локальна комп'ютерна мережа.

ПК — Персональний комп'ютер.

КМ — комп'ютерна мережа.

ЕТН — Ethernet.

FE(FA) — Fast Ethernet.

GE(GIG) — Gigabit Ethernet.

MAC — Media Access Control — Управління доступом до середовища.

RID — Router Identifier – Ідентифікатор маршрутизатора.

IP — Internet Protocol.

VLAN — Virtual Local Area Network.

ACL — Access Control List.

VPN — Virtual Private Network.

ПК — персональний комп'ютер.

OSPF — Open Shortest Path First.

ASA — Adaptive Security Appliances.

ОС — операційна система.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	7
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Аналіз теми. З початку 21 сторіччя комп'ютери стали невід'ємною частиною нашого повсякденного життя. Розвиток Інтернету привів до зростання обсягу інформації, яка передається через комп'ютерні мережі. Це зумовило потребу в створенні надійних і безпечних комп'ютерних мереж у різних організаціях.

Одним з ключових аспектів забезпечення безпеки і надійності комп'ютерних мереж є використання високоякісного обладнання. У цьому контексті компанія Cisco визнана світовим лідером у галузі мережевих технологій. Вона пропонує широкий спектр рішень і продуктів, що задовольняють потреби організацій у побудові безпечних та надійних комп'ютерних мереж.

Завдання на кваліфікаційну роботу:

- аналіз теоретичних даних створення комп'ютерної мережі;
- вивчення завдання забезпечення функціонування КМ;
- проектування надійно захтщеної комп'ютерної мережі;
- налагодження та тестування функціонування створеної мережі;
- перевірка працездатності комп'ютерної мережі.

Метою проекту є розробка підсистеми захисту корпоративної мережі на базі обладнання Cisco.

Об'єктом дослідження процес проектування підсистеми захисту корпоративної мережі на базі обладнання Cisco.

Предметом дослідження є можливості, функціонал та переваги використання обладнання Cisco у побудові та захисті комп'ютерних мереж.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту корпоративної мережі на базі рішень Cisco ASA. Налаштовано та перевірено функціональність мережі.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	8
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ І. ПРИНЦИПИ ТА ТЕХНОЛОГІЇ ПОБУДОВИ ПІДСИСТЕМ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ.

1.1. Загальні підходи до побудови підсистем захисту корпоративних мереж.

В сучасному світі, де інформація стає все більш цінним активом, захист корпоративних мереж перетворюється на критично важливе завдання. Кіберзагрози постійно еволюціонують, стаючи все більш витонченими та руйнівними, тому організаціям необхідно вживати проактивних заходів для захисту своїх даних, систем та співробітників від кібератак.

Вибір правильного підходу до побудови підсистеми захисту корпоративної мережі є ключовим фактором у забезпеченні стійкості та кібербезпеки організації. Існує декілька ефективних підходів, кожен з яких має свої переваги та недоліки.

Захист корпоративних мереж є безперервним процесом, який потребує постійної оцінки ризиків та адаптації до нових загроз. Вибір правильного підходу до побудови підсистеми захисту є критично важливим для забезпечення безпеки та стійкості організації в динамічному цифровому середовищі.

Найпоширенішими підходами до побудови підсистем захисту корпоративних мереж є:

1. Багатошаровий захист.
2. Глибокий захист.
3. Захист на основі ризиків.
4. Захист на основі нульового довіри (Zero Trust).
5. Захист на основі хмарних технологій. [2]

Багатошаровий захист передбачає комплексне використання декількох рівнів захисту, кожен з яких доповнює та посилює інші. Наприклад, можна комбінувати:

- брандмауери;
- антивірусне програмне забезпечення;

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	9
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

- системи виявлення вторгнень (IDS);
- системи запобігання вторгненням (IPS): для блокування атак.

Брандмауери призначені для блокування несанкціонованого доступу до мережі. Антивірусне програмне забезпечення призначене для нейтралізації шкідливого програмного забезпечення. Системи виявлення вторгнень (IDS) слугують для ідентифікації підозрілої активності, а системи запобігання вторгненням (IPS) – для блокування атак.

До переваг багатоварового захисту відносяться його підвищена стійкість, гнучкість та масштабованість. Говорячи про підвищену стійкість мається на увазі, що навіть якщо один рівень захисту буде подолано, інші рівні можуть зупинити атаку. При реалізації багатоварового захисту в корпоративній мережі можна використовувати різні типи рішень для захисту від різних типів загроз, а також можна легко додати нові рівні захисту в міру зростання потреб організації.

Проте рішень, що не мають недоліків не існує. До недоліки багатоварового захисту відносяться:

1. Складність;
2. Витрати;
3. Можливі помилки.

Управління та налаштування декількох рівнів захисту може бути складним. Також може знадобитися значна інвестиція в апаратне та програмне забезпечення, а також у персонал для адміністрування. Кожен рівень захисту може мати свої помилки, що може призвести до помилкових спрацьовувань або невиявлення загроз.

Настуним розглянемо глибокий захист. Цей підхід пропонує інтегровані рішення, які об'єднують в одному продукті декілька функцій захисту. Наприклад, сучасні брандмауери часто мають вбудовані антивірусні та IPS-модулі, що спрощує адміністрування та підвищує ефективність захисту[10].

Переваги глибокого захисту:

- простота;

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	10
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

- ефективність;
- зниження витрат

Простота глибокого захисту полягає в тому, що легко налаштувати та керувати одним продуктом, який пропонує декілька функцій захисту. Ефективність глибокого захисту полягає в тому, що інтегровані рішення можуть краще координувати свою роботу, що може призвести до кращого виявлення та блокування загроз. Зниження затрат полягає в тому, що може знадобитися менше інвестицій в апаратне та програмне забезпечення, а також у персонал для адміністрування.

Недоліками глибокого захисту можна вважати обмежену гнучкість, залежність від постачальників та високу ймовірність помилки.

Через обмежену гнучкість даного підходу може бути складно знайти продукт, який пропонує всі необхідні функції захисту. Окремо організація стає залежною від одного постачальника для забезпечення захисту. А також у випадку коли продукт має помилку, вона може вплинути на всі функції захисту.

Підхід захисту на основі ризиків ґрунтується на оцінці ризиків, з якими стикається мережа організації. Організація повинна ідентифікувати свої критичні активи, такі як конфіденційні дані, фінансові системи та інтелектуальна власність. Потім необхідно визначити потенційні загрози цим активам та ймовірність їх реалізації. Нарешті, організація повинна впровадити заходи захисту в залежності від ступеню ризику[1].

Хоча оцінка ризиків на рівні організації є складним процесом, який потребує знань та досвіду, завжди існує необхідність регулярно переглядати існуючі кіберзагрози через їх постійні зміни та є повинна постійно моніторити свою мережу, щоб виявляти нові загрози захист на основі ризиків має і ряд переваг, серед яких важливо виокремити:

- Ефективне використання ресурсів;
- Підвищення рентабельності інвестицій;
- Зниження витрат на управління.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	11
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Захист фокусується на найбільш критичних активах та найбільш ймовірних загрозах. Інвестиції в засоби безпеки спрямовуються туди, де вони принесуть найбільшу користь. Окремо, немає потреби витрачати ресурси на захист від малоймовірних загроз.

Підхід захисту на основі нульового довіри (Zero Trust) передбачає, що всім користувачам і пристроям, які намагаються отримати доступ до мережі, за замовчуванням відмовляється в доступі. Доступ надається лише після того, як їх буде аутентифіковано та авторизовано. Навіть користувачам всередині мережі може бути надано доступ лише до тих ресурсів, які їм дійсно потрібні для виконання їхніх завдань[1].

Захист на основі хмарних технологій передбачає використання хмарних сервісів для забезпечення захисту мережі. Хмарні сервіси можуть пропонувати широкий спектр функцій захисту, таких як брандмауери, IPS, антивірусне програмне забезпечення та шифрування даних. [2]

Не існує єдиного найкращого підходу до побудови підсистеми захисту корпоративної мережі. Найкращий підхід буде залежати від конкретних потреб та вимог організації. При виборі підходу слід врахувати ріноманітні фактори, котрі охоплюють широке коло загроз та методик захисту. Для великих та складних мереж може знадобитися більш комплексний підхід, який включає в себе декілька рівнів захисту. Якщо в мережі зберігаються або обробляються конфіденційні дані, може знадобитися більш високий рівень захисту, ніж звичайний. Важливим аспектом є вартість реалізації, адже різні підходи до захисту можуть мати різну вартість [11]. А також велику роль відіграє кваліфікація фахівців, що організовують системи захисту корпоративних мереж — для деяких підходів може знадобитися більше навичок та досвіду, ніж для інших.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	12
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2. Периметровий захист як основа побудови систем захисту корпоративних мереж.

Обмін інформацією в мережі інтернет є невід’ємною складовою нашого життя. Уявити світ, в якому немає електронних листувань, месенджерів, додатків для перегляду контенту в режимі «онлайн» зараз неможливо. Сучасні реалії також змінили підхід до виконання робочих обов’язків в багатьох аспектах. Щодня все більше працівників різних компаній змушені працювати дистанційно, з використанням мережі Інтернет. Це все сприяє збільшенню трафіку в глобальній мережі кожного дня, а також збільшує кількість трафіку, що проходить через мережі організацій, локальні чи глобальні. Разом з тим активно зростає і кількість зловмисників, що використовують найрізноманітніші способи проникнень до, зокрема, вищезгаданих корпоративних мереж підприємств.

Кількість «паперових» операцій в усьому світі поступово зменшується та змінюється електронними аналогами, для прикладу електронний документообіг чи електронні платежі. Тому критично важливо не допускати збоїв мереж, оскільки вони можуть спричинити порушення чи повну зупинку роботи як окремих фізичних осіб, так і глобальних організацій. Для запобігання цьому необхідною є організація захисту інформаційних мереж. Необхідною компонентою систем інформаційної безпеки є захист периметру мереж.

Максимальне зменшення впливу зовнішніх загроз може бути досягнута впровадженням системи багаторівневого захисту інформації, насамперед на зовнішніх кордонах мережі. Головним завданням периметрових систем захисту інформації є поділ мережі на зовнішню та внутрішню зони. Важливо пам’ятати, що будь-які гарно захищені мережі, від локальних до глобальних, мають відповідати основоположним принципам інформаційної безпеки: конфіденційність, цілісність і доступність.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	13
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Розглянемо периметровий захист, як основу побудови захищених мереж. Захист периметра мережі є обов'язковим елементом системи інформаційної безпеки організації. Мінімізація зовнішніх загроз досягається шляхом впровадження багаторівневої системи захисту інформації, і насамперед на зовнішньому кордоні мережі[6].

Використання рішень для захисту периметра корпоративних мереж може бути застосовано в:

- комерційних організаціях, підключених до мереж загального користування;
- державних організаціях, підключених до мережі Інтернет;
- територіально-розподілених організаціях;
- організаціях-операторах зв'язку;
- фінансово-кредитних організаціях.

Захист периметра корпоративних мереж дає змогу:

- домогтися захищеності доступу внутрішніх користувачів до зовнішніх мереж; надання доступу із зовнішніх мереж до публічних корпоративних ресурсів;
- захисту від мережевих атак на корпоративні ресурси;
- організації системи електронної комерції;
- створення єдиної точки антивірусної та антиспам фільтрації;
- запобігання витоку конфіденційної інформації;
- моніторингу та аналізу подій інформаційної безпеки.

Периметровий захист є фундаментальним елементом загальної стратегії кібербезпеки корпоративних мереж. Він слугує першою лінією оборони, яка запобігає несанкціонованому доступу зловмисників до внутрішніх ресурсів організації. Периметровий захист допомагає захистити конфіденційні дані, такі як фінансова інформація, особисті дані та інтелектуальна власність, від несанкціонованого доступу, витоку та крадіжки. Також він може блокувати

кібератаки, такі як DDoS-атаки, атаки типу "людина посередині" та шкідливе програмне забезпечення, перш ніж вони завдадуть шкоди внутрішнім системам. І додатково, може значно знизити ризики кібербезпеки, з якими стикається організація, роблячи її більш стійкою до кібератак[14].

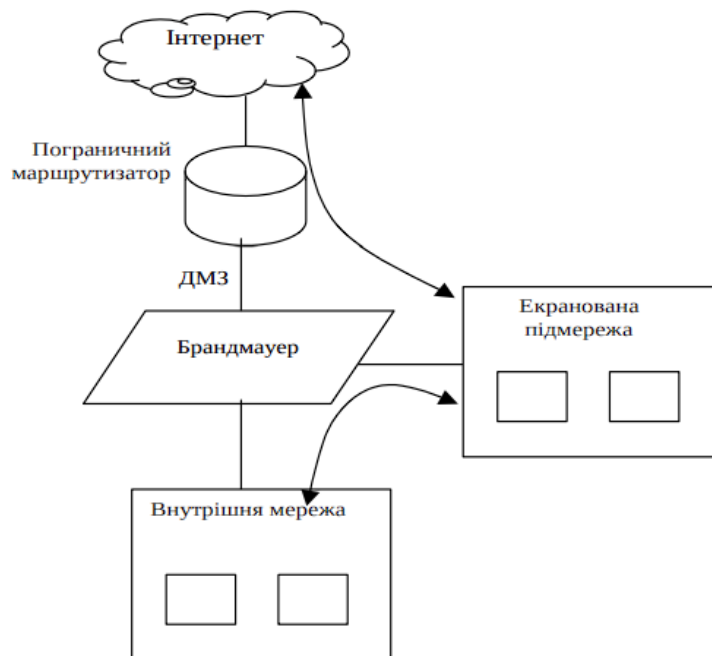


Рисунок 1.1 – Компоненти багаторівневого захисту мережного периметру.

Нижче розглянемо основні компоненти периметрового захисту.

Брандмауер (firewall, чи міжмережний екран) являє собою пристрій, який аналізує трафік з використанням набору правил, що дозволяють визначити, чи можна передавати цей трафік по мережі, чи не можна. Брандмауер вступає в дію після дії граничного маршрутизатора, фільтруючи трафік, він виконує ретельну перевірку всіх пакетів даних. Існує кілька різних типів брандмауерів, до яких відносяться статичні пакетні фільтри (для блокування доступу до підмережі можна використовувати, наприклад, вбудований статичний пакетний фільтр маршрутизатора Nortel Accellar), брандмауери експертного рівня (для контролю за дозволеними сервісами, наприклад Cisco PIX), а також проксі-брандмауери (для контролю за вмістом, наприклад Secure Computing's Sidewinder). Незважаючи на те, що брандмауери не є досконалими модулями, вони зможуть заблокувати або дозволити усе, що їм вкажуть[9].

Система запобігання вторгненням (Intrusion Prevention System): IPS — це програмне забезпечення, яке може не лише виявляти кібератаки, але й автоматично вживати заходів для їх блокування. IPS може блокувати шкідливий трафік, переривати з'єднання зловмисників та ізолювати заражені системи. У випадку виявлення інцидентів безпеки IDS сповіщають адміністратора різними способами: надсилаючи інформацію на електронну пошту, пейджинговий зв'язок чи зберігаючи інформацію про інцидент в log-файлі.

DMZ (DeMilitarized Zone – демілітаризована зона) являє собою незахищену область між захищеними ділянками. DMZ розміщена перед брандмауером, у той час як екранована підмережа розміщується за брандмауером.

Екранована підмережа являє собою ізольовану мережу, з'єднану з визначеним інтерфейсом брандмауера чи іншого пристрою, що фільтрує мережевий трафік. Екранована підмережа часто застосовується для ізоляції серверів, до яких необхідно забезпечити доступ з Інтернету, що використовуються тільки внутрішніми користувачами даної організації. Екранована підмережа, зазвичай, містить сервіси "загального використання": DNS-сервери, пошту пошту і web.

Віртуальні приватні мережа (VPN): VPN — це зашифрований тунель, який використовується для безпечного підключення віддалених користувачів та філій до корпоративної мережі. VPN може захистити конфіденційність даних, що передаються через Інтернет.

Антивірусне програмне забезпечення: Антивірусне програмне забезпечення може сканувати мережевий трафік, електронні листи та файли на предмет шкідливого програмного забезпечення. Воно може блокувати або видаляти шкідливе програмне забезпечення, перш ніж воно завдасть шкоди системам.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	16
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Важливими перевагами в рамках захисту корпоративних мереж від кіберзагроз є те, що периметровий захист може блокувати більшість кібератак, перш ніж вони досягнуть внутрішніх систем, його можна реалізувати за допомогою доступних технологій та рішень, захист периметру можна легко масштабувати, щоб відповідати потребам мереж будь-якого розміру, а також можна налаштувати відповідно до конкретних потреб та вимог організації[9].

Щодо недоліків периметрового захисту, розглянемо основні з них:

1. Обмежена видимість;
2. Необхідність постійного оновлення;
3. Потенційні проблеми з продуктивністю.

Якщо підсумувати інформацію, то можна отримати наступні твердження:

- Периметровий захист не може бачити трафік, який вже знаходиться в мережі.
- Зловмисники постійно розробляють нові методи обходу периметрового захисту, тому його необхідно постійно оновлювати.
- Деякі рішення для периметрового захисту можуть впливати на продуктивність мережі.

1.3. Забезпечення захищеного обміну даними на базі VPN в корпоративних мережах.

VPN (Virtual Private Network – віртуальна приватна мережа) – це технологія, яка використовується для створення захищеного тунелю між двома точками в незахищеній мережі, наприклад Інтернеті. VPN шифрує весь трафік, що передається через цей тунель, захищаючи його від перехоплення та підслуховування. Дуже часто під поняттям VPN мають на увазі апаратний компонент периметра, що підтримує шифрування сеансів. Доступ до корпоративної мережі через VPN можуть використовувати всі співробітники, що не працюють в офісі безпосередньо, та при цьому, безпосереднє підключення до

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	17
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

внутрішньої мережі компанії VPN дозволяє віддаленим користувачам працювати в ній так, ніби вони знаходяться в офісі.

Загалом, VPN є незамінним інструментом для забезпечення безпеки корпоративних мереж у сучасному цифровому світі. Завдяки шифруванню, захисту віддаленого доступу та іншим функціям безпеки VPN допомагає захищати конфіденційні дані, запобігати кіберзагрозам та забезпечувати відповідність нормативним вимогам. VPN є клієнт-серверною технологією[10].

Віртуальні приватні мережі складаються з двох основних частин: зовнішньої мережі (через яку проходять дані, що були інкапсульовані та зашифровані) та внутрішньої мережі (підконтрольної). Кількість внутрішніх частин може бути більше однієї.

Підключення віддалених клієнтів до VPN мережі відбувається за допомогою сервера доступу, що підключений і до внутрішньої, і до зовнішньої мережі. При стандартних налагодженнях, після підключення віддаленого користувача чи після встановлення зв'язку з іншою захищеною мережею відбуваються процеси ідентифікації та аутентифікації. Після того, як два вищезгадані процеси пройшли успішно — сервер доступу ініціює процес авторизації, тобто віддалені користувач чи мережа отримують повноваження для роботи в захищеній мережі та можливість обміну інформацією в незахищених сегментах мережі[11].

Захист інформації в розумінні VPN включає в себе шифрування (encryption), підтвердження справжності (authentication) та контроль доступу (access control). Під кодуванням маємо на увазі шифрування переданої через VPN інформації. Читати всі отримані дані може лише володар ключа до шифру. Найбільш часто використовуваними в VPN-рішеннях алгоритмами кодування в наш час є DES, Triple DES і різні реалізації AES. Підтвердження справжності включає в себе перевірку цілісності даних та ідентифікацію осіб та об'єктів, задіяних у VPN. Перша гарантує, що дані дійшли до адресата саме в тому

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	18
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

вигляді, в якому були послані. Найпопулярніші алгоритми перевірки цілісності даних на сьогодні - MD5 і SHA1[7].

