

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

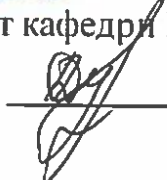
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми периметрового захисту
комп'ютерної мережі організації на базі міжмережних
екранів Cisco ASA 5506»

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

 Д.В. Боговик
Керівник к.т.н., доцент кафедри КІ та КБ

 О.В. Пірог
Рецензент к.т.н., доцент, доцент кафедри БІ та Т

 О.Ф. Дубина

Житомир – 2021

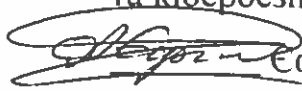
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Боговика Дмитра Васильовича**

Тема роботи: **Проект підсистеми периметрового захисту комп'ютерної мережі організації на базі міжмережних екранів Cisco ASA 5506**
затверджена Наказом по університету від «12» Квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «24» Червня 2021р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Міжмережеві екрани Cisco ASA
5. Симулятор Packet Tracer

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Пірог О.В.	12.04.21 	12.04.21 
2	Пірог О.В.	28.04.21 	28.04.21 
3	Пірог О.В.	20.05.21 	20.05.21 

Керівник  Пірог О.В.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання. Опрацювання літературних джерел.	15 березня 2021 – 15 квітня 2021	
2	Проектування топології мережі та схеми адресації	16 квітня 2021 – 10 травня 2021	
3	Написання програмного коду	11 травня 2021 – 26 травня 2021	
4	Тестування	27 травня 2021 – 10 червня 2021	
5	Захист		

Студент 
(підпис)

Керівник 
(підпис)

РЕФЕРАТ

Випускна робота бакалавра складається з побудови підсистеми периметрового захисту мережі організації на базі міжмережних екранів Cisco ASA.

Пояснювальна записка має 10 сторінок додатків. Список використаних джерел містить 17 найменувань і займає 2 сторінки. В роботі наведено 38 рисунків і 5 таблиць. Загальний обсяг роботи – 56 сторінок.

Метою роботи є розробка за допомогою Cisco Packet Tracer підсистему мережі периметрового захисту комп'ютерної мережі організації на базі міжмережних екранів, глибоке дослідження задач, що пов'язані з темою роботи.

В роботі визначено основні завдання для розробки системи, проаналізовано методи вирішення поставленої задачі. Наведено теоретичні відомості про застосування міжмережних екранів в комп'ютерній мережі. Також описана програмна реалізація підсистеми периметрового захисту мережі.

Наводяться результати перевірки працездатності системи.

КЛЮЧОВІ СЛОВА: КОМП'ЮТЕРНА МЕРЕЖА, МІЖМЕРЕЖНИЙ ЕКРАН, CISCO ASA, ASA 5506, CISCO PACKET TRACER.

					КБ.КР.Б – 125 – 20 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дат			
Розроб.		Д.В. Босовик		23.06.21	Проект підсистеми захисту комп'ютерної мережі організації на базі міжмережних екранів Cisco ASA 5506		
Керівник		О.В. Пірог		23.06.21			
Рецензент		О.Ф. Дубина		23.06.21	Житомирська політехніка, група КБ - 1		
Зав. Каф.		А.А. Сфіменко		23.06.21			

ABSTRACT

The bachelor's thesis consists of building a subsystem for protecting the organization's network based on Cisco ASA firewalls.

The explanatory note has 10 pages of appendices. The list of used sources contains 17 names and occupies 2 page. The paper contains 38 figures and 5 tables. The total volume of the work is 56 pages.

The aim of the work is to develop with the help of Cisco Packet Tracer a subsystem of the perimeter security network of the computer network of the organization on the basis of firewalls, in-depth study of tasks related to the topic of work.

The main tasks for system development are defined in the work, the methods of solving the set task are analyzed. Theoretical information on the use of firewalls in a computer network is given. The software implementation of the perimeter network protection subsystem is also described.

KEY WORDS: ASA 5506, CISCO ASA, CISCO PACKET TRACER, COMPUTER NETWORK.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ.....	10
1.1 Аналіз необхідності захисту комп'ютерної мережі.....	10
1.2 Захист периметра мережі.....	12
1.3 Міжмережевий екран.....	17
1.4 Cisco ASA.....	21
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	29
2.1. Визначення варіантів використання	29
2.2 Розробка топології комп'ютерної мережі.....	31
2.3 Розробка схеми адресації пристроїв	36
РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ	39
3.1 Вибір обладнання для побудови мережі.....	39
3.2 Налагодження обладнання мережі.....	42
3.3 Перевірка працездатності мережі	49
ВИСНОВКИ	55
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	57
ДОДАТКИ.....	59

ВСТУП

На даний момент неможливо уявити роботу малого бізнесу без використання комп'ютерних технологій. Частіше за все необхідно будувати локальні або корпоративні мережі, в яких зазвичай задіяні майже всі комп'ютери компанії. Однак з моменту появи мереж виникла проблема безпеки. Багато керівників бізнесу навіть не замислюються над тим, як несанкціонований вхід у корпоративну мережу може вплинути на роботу організації.

Кожен керівник повинен розуміти важливість захисту своєї мережі від несанкціонованих втручань в роботу системи з глобальної, локальної мережі тощо. Кожна поважаючи себе компанія спілкується з іншими локальними мережами через Інтернет, оскільки встановити окремі канали зв'язку між окремими філіями досить дорого, а дозволити собі це можуть лише найбільші компанії.

Як результат, можна очікувати порушення захисту мережі не лише від співробітників їхньої компанії, але і від хакерів через Інтернет та збоку конкуруючих компаній, які можуть наймати тих самих хакерів і направити їх діяльність на завдання матеріальної шкоди компанії шляхом виходу із строю якихось зовнішніх чи внутрішніх ресурсів, або викрадення інформації, що являється комерційною таємницею.

Стрімкий розвиток інформаційних систем (ІС) та технологій всебічно впливає на всі сфери діяльності суспільства. Значна кількість сучасних державних та приватних підприємств використовує ІС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо.

Разом з цим збільшується кількість уразливостей та загроз ІС і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки. Слід зазначити, що одним із

актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІС з боку неавторизованої сторони.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережових вторгнень використовуються сучасні методи, моделі, засоби, програмне забезпечення (ПЗ) і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз.

Метою є створити захист периметра мережі який є обов'язковим елементом системи інформаційної безпеки організації. Мінімізація зовнішніх загроз досягається шляхом впровадження багаторівневої системи захисту інформації, і в першу чергу на зовнішньому кордоні мережі.

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.

Предметом дослідження є використання Cisco Packet Tracer для розробки комп'ютерної мережі організації.

Захист периметра корпоративних мереж дозволяє домогтися захищеності доступу внутрішніх користувачів в зовнішні мережі; надання доступу з зовнішніх мереж до публічних корпоративних ресурсів; захисту від мережових атак на корпоративні ресурси; організації системи електронної комерції; створення єдиної точки антивірусної і антиспам фільтрації; запобігання витоку конфіденційної інформації; моніторингу та аналізу подій інформаційної безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Аналіз необхідності захисту комп'ютерної мережі

У світі, де правлять інформаційні технології, складно сьогодні знайти сферу діяльності людини, яка б не потребувала використання комп'ютерних мереж. Науково-дослідні, проектно-конструкторські, виробничі, торговельні, фінансові, консультаційні, освітні та адміністративні установи; міжнародні корпорації та малий бізнес, – усі ці та багато інших підприємств для своєї діяльності потребують надійної та ефективної роботи комп'ютерних мереж.

Даний дипломний проект присвячений розробці підсистеми периметрового захисту комп'ютерної мережі організації на базі міжмережних екранів Cisco ASA. Комп'ютеризація стала невід'ємною частиною нашого буття. Але разом з тим вона перетворилася на камінь спотикання саме, з точки зору інформаційної безпеки.

Несанкціоновані дії “білокомірцевих злочинців” з конфіденційною, а також таємною електронною машинною інформацією, що є приватною власністю фізичних, юридичних осіб чи організацій, як результат приводять до: викрадення комп'ютерних даних, їх блокування, маніпуляції, порушенні її маршрутизації чи знищення такої. Зазначені злочинні дії осіб в кінцевому результаті спричиняють небажаних, а також шкідливих наслідків.

Як свідчить зарубіжна практика, провідні державні та приватні установи щорічно витрачають від 20 до 40 % чистого прибутку на придбання оновлених систем захисту програмних продуктів від їх викрадення. Хоч загально відомо, що не існує єдиного досконалого програмного забезпечення, яке на 100% змогло б гарантувати безпечність витоків комп'ютерної інформації, а значить, не виключається можливість бути потенційно пограбованим.