Розглянемо класифікацію VPN:

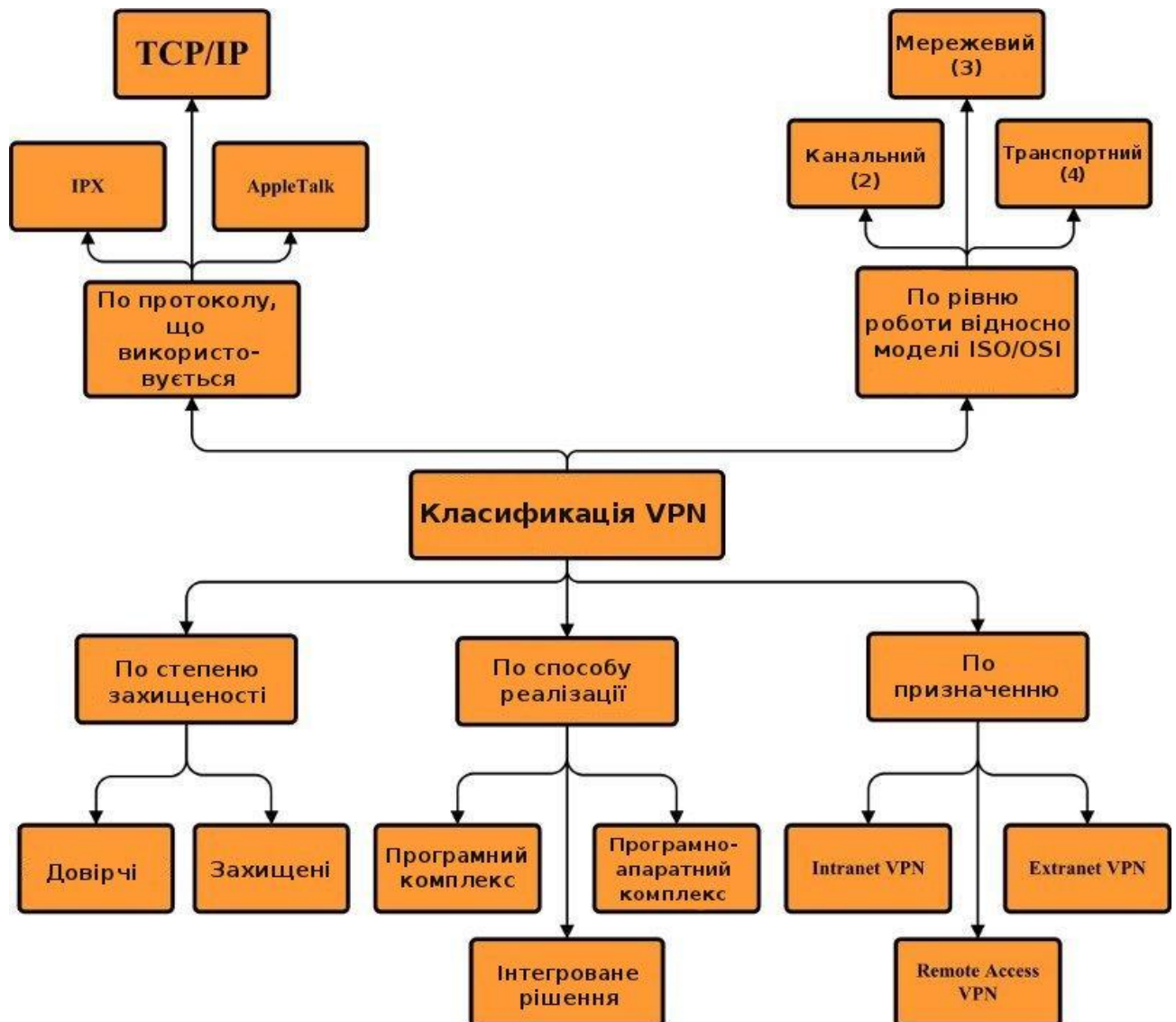


Рисунок 1.2 – Класифікація VPN.

За типом середовища, що використовується VPN класифікують як захищені або довірчі[13].

Захищені: Найбільш популярний варіант віртуальних приватних мереж. Він дає можливість створити захищену та надійну підмережу на базі ненадійної мережі (найчастіше захищена підмережа утворюється поверх небезпечної мережі Інтернет). Прикладами є такі захищені протоколи віртуальних мереж, як: SSL, PTP і IPSec. Прикладом використання протоколу IPSec є програмне забезпечення Surfshark VPN.

Довірчі: Їх використовують у випадках, коли є необхідність створення віртуальної підмережі в рамках більшої мережі без врахування захищеності даних. Прикладами подібних рішень є L2tp (Layer 2 Tunnelling Protocol) або Multi-protocol label switching (MPLS). Завдання забезпечення безпеки даними протоколами, зазвичай, покладаються на інші протоколи. Стандартним прикладом цього може послужити L2tp тунель, що використовується в парі з IPSec, поєднання цих протоколів дозволяє створити захищений тунель, який забезпечить інформаційний обмін у віртуальній приватній мережі.

При створенні віртуальних локальних мереж часто використовують під'єднання типу точка-точка до певних серверів, або встановлення тунелю Ethernet з певним сервером, при якому тунель має власну призначену підмережу. Сервери VPN в таких з'єднаннях виконують ролі маршрутизації та фільтрування трафіку для доступу до локальної мережі. З'єднання такого типу називають мостами.

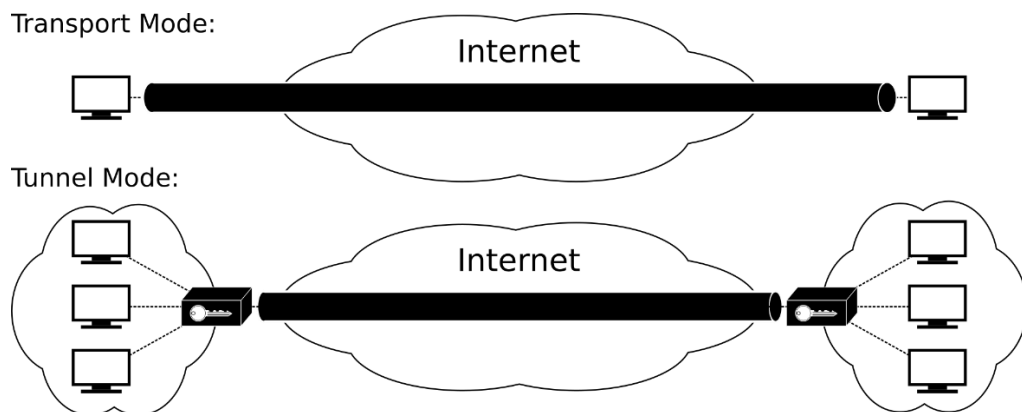


Рисунок 1.3 – Зображення VPN тунелю на різних рівнях моделі OSI.

Розглянемо типи VPN, які використовуються в корпоративних мережах:

1. VPN з віддаленим доступом (Remote Access VPN): Цей тип VPN використовується для підключення віддалених користувачів та філій до корпоративної мережі.
2. VPN типу сайт-сайт (Site-to-Site VPN): Цей тип VPN використовується для з'єднання двох або більше корпоративних мереж через Інтернет.
3. VPN через хмару (Cloud VPN): Цей тип VPN використовується для підключення до корпоративної мережі через хмарний сервіс.

При виборі VPN-рішення для корпоративної мережі слід врахувати такі фактори:

1. Рішення VPN повинно підтримувати необхідну кількість одночасних користувачів.
2. Рішення VPN повинно мати достатню пропускну здатність, щоб обробляти весь трафік, який буде передаватися через нього.
3. Рішення VPN повинно пропонувати такі функції безпеки, як шифрування, аутентифікація та авторизація.
4. Рішення VPN повинно бути простим у використанні для користувачів.
5. Рішення VPN повинно відповідати бюджету організації.

Протоколи VPN:

- IPSec (IP security) — стандартно використовується поверх IPv4.
- PPTP (Point-to-point tunneling protocol) — розроблявся спільними зусиллями декількох компаній, включаючи Microsoft.
- PPPoE або PPP (Point-to-Point Protocol over Ethernet)
- L2TP (англ. Layer 2 Tunnelling Protocol) — широко застосовується продуктами Microsoft і Cisco.
- L2TPv3 (англ. Layer 2 Tunnelling Protocol version 3).
- OpenVPN SSL.

Розглянемо також надійні VPN-рішення для корпоративних мереж:

1. Cisco AnyConnect: Це популярне VPN-рішення, яке пропонує широкий спектр функцій безпеки та можливостей управління.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	21
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

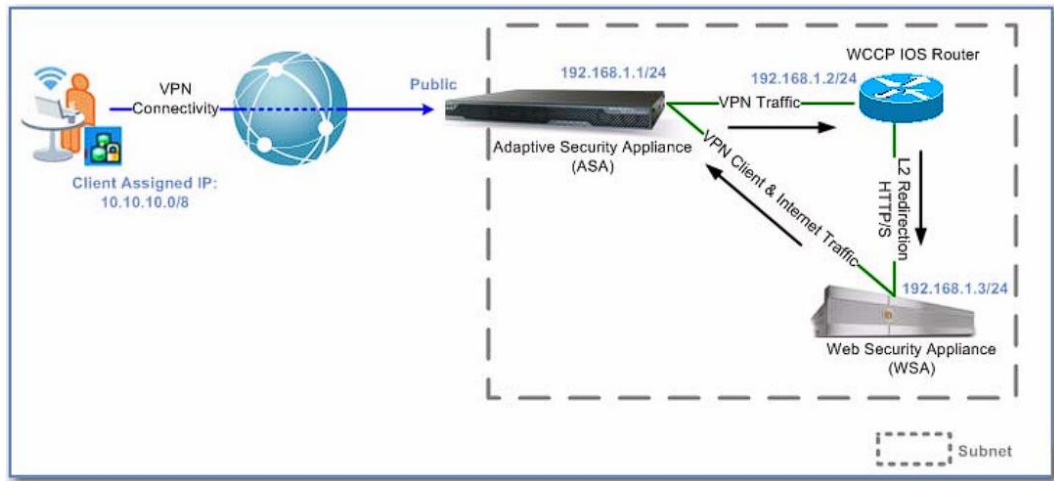


Рисунок 1.3 – Cisco AnyConnect.

2. Palo Alto Networks GlobalProtect: Це надійне VPN-рішення, яке відоме своїми високими показниками безпеки та зручністю використання.

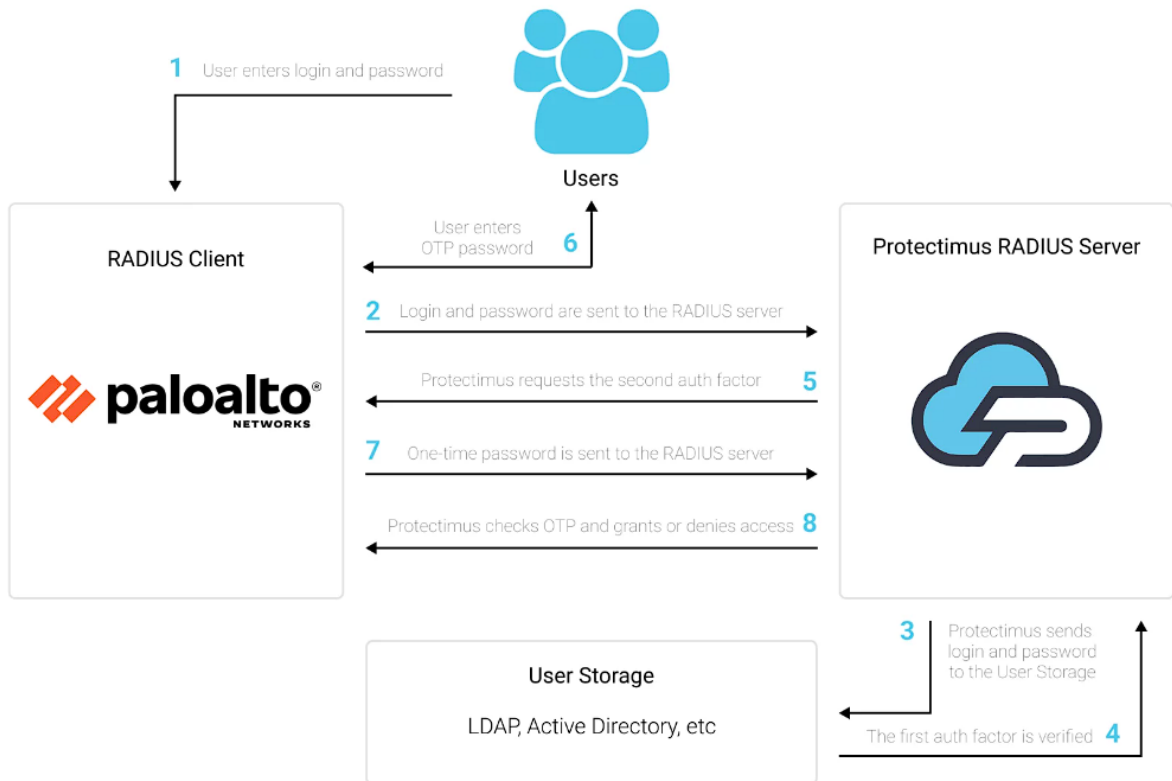


Рисунок 1.4 - Palo Alto Networks GlobalProtect.

3. Fortinet FortiGate SSL VPN: Це гнучке VPN-рішення, яке може бути налаштоване відповідно до потреб різних організацій.

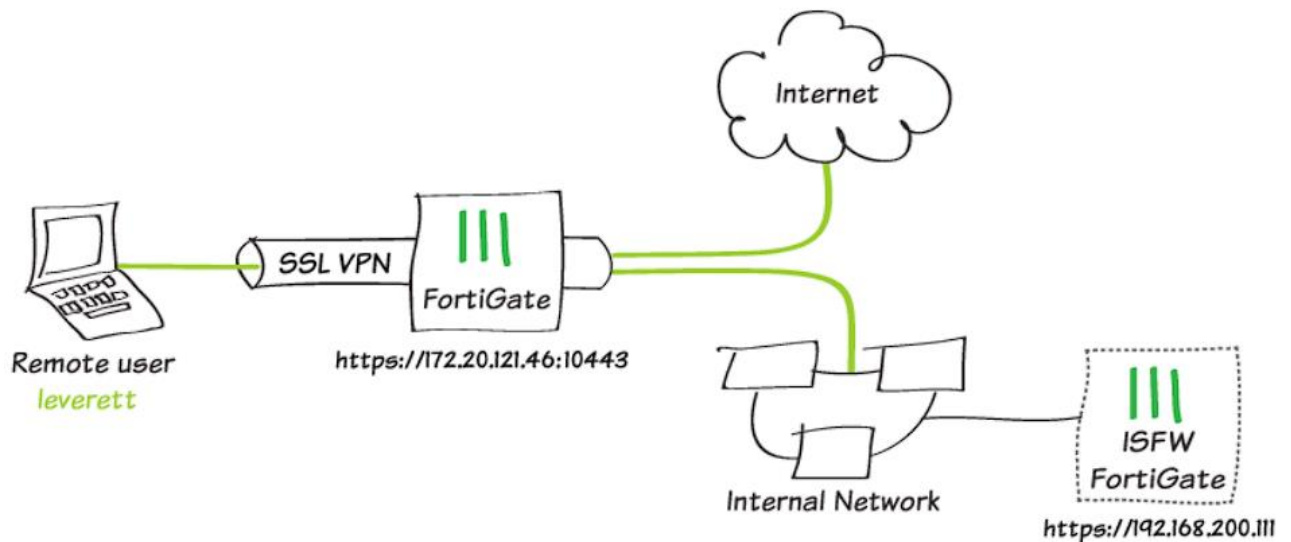


Рисунок 1.5 - Fortinet FortiGate SSL VPN.

4. SonicWall Mobile Connect: Це просте у використанні VPN-рішення, яке ідеально підходить для віддалених користувачів.

9:20



 CONNECTION

 MONITOR

 SETTINGS

 ABOUT

Status

Connected 00:32

Server

10.103.220.246

Client IP

192.168.200.100

Protocol

TLSv1.2

Cipher

ECDHE-RSA-AES128-GCM-SHA256

Statistics

Packets Sent

1.39 KB / 19 packets

Packets Received

0 bytes / 0 packets

Throughput

0 bytes/Sec

Max Throughput

287 bytes/Sec

Average Throughput

44 bytes/Sec

Рисунок 1.6 – Інформація про VPN з'єднання SonicWall Mobile Connect.

5. Zscaler Private Access: Це хмарне VPN-рішення, яке пропонує високу масштабованість та простоту розгортання.

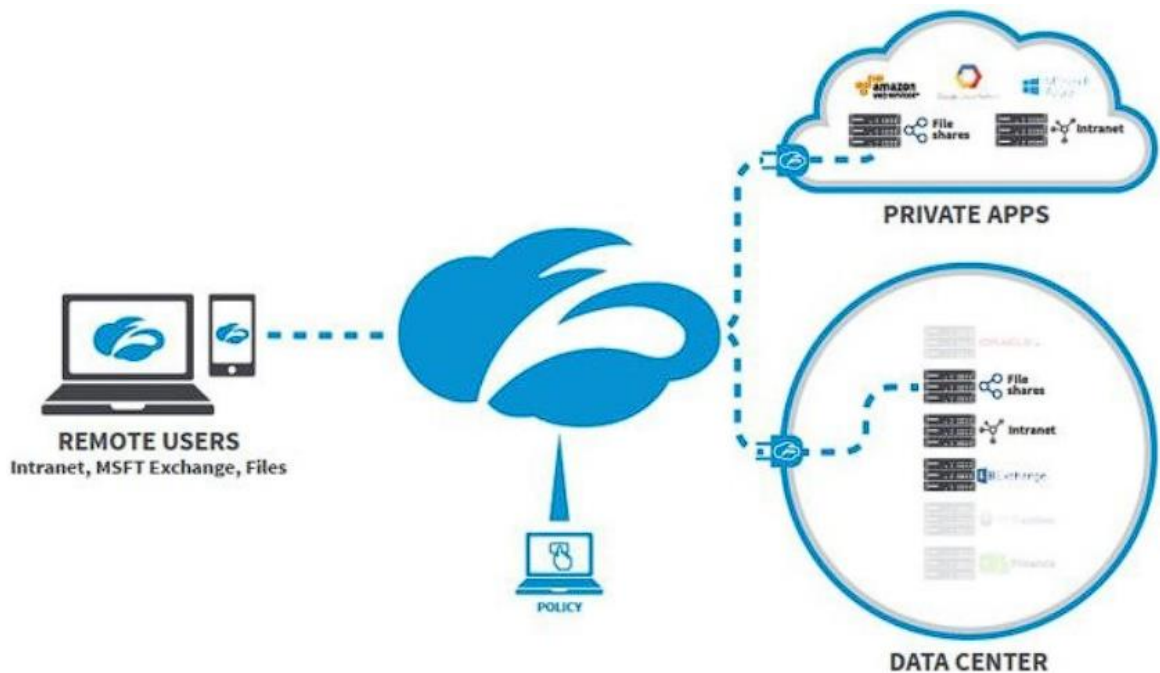


Рисунок 1.7 – Zscaler Private Access.

VPN є необхідним інструментом для забезпечення безпечного обміну даними в корпоративних мережах. Вибір правильного VPN-рішення може допомогти організаціям захистити свої конфіденційні дані, забезпечити безпечний доступ до корпоративних ресурсів та знизити ризики кібербезпеки[13].

Важливо пам'ятати, що VPN – це лише один із компонентів комплексної стратегії кібербезпеки. Організаціям також слід вживати інших заходів, таких як використання брандмауерів, антивірусного програмного забезпечення та систем виявлення вторгнень, щоб захистити свої мережі.

1.4. Аналіз комплексних рішень для побудови систем захисту корпоративних мереж

Щоденно збільшується кількість організацій, що надають партнерам віддалений доступ до своїх мереж, щоб зменшити витрати на обслуговування систем. Таким чином, захист кінцевої точки обміну трафіком є одним з найважливіших завдань забезпечення безпеки корпоративної мережі. У місцях, де корпоративна мережа підключається до мережі Інтернет, визначається периметр безпеки. У цих точках вхідний і вихідний трафік перетинаються. Для

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	24
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

корпоративних користувачів трафік виходить за межі мережі, а запити зовнішніх користувачів на доступ до веб-додатків та програм електронної пошти надходять у мережу компанії.

Кінцеві точки мають постійне підключення до Інтернету і часто є основною метою шкідливих атак, оскільки зовнішній трафік може проникати в корпоративну мережу. При створенні корпоративної мережі захисту даних брандмауер встановлюється по периметру мережі там, де є точки доступу в інтернет. Ці пристрої дозволяють запобігати і блокувати зовнішні загрози при виході з VPN-тунелю[3].

Основними компонентами комплексного рішення для захисту корпоративних мереж можна вважати:

1. Брандмауер: Брандмауер є програмним або апаратним засобом, який контролює та фільтрує трафік, що надходить до мережі та виходить з неї. Він може блокувати небажаний трафік, а також дозволяти легітимний трафік.
2. Система виявлення вторгнень (IDS): IDS - це програмне забезпечення, яке відстежує мережну активність на предмет підозрілих або шкідливих дій. IDS може попередити адміністраторів про потенційні кібератаки, щоб вони могли вжити заходів.
3. Система запобігання вторгненням (IPS): IPS - це програмне забезпечення, яке може не лише виявляти кібератаки, але й автоматично вживати заходів для їх блокування. IPS може блокувати шкідливий трафік, переривати з'єднання зловмисників та ізолювати заражені системи.
4. Антивірусне програмне забезпечення: Антивірусне програмне забезпечення може сканувати мережевий трафік, електронні листи та файли на предмет шкідливого програмного забезпечення. Воно може

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	25
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

блокувати або видаляти шкідливе програмне забезпечення, перш ніж воно завдасть шкоди системам.

5. Система запобігання втратам даних (DLP): DLP - це програмне забезпечення, яке використовується для запобігання несанкціонованому розголошенню конфіденційних даних. DLP може блокувати передачу даних на зовнішні пристрої, шифрувати дані та відстежувати доступ до даних.
6. Система захисту електронної пошти (Email Security): Система захисту електронної пошти може блокувати спам, фішинг-атаки та шкідливі вкладення. Вона також може шифрувати електронні листи та відстежувати їх доставку.
7. Система управління вразливістю (Vulnerability Management): Система управління вразливістю використовується для сканування систем та програмного забезпечення на предмет вразливостей. Вона може допомогти адміністраторам виявити та виправити вразливості, перш ніж вони будуть використані зловмисниками.
8. Система управління доступом та ідентифікацією (IAM): IAM - це система, яка використовується для управління доступом користувачів до ресурсів мережі. IAM може допомогти адміністраторам контролювати, хто має доступ до чого, а також відстежувати активність користувачів.