В залежності від можливих видів порушень роботи мережі чи несанкціонованого доступу, засоби захисту поділяються на: технічні засоби та програмні засоби. Сучасні технології розвиваються в напрямку поєднання цих засобів з метою підвищення захисту. Також до засобів захисту відносять організаційні, які, в свою чергу, розділяють на організаційно-технічні та організаційно-правові.

Фахівці галузі рекомендують використовувати комплексний підхід до застосування та розвитку всіх засобів і способів захисту інформації. Це підтверджується тим, що окремі сфери діяльності, які пов'язані з банківською справою чи системою державного управління, вимагають більш спеціалізованих заходів безпеки даних і висувають підвищені вимоги до надійності функціонування та захисту мереж, відповідно до характеру і важливості вирішуваних ними задач.

З вищесказаного можна зробити висновок, що правильний і повноцінний захист периметру сучасних корпоративних мереж дозволяє домогтися захищеності доступу внутрішніх користувачів в зовнішній мережі, надає доступ з зовнішніх мереж до публічних корпоративних ресурсів, захищає від мережових атак на корпоративні ресурси, організовує системи електронної комерції, створює єдину точку антивірусної і антиспам фільтрації, запобігає витоку конфіденційної інформації, проводить моніторинг та аналіз подій інформаційної безпеки.

1.2 Захист периметра мережі

Однією з технічних заходів організації інформаційної безпеки є побудова периметра безпеки. Організація зовнішнього периметра безпеки - побудова системи захисту корпоративної мережі від загроз, що виходять від глобальних мереж. Організація внутрішнього периметра безпеки - побудова системи захисту корпоративної мережі від загроз, що виходять від користувачів.

Забезпечення безпеки корпоративної мережі, впровадження програмно-апаратного комплексу контролю доступу до корпоративної та глобальної мережі дозволить значно знизити рівень загрози. Рішення від світових лідерів Cisco, Juniper Networks, Microsoft відмінно зарекомендували себе на ринку. Побудова периметра безпеки мережі є найважливішим компонентом якісної системи забезпечення інформаційної безпеки на підприємстві.

Число інцидентів, пов'язаних з інформаційною безпекою, за даними провідних аналітичних агентств, постійно зростає. Фахівці, відповідальні за захист інформації, відзначають зростаючу активність зовнішніх зловмисників, що використовують останні розробки в області нападу, що намагаються проникнути в корпоративні мережі.

Найбільш поширені загрози для інформаційних ресурсів організації це:

1. Мережеві атаки, спрямовані на недоступність інформаційних ресурсів (Web-серверів, сервісів електронної пошти і т.д.) — атаки класу DoS і DDoS;
2. Компрометація інформаційних ресурсів та ескалація привілеїв — як з боку інсайдерів, так і зовнішніх зловмисників, як з метою використання ваших ресурсів, так і з метою нанесення шкоди;
3. Дії шкідливого програмного коду (віруси, мережеві черв'яки, трояни, програми-шпигуни і т.д.);

4. Витік конфіденційної інформації і викрадення даних — як через мережу (e-mail, FTP, web тощо), так і через зовнішні носії;
5. Різні мережеві атаки на додатки;
6. Захист периметра інформаційної системи є обов'язковим елементом системи інформаційної безпеки організації.

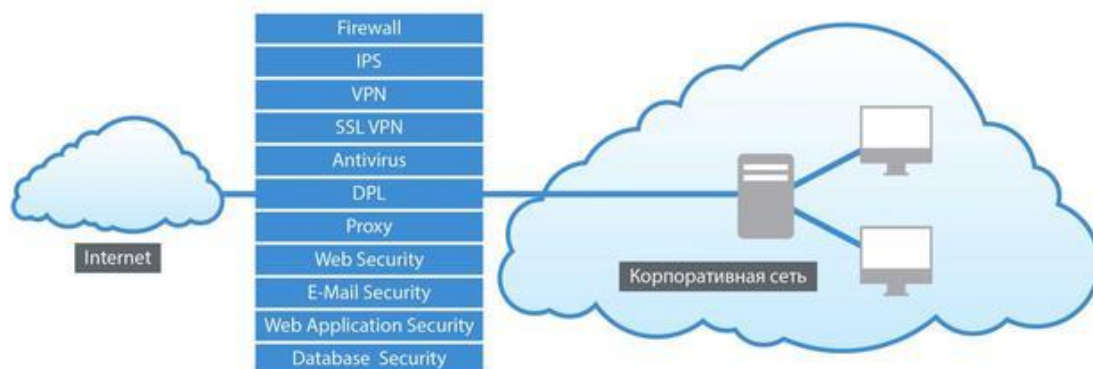


Рис.1.1 - Забезпечення безпеки корпоративної мережі

Для мінімізації загроз інформаційній безпеці необхідне впровадження багаторівневої системи захисту інформації. Першим рівнем забезпечення інформаційної безпеки, яка блокує несанкціонований доступ хакерів в корпоративну мережу, є міжмережевий екран.

Серед функцій міжмережевого екрану є:

1. Фільтрація пакетів. Це одна з трьох загальновідомих функцій мережевого екрану. У цьому випадку виконуються зовсім прості функції (фактично як у спеціалізованого маршрутизатора), які полягають у перегляді заголовка кожного пакету та перевірки IP адреси та порта на правильність. Наприклад, пакет, який передається в Інтернет, але має локальну адресу призначення, блокується. Ця функція присутня у всіх сучасних мережевих екранах і відрізняється високою швидкістю та відсутністю необхідності діалогу з користувачем.
2. Проксі сервер. Це друга загальновідома функція. Різниця між проксі сервером та фільтрацією пакетів полягає в тому, що проксі сервер вимагає, щоб всі сеанси зв'язку встановлювались через нього, а

не напряму. Отримавши дані, проксі сервер відсилає їх далі від свого імені, а отримавши відповідь, пересилає її потрібному комп'ютеру внутрішньої мережі. Як можна здогадатись, продуктивність не є такою ж високою, як при фільтрації пакетів, але достатньою, оскільки відбувається тільки заміна заголовка пакета. Головною перевагою проксі сервера є те, що він приховує справжні адреси ваших комп'ютерів, замінюючи їх на свою. Це унеможливорює атаку на конкретний комп'ютер в підмережі.

3. Проксі сервер програм. Це третя функція. Цей різновид проксі сервера відрізняється “розумінням” протоколів програм, що ведуть передачу даних. Хороший приклад такого сервера –поштовий сервер. Проксі сервер програм може проводити ідентифікацію користувачів, а не тільки покладатись на IP адресу, в деяких випадках можливе виявлення передавання вірусів та іншого шкідливого коду. Це все звичайно потребує набагато більших обчислювальних потужностей, а також в більшості випадків вимагає значного перенастроювання робочих станцій, через що втрачається прозорість роботи мережевого екрану.
4. Кешування даних. Це не є традиційною функцією мережевих екранів, але на даний час стає надзвичайно популярною властивістю. Ідея полягає у тому, що, оскільки всі дані проходять через мережевий екран, він може зберігати найбільш популярну інформацію і при наступному звертанні за нею видати її зі свого кешу.
5. Статистика та повідомлення. Важливою властивістю мережевого екрану є ведення історії всіх мережевих з'єднань, а також вивід повідомлень про атаки на мережу чи комп'ютер. Історія з'єднань допомагає правильно настроїти мережевий екран, щоб комп'ютер був

одночасно захищений від нападів і відкритий для доступу авторизованим користувачам.

6. Керування. Для персональних мережевих екранів основна характеристика – зручність їхнього налаштування. Керування міжмережними екранами здебільшого відбувається дистанційно (використовуючи HTML інтерфейс чи інший), що потребує впевненості в надійності авторизації та каналу зв'язку.

Основним функціоналом міжмережевих екранів є розмежування і контроль доступу, трансляція адрес, приховування топології вашої обчислювальної мережі від зовнішнього світу і організація нейтральних зон. Однак необхідно відзначити, що міжмережеві екрани головним чином здійснюють фільтрацію і аналіз трафіку на третьому і четвертому рівнях моделі OSI, і лише обмежено — на більш високих рівнях.