Ряд інтегрованих рішень для безпечних підключень від Cisco Systems забезпечує захищеність інформаційного трафіку. Мережа вивчає всі кінцеві точки та методи доступу всіх корпоративних мереж: локальної мережі, глобальної мережі та бездротових мобільних мереж. Функції брандмауера включають фільтрацію вхідного та вихідного трафіку, безпечний вихідний доступ для користувачів, безпечний доступ до Інтернету та доступ до демілітаризованої зони для користувачів.[8]

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	26
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Комплексні рішення корпоративної мережевої безпеки від Cisco Systems, Juniper Networks і Huawei Technologies пропонують безліч переваг, критично важливих для захисту корпоративних мереж:

- Скорочення ІТ-бюджетів на експлуатацію та обслуговування програмного та апаратного забезпечення;
- Підвищена гнучкість мережі;
- Зменшення розходів на впровадження;
- Знизити сукупну вартість володіння;
- Зміцнення управління за рахунок впровадження уніфікованих політик управління та безпеки;
- Збільшення прибутку і поліпшення показників діяльності компанії;
- Зниження загроз безпеці мережі та СГД;
- Використання ефективних політик і правила безпеки до кінцевих вузлів мережі: ПК, КПК і серверів;
- Зменшення часу, необхідного для впровадження нових рішень безпеки;
- Ефективне запобігання мережевих атак;
- Інтеграція з програмним забезпеченням інших розробників в області безпеки і адміністрування;
- Повномасштабний контроль доступу до мережі.

Продукти безпеки Cisco Systems на всіх рівнях мережі:

- Безпека кінцевих точок: додаток Cisco Security Agent захищає комп'ютери і сервери від атак черв'яків;
- Вбудований брандмауер: модуль Pix Security Appliance, сервісний модуль брандмауера Catalyst 6500 і ряд функцій брандмауера захищають мережу по периметру і навколо нього;
- Захист від мережевих атак: датчики серії IPS4200, IDs Catalyst6500 (IDSМ-2) або сервісний модуль IOS IPS ідентифікують, аналізують і блокують шкідливий і небажаний трафік;

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	27
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

- Виявлення та усунення DDoS-атак: Cisco Traffic Anomaly Detector XT і Guard XT забезпечують нормальну роботу в разі атаки, що перериває обслуговування. Модулі Cisco Traffic Anomaly Detector і Cisco Guard Service забезпечують надійний захист від DDoS-атак на комутатори Catalyst серії 6500 і маршрутизатори серії 7600;
- Безпека контенту: Модуль Content Engine маршрутизатора доступу захищає бізнес-додатки, що працюють в Інтернеті, і забезпечує безпомилкове поширення веб-контенту;
- Інтелектуальне управління мережею і служби безпеки: виявлення і блокування небажаного трафіку та додатків на маршрутизаторах і комутаторах Cisco.

Управління доступом до мережі (NAC — Network Admission Control) — це набір технологій і рішень, заснованих на галузевих ініціативах, реалізованих під егідою Cisco Systems. NAC використовує мережеву інфраструктуру для моніторингу всіх пристроїв, які намагаються отримати доступ до мережевих ресурсів[3]. Це зменшує шкоду мережі, завдану загрозами безпеці. Багатофункціональний пристрій безпеки надає співробітникам і діловим партнерам безпечний віддалений доступ до корпоративних VPN з використанням протоколів SSL і IPSec VPN для запобігання вторгнення IPS-вторгнень.

Мережа, що сама захищається (Self-Defending Network) — це майбутня стратегія розвитку Cisco. За допомогою цієї технології ви можете захистити свої бізнес-процеси, виявляючи та запобігаючи атакам, а також адаптуючись до внутрішніх та зовнішніх загроз вашої мережі в автоматичному режимі. Підприємства можуть більш ефективно використовувати інтелектуальні можливості мережевих ресурсів, оптимізувати бізнес-процеси і знизити витрати[12].

Cisco Security Management Suite — це набір продуктів і технологій, призначених для масштабованого управління і поліпшених політик безпеки для

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	28
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Self-DefendingNetwork від Cisco. За допомогою інтегрованих продуктів Cisco ви можете автоматизувати завдання управління безпекою, використовуючи ключові компоненти, такі як Менеджер управління і Cisco Security MARS, системи моніторингу, аналізу та реагування. Cisco Security Management Manager надає набір інструментів для налаштування брандмауерів, VPN та систем запобігання вторгненням (IPS) на пристроях безпеки, брандмауерах, маршрутизаторах та комутаторах Cisco.

Висновки до першого розділу.

В межах першого розділу кваліфікаційної роботи було розглянуто загальні підходи до побудови підсистем захисту корпоративних мереж, поняття периметрового захисту, як основи побудови ззахисту мереж корпорацій, поняття та основи роботи систем обміну даними на базі віртуальних приватних мереж, а також проаналізовано комплексні рішення, що застосовуються для побудови підсистем захисту корпоративних мереж.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	29
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ II. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ.

2.1. Проектування політик безпеки корпоративної мережі.

Політика інформаційної безпеки – це набір правил, рекомендацій, вимог та обмежень, які характеризують та регламентують порядок ІБ на підприємстві. Важливо зазначити, що політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головним завданням створення такого документу є визначення основних правил використання ресурсів підприємства, регламентування програмних засобів, що використовуються на підприємстві, сегментація доступу до ресурсів, порядок та правила протидії порушень.

Проводячи аналіз теми введення політики інформаційної безпеки підприємства можна сформулювати її основні завдання:

1. Захист інформаційних активів тобто забезпечення того, щоб доступ до інформації мали лише авторизовані особи, запобігання несанкціонованому змінненню або знищенню інформації, а також збезпечення того, щоб інформація була доступна авторизованим користувачам, коли їм це потрібно.
2. Забезпечення відповідності нормативним вимогам та виконання вимог законодавства та нормативних актів, що стосуються інформаційної безпеки і Впровадження стандартів та найкращих практик з інформаційної безпеки.
3. Управління інформаційними активами в наступних проявах:
 - Інвентаризація інформаційних активів підприємства.
 - Класифікація інформаційних активів за рівнем їх важливості.
 - Застосування відповідних заходів захисту до кожного класу інформаційних активів.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	30
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Надання користувачам лише тих дозволів, які їм дійсно необхідні для виконання їхніх завдань.
5. Використання механізмів аутентифікації та авторизації для контролю доступу до інформаційних ресурсів.
6. Регулярний перегляд та оновлення дозволів користувачів.
7. Захист інформаційних систем за допомогою використання брандмауерів, антивірусного програмного забезпечення та інших засобів захисту для захисту інформаційних систем від кіберзагроз, їх регулярне оновлення і створення резервних копій інформаційних систем.

Основною метою політики ІБ є захист інформації на підприємстві, що обробляється в автоматизованих системах, створення та підтримка у належному та дієздатному стані системи організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Захист корпоративної мережі від кіберзагроз є критично важливим завданням для будь-якої організації. У сучасному динамічному світі, де кіберзагрози постійно еволюціонують, стає все більш важливо мати надійну та гнучку систему кібербезпеки. Cisco ASA (Adaptive Security Appliance) - це потужний брандмауер, який може слугувати основою для ефективної системи кібербезпеки.

Adaptive Security Appliance пропонує широкий спектр функцій, що дозволяють захищати мережу від різних типів кіберзагроз. Для прикладу Cisco ASA використовує правила брандмауера та списки доступу (ACL) для контролю трафіку, що проходить через мережу, і запобігає несанкціонованому доступу до критичних ресурсів. Міжмережевий екран оснащений функціями IPS (Intrusion Prevention System), які дозволяють виявляти та блокувати зловмисне програмне забезпечення, що намагається проникнути в мережу. Cisco ASA може блокувати фішингові веб-сайти та інші шкідливі ресурси, захищаючи користувачів від

крадіжки даних та інших кіберзлочинів. Фаєрвол також може захищати мережу від DDoS-атак (Distributed Denial-of-Service), які можуть призвести до її відключення[18].

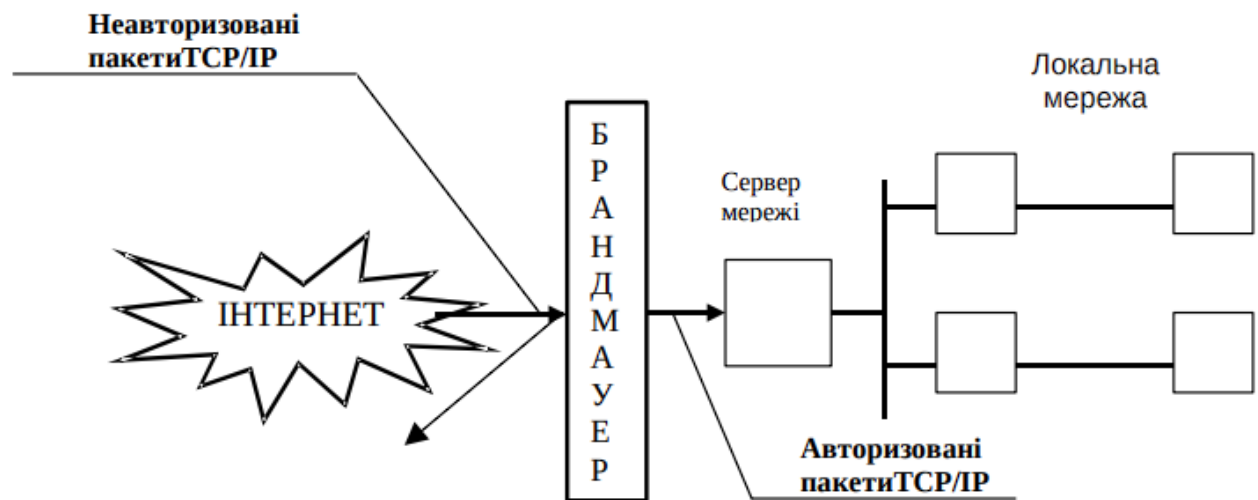


Рисунок 2.1 – Умовна схема розміщення та роботи брандмауера з пакетами TCP/IP.

В рамках забезпечення створення надійного та відмовостійкого периметрового захисту мережі Cisco ASA пропонує широкий спектр функцій, таких як правила брандмауера, ACL, VPN, IPS, QoS, URL-фільтрація та багато іншого, що дозволяє створити багаторівневий захист мережі.

Безпекове рішення Cisco ASA пропонується в різних моделях, що підходять для мереж різного розміру та складності. Брандмауер можна масштабувати для задоволення потреб організації, що робить його чудовим рішенням для мереж, що постійно розвиваються.

Важливо зазначити, що пристроєм можна легко керувати за допомогою ASDM (Adaptive Security Device Manager), який пропонує зручний графічний інтерфейс. Крім того, брандмауер підтримує керування через командний рядок для досвідчених адміністраторів. А також Cisco ASA може інтегруватися з іншими рішеннями безпеки Cisco, такими як Cisco ISE (Identity Services Engine) та Cisco NGFW (Next-Generation Firewall), що дозволяє створити єдину систему безпеки з централізованим управлінням[11].

Брандмауер з фільтрацією пакетів являє собою маршрутизатор чи працюючу на сервері програму, сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети. Брандмауер пропускає чи відкидає пакети відповідно до інформації, що міститься в IP-заголовках пакетів: адреси відправника, адреси одержувача, інформації про додаток чи протокол, номери порту джерела, номери порту одержувача.

Пакетна фільтрація – одне із найстаріших і найбільш розповсюджених засобів керування доступом до мережі. Ідея пакетної фільтрації – установити, чи дозволено даному пакету входити в мережу чи виходити з неї. Однак вона не вміє відрізняти один від одного різні типи трафіка. Оскільки пакетні фільтри не аналізують потоки трафіка так глибоко, як це роблять інші технології брандмауерів, вони працюють помітно швидше.

Брандмауер з фільтрацією пакетів перед відправленням пакета одержувачу порівнює його повну асоціацію з таблицею правил, у відповідності, з якою він повинний пропустити чи відкинути даний пакет. Брандмауер продовжує перевірку доти, поки не знайде правила, з яким погодиться повна асоціація пакета. Якщо брандмауер одержав пакет, який не відповідає жодному з табличних правил, він застосовує правило, задане за замовчуванням, яке також повинне бути чітко визначене в таблиці брандмауера. З розумінь безпеки це правило звичайно вказує на необхідність відкидання всіх пакетів, що не задовольняють жодному з інших правил.

Cisco ASA - це потужний брандмауер, який може слугувати основою для ефективної системи кібербезпеки корпоративної мережі. Ретельне проектування політик безпеки з урахуванням рекомендацій, наведених вище, дозволить організаціям захистити свої цінні активи від кіберзагроз та забезпечити їх безперебійну роботу.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	33
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2. Проектування загальної структури підсистеми захисту корпоративної мережі.

Першим етапом проектування є пошук найоптимальнішого варіанту побудови корпоративної мережі базуючись на потребах підприємства, можливостях сучасних технологій та перспективі їх розвитку і вдосконалення, фінансових можливостях клієнта.

Почнемо з вибору основної технології VLAN для корпоративних мереж. VLAN забезпечить чіткий розподіл корпоративної мережі на підмережі окремих підрозділів та забезпечить розподіленість даних та взаємодію між підрозділами, що у свою чергу забезпечить певну цілісність структури та захист.

Розглянемо організацію та використання віртуальних локальних мереж (VLAN) для захисту комп'ютерних мереж.

VLAN — це віртуальні локальні мережі, які можуть ізолювати мережу без необхідності фізичної логічної ізоляції. Віртуальні локальні мережі дуже гнучкі і можуть використовуватися для підвищення безпеки, відмовостійкості та продуктивності. VLAN містить ідентифікатор VLAN, який працює шляхом інкапсуляції кадру Ethernet у заголовок VLAN. Цей ідентифікатор використовується для визначення того, який пристрій належить до якої VLAN[15].

Віртуальні локальні мережі створюються шляхом додавання порту комутатора до певної віртуальної локальної мережі. Пристрої, що належать до однієї VLAN, можуть спілкуватися між собою без використання роутера. Це робить віртуальні локальні мережі дуже ефективними та простими в управлінні. Ви можете вважати віртуальні локальні мережі віртуальним комутатором, що розділяють пристрої.

Віртуальна локальна мережа (VLAN) — це логічна мережа, створена комутатором, де ви можете налаштувати кілька віртуальних локальних мереж на одному фізичному комутаторі з унікальними ідентифікаторами, які називаються ідентифікаторами віртуальних локальних мереж.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	34
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Коли пристрій надсилає дані в мережу, він містить поле, яке називається тегом, яке вказує VLAN, до якого були надіслані дані. Комутатор бачить цю мітку і передає дані на всі пристрої в цій віртуальній локальній мережі.

Однією з переваг використання VLAN є зменшення широкомовного трафіку в мережі. Розділяючи пристрої на різні віртуальні локальні мережі, ви можете контролювати широкомовний трафік, який отримує кожен пристрій, і підвищувати продуктивність мережі.

На основі інформації, що міститься в тезі VLAN, комутатор ідентифікує пакети, що надходять з різних пакетів VLAN: стандарт IEEE 802.1Q містить 4-байтову мітку VLAN, вставлену між MAC-адресою джерела/призначення та полем довжини /типу кадру Ethernet, щоб визначити VLAN, до якої належить кадр VLAN[15].

Звичайний кадр даних Ethernet

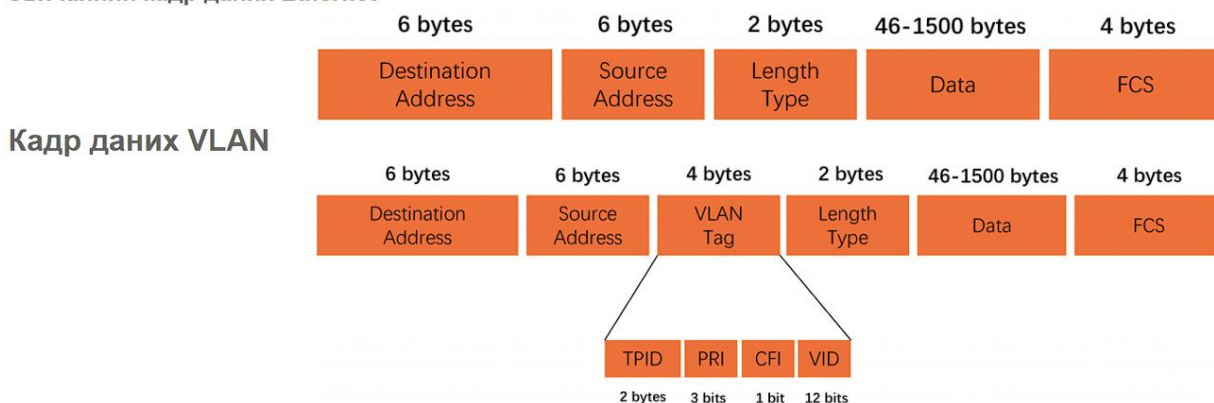


Рисунок 2.2 – Порівняння кадрів.

Транкінг VLAN — це процес надсилання трафіку з декількох Vlan по одному фізичному каналу. Це підвищує гнучкість і ефективність налаштування мережевих пристроїв. У більшості випадків кожній віртуальній локальній мережі присвоюється унікальний ідентифікатор (ID). Коли ви налаштовуєте агрегацію VLAN, використовуйте цей ідентифікатор для визначення трафіку, що надсилається завантаженням.

Є 2 основні переваги використання пулу VLAN. По—перше, ви можете підвищити продуктивність мережі, зменшивши перевантаження мережі. По—друге, ви можете забезпечити більш високий рівень безпеки, розділивши трафік

з різних віртуальних локальних мереж. Це запобігає несанкціонованому доступу до конфіденційних даних.

При налаштуванні каналу VLAN в режимі транкування необхідно враховувати кілька аспектів. По—перше, важливо переконатися, що порт комутатора налаштований правильно. Тоді ідентифікатор для кожної віртуальної локальної мережі повинен бути унікальним і не повинен повторно використовуватися іншими частинами мережі. Нарешті, важливо протестувати конфігурацію перед розгортанням у виробничому середовищі.

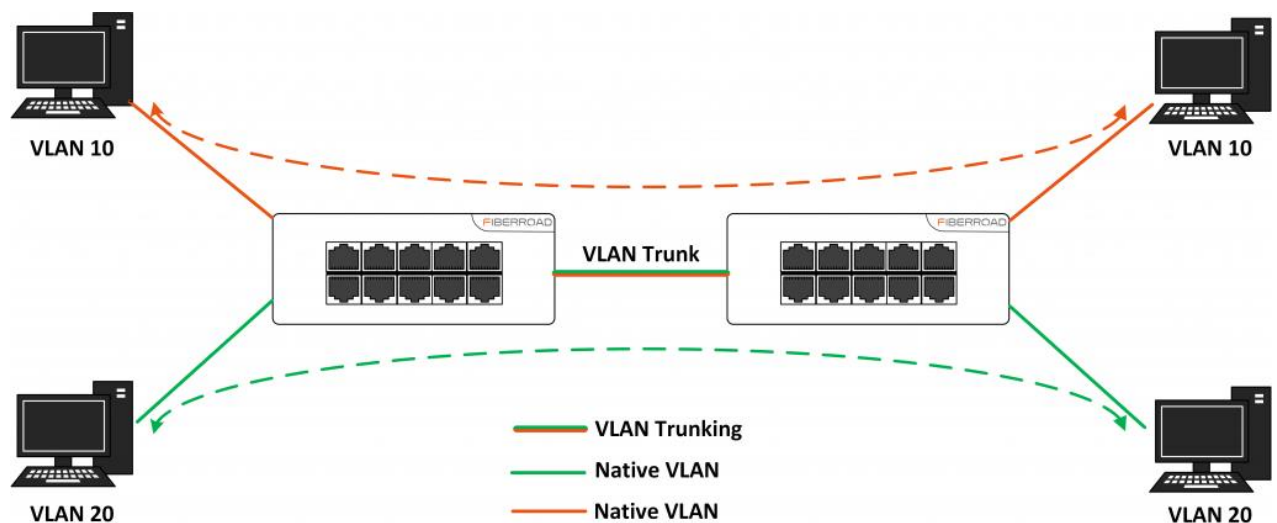


Рисунок 2.3 – Демонстрація транкування.

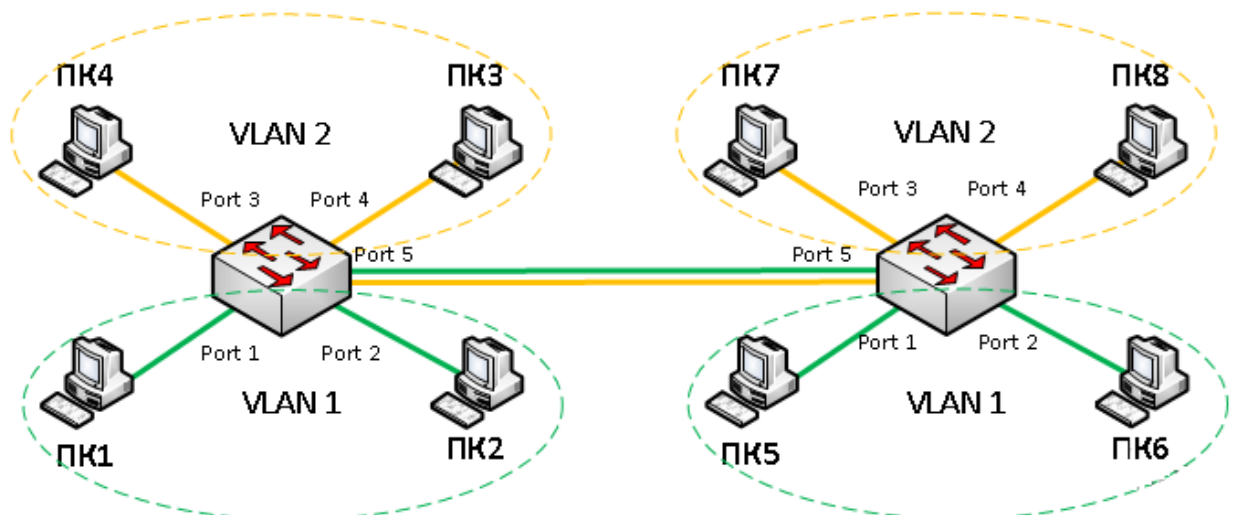


Рисунок 2.4 – Схематичне позначення роботи VLAN.

Переваги налаштування VLAN за допомогою пристроїв Cisco:

- Легше переміщати, додавати обладнання і змінювати з'єднання девайсів один з одним.

- Збільшуються можливості контролю завдяки наявності девайса, який маршрутизує віртуальні мережі на третьому рівні.
- При використанні декількох широкомовних доменів збільшується смуга пропускання.
- Зниження невиробничого застосування ЦП стає можливим, оскільки пересилання повідомлень широкомовного типу скорочується.
- Збільшення безпеки мережі: запобігає виникненню петель і широкомовних штормів.

Загалом, віртуальні локальні мережі є цінним інструментом для підвищення безпеки комп'ютерних мереж. Завдяки сегментації, контролю доступу та іншим функціям, віртуальні локальні мережі допомагають захистити мережі від несанкціонованого доступу, кібератак та інших загроз.

Важливо зазначити, що віртуальні локальні мережі не є панацеєю від усіх проблем мережевої безпеки. Їх слід використовувати разом з іншими заходами безпеки, такими як брандмауери, програмне забезпечення для кібербезпеки та відкриті політики безпеки.

Перейдемо до вибору способу об'єднання підмереж за допомогою маршрутизації. Одним із поширених протоколів динамічної є протокол OSPF. Технологія протоколу полягає у відстеженні стану каналу і пошуку найкоротшого шляху з використанням алгоритму Дейкстри[22].

Статус каналу цього протоколу означає опис інтерфейсу (наприклад, IP—адреса, маска, тип мережі тощо) і зв'язок з сусіднім маршрутизатором. На основі наведеного вище опису інтерфейсу створюється база даних стану каналу.

База даних отримує повідомлення про стан каналу («Link – State Advertisement – LSA»), які надсилаються або відразу після зміни топології мережі, або періодично зі змінами в маршрутизаторі. Ці повідомлення є невеликими пакетами. LSA містить інформацію про підключені інтерфейси, метрики та інші параметри[21].

На основі отриманих повідомлень LSA маршрутизатор використовує алгоритм SPF для створення дерева найкоротших маршрутів. Алгоритм виконує обчислення в базі даних топології мережі та видаляє непотрібні гілки (усі гілки є можливими шляхами). Отриманий маршрут заноситься в таблицю маршрутизації.

Протокол OSPF є внутрішнім протоколом маршрутизації і працює в рамках єдиної автономної системи. Його можна розділити на зони (області), які є логічними розділами автономних систем.

OSPF виконує наступні функції:

- формує стосунки з сусідами;
- розсилає LSA щоб сформувати бази даних на кожному маршрутизаторі;
- запускає SPF для обчислення найкращого маршруту до всіх одержувачів;
- заповнює таблиці маршрутизації найкращими маршрутами до кожного з отримувачів.

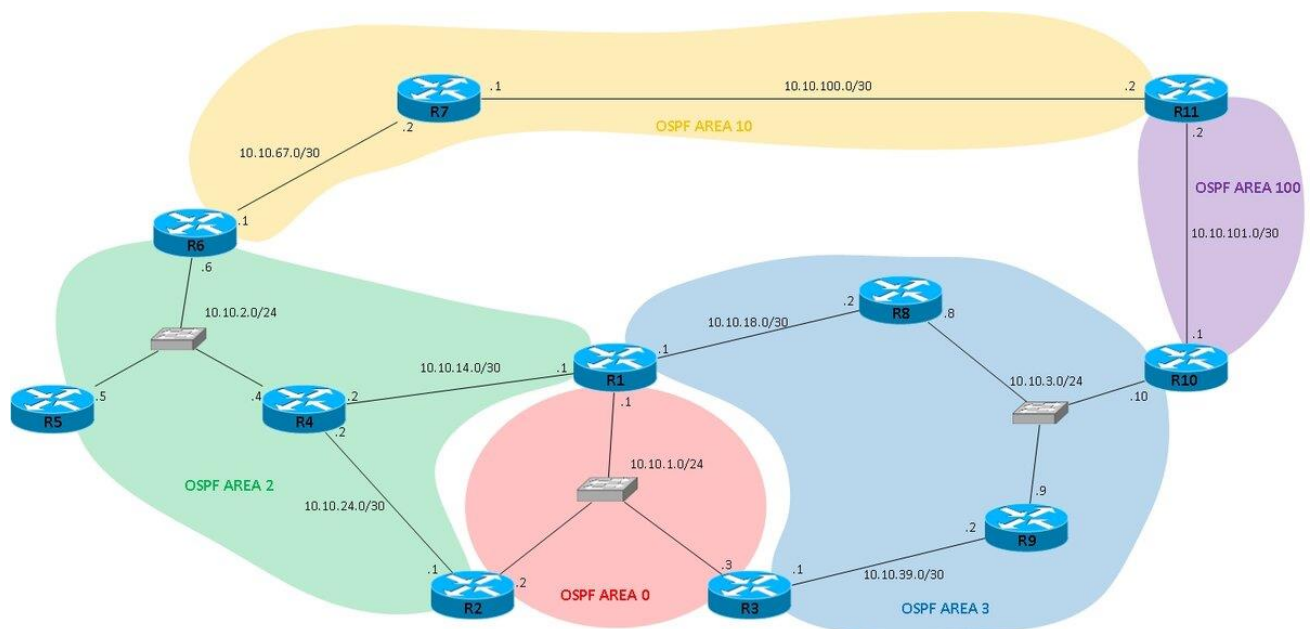


Рисунок 2.5 – Приклад топології OSPF.

Протокол OSPF встановлює відносини з сусідом наступним чином: 2 маршрутизатори, тобто сусідні маршрутизатори, що працюють за протоколом

OSPF, повинні «бачити» один одного в мережі, перш ніж вони зможуть обмінюватися інформацією. Цей процес виконується за допомогою протоколу Hello. Маршрутизатори, в яких реалізований протокол OSPF, надсилають «хелоу—пакети» з усіх інтерфейсів (широкомовна розсилка – 224.0.0.6). Пакет hello в сусідніх областях повинні бути ідентичними[20].

Таблиця 2.2

Порівняння протоколів маршрутизації.

Протокол маршрутизації	RIPv2	OSPF	EIGRP
Алгоритм	Вектор відстаней (Белмана—Форда)	Стан кластеру (Дейскстри)	Комбінований (DUAL)
Оновлення маршрутної інформації	Вся таблиця	Тільки зміни	Тільки зміни
Безкласовий	так	так	так
Максимальна кількість маршрутизаторів	15	—	255
Відкритий стандарт	так	так	ні
Метрика	Одна основна	Одна основна	Комбінована
Планування мережі	ні	Так (вибір зон)	ні
Балансування навантаження	на	Однакові метрики	ні
Складність конфігурації	■	■	■

Оскільки мережа, планується, як частина глобальної корпоративної мережі, в якій можливе використання пристроїв від різних виробників, було обрано протокол динамічної маршрутизації Open Shortest Path First, так як пропрієтарний протокол EIGRP підтримується лише пристроями Cisco. OSPF — це відкритий стандарт, що робить його доступним і недорогим, а отже зручним для створення ефективно працюючих комп'ютерних мереж. Якщо ви шукаєте

надійний, масштабований та гнучкий протокол маршрутизації, OSPF — це чудовий вибір.

2.3. Проектування основних елементів підсистеми захисту корпоративної мережі.

При створенні корпоративної мережі було використано трирівневу структуру. Трирівнева структура комп'ютерної мережі допомагає організувати мережу з урахуванням фізичної і логічної інфраструктури, забезпечити ефективну передачу даних, забезпечити безпеку та керування мережею. Кожен рівень виконує важливі функції для забезпечення надійної та ефективної роботи мережі в організації.

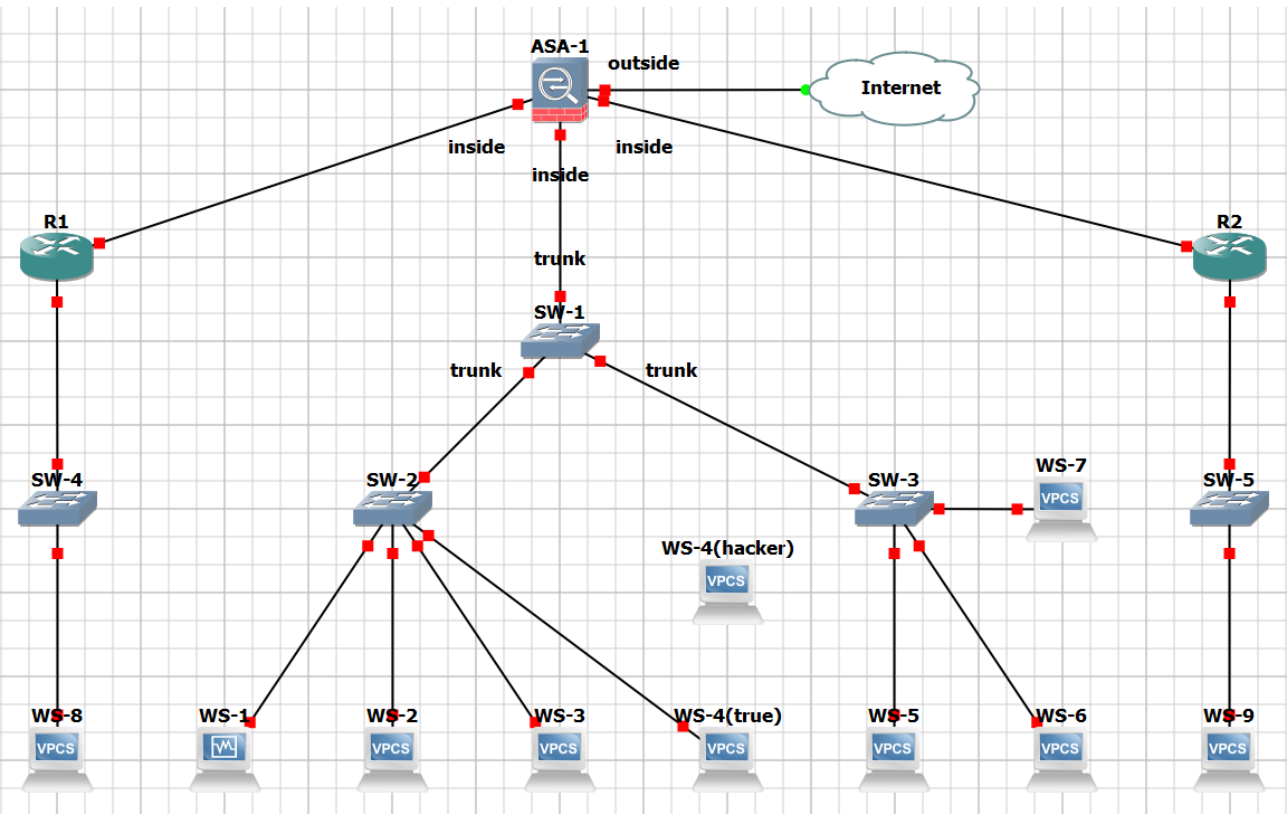


Рисунок 2.6 – Розроблена топологія мережі.

Загалом маємо Cisco ASA Firewall що виконує деякі функції рівня ядра, два маршрутизатори та комутатор на рівні доступу, які будуть налаштовані таким чином, щоб всі пристрої мережі могли обмінюватися різними пакетами даних, а також мати доступ до глобальної мережі інтернет через Cisco ASA Firewall, що

має правила роботи з пакетами, які надходять з зовнішньої мережі, також на рівні доступу ми маємо чотири комутатори та десять робочих станцій, які будуть налаштовані для ефективної роботи в спроектованій мережі.

Під час розробки ситеми захисту мережі було прийнято рішення створити кілька VLAN, які розподілені на комутаторах мережі.

Комутатор SW-2 налаштовано для одночасної роботи з трьома VLAN, отже кожна з підмереж відокремлена фізично від всіх інших, а пристрої в одній підмережі не можуть безпосередньо обмінюватися пакетами з пристроями з інших підмереж. Кожна VLAN має свою назву, це дозволяє спростити ідентифікацію різних підмереж.

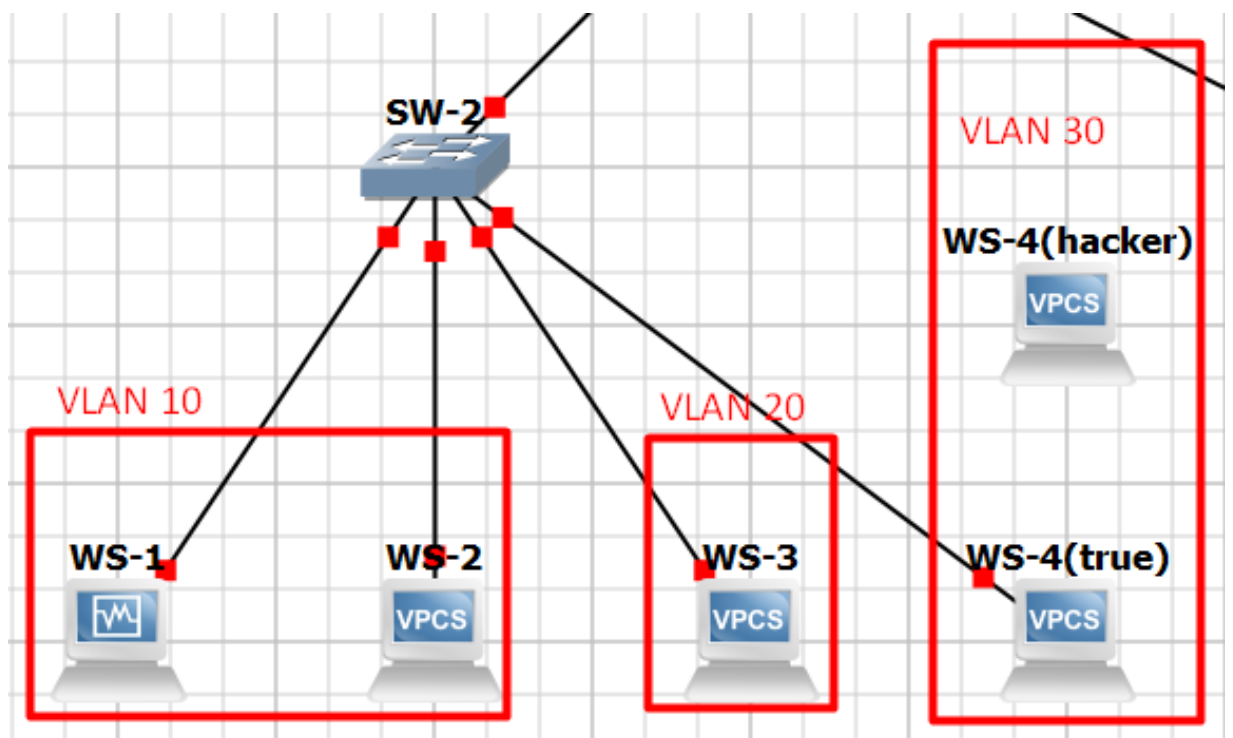


Рисунок 2.7 — Приклад трьох підмереж VLAN налаштованих на одному комутаторі.

Віртуальні локальні мережі можна використовувати для більш ефективного сегментування мереж, ізоляції логічних груп пристроїв і контролю доступу до ресурсів. Це позитивно впливає на безпеку і забезпечує гнучкість у конфігуруванні та управлінні комп'ютерними мережами.

Як згадувалося вище, пристрої, що належать до однієї VLAN, не можуть взаємодіяти з пристроями, що належать до іншої VLAN. Це призвело до використання протоколу маршрутизації OSPF для забезпечення зв'язку між різними підмережами. OSPF налаштовується на всіх маршрутизаторах в мережі, щоб забезпечити обмін інформацією між окремими сегментами мережі шляхом правильного налаштування OSPF, Зв'язок між різними VLAN і обмін інформацією через маршрутизатори в мережі; конфігурація OSPF дозволяє маршрутизаторам автоматично визначати найкоротший шлях між VLAN на основі різних показників, таких як пропускна здатність і вартість каналу.

Створюючи кілька VLAN і налаштовуючи OSPF, можна забезпечити надійний і ефективний зв'язок між усіма пристроями в мережі. Протокол маршрутизації OSPF автоматично перенастроюється при зміні топології мережі, завжди забезпечуючи найкращий шлях для пересилання пакетів між усіма пристроями в мережі. Такий розподіл трафіку підвищує продуктивність і безпеку створеної мережі.

В рамках дипломного проекту також було встановлено протокол захисту портів. Port Security - це функція канального рівня, яка створена для запобігання несанкціонованій зміні MAC—адреси мережевого підключення. Також ця функція захищає комутатор від атак, які можуть бути спрямовані на переповнення таблиці MAC—адрес. За допомогою Port Security можна обмежити (на канальному рівні) кількість під'єднань (MAC—адрес) на інтерфейсі, а також, за необхідності, ввести безпечні MAC—адреси вручну (статичні MAC-адреси). Залежно від MAC—адреси, кількості підключених пристроїв і типу пристрою, захист портів може бути налаштований на обмеження. Цей протокол можна налаштувати так, щоб запобігти несанкціонованому доступу і захистити мережу від шкідливих пристроїв, чи пристроїв якими заволоділи зловмисники.

Щоб ще більше посилити систему безпеки комп'ютерної мережі, налаштуємо списки контролю доступу між окремими сегментами мережі, та, найважливіше, на міжмережевому екрані. Кожен список містить свій набір правил, які

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	42
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

визначають, чи дозволений трафік, чи заблокований. Окремо буде налаштовано фільтрацію трафіку з певних веб-сайтів для демонстрації роботи списків контролю доступу міжмережевому екрані.

Правильно впроваджені та налаштовані списки контролю доступу в комп'ютерній мережі дозволяють контролювати трафік, що проходить через мережу, забезпечити додатковий захист і знизити ризик несанкціонованого доступу до мережевих ресурсів.

Ще одним кроком в налаштуванні безпеки комп'ютерної мережі є створення тунелю L2TP/IPSec між маршрутизаторами R—1 і R—2. Цей протокол можна використовувати для створення віртуальної приватної мережі між обраними кінцевими точками.

Налаштування L2TP/IPSec між маршрутизаторами R—1 і R—2 в мережі означає, що всі дані, що передаються, будуть зашифровані.

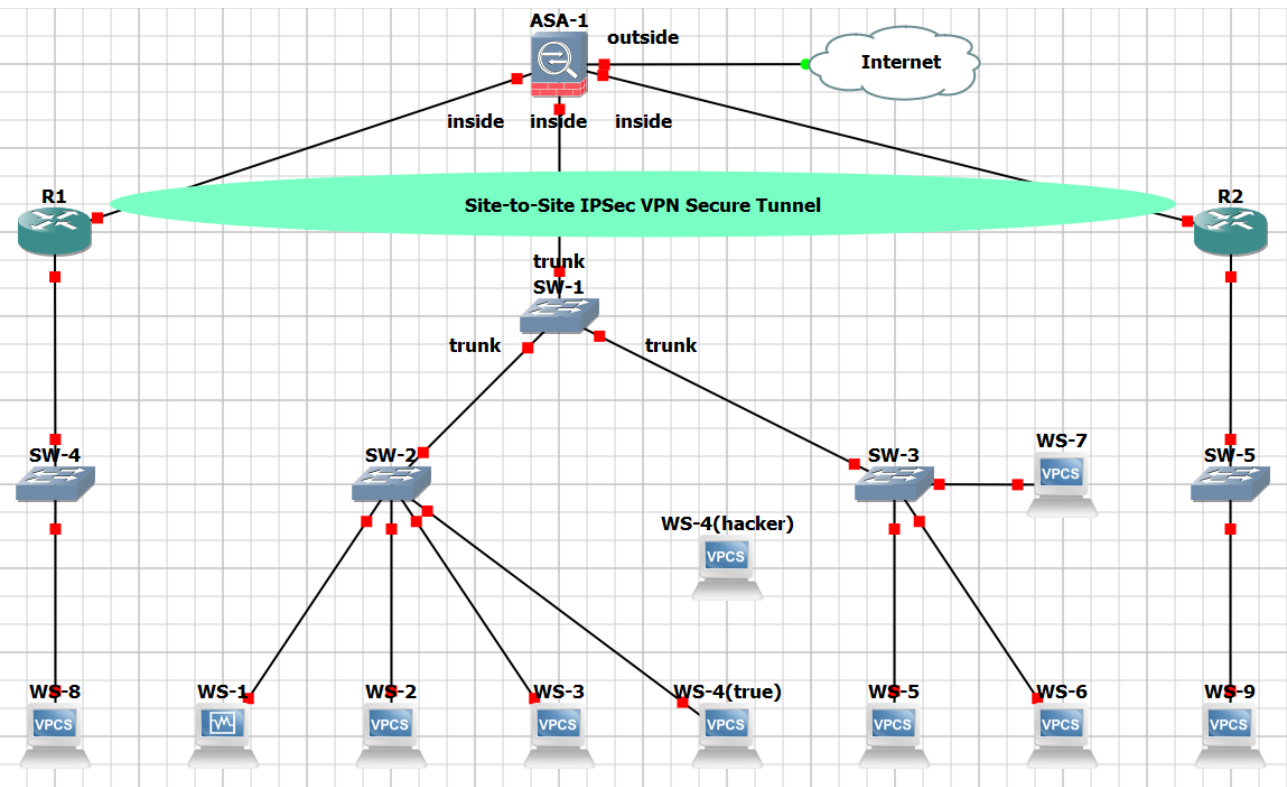


Рисунок 2.8 — L2TP/IPSec тунель.