Для моніторингу та боротьби з атаками і несанкціонованою мережевою активністю рекомендується використовувати спеціалізовані продукти мережевої системи виявлення та запобігання атак (IDS / IPS). Дані системи дозволяють відстежити і зареєструвати спроби несанкціонованої мережевої активності і опціонально блокувати атаки в режимі реального часу[1].

Підтримка безперебійної роботи мережі і відсутність інцидентів - завдання будь-якого системного адміністратора. Здавалося б, це просто, але на ділі потрібна складна багаторівнева система захисту від небезпек, що підстерігають конфіденційні данні компанії в умовах одночасного доступу до них людей різної кваліфікації.

Навіть незначний пролом в системі безпеки може сильно нашкодити компанії: шалений троянець або, того гірше, крадіжка даних співробітниками дійсно здатні заподіяти компанії цілком відчутний збиток, виражений в грошових одиницях.

Наприклад, в квітні 2006 року витік інформації стався з військової компанії Lockheed Martin. Вона звинуватила в промисловому шпигунстві свого прямого конкурента. Три інсайдера з Lockheed вкрали результати проекту з розробки системи тренувань пілотів ВПС США і продали її конкуренту за велику суму. В результаті їх дій під загрозу було поставлено мільярдний контракт.

Звичайно, наведений випадок в абсолютному вираженні не можна порівняти зі шкодою від троянської програми, випадково підхопленою недбайливим співробітником. У відсотковому ж відношенні і для корпорації з мільярдними оборотами, і для невеликої організації, що працює в секторі середнього і малого бізнесу, будь-яка з проблем безпеки мережі може обернутися неприємними наслідками різного масштабу[2].

Щоб захистити фортецю, необхідно в першу чергу зміцнити її стіни і тільки потім озброювати жителів. У випадку з мережею компанії ситуація аналогічна: спочатку потрібно визначити, що підлягає першочерговому захисту. Периметр мережі, що складається з ключових вузлів захисту, - це саме ті стіни, які підлягають зміцненню.

Найважливіші форпости корпоративної безпеки різноманітні - в це поняття входить і сервер, завідувач електронною кореспонденцією, і брандмауер, і робочі станції. Критично важливі вузли варто об'єднати в дві групи: привабливі з точки зору зловмисника і схильні до атак інсайдерів - недоброзичливців, присутніх в компанії[Зос].

1.3 Міжмережевий екран

Міжмережевий екран (Firewall, брандмауер) призначений для захисту пристроїв локальної мережі від атак ззовні

Міжмережевий екран називають локальний або функціонально розподілений програмний (програмно—апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему і/або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall (англ. вогняна стіна).

Міжмережевий екран служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, впливаючі вікна та інше, не надсилати іншим «чужим» серверам інформацію про ваш комп'ютер, робить даремною роботу програм—троянів і засобів віддаленого адміністрування.

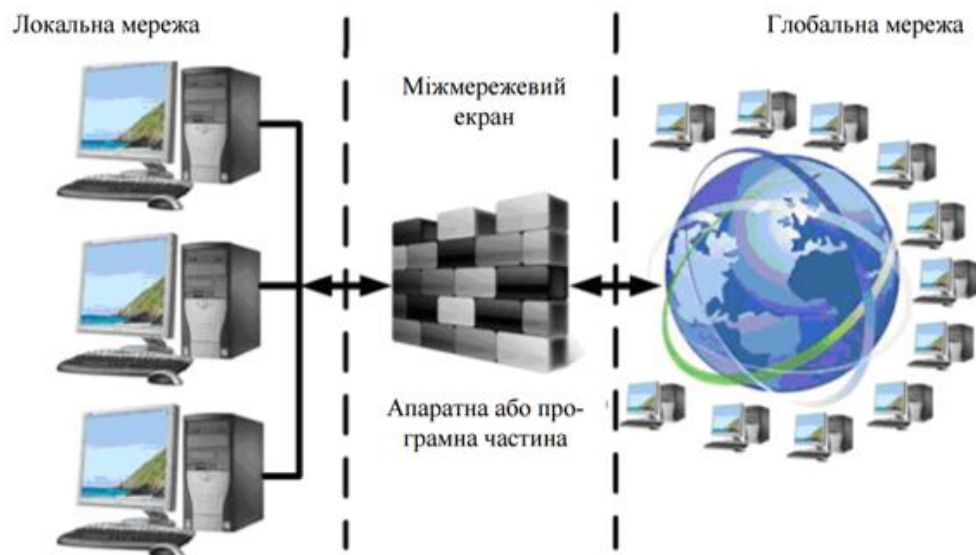


Рис.2.1. – Міжмережевий екран

Робота міжмережевого екрану полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від

результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує. Ефективність роботи міжмережевого екрану, що працює під управлінням Windows, зумовлена тим, що він повністю заміщує реалізований стек протоколів TCP/IP, і тому порушення його роботи хакерами з допомогою спотворення протоколів зовнішньої мережі є неможливим[4].