Застосування L2TP/IPSecL2TP/IPSec в мережі дозволяє створити безпечне тунельоване з'єднання між обраними пристроями, яке забезпечить цілісність та захист даних, що передаються між ними. Це рішення дадуть змогу підтримувати

безпеку передачі даних між віддаленими сегментами мережі та запобігти перехопленню чи заміні даних під час їх передачі.

Останнім кроком в налаштуваннях мережі є налаштування логуювання на Syslog Server. Ведення логів на окремому сервері дасть нам чітке уявлення про те, що відбувається у мережі. Це може допомогти виявити та вирішити проблеми, а також відстежувати активність користувачів та мережевий трафік. Також запис логів Syslog може допомогти виявити підозрілу активність і кібератаки. Наприклад, можна відстежувати невдалі спроби входу в систему, несанкціонований доступ до файлів і шкідливий трафік. Також, за потреби, це може допомогти усунути несправності мережевого обладнання та програмного забезпечення. Аналізуючи логи, з'являється можливість визначити причину проблеми та вжити заходів для її вирішення.

Висновки до другого розділу.

В межах другого розділу кваліфікаційної роботи було розглянуто важливі питання, що стосуються проектування топології, передбачення потоків трафіку та побудови підсистеми захисту корпоративної мережі. Спроектовано політики безпеки корпоративної мережі, загальну структуру підсистеми захисту корпоративної мережі та основні елементи підсистеми захисту корпоративної мережі.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	44
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ ІІІ. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ.

3.1. Обґрунтування вибору обладнання та програмного забезпечення для побудови підсистеми захисту.

При створенні захищеної комп'ютерної мережі з використанням обладнання Cisco особливу увагу було приділено вибору обладнання, яке б відповідало потребам організації та її вимогам до продуктивності, надійності та безпеки мережі.

На вибір Cisco для реалізації мережевого проекту вплинуло кілька ключових факторів:

- Надійність: Компанія Cisco відома високою надійністю та стабільністю своїх продуктів. Вони проводять ретельне тестування та випробування, щоб забезпечити безперебійну роботу мережі.
- Масштабованість: Обладнання Cisco можна легко масштабувати від малих мереж до великих у міру зростання вашої організації. Це дозволяє мережі гнучко адаптуватися до мінливих вимог.
- Висока продуктивність: Cisco пропонує високопродуктивні комутатори та маршрутизатори, які забезпечують високошвидкісний мережевий зв'язок. Це особливо важливо для організацій, яким потрібні великі обсяги даних і висока пропускна здатність.
- Підтримка стандартів: Cisco активно підтримує та впроваджує мережеві галузеві стандарти, що забезпечує легку інтеграцію з іншими пристроями та послугами.
- Безпека: Cisco відома своїми рішеннями для забезпечення мережевої безпеки. Вона пропонує широкий спектр інструментів і технологій для захисту мереж від зовнішніх загроз і витоку даних.
- Інновації: Cisco активно інвестує в дослідження і розробку нових технологій в області мережевих рішень. Cisco намагається слідувати

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	45
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

ринковим тенденціям і впроваджувати нові можливості та функції у свої продукти.

- Екосистема та підтримка: Розгалужена екосистема партнерів та глобальна підтримка Cisco гарантує, що ви отримаєте необхідну допомогу та консультації під час побудови та експлуатації вашої мережі.

Враховуючи ці переваги, обладнання Cisco є найкращим вибором для побудови надійних, масштабованих і безпечних комп'ютерних мереж.

Для побудови захищеної комп'ютерної мережі були обрані маршрутизатори Cisco 7200 серії VXR. Це мережеве обладнання відрізняється своєю потужністю і надійністю та має розширені можливості для побудови складних мережевих інфраструктур. Основними причинами вибору цього маршрутизатора стали висока швидкість передачі даних, надійність, здатність ефективно обробляти великі обсяги трафіку та вимогливі додатки. Ці характеристики відповідали вимогам проекту, метою якого була побудова високопродуктивної та безпечної мережі.



Рисунок 3.1. – Маршрутизатор Cisco 7200 Series VRX.

Однією з найважливіших переваг маршрутизаторів Cisco 7200 серії VRX є їх висока масштабованість. Завдяки підтримці інтерфейсів з різною швидкістю вони можуть легко задовольнити зростаючі потреби мережі. Це забезпечує гнучкість підключення і високу пропускну здатність мережі. Крім того, маршрутизатори Cisco 7200 серії VRX мають розширені можливості

маршрутизації і підтримують різні протоколи маршрутизації, такі як OSPF, EIGRP і BGP. Це дозволяє створювати складні мережі з декількома маршрутизаторами і забезпечує найкращий маршрут для передачі даних в мережі. Таким чином, маршрутизатори Cisco 7200 серії VRX пропонують потужні функції масштабування та оптимізації мережі, які ідеально підходять для досягнення цілей, поставлених в курсовому проекті.

В процесі вибору обладнання для комутації мережевого трафіку в комп'ютерній мережі було обрано комутатор Cisco Catalyst WS—C2960—24TT—L. Даний комутатор забезпечує швидку та надійну комутацію даних, підтримує різні мережеві протоколи та функції безпеки. Він є ідеальним рішенням для побудови локальних мереж з високою продуктивністю і надійністю та сприяє ефективному обміну даними всередині мережі.



Рисунок 3.2. – Комутатор Cisco Catalyst WS—C2960—24TT—L.

Cisco Catalyst WS—C2960—24TT—L — це комутатор з 24 портами Fast Ethernet для підключення до 24 робочих станцій або інших мережевих пристроїв. Комутатор підтримує технологію Power over Ethernet (PoE), яка дозволяє підключеним пристроям, таким як IP—телефони і бездротові точки доступу, отримувати живлення через мережеві кабелі. Це спрощує розгортання мережі і забезпечує живлення широкого спектру пристроїв.

Крім того, комутатор Cisco Catalyst WS—C2960—24TT—L пропонує розширені функції управління і безпеки, які підтримують різні протоколи управління, такі як SNMP, SSH і Telnet, що дозволяє здійснювати віддалене управління і моніторинг комутатора. Він також підтримує стандартні функції безпеки, такі як списки доступу, ізоляція VLAN і безпечний доступ до управління для контролю мережевого трафіку і захисту мережі від несанкціонованого доступу.

Комутатор Cisco Catalyst WS—C2960—24TT—L також відомий своєю надійністю і високою продуктивністю. Він використовує оптимізовану апаратну платформу для обробки мережевого трафіку на високих швидкостях і мінімізації втрат пакетів даних. Крім того, комутатор підтримує резервні джерела живлення для забезпечення безперервної роботи мережі в разі збою в електропостачанні.

Cisco ASA 5500 — це серія апаратних міжмережевих екранів нового покоління (NGFW) від Cisco Systems, призначених для забезпечення комплексного захисту малих і середніх мереж, а також віддалених і філіальних офісів.



Рисунок 3.3 – Міжмережевий екран Cisco ASA 5500.

Ці брандмауери пропонують широкий спектр функцій безпеки, включаючи:

1. Фільтрація брандмауера: блокує небажаний трафік на основі визначених користувачем правил.
2. VPN: забезпечує безпечний віддалений доступ до корпоративної мережі.
3. Системи запобігання вторгненням (IPS): запобігають відомим і невідомим кібератакам.
4. Захист від шкідливих програм: захищає мережу від вірусів, троянів, шпигунських та інших шкідливих програм.
5. Контроль додатків: підвищує продуктивність і безпеку, обмежуючи доступ до веб—сайтів і додатків.
6. Фільтрація URL—адрес: блокує доступ до шкідливих або небажаних веб—сайтів.
7. Балансування навантаження: розподіляє трафік між декількома серверами для підвищення продуктивності та відмовостійкості.

Переваги Cisco ASA 5500:

- Комплексний захист: Надає широкий спектр функцій безпеки для захисту мережі від різноманітних загроз.
- Висока продуктивність: обробляє великі обсяги трафіку без втрати продуктивності.
- Масштабованість: Масштабується відповідно до потреб мережі будь-якого розміру.
- Простота в управлінні: легко налаштовується і управляється через веб—інтерфейс або командний рядок.
- Надійність: Забезпечує надійний захист мережі 24/7.

Ці фактори роблять Cisco ASA 5500 найкращим вибором для побудови мереж, які вимагають комплексної безпеки, високої продуктивності, масштабованості і простоти управління.

Windows 7 — операційна система Windows NT від компанії Microsoft для персональних комп'ютерів і ноутбуків, яка повністю вийшла 22 жовтня 2009 року, менше, ніж через три роки після випуску попередньої операційної системи, комерційно невдалої Windows Vista. Розробка Windows 7 під різними кодовими назвами велась з 2000 року. Над нею працювали 2500 осіб.

Станом на травень 2022 року, 12.62 % ПК з ОС Windows працюють під управлінням Windows 7, (і, таким чином 5,37 % усіх пристроїв на різних платформах), а в Україні — 25.06 %. Ця версія все ще залишається популярною в таких країнах, як Венесуела (50 %), Туркменістан (46 %), Китай (40 %), Сирія (40 %) й Індія (25.18 %).

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	49
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

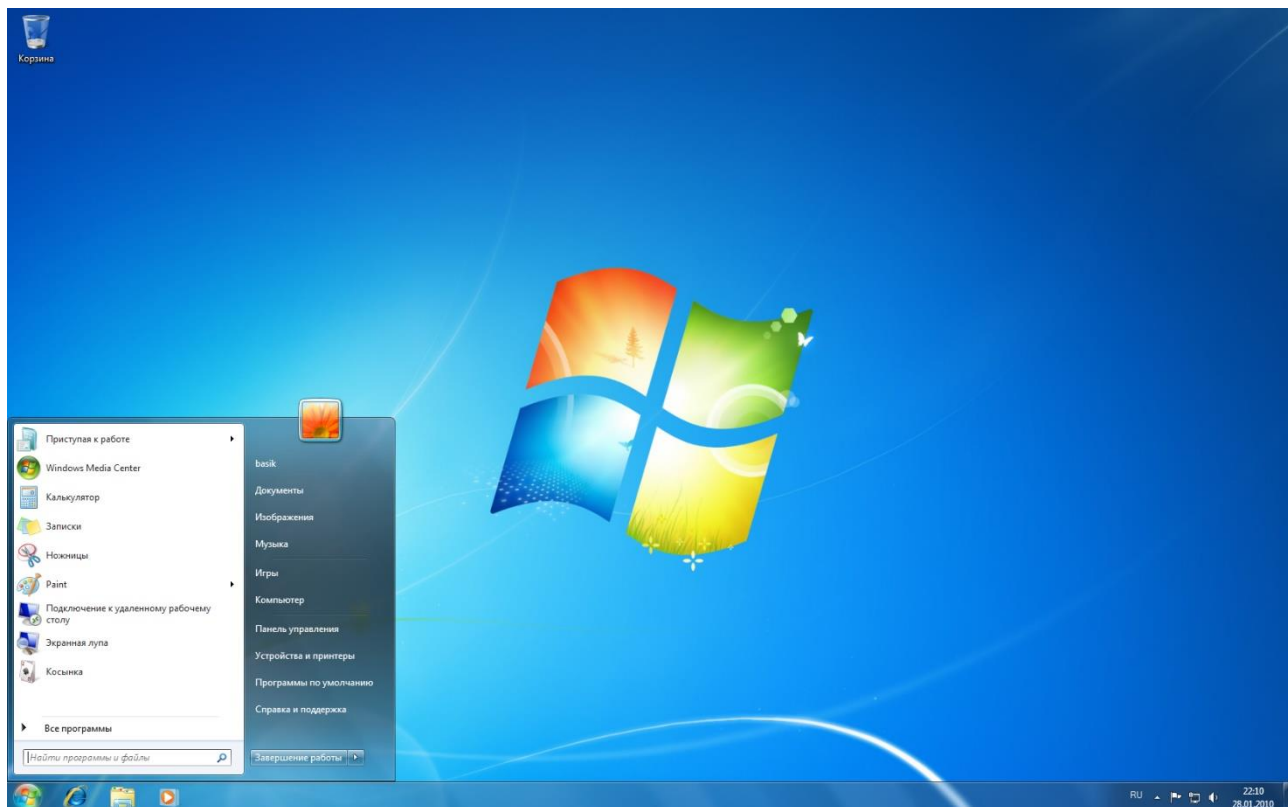


Рисунок 3.4 – Головне вікно та меню пуск операційної системи Windows 7.

Переваги Windows 7 для побудови локальних мереж:

- Простота налаштування та використання: Windows 7 має зручний інтерфейс користувача та інтуїтивно зрозумілі інструменти для налаштування локальних мереж. Це робить її чудовим вибором як для досвідчених користувачів, так і для початківців.
- Вбудована підтримка загального доступу до файлів і принтерів: Windows 7 має вбудовану підтримку загального доступу до файлів і принтерів, що робить їх легко доступними для інших комп'ютерів у мережі.
- Підтримка різних протоколів мережі: Windows 7 підтримує широкий спектр протоколів мережі, включаючи TCP/IP, NetBIOS та IPX/SPX. Це робить її сумісною з різними типами мережевих пристроїв.
- Надійність та безпека: Windows 7 - це надійна та безпечна операційна система, яка пропонує різні функції безпеки для захисту вашої локальної мережі від загроз.

- Широкий спектр програмного забезпечення: Для Windows 7 доступно безліч програмного забезпечення для локальних мереж, включаючи антивірусні програми, брандмауери та програмне забезпечення для спільного використання файлів.

Сервер Syslog - це цінний інструмент для будь-якої мережі, який може допомогти покращити безпеку, надійність та керованість. Рішення використання Syslog сервера у мережі має ряд переваг, які описані нижче.

Сервер Syslog може збирати журнали з різних пристроїв у вашій мережі, таких як маршрутизатори, комутатори, веб-сервери та навіть ваші власні комп'ютери. Це робить моніторинг та аналіз журналів набагато простішим, оскільки вам не потрібно переходити до кожного пристрою, щоб переглянути його журнали.

Записуючи всі події, що відбуваються у вашій мережі, сервер Syslog може допомогти вам виявити підозрілу активність, яка може свідчити про спробу злому. Це може допомогти вам вжити заходів для запобігання порушенням безпеки до того, як вони завдадуть шкоди.

Аналізуючи журнали, записані сервером Syslog, ви можете виявити потенційні проблеми, перш ніж вони призведуть до збоїв. Це може допомогти вам мінімізувати час простою та забезпечити безперебійну роботу вашої мережі.

Сервер Syslog можна легко масштабувати, щоб підтримувати зростаючу мережу. Ви можете просто додати більше пристроїв до мережі, і сервер Syslog автоматично почне збирати з них журнали. Також сервер Syslog можна налаштувати для запису журналів з різних пристроїв у різних форматах. Це дозволяє вам збирати саме ті журнали, які вам потрібні, у форматі, який вам зручний.

Syslog сервер можна інтегрувати з іншими системами моніторингу, такими як системи управління мережею (NMS) та системи виявлення вторгнень (IDS). Це дозволяє вам отримувати комплексне уявлення про стан вашої мережі.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	51
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Також варто гадати. Що багато серверів Syslog підтримують шифрування, що може допомогти захистити ваші журнали від несанкціонованого доступу.

Архівування та резервне копіювання: Журнали Syslog можна архівувати та резервувати, що може бути корисно для цілей аудиту та відновлення після збоїв.

Для додавання в побудовану мережу було обрано рішення від SOLARWINDS – Kiwi Syslog Server, як зручний, швидкий та невибагливий до ресурсів продукт.

!	Date	Time	Priority	Hostname	Message
!	09-06-2012	16:44:54	System4.Warning	10.100.1.192	Test user connected to website http://215.147.16.31/index.html
!	09-06-2012	16:44:53	Local5.Info	10.100.1.192	Test user connected to website http://195.127.200.148/index.html
!	09-06-2012	16:44:52	System5.Warning	10.100.1.192	Test user connected to website http://222.169.198.63/index.html
!	09-06-2012	16:44:51	Local5.Alert	10.100.1.192	Test user connected to website http://194.25.191.172/index.html
!	09-06-2012	16:44:50	UUCP.Alert	10.100.1.192	Test user connected to website http://220.245.188.16/index.html
!	09-06-2012	16:44:49	Auth.Critical	10.100.1.192	Test user connected to website http://220.234.172.242/index.html
!	09-06-2012	16:44:48	Local2.Warning	10.100.1.192	Test user connected to website http://203.44.165.1/index.html
!	09-06-2012	16:44:47	Auth.Error	10.100.1.192	Test user connected to website http://201.87.195.218/index.html
!	09-06-2012	16:44:45	Local5.Error	10.100.1.192	Test user connected to website http://200.119.197.212/index.html
!	09-06-2012	16:44:44	Local0.Notice	10.100.1.192	Test user connected to website http://204.135.209.16/index.html
!	09-06-2012	16:44:43	Kernel.Critical	10.100.1.192	Test user connected to website http://218.120.20.60/index.html
!	09-06-2012	16:44:42	Local3.Error	10.100.1.192	Test user connected to website http://204.138.2.38/index.html
!	09-06-2012	16:44:41	Syslog.Info	10.100.1.192	Test user connected to website http://210.112.153.158/index.html
!	09-06-2012	16:44:40	Local7.Debug	10.100.1.192	Test user connected to website http://204.160.214.145/index.html
!	09-06-2012	16:44:39	Mail.Error	10.100.1.192	Test user connected to website http://196.182.33.60/index.html
!	09-06-2012	16:44:38	UUCP.Alert	10.100.1.192	Test user connected to website http://209.214.132.220/index.html
!	09-06-2012	16:44:37	Local2.Warning	10.100.1.192	Test user connected to website http://218.112.12.113/index.html
!	09-06-2012	16:44:36	System5.Notice	10.100.1.192	Test user connected to website http://207.212.93.24/index.html
!	09-06-2012	16:44:35	UUCP.Critical	10.100.1.192	Test user connected to website http://212.127.130.92/index.html
!	09-06-2012	16:44:34	Local2.Alert	10.100.1.192	Test user connected to website http://222.245.162.138/index.html
!	09-06-2012	16:44:33	User.Notice	10.100.1.192	Test user connected to website http://214.185.211.162/index.html
!	09-06-2012	16:44:32	User.Critical	10.100.1.192	Test user connected to website http://213.153.135.176/index.html
!	09-06-2012	16:44:31	System0.Critical	10.100.1.192	Test user connected to website http://211.94.23.143/index.html
!	09-06-2012	16:44:30	Local3.Info	10.100.1.192	Test user connected to website http://208.183.114.103/index.html
!	09-06-2012	16:44:29	Kernel.Notice	10.100.1.192	Test user connected to website http://200.195.17.96/index.html

Рисунок 3.5 – Зажурнальована інформація на Kiwi Syslog Server.

Загалом, додавання сервера Syslog до вашої мережі - це розумне вкладення, яке може допомогти вам покращити безпеку, надійність та керованість.

Cisco Adaptive Security Device Manager (ASDM) - це веб-інтерфейс управління, який використовується для налаштування, моніторингу та усунення несправностей брандмауерів Cisco ASA та модулів служб брандмауера. ASDM пропонує простий у користуванні графічний інтерфейс, який полегшує адміністрування брандмауерів Cisco, не потребуючи знань про командний рядок.

ASDM дозволяє налаштовувати всі аспекти брандмауерів Cisco ASA, включаючи правила брандмауера, списки доступу (ACL), VPN, IPS, QoS та багато іншого. Також пропонує широкий спектр функцій моніторингу, які

дозволяють адміністраторам відстежувати стан брандмауерів Cisco ASA, трафік, що проходить через них, та події безпеки. Ще однією перевагою є те, що Cisco Adaptive Security Device Manager надає інструменти для усунення несправностей, які допомагають адміністраторам визначати та вирішувати проблеми з брандмауерами Cisco ASA. А також веб-інтерфейс дозволяє генерувати звіти про стан брандмауерів Cisco ASA, трафік та події безпеки.



Рис. 3.6 – Головний екран Cisco ASDM.

3.2. Налаштування підсистеми захисту корпоративної мережі.

В межах даного підрозділу буде покроково описано налаштування комп'ютерної мережі задля забезпечення вимог дипломного проекту, налаштування всіх необхідних технологій, а також буде представлено проміжні перевірки роботоздатності мережі та її вузлів чи сегментів.

Першим кроком є налаштування **outside** інтерфейсу Cisco ASA Firewall, який буде слугувати для доступу до мережі WAN.

```
ciscoasa(config)# int gig0/0
ciscoasa(config-if)# ip add 192.168.1.100 255.255.255.0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# no sh
```

Рисунок 3.7 – Налаштування **outside** інтерфейсу Cisco ASA Firewall.

Наступним кроком є налаштування статичного маршруту до мережі WAN.

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.1.1
ciscoasa(config)# exit
ciscoasa# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, U - UPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
C     192.168.1.0 255.255.255.0 is directly connected, outside
L     192.168.1.100 255.255.255.255 is directly connected, outside
C     192.168.10.0 255.255.255.0 is directly connected, inside_lan
L     192.168.10.1 255.255.255.255 is directly connected, inside_lan
C     192.168.20.0 255.255.255.0 is directly connected, inside_storage
L     192.168.20.1 255.255.255.255 is directly connected, inside_storage
C     192.168.30.0 255.255.255.0 is directly connected, inside_cctv
L     192.168.30.1 255.255.255.255 is directly connected, inside_cctv
```

Рисунок 3.8 – Налаштування статичного маршруту та перевірка успішності проведеного налаштування.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
```

Рисунок 3.9 – Налаштування політики для пропускання ісmp-пакетів.

Після конфігурації інтерфейсу для виходу в інтернет налаштуємо підінтерфейси для роботи з VLAN. Це необхідно для майбутньої реалізації Router-on-a-stick.

```
ciscoasa(config)# int gig0/1.10
ciscoasa(config-subif)# vlan 10
ciscoasa(config-subif)# nameif inside_lan
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip add 192.168.10.1 255.255.255.0
ciscoasa(config-subif)# no sh
ciscoasa(config-subif)# exit
```

Рисунок 3.10 – Налаштування підінтерфейсу для VLAN 10.

```
ciscoasa(config)# int gig0/1.20
ciscoasa(config-subif)# vlan 20
ciscoasa(config-subif)# nameif inside_storage
INFO: Security level for "inside_storage" set to 0 by default.
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip add 192.168.20.1 255.255.255.0
ciscoasa(config-subif)# no sh
ciscoasa(config-subif)# exit
```

Рисунок 3.11 – Налаштування підінтерфейсу для VLAN 20.

```
ciscoasa(config)# int gig0/1.30
ciscoasa(config-subif)# vlan 30
ciscoasa(config-subif)# nameif inside_cctv
INFO: Security level for "inside_cctv" set to 0 by default.
ciscoasa(config-subif)# security-level 100
ciscoasa(config-subif)# ip add 192.168.30.1 255.255.255.0
ciscoasa(config-subif)# no sh
ciscoasa(config-subif)# exit
```

Рисунок 3.12 – Налаштування підінтерфейсу для VLAN 30.

Далі проведемо ретельне налаштування DHCP сервера на базі Cisco ASA Firewall. Цей крок потребує особливої ретельності, оскільки важливо точно вказати всі IP-адреси з метою запобігання помилок в майбутньому.

```
ciscoasa(config)# dhcpd add 192.168.10.2-192.168.10.254 inside_lan
ciscoasa(config)# dhcpd dns 8.8.8.8
ciscoasa(config)# dhcpd enable inside_lan
ciscoasa(config)#
ciscoasa(config)# dhcpd add 192.168.20.2-192.168.20.254 inside_storage
ciscoasa(config)# dhcpd dns 8.8.8.8
ciscoasa(config)# dhcpd enable inside_storage
ciscoasa(config)#
ciscoasa(config)# dhcpd add 192.168.30.2-192.168.30.254 inside_cctv
ciscoasa(config)# dhcpd dns 8.8.8.8
ciscoasa(config)# dhcpd enable inside_cctv
```

Рисунок 3.13 – Налаштування DHCP сервера для трьох різних мереж на базі Cisco ASA Firewall.

Тепер можемо перейти до конфігурації VLAN на комутаторах мережі.

```
SW-1(config)#vlan 10
SW-1(config-vlan)#ex
SW-1(config)#vlan 20
SW-1(config-vlan)#ex
SW-1(config)#vlan 30
SW-1(config-vlan)#ex
```

Рисунок 3.14 – Створення VLAN на комутаторі SW-1.

Окремо виділимо створення віртуальної локальної мережі для портів комутатора, що не використовуються.

```
SW-1(config)#vlan 99
SW-1(config-vlan)#name unused
SW-1(config-vlan)#exit
```

Рисунок 3.15 – Створення VLAN unused на комутаторі SW-1.

Крайнім налаштуванням для комутатора SW-1 буде переведення його портів, що сполучають пристрої рівня доступу та DHCP-сервер в режим trunk.

```
SW-1(config-if-range)#switchport trunk encapsulation dot1q
SW-1(config-if-range)#switchport mode trunk
SW-1(config-if-range)#exit
```

Рисунок 3.16 - Переведення портів комутатора, що сполучають пристрої рівня доступу та DHCP-сервер в режим trunk.

Тепер налаштуємо порти комутатора SW-2. Порт, який підключено до SW-1 необхідно налаштувати в режимі trunk, порти, до яких підключені кінцеві пристрої в режим access, інші порти віднесемо до VLAN unused.

```
SW-2(config)#vlan 99
SW-2(config-vlan)#name unused
SW-2(config-vlan)#exit
SW-2(config)#int range eth1/1-3, eth2/0-3, eth3/003
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 99
SW-2(config-if-range)#sh
SW-2(config-if-range)#exit
```

Рисунок 3.17 – Створення VLAN unused та вимкнення портів, що не використовуються.

```

SW-2(config)#int eth0/0
SW-2(config-if)#switchport trunk encapsulation dot1q
SW-2(config-if)#switchport mode trunk
SW-2(config-if)#no sh
SW-2(config-if)#exit
SW-2(config)#int ra
SW-2(config)#int range e0/1-2
SW-2(config-if-range)#switchport mode access
SW-2(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-2(config-if-range)#exit
SW-2(config)#int eth0/3
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-2(config-if)#exit
SW-2(config)#int eth1/0
SW-2(config-if)#switchport mode access
SW-2(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW-2(config-if)#exit

```

Рисунок 3.18 – Налаштування інтерфейсів комутатора у відповідності до запланованого проекту мережі.

Аналогічні налаштування слід провести на SW-3.

```

SW-3(config-if)#switchport trunk encapsulation dot1q
SW-3(config-if)#switchport mode trunk
SW-3(config-if)#exit
SW-3(config)#int eth0/1
SW-3(config-if)#switchport mode access
SW-3(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SW-3(config-if)#int eth0/2
SW-3(config-if)#switchport mode access
SW-3(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-3(config-if)#int eth0/3
SW-3(config-if)#switchport mode access
SW-3(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW-3(config-if)#end

```

Рисунок 3.19 – Налаштування інтерфейсів комутатора у відповідності до запланованого проекту мережі.

```
SW-3(config)#vlan 99
SW-3(config-vlan)#name unused
SW-3(config-vlan)#exit
SW-3(config)#int range eth1/0-3, eth2/0-3, eth3/0-3
SW-3(config-if-range)#switchport mode access
SW-3(config-if-range)#switchport access vlan 99
SW-3(config-if-range)#sh
SW-3(config-if-range)#exit
```

Рисунок 3.20 – Створення VLAN unused та вимкнення портів, що не використовуються.

Тепер застосуємо команду, яка дозволить пристроям, що знаходяться в різних віртуальних локальних мереж, але в межах портів з однаковим рівнем захисту на фаєрволі, обмінюватися даними. Також перевіримо який рівень захищеності мають налаштовані нами інтерфейси.

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config)# sh nameif
```

Interface	Name	Security
GigabitEthernet0/0	outside	0
GigabitEthernet0/1.10	inside_lan	100
GigabitEthernet0/1.20	inside_storage	100
GigabitEthernet0/1.30	inside_cctv	100

Рисунок 3.21 – Налаштування Cisco ASA.

Почнемо налаштування IPSec тунелю між маршрутизаторами R-1 та R-2.

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
```

Рисунок 3.22 – Створення ISAKMP (IKE).

Наведені вище команди визначають наступне (у порядку списку):

- 3DES – метод шифрування, який буде використовуватися для Фази 1.

- MD5 — Алгоритм хешування
- Pre-share – використовуйте попередній спільний ключ як метод автентифікації
- Group 2 — група Діффі-Хеллмана, яка буде використана
- 86400 – Час життя ключа сеансу. Виражається в кілобайтах (після х-кількості трафіку, змініть ключ) або секундах. Набір значень є значенням за умовчанням.

Слід зазначити, що політика ISAKMP Phase 1 визначається глобально. Це означає, що якщо у нас є п'ять різних віддалених сайтів і налаштовано п'ять різних політик ISAKMP Phase 1 (по одній для кожного віддаленого маршрутизатора), коли наш маршрутизатор намагається узгодити VPN-тунель з кожним сайтом, він надішле всі п'ять політик і використає перший збіг, який приймається обома сторонами.

Далі ми збираємося визначити попередній спільний ключ для автентифікації з нашим партнером (маршрутизатором R2) за допомогою такої команди:

```
R1(config)#crypto isakmp key firewallcx address 10.10.10.5
R1(config)#exit
```

Рисунок 3.23 – Конфігурування ключа.

Попередній спільний ключ однорангового вузла встановлено на firewallcx, а його публічна IP-адреса – 10.10.10.5. Кожного разу, коли R1 намагається встановити VPN-тунель за допомогою R2, використовуватиметься цей попередньо спільний ключ.

Наступним кроком є створення списку доступу та визначення трафіку, який ми хочемо, щоб маршрутизатор пропускав через тунель VPN. У цьому прикладі це буде трафік від однієї мережі до іншої, 192.168.40.0/24 до 192.168.50.0/24. Списки доступу, які визначають трафік VPN, іноді називають криптографічним списком доступу або списком доступу цікавого трафіку.

```
R1(config)#ip access-list extended VPN-TRAFFIC
R1(config-ext-nacl)#permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
R1(config-ext-nacl)#exit
```

Рисунок 3.24 – Налаштування списку доступу.

Наступним кроком є створення набору трансформацій для захисту наших даних. Ми назвали цей TS:

```
R1(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#exit
```

Рисунок 3.25 – Створення набору трансформацій.

Наведена вище команда визначає наступне:

- ESP-3DES - Метод шифрування.
- MD5 - Алгоритм хешування.

Crypto map є останнім кроком нашого налаштування та об'єднує раніше визначені конфігурації ISAKMP та IPSec разом:

```
R1(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.10.10.5
R1(config-crypto-map)#set transform-set TS
R1(config-crypto-map)#match address VPN-TRAFFIC
R1(config-crypto-map)#exit
```

Рисунок 3.26 – Створення криптомапи.

Ми назвали нашу криптомапу CMAP. Тег ipsec-isakmp повідомляє маршрутизатору, що ця крипто-карта є крипто-картою IPsec. Незважаючи на те, що в цій криптомапі оголошено лише один одноранговий вузол, у певній криптомапі можна мати кілька однорангових вузлів.

Останнім кроком є застосування криптомапи до вихідного інтерфейсу маршрутизатора.

```
R1(config)#int fa0/0
R1(config-if)#crypto map CMAP
R1(config-if)#
*Mar 1 00:13:02.531: %CRYPTO-6-ISAAMP ON OFF: ISAAMP is ON
```

Рисунок 3.27 – Застосування криптомапи до інтерфейсу.

Тепер ми переходимо до налаштування IPSec VPN на маршрутизаторі, який буде знаходитися на іншому боці сконфігурованого тунелю. Налаштування є аналогічними, з відмінністю у вказаних IP-адресах.

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr 3des
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key firewallcx address 10.10.10.1
R2(config)#ip access-list extended VPN-TRAFFIC
R2(config-ext-nacl)#permit ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
R2(config-ext-nacl)#exit
R2(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
R2(cfg-crypto-trans)#exit
R2(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 10.10.10.1
R2(config-crypto-map)#set transform-set TS
R2(config-crypto-map)#match address VPN-TRAFFIC
R2(config-crypto-map)#exit
R2(config)#int fa0/0
R2(config-if)#crypto map CMAP
```

Рисунок 3.28 – Налаштування IPSec VPN на маршрутизаторі R-2.

Перетворення мережевих адрес (NAT) буде налаштовано для надання доступу до Інтернету внутрішнім хостам. Під час налаштування VPN-тунелю Site-to-Site обов'язково слід вказати маршрутизатору не виконувати NAT (заборонити NAT) для пакетів, призначених до віддалених мереж VPN.

Це легко зробити, вставивши оператор deny на початку списків доступу NAT , як показано нижче:

```
R1(config)#ip nat inside source list 100 interface fastethernet0/0 overload
R1(config)#access-list 100 remark --[Define NAT Service]--
R1(config)#
*Mar  1 00:17:47.567: %LINEPROTO-5-UPDOWN: Line protocol on Interface NV10, changed state t
o up
R1(config)#$ 100 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
R1(config)#access-list 100 permit ip 192.168.40.0 0.0.0.255 any
R1(config)#access-list 100 remark
R1(config)#exit
```

Рисунок 3.29 – Перетворення NAT на маршрутизаторі R-1.

Аналогічне налаштування слід провести і на R-2:

```
R2(config)#ip nat inside source list 100 interface fastethernet0/0 overload
R2(config)#
*Mar  1 00:19:35.279: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state t
o up
R2(config)#access-list 100 remark ==[Define NAT Service]==
R2(config)#$ 100 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
R2(config)#access-list 100 permit ip 192.168.50.0 0.0.0.255 any
R2(config)#access-list 100 remark
```

Рисунок 3.30 – Перетворення NAT на маршрутизаторі R-2.

На цьому етапі ми завершили нашу конфігурацію, і VPN-тунель готовий до запуску. Щоб ініціювати VPN-тунель, нам потрібно змусити один пакет пройти через VPN, і цього можна досягти за допомогою ping від одного маршрутизатора до іншого:

```
R1#ping 192.168.50.1 source fa0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.40.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/116/144 ms
```

Рисунок 3.31 – Надсилання пакету, що ініціює VPN-тунель.

Щоб перевірити тунель VPN, скористайтеся командою show crypto session:

```
R1#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.5 port 500
  IKE SA: local 10.10.10.1/500 remote 10.10.10.5/500 Active
  IPSEC FLOW: permit ip 192.168.40.0/255.255.255.0 192.168.50.0/255.255.255.0
    Active SAs: 2, origin: crypto map
```

Рисунок 3.32 – Виконання діагностичної команди.

Як наступний крок налаштування мережі було прийнято рішення налаштувати логування маршрутизаторів на Syslog-сервері, для цього виконано наступну команду:

```
R1(config)#logging 192.168.10.2
R1(config)#exit
R1#
*Mar  1 00:03:28.635: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Mar  1 00:03:29.635: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 started -
CLI initiated
```

Рисунок 3.33 – Налаштування журналювання на Syslog-сервер (маршрутизатор R-1).

```

R2(config)#logging 192.168.10.2
R2(config)#
R2#
*Mar  1 00:05:20.739: %SYS-5-CONFIG_I: Configured from console by console
R2#
*Mar  1 00:05:21.739: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 started -
CLI initiated

```

Рисунок 3.34 – Налаштування журналювання на Syslog-сервер (маршрутизатор R-2).

Останнім кроком в налаштуванні мережі буде конфігурація port-security на портах комутаторів:

```

SW-2(config)#int range eth0/1-3, eth1/0
SW-2(config-if-range)#switchport port-security
SW-2(config-if-range)#switchport port-security violation shutdown
SW-2(config-if-range)#switchport port-security maximum 1
SW-2(config-if-range)#switchport port-security mac-address sticky
SW-2(config-if-range)#switchport port-security aging type inactivity
SW-2(config-if-range)#switchport port-security aging time 100
SW-2(config-if-range)#exit
SW-2(config)#errdisable recovery cause psecure-violation
SW-2(config)#errdisable recovery interval 60
SW-2(config)#exit

```

Рисунок 3.35 – Налаштування port-security на комутаторі SW-2.

```

SW-3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-3(config)#int range eth0/1-3
SW-3(config-if-range)#switchport port-security
SW-3(config-if-range)#switchport port-security violation shutdown
SW-3(config-if-range)#switchport port-security maximum 1
SW-3(config-if-range)#switchport port-security mac-address sticky
SW-3(config-if-range)#switchport port-security aging type inactivity
SW-3(config-if-range)##switchport port-security aging time 100
SW-3(config-if-range)##exit
SW-3(config-if-range)#switchport port-security aging time 100
SW-3(config-if-range)#exit
SW-3(config)#errdisable recovery cause psecure-violation
SW-3(config)#errdisable recovery interval 60
SW-3(config)#exit

```

Рисунок 3.36 – Налаштування port-security на комутаторі SW-3.

На даному етапі ми закінчили налаштування нашої мережі, тепер перейдемо до перевірки проведених налаштувань шляхом виконання діагностичних команд та аналізу виведених відомостей.

3.3. Тестування функціоналу підсистеми захисту.

Почнемо перевірку з виконання діагностичних команд, що стосуються маршрутизації в створеній мережі:

```
R1#show ip ospf
Routing Process "ospf 14" with ID 1.1.1.2
Start time: 00:00:08.696, Time elapsed: 00:04:20.684
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 00:03:29.356 ago
    SPF algorithm executed 3 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x013172
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

Рисунок 3.36 – Виконання діагностичної команди *show ip ospf* на R-1.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	64
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R2#show ip ospf
Routing Process "ospf 14" with ID 1.1.1.3
Start time: 00:00:07.644, Time elapsed: 00:04:46.504
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1.1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 00:03:55.280 ago
    SPF algorithm executed 3 times
    Area ranges are
      Number of LSA 5. Checksum Sum 0x013172
      Number of opaque link LSA 0. Checksum Sum 0x000000
      Number of DCbitless LSA 0
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0

```

Рисунок 3.38 – Виконання діагностичної команди *show ip ospf* на R-2.

```

ciscoasa# show route ospf

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

O        192.168.40.0 255.255.255.0
          [110/20] via 10.10.10.1, 00:06:28, inside_lanA
O        192.168.50.0 255.255.255.0
          [110/20] via 10.10.10.5, 00:06:28, inside_lanB

```

Рисунок 3.39 – Виконання діагностичної команди *show route ospf* на ASA-1.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	65
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Routing Process "ospf 14" with ID 1.1.1.1
Start time: 00:00:09.980, Time elapsed: 00:07:28.280
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
  Area BACKBONE(0)
    Number of interfaces in this area is 6
    Area has no authentication
    SPF algorithm last executed 00:07:26.770 ago
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x13172
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

Рисунок 3.40 – Виконання діагностичної команди *show route ospf* на ASA-1.

```

ciscoasa# show ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.3	1	FULL/DR	0:00:37	10.10.10.5	inside_lanB
1.1.1.2	1	FULL/DR	0:00:37	10.10.10.1	inside_lanA

Рисунок 3.41 – Виконання діагностичної команди *show ospf neighbor* на ASA-1.

Також виконаємо команду для перевірки IP-конфігурації на ASA-1.

```

ciscoasa# show int ip br

```

Interface	IP-Address	OK?	Method	Status	Prot
GigabitEthernet0/0	192.168.1.10	YES	CONFIG	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.10	192.168.10.1	YES	CONFIG	up	up
GigabitEthernet0/1.20	192.168.20.1	YES	CONFIG	up	up
GigabitEthernet0/1.30	192.168.30.1	YES	CONFIG	up	up
GigabitEthernet0/2	10.10.10.2	YES	CONFIG	up	up
GigabitEthernet0/3	10.10.10.6	YES	CONFIG	up	up
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
GigabitEthernet0/6	unassigned	YES	unset	administratively down	down
Management0/0	unassigned	YES	unset	administratively down	down

Рисунок 3.42 – Виконання діагностичної команди *show int ip br* на ASA-1.

Спробуємо отримати динамічні IP-адреси з пристроїв, що належать до різних підмереж.

```
PC1> ip dhcp
DORA IP 192.168.30.2/24 GW 192.168.30.1
```

Рисунок 3.43 – Отримання динамічної IP-адреси робочою станцією, що належить до VLAN 30.

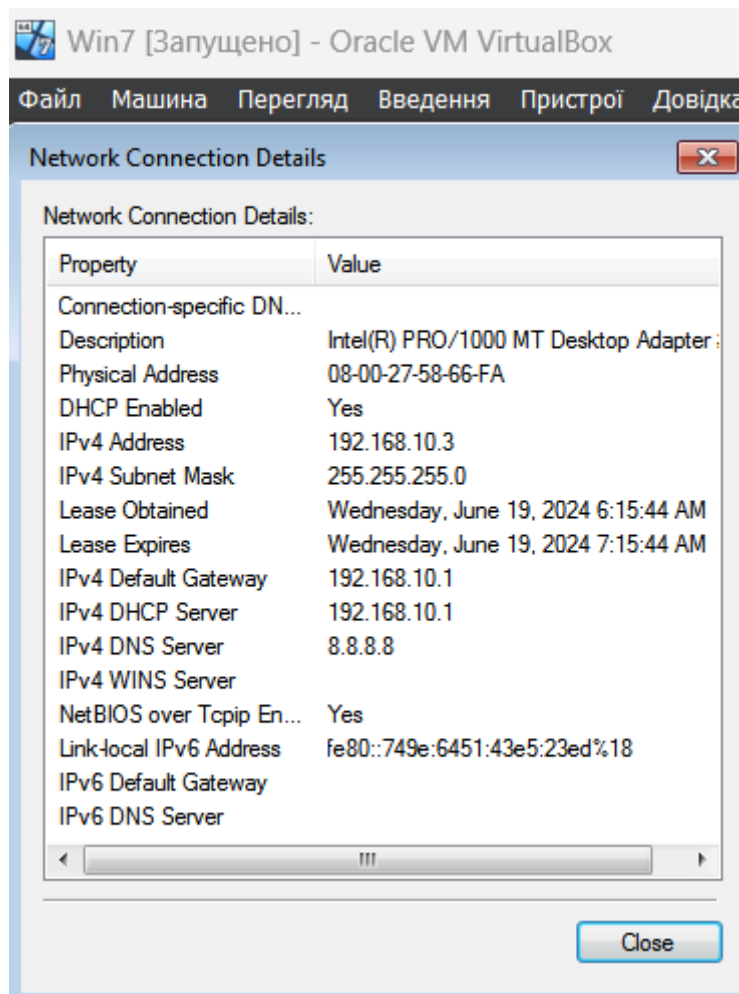


Рисунок 3.44 – Отримання динамічної IP-адреси робочою станцією, що належить до VLAN 10.