Міжмережеві екрани виконують такі функції:

- фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;
- багатоетапну ідентифікацію запитів, що надходять в мережу;
- перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
- реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
- контроль цілісності програмного забезпечення і даних;
- економію адресного простору мережі;
- приховування IP—адреси внутрішніх серверів з метою захисту від хакерів.

Розрізняють два типи міжмережевого екрану: апаратний і програмний. Апаратний являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер. Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запуснений на кінцевому комп'ютері або шлюзі. Найбільшого розповсюдження отримав програмний тип реалізації мережевого екрану.

Міжмережеві екрани можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних

пакетів по IP-адресам (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання).

На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь—яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Міжмережевий екран розділяють на три види:

- пакетні фільтри (packet filter);
- сервера прикладного рівня (application gateways);
- сервера рівня з'єднання (circuit gateways).

Міжмережевий екран з пакетними фільтрами приймають рішення про те чи пропускати пакет, чи відкинути, переглядаючи IP-адреси, прапорці або номери TCP портів в заголовку цього пакета. IP-адреса та номер порту – це інформація мережевого і транспортного рівнів. Водночас, пакетні фільтри використовують також інформацію прикладного рівня, тобто всі стандартні сервіси в TCP/IP асоціюються з певним номером порту.

Переваги пакетних фільтрів: відносно невисока вартість; гнучкість у визначенні правил фільтрації; невелика затримка при проходженні пакетів.

Недоліки: локальна мережа стає видима з мережі Internet; правила фільтрації пакетів важкі в описі, потрібні дуже хороші знання технологій TCP і UDP; при порушенні працездатності міжмережевого екрану всі комп'ютери стають повністю незахищеними або недоступними; аутентифікацію з використанням IP—адреси можна обдурити використанням IP—спуфінга (атакуюча система видає себе за іншу, використовуючи її IP—адресу); відсутня аутентифікація на рівні користувача[5].

Міжмережевий екран прикладного рівня використовують сервера конкретних сервісів – TELNET, FTP і т.д. Proxy—server, що відносяться до даного сервісу, запускаються на екрані та пропускають через себе весь трафік. Таким чином, між клієнтом і сервером утворюються два з'єднання: від клієнта до міжмережевого екрану і від нього до місця призначення. Використання серверів прикладного рівня дозволяє вирішити важливе завдання— приховати від зовнішніх користувачів структуру локальної мережі, включаючи інформацію в заголовках поштових пакетів або служби доменних імен (DNS).

Переваги серверів прикладного рівня: локальна мережа стає невидимою з мережі Internet; при порушенні працездатності міжмережевого екрану пакети перестають проходити через нього, тим самим не виникає загрози для захисту локальної мережі; захист серверів прикладного рівня дозволяє здійснювати велику кількість додаткових перевірок, знижуючи тим самим імовірність злому з використанням дірок у програмному забезпеченні; за допомогою аутентифікації на рівні користувача може бути реалізована система негайного попередження про спробу злому.

Недоліки: більш висока вартість, продуктивність нижча ніж у пакетних фільтрів; неможливість використання протоколів RPC і UDP.

Сервер рівня з'єднання схожий на міжмережевий екран прикладного рівня тим, що вони обидва є серверами—посередниками. Користувач утворює з'єднання з певним портом на екрані, після чого останній з'єднується з місцем призначення по іншу сторону від міжмережевого екрану. Під час сеансу цей канал зв'язку копіює байти в обох напрямках. Як правило, пункт призначення задається заздалегідь, у той час як джерел може бути багато. Використовуючи різні порти, можна створювати різні конфігурації. Такий тип сервера дозволяє створювати канал зв'язку для

будь—якого сервісу, що базується на ТСП