На наступних скриншотах ми перевіряємо зв'язок робочої станції з встановленою операційною системою Windows 7 з підмережею, в якій знаходиться робоча станція, віддаленою підмережею, а також підмережею, яка знаходиться в глобальній мережі інтернет, а також пробуємо отримати доступ до сервісів google та youtube.



C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
 Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ vboxuser>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
 Reply from 192.168.10.1: bytes=32 time=3ms TTL=255
 Reply from 192.168.10.1: bytes=32 time=3ms TTL=255
 Reply from 192.168.10.1: bytes=32 time=2ms TTL=255
 Reply from 192.168.10.1: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.10.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\ vboxuser>ping 192.168.50.2

Pinging 192.168.50.2 with 32 bytes of data:
 Request timed out.
 Reply from 192.168.50.2: bytes=32 time=25ms TTL=63
 Reply from 192.168.50.2: bytes=32 time=36ms TTL=63
 Reply from 192.168.50.2: bytes=32 time=101ms TTL=63

Ping statistics for 192.168.50.2:
 Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 25ms, Maximum = 101ms, Average = 54ms

C:\Users\ vboxuser>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
 Reply from 8.8.8.8: bytes=32 time=19ms TTL=117
 Reply from 8.8.8.8: bytes=32 time=18ms TTL=117
 Reply from 8.8.8.8: bytes=32 time=19ms TTL=117
 Reply from 8.8.8.8: bytes=32 time=18ms TTL=117

Ping statistics for 8.8.8.8:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 18ms, Maximum = 19ms, Average = 18ms

Рисунок 3.45 – Перевірка зв'язку з пристроями.

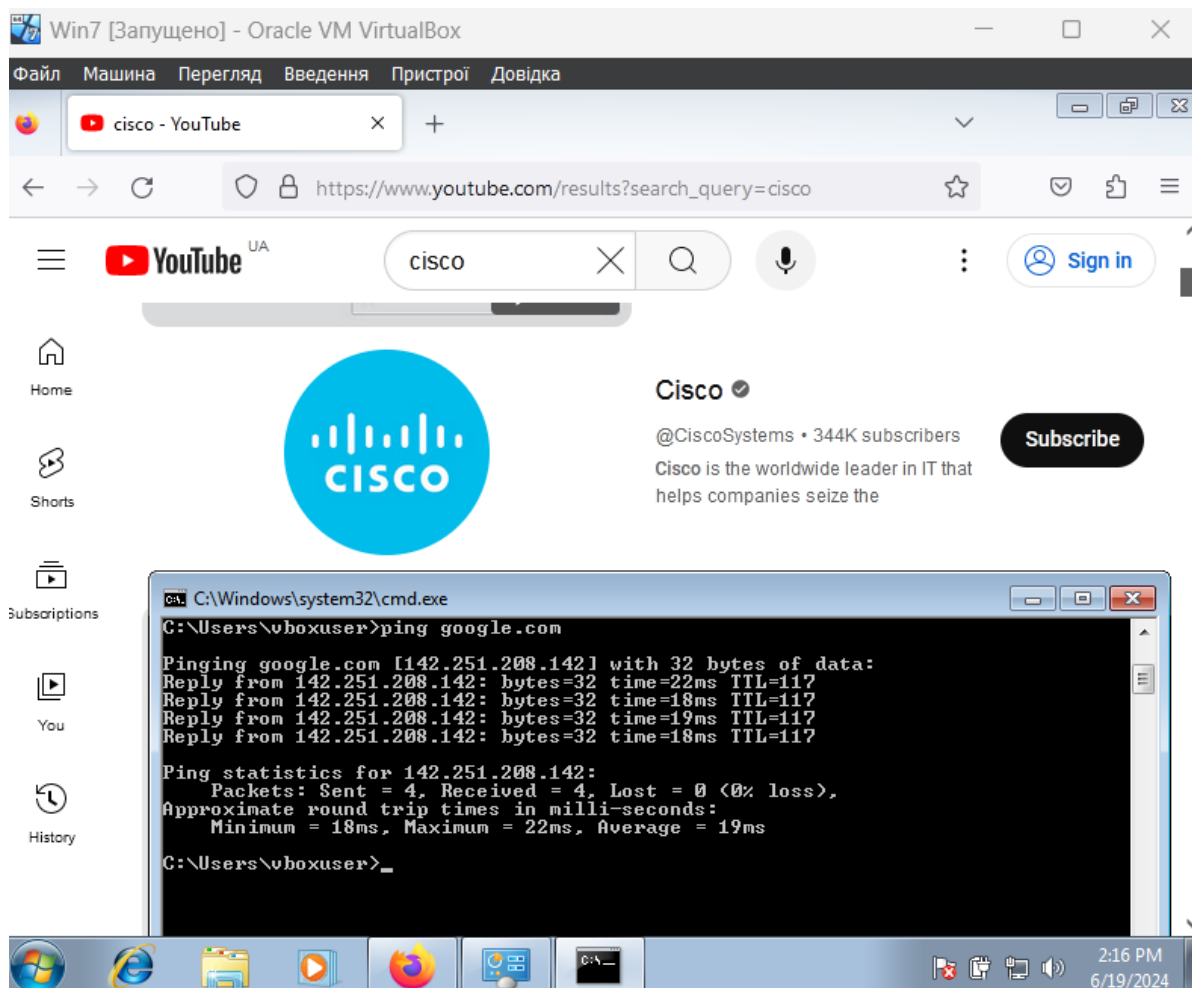


Рисунок 3.46 – Отримання доступу до google та youtube.

Тепер перевіримо інтерфейси та віртуальні локальні мережі, сконфігуровані в пункті 3.2:

```
ciscoasa# sh vlan
10,20,30
```

Рисунок 3.47 – Віртуальні локальні мережі на ASA-1.

```
SW-2#show vlan br
```

VLAN	Name	Status	Ports
1	default	active	
10	VLAN0010	active	Et0/1, Et0/2
20	VLAN0020	active	Et0/3
30	VLAN0030	active	Et1/0
99	unused	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 3.48 – Віртуальні локальні мережі на SW-2.

```
SW-3#show vlan br
```

VLAN	Name	Status	Ports
1	default	active	
10	VLAN0010	active	Et0/1
20	VLAN0020	active	Et0/2
30	VLAN0030	active	Et0/3
99	unused	active	Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 3.49 – Віртуальні локальні мережі на SW-3.

```
SW-1#show vlan br
```

VLAN	Name	Status	Ports
1	default	active	
10	VLAN0010	active	
20	VLAN0020	active	
30	VLAN0030	active	
99	unused	active	Et0/3, Et1/0, Et1/1, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Рисунок 3.50 – Віртуальні локальні мережі на SW-1.

```
SW-1#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	1
Et0/1	on	802.1q	trunking	1
Et0/2	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Et0/0	1-4094
Et0/1	1-4094
Et0/2	1-4094

Port	Vlans allowed and active in management domain
Et0/0	1,10,20,30,99
Et0/1	1,10,20,30,99
Et0/2	1,10,20,30,99

Port	Vlans in spanning tree forwarding state and not pruned
Et0/0	none
Et0/1	1,10,20,30,99
Et0/2	none

Рисунок 3.51 – Виконання діагностичної команди *show int trunk* на SW-1.

```
SW-1#show int status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	auto	auto	unknown
Et0/1		connected	trunk	auto	auto	unknown
Et0/2		connected	trunk	auto	auto	unknown
Et0/3		disabled	99	auto	auto	unknown
Et1/0		disabled	99	auto	auto	unknown
Et1/1		disabled	99	auto	auto	unknown
Et1/2		disabled	99	auto	auto	unknown
Et1/3		disabled	99	auto	auto	unknown
Et2/0		disabled	99	auto	auto	unknown
Et2/1		disabled	99	auto	auto	unknown
Et2/2		disabled	99	auto	auto	unknown
Et2/3		disabled	99	auto	auto	unknown
Et3/0		disabled	99	auto	auto	unknown
Et3/1		disabled	99	auto	auto	unknown
Et3/2		disabled	99	auto	auto	unknown
Et3/3		disabled	99	auto	auto	unknown

Рисунок 3.52 – Виконання діагностичної команди *show int status* на SW-1.

```
SW-2#show int status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	auto	auto	unknown
Et0/1		connected	10	auto	auto	unknown
Et0/2		connected	10	auto	auto	unknown
Et0/3		connected	20	auto	auto	unknown
Et1/0		connected	30	auto	auto	unknown
Et1/1		disabled	99	auto	auto	unknown
Et1/2		disabled	99	auto	auto	unknown
Et1/3		disabled	99	auto	auto	unknown
Et2/0		disabled	99	auto	auto	unknown
Et2/1		disabled	99	auto	auto	unknown
Et2/2		disabled	99	auto	auto	unknown
Et2/3		disabled	99	auto	auto	unknown
Et3/0		disabled	99	auto	auto	unknown
Et3/1		disabled	99	auto	auto	unknown
Et3/2		disabled	99	auto	auto	unknown
Et3/3		disabled	99	auto	auto	unknown

Рисунок 3.53 – Виконання діагностичної команди *show int status* на SW-2.

```
SW-3#show int status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Et0/0		connected	trunk	auto	auto	unknown
Et0/1		connected	10	auto	auto	unknown
Et0/2		connected	20	auto	auto	unknown
Et0/3		connected	30	auto	auto	unknown
Et1/0		disabled	99	auto	auto	unknown
Et1/1		disabled	99	auto	auto	unknown
Et1/2		disabled	99	auto	auto	unknown
Et1/3		disabled	99	auto	auto	unknown
Et2/0		disabled	99	auto	auto	unknown
Et2/1		disabled	99	auto	auto	unknown
Et2/2		disabled	99	auto	auto	unknown
Et2/3		disabled	99	auto	auto	unknown
Et3/0		disabled	99	auto	auto	unknown
Et3/1		disabled	99	auto	auto	unknown
Et3/2		disabled	99	auto	auto	unknown
Et3/3		disabled	99	auto	auto	unknown

Рисунок 3.54 – Виконання діагностичної команди *show int status* на SW-3.

Перевіримо також налаштування port-security на прикладі комутатора SW-2. На першому скриншоті ми можемо побачити як комутатор відреагував на інцидент безпеки (відключив порт та заніс в таблицю відповідну інформацію), а на другому видно як відновився інтерфейс після атаки.

```
SW-2#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)         (Count)         (Count)
-----
      Et0/1             1             1             0             Shutdown
      Et0/2             1             0             0             Shutdown
      Et0/3             1             0             0             Shutdown
      Et1/0             1             1             0             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW-2#
*Jun 19 17:06:33.880: %PM-4-ERR_DISABLE: psecure-violation error detected on Et1/0, putting
Et1/0 in err-disable state
SW-2#
*Jun 19 17:06:33.889: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caus
ed by MAC address 0050.7966.6800 on port Ethernet1/0.
*Jun 19 17:06:34.925: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed
state to down
SW-2#
*Jun 19 17:06:35.892: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
SW-2#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)         (Count)         (Count)
-----
      Et0/1             1             1             0             Shutdown
      Et0/2             1             0             0             Shutdown
      Et0/3             1             0             0             Shutdown
      Et1/0             1             1             1             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Рисунок 3.55 – Перевірка налаштувань port-security.

```
SW-2#
*Jun 19 17:07:33.908: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-d
isable state on Et1/0
SW-2#
*Jun 19 17:07:35.937: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Jun 19 17:07:36.993: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed
state to up
SW-2#
```

Рисунок 3.56 – Перевірка налаштувань port-security.

Спробуємо підключитися до Cisco ASA за допомогою Cisco Adaptive Security Device Manager та перевірити деякі налаштування:

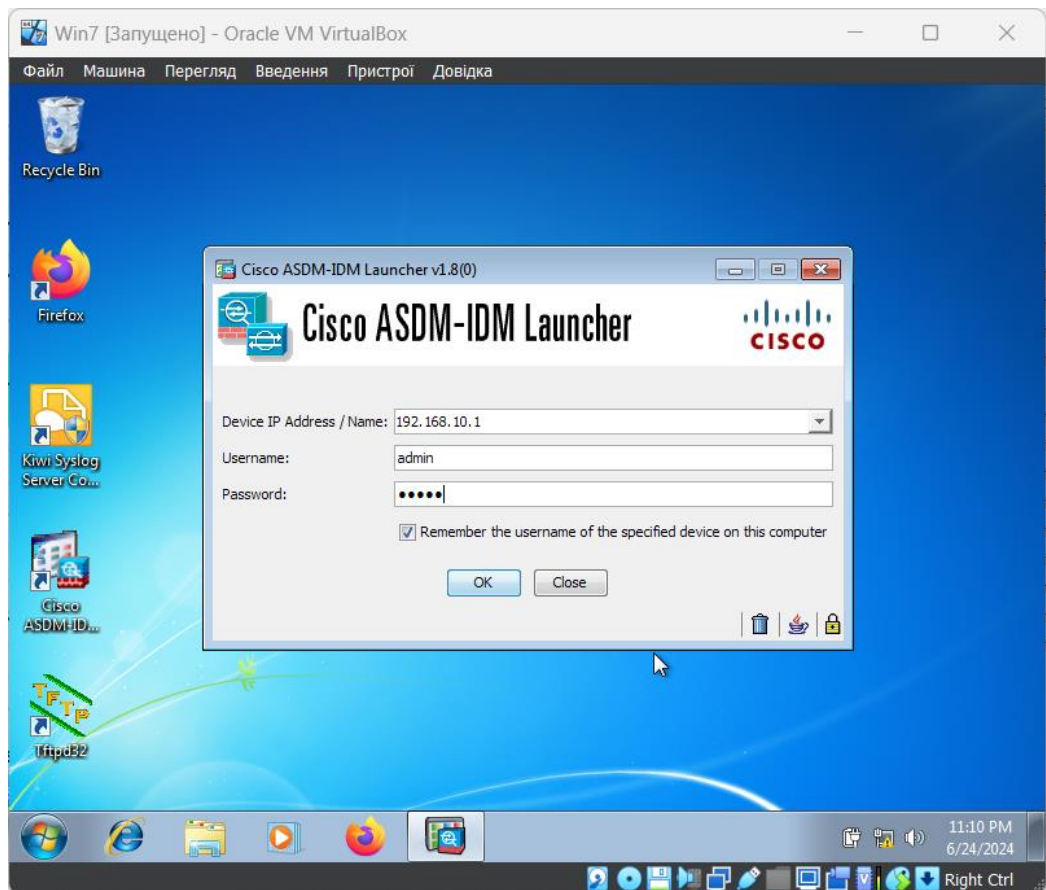


Рисунок 3.57 – Підключення до Cisco ASA.

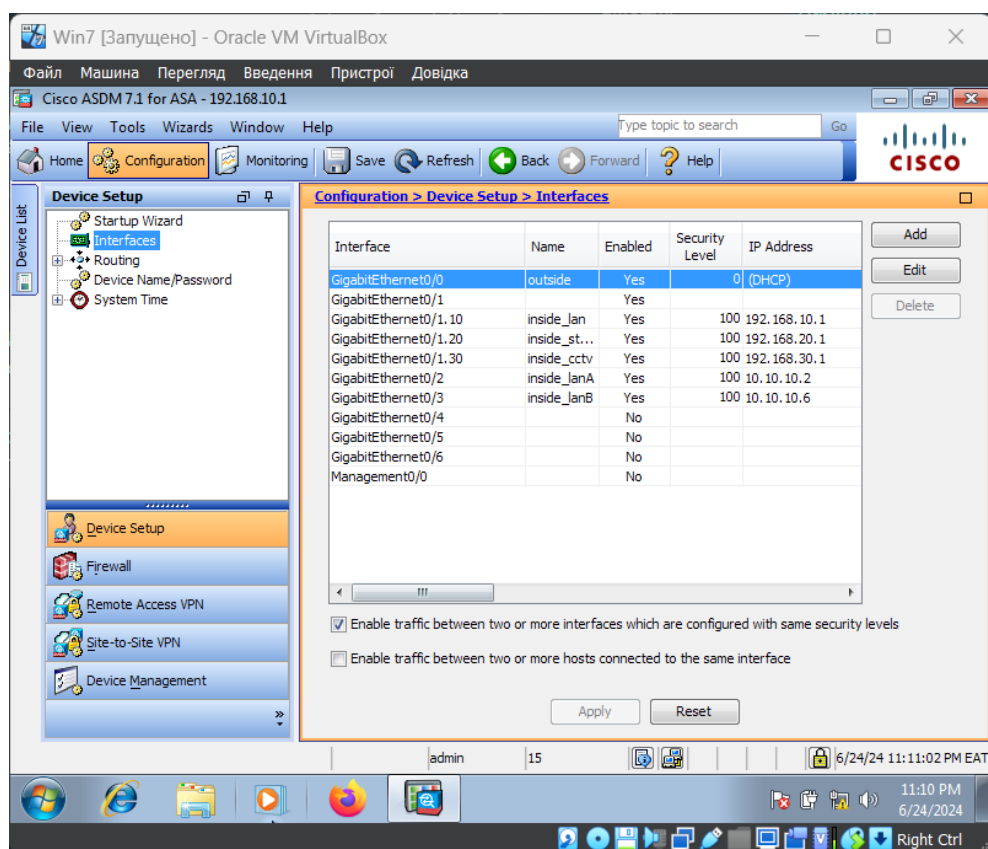


Рисунок 3.58 – Перевірка налаштувань інтерфейсів за допомогою ASDM.

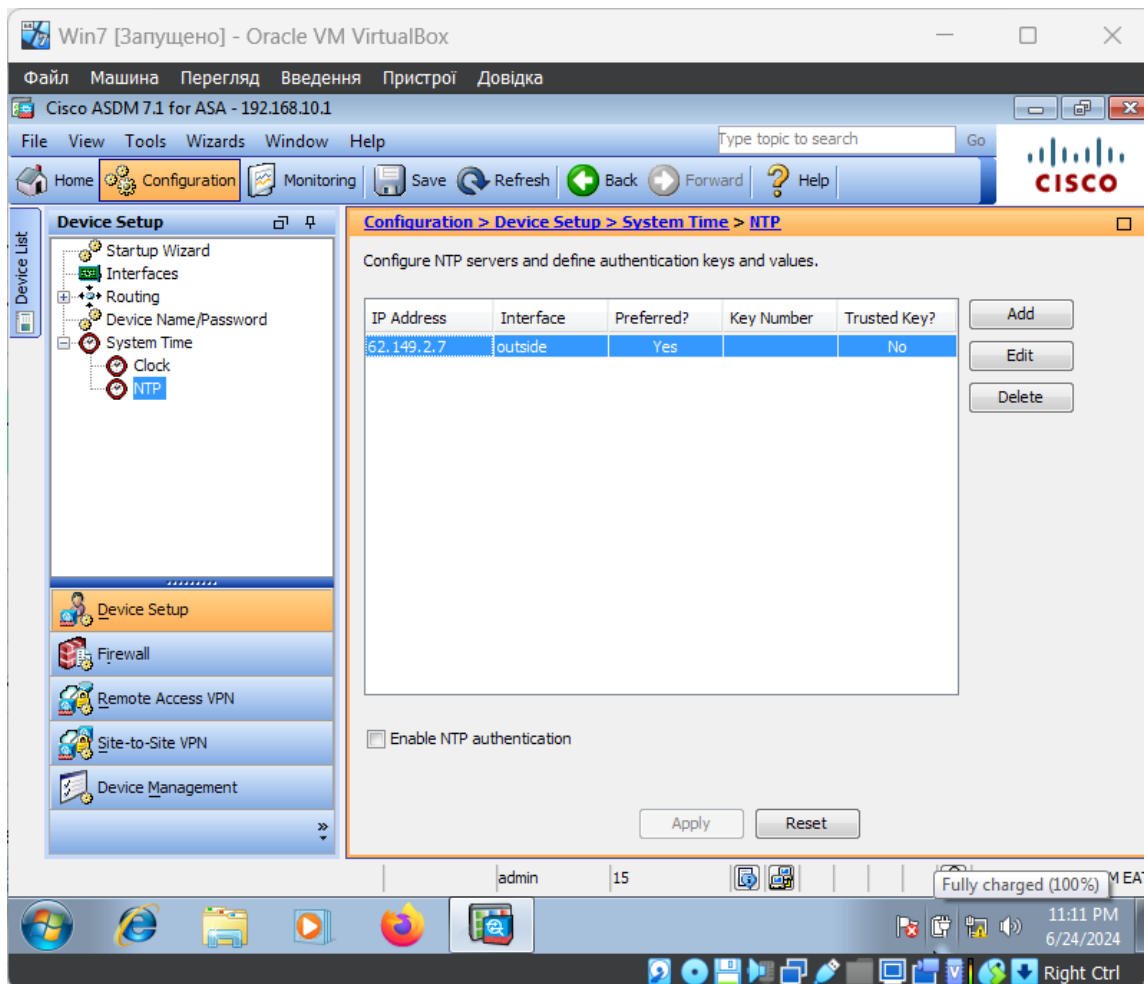


Рисунок 3.59 – Перевірка налаштувань NTP за допомогою ASDM

Також варто перевірити функціонування Syslog-сервера. На скриншоті показано деякі повідомлення, які дають зрозуміти, що логування успішно працює.

Win7 [Запущено] - Oracle VM VirtualBox				
Київський системний сервер (14 Day evaluation - Version 9.4)				
File Edit View Help				
Display 00 (Default) 14 Days left in evaluation Buy Now				
Date	Time	Priority	Hostname	Message
06-19-2024	14:52:08	Local7.Info	10.10.10.1	33: *Mar 1 00:01:13.999: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 started - CLI initiated
06-19-2024	14:52:08	Local7.Info	10.10.10.1	32: *Mar 1 00:01:13.999: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 stopped - CLI initiated
06-19-2024	14:52:06	Local7.Notice	10.10.10.1	31: *Mar 1 00:01:07.999: %SYS-5-CONFIG_I: Configured from console by
06-19-2024	14:51:40	Local7.Info	10.10.10.5	31: *Mar 1 00:00:47.959: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 started - CLI initiated
06-19-2024	14:51:39	Local7.Notice	10.10.10.5	30: *Mar 1 00:00:46.959: %SYS-5-CONFIG_I: Configured from console by
06-19-2024	14:41:11	Local7.Notice	10.10.10.5	30: *Mar 1 00:05:20.739: %SYS-5-CONFIG_I: Configured from console by
06-19-2024	14:40:06	Local7.Notice	10.10.10.1	32: *Mar 1 00:04:19.387: %SYS-5-CONFIG_I: Configured from console by
06-19-2024	14:39:17	Local7.Info	10.10.10.1	31: *Mar 1 00:03:29.635: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.2 started - CLI initiated
06-19-2024	14:39:16	Local7.Notice	10.10.10.1	30: *Mar 1 00:03:28.635: %SYS-5-CONFIG_I: Configured from console by

Рисунок 3.60 – Перевірка Syslog-сервера.

Переглянемо виводи діагностичних команд, що стосуються налаштувань DHCP-сервера на базі Cisco ASA:

```
ciscoasa# show dhcpd binding
```

IP address	Client Identifier	Lease expiration	Type
192.168.10.2	0100.5079.6668.00	3512 seconds	Automatic
192.168.10.3	0100.5079.6668.03	3515 seconds	Automatic
192.168.10.4	0108.0027.5866.fa	3521 seconds	Automatic
192.168.20.2	0100.5079.6668.01	3499 seconds	Automatic
192.168.20.3	0100.5079.6668.04	3514 seconds	Automatic
192.168.30.2	0100.5079.6668.05	3514 seconds	Automatic
192.168.30.3	0100.5079.6668.08	3587 seconds	Automatic

Рисунок 3.61 – Перевірка прив'язки адрес.

```
ciscoasa# show dhcpd state
Context Configured as DHCP Server
Interface outside, Not Configured for DHCP
Interface inside_lan, Configured for DHCP SERVER
Interface inside_storage, Configured for DHCP SERVER
Interface inside_cctv, Configured for DHCP SERVER
Interface inside_lanA, Not Configured for DHCP
Interface inside_lanB, Not Configured for DHCP
```

Рисунок 3.62 – Перевірка інтерфейсів.

```
ciscoasa# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools      3
Automatic bindings 7
Expired bindings   0
Malformed messages 0

Message           Received
BOOTREQUEST       0
DHCPDISCOVER       7
DHCPREQUEST       7
DHCPDECLINE        0
DHCPRELEASE        0
DHCPINFORM         1

Message           Sent
BOOTREPLY          0
DHCPOFFER          7
DHCPACK            8
DHCPNAK            0
```

Рисунок 3.63 – Перевірка DHCP статистики на ASA-1.

Наостанок перевіримо конфігурацію VPN тунелю:

```

interface: FastEthernet0/0
  Crypto map tag: CMAP, local addr 10.10.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.40.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.50.0/255.255.255.0/0/0)
current_peer 10.10.10.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.5
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x54D4480D(1423198221)

inbound esp sas:
  spi: 0xA8EE3241(2834182721)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2001, flow_id: SW:1, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4514338/3557)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x54D4480D(1423198221)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: SW:2, crypto map: CMAP
    sa timing: remaining key lifetime (k/sec): (4514338/3549)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE
  
```

Рисунок 3.64 – Виконання діагностичної команди на R-1.

```

R1#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.5 port 500
IKE SA: local 10.10.10.1/500 remote 10.10.10.5/500 Active
IPSEC FLOW: permit ip 192.168.40.0/255.255.255.0 192.168.50.0/255.255.255.0
Active SAs: 2, origin: crypto map
  
```

Рисунок 3.65 – Виконання діагностичної команди show crypto session.

Висновки до третього розділу.

У рамках виконання завдань третього розділу було описано пристрої та операційні системи, які використовувалися для побудови мережі, описано сценарій налагодження всіх пристроїв мережі і її захисту, а також здійснено успішну перевірку конфігурацій пристроїв мережі.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено поняття периметрових підсистем захисту корпоративних мереж, досліджено способи реалізації захищених корпоративних мереж з використанням рішень Cisco ASA і пристроїв та технологій, розроблених Cisco Systems.

В межах першого розділу кваліфікаційної роботи було розглянуто загальні підходи до побудови підсистем захисту корпоративних мереж, поняття периметрового захисту, як основи побудови ззахисту мереж корпорацій, поняття та основи роботи систем обміну даними на базі віртуальних приватних мереж, а також проаналізовано комплексні рішення, що застосовуються для побудови підсистем захисту корпоративних мереж.

В межах другого розділу кваліфікаційної роботи було розглянуто важливі питання, що стосуються проектування топології, передбачення потоків трафіку та побудови підсистеми захисту корпоративної мережі. Спроектовано політики безпеки корпоративної мережі, загальну структури підсистеми захисту корпоративної мережі та основні елементи підсистеми захисту корпоративної мережі.

У рамках виконання завдань третього розділу було описано пристрої та операційні системи, які використовувалися для побудови мережі, такі як маршрутизатор Cisco 7200 Series VRX, комутатор Cisco Catalyst WS-C2960-24TT-L, Cisco ASA 5500X, операційну систему Windows 7 та SOLARWINDS Kiwi Syslog Server, описано сценарій налагодження всіх пристроїв мережі і її захисту, а також здійснено успішну перевірку конфігурацій пристроїв мережі.

Загалом, дипломна кваліфікаційна робота успішно розглянула ключові аспекти забезпечення безпеки мереж з використанням обладнання Cisco, охоплюючи різноманітні технології, протоколи та сервіси. Проектування підсистеми захисту корпоративної мережі та її топології, впровадження заходів безпеки та успішні налаштування всіх компонентів свідчать про готовність розробленої мережі до експлуатації.

		Ляшенко Н.Б.			ДУ «Житомирська політехніка».24.125.14 КБ-20-1 – ПЗ	77
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Головка, А. А., & Лисенко, О. М. (2017). Інформаційна безпека: теорія та практика. Київ: Ліра-К.
2. Головка, М. В. (2015). Захист інформації: Навчальний посібник. Київ: Центр навчальної літератури.
3. Горощенко, О. В. (2021). Захист інформації в комп'ютерних системах: навч. посіб. Київ: Центр учбової літератури.
4. Дойл, Д. С. (2019). Cisco для "чайників". 7-е вид., перероб. і доп. Москва: Ексмо.
5. Петренко, А. І., & Петренко, О. І. (2018). Захист інформації в комп'ютерних системах: Навчальний посібник. Київ: Видавничо-поліграфічний центр "Київський університет".
6. Петренко, О. В., & Петренко, А. О. (2019). Периметровий захист інформаційних систем: теорія та практика. Київ: НТЦ "Інтелект".
7. Підоплічко, О. М. (2019). Інформаційна безпека: навч. посіб. Київ: МАУП.
8. Симоненко, О. В., & Симоненко, О. О. (2020). Комп'ютерна безпека: навч. посіб. Київ: МАУП.
9. Солодов, Г. В. (2018). Захист інформації: теорія та практика. Київ: Центр навчальної літератури.
10. Стасов, В. В., & Симоненко, О. М. (2016). Інформаційна безпека: Навчальний посібник. Харків: Видавництво НТУ "ХП".
11. Швайко, О. О. (2018). Комп'ютерна безпека: навч. посіб. Київ: НТУУ "КПІ" ім. І. Сікорського.
12. Штейнберг, Р. М. (2018). Мережеві технології Cisco: початковий курс: [підручник для студ. вищ. навч. закл.]. 2-е вид., перероб. і доп. Харків: НТЦ «Еко-Трейд».
13. Авраменко, О. М., & Петренко, А. О. (2022). Застосування віртуальних приватних мереж (VPN) для забезпечення інформаційної безпеки в

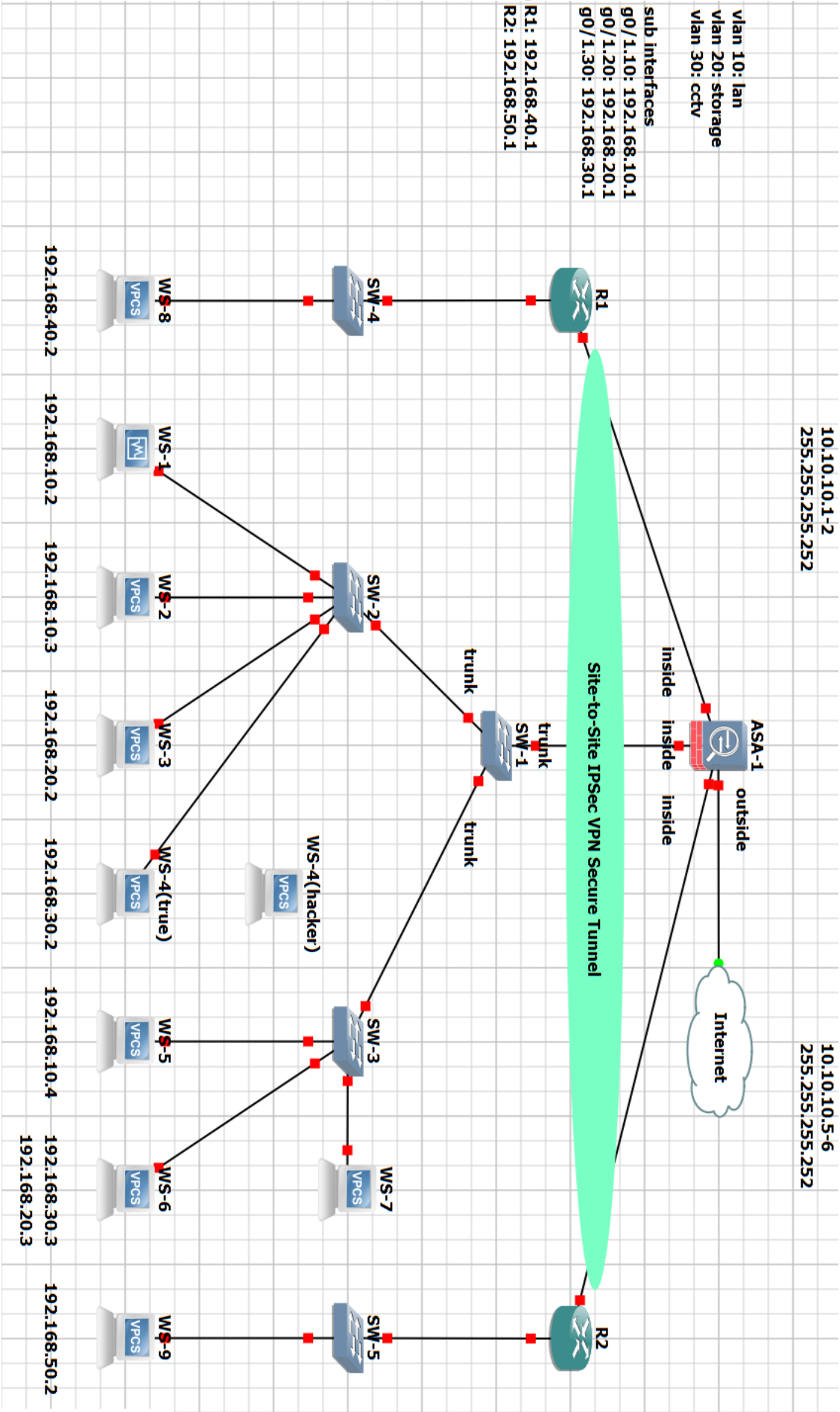
		Ляшенко Н.Б.			ДУ «Житомирська політехніка». 24.125.14 КБ-20-1 – ПЗ	78
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

корпоративних мережах. Вісник Національного технічного університету "Київський політехнічний інститут", 83, 64-69.

- 14.Павлов, О. В., & Шевченко, О. М. (2023). Загальні підходи до побудови підсистем захисту корпоративних мереж. Вісник Національного технічного університету "КПІ". Серія "Інформатика та комп'ютерна наука", 80, 5-12.
- 15.Сидоренко, О. В. (2019). Налаштування віртуальних локальних мереж (VLAN) на комутаторах Cisco. Системи та засоби інформатизації, 1, 78-82.
- 16.ACL Cisco: Повний посібник (2023) - Джон Дорман, Том Лайонел
<https://www.ciscopress.com/articles/article.asp?p=3089353&seqNum=8>
- 17.Cisco Networking Academy: Routing, Switching, Security and Wireless Essentials Comprehensive Lab Manual (2022) - Cisco Networking Academy
<https://www.youtube.com/playlist?list=PL045B070715AA1FE9>
- 18.Cisco Networking Academy: Routing, Switching, Security and Wireless Essentials Companion Guide (2022) - Cisco Networking Academy
- 19.Cisco OSPF Command Reference (2023). Cisco Press.
- 20.OSPF Network Design and Implementation (2022) by Tom Lamiel. Cisco Press.
- 21.OSPF for Cisco Networks (2021) by David Bombardieri.

ДОДАТКИ

Схема побудованої мережі



[illegible]


```

shutdown
clock rate 2000000
!
interface Serial0/3
no ip address
shutdown
clock rate 2000000
!
router ospf 14
router-id 1.1.1.3
log-adjacency-changes
network 10.10.10.4 0.0.0.3 area 0
network 192.168.50.0 0.0.0.255 area 0
!
!
!
no ip http server
no ip http secure-server
ip nat inside source list 100 interface
FastEthernet0/0 overload
!
ip access-list extended VPN-TRAFFIC
permit ip 192.168.50.0 0.0.0.255
192.168.40.0 0.0.0.255
!
logging 192.168.10.2
access-list 100 remark -=[Define NAT
Service]=-
access-list 100 deny ip 192.168.50.0
0.0.0.255 192.168.40.0 0.0.0.255
access-list 100 permit ip 192.168.50.0
0.0.0.255 any
access-list 100 remark
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End

```

```

SW-1#show run
Building configuration...

Current configuration : 2438 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/2

```

```

switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/0
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/1
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/2
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/3
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/1
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/3
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet3/0
switchport access vlan 99
switchport mode access
shutdown
duplex auto

```

```

!
interface Ethernet3/1
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet3/2
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet3/3
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Vlan1
no ip address
shutdown
!
!
no ip http server
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

SW-2#show run
Building configuration...

Current configuration : 3234 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-2
!
boot-start-marker
boot-end-marker
!
!

```

```

logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
!
!
errdisable recovery cause psecure-
violation
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security aging time 100
switchport port-security aging type
inactivity
switchport port-security mac-address
sticky
switchport port-security mac-address
sticky 0800.2758.66fa
duplex auto
!
interface Ethernet0/2
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security aging time 100
switchport port-security aging type
inactivity

```

```

switchport port-security mac-address
sticky
duplex auto
!
interface Ethernet0/3
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security aging time 100
switchport port-security aging type
inactivity
switchport port-security mac-address
sticky
duplex auto
!
interface Ethernet1/0
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security aging time 100
switchport port-security aging type
inactivity
switchport port-security mac-address
sticky
switchport port-security mac-address
sticky 0050.7966.6808
duplex auto
!
interface Ethernet1/1
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/2
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet1/3
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/1
switchport access vlan 99
switchport mode access
shutdown
duplex auto
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
shutdown
duplex auto

```



```

    switchport port-security mac-address
    sticky
    duplex auto
    !
interface Ethernet0/2
    switchport access vlan 20
    switchport mode access
    switchport port-security
    switchport port-security aging time 100
    switchport port-security aging type
    inactivity
    switchport port-security mac-address
    sticky
    duplex auto
    !
interface Ethernet0/3
    switchport access vlan 30
    switchport mode access
    switchport port-security
    switchport port-security aging time 100
    switchport port-security aging type
    inactivity
    switchport port-security mac-address
    sticky
    duplex auto
    !
interface Ethernet1/0
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet1/1
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet1/2
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet1/3
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet2/0
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet2/1
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet2/2

```

```

    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet2/3
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet3/0
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet3/1
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet3/2
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Ethernet3/3
    switchport access vlan 99
    switchport mode access
    shutdown
    duplex auto
    !
interface Vlan1
    no ip address
    shutdown
    !
    !
no ip http server
    !
    !
    !
    !
control-plane
    !
    !
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login
    !
End

```

```
SW-4#show run
Building configuration...
```

```
Current configuration : 1462 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
```

```
duplex auto
!
interface Ethernet1/0 SW-5#show run
Building configuration...
```

```
Current configuration : 1462 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-5
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity
drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
```

```

interface Ethernet0/3
    duplex auto
!
interface Ethernet1/0
    duplex auto
!
interface Ethernet1/1
    duplex auto
!
interface Ethernet1/2
    duplex auto
!
interface Ethernet1/3
    duplex auto
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    no ip address
    shutdown
!
!
no ip http server
!
!
!
!
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login

```

```

!
end
    duplex auto
!
interface Ethernet1/1
    duplex auto
!
interface Ethernet1/2
    duplex auto
!
interface Ethernet1/3
    duplex auto
!
interface Ethernet2/0
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!
interface Ethernet2/3
    duplex auto
!
interface Ethernet3/0
    duplex auto
!
interface Ethernet3/1
    duplex auto
!
interface Ethernet3/2
    duplex auto
!
interface Ethernet3/3
    duplex auto
!
interface Vlan1
    no ip address
    shutdown
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line vty 0 4
    login
!
End

```

```

ciscoasa# show run
: Saved

:
: Serial Number: 9ABU7S6H4XU
: Hardware:   ASAv, 2048 MB RAM, CPU
Pentium II 3293 MHz
:
ASA Version 9.8(1)
!
hostname ciscoasa
enable password
$sha512$5000$EJHLhg1xYhdIUqKEY72z9Q==$Rx
AK3IkoVpmTe8s3EHGdwg== pbkdf2
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

!
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 192.168.1.10 255.255.255.0
!
interface GigabitEthernet0/1
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/1.10
  vlan 10
  nameif inside_lan
  security-level 100
  ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1.20
  vlan 20
  nameif inside_storage
  security-level 100
  ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/1.30
  vlan 30
  nameif inside_cctv
  security-level 100
  ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/2
  nameif inside_lanA
  security-level 100

  ip address 10.10.10.2 255.255.255.252
!
interface GigabitEthernet0/3
  nameif inside_lanB
  security-level 100
  ip address 10.10.10.6 255.255.255.252
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/6
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  shutdown
  no nameif
  no security-level
  no ip address
!
ftp mode passive
same-security-traffic permit inter-interface
object network nat_lan
  subnet 192.168.10.0 255.255.255.0
pager lines 23
mtu outside 1500
mtu inside_lan 1500
mtu inside_storage 1500
mtu inside_cctv 1500
mtu inside_lanA 1500
mtu inside_lanB 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
!
object network nat_lan
  nat (inside_lan,outside) dynamic
interface
  router ospf 14
  router-id 1.1.1.1
  log-adj-changes
!
route outside 0.0.0.0 0.0.0.0
192.168.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30

```

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

```
3082010a 02820101 00af2408 08297a35
9e600caa e74b3b4e dc7cbc3c 451cbb2b
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 0.0.0.0 0.0.0.0 inside_lanA
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 8.8.8.8
!
dhcpd address 192.168.10.2-
192.168.10.254 inside_lan
dhcpd enable inside_lan
!
dhcpd address 192.168.20.2-
192.168.20.254 inside_storage
dhcpd enable inside_storage
```

```

!
dhcpd address 192.168.30.2-
192.168.30.254 inside_cctv
dhcpd enable inside_cctv
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-
intercept
dynamic-access-policy-record
DfltAccessPolicy
username sshusr password
$sha512$5000$L1vZ5sUFx9inz/lMcaF1Yw==$I8
sh4n07Bl/j84kLrCqUog== pbkdf2
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns
preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map global-policy
policy-map global_policy
class inspection_default
inspect ip-options
inspect netbios
inspect rtsp
inspect sunrpc
inspect tftp
inspect xdmcp
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect esmtp
inspect sqlnet
inspect sip
inspect skinny
inspect icmp
policy-map type inspect dns
migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
policy-map type inspect dns
migrated_dns_map_1
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/DDCEService
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/DDCEService
destination transport-method http
Cryptochecksum:324baa7b3cd990cf58385e68e4ebf793
: end

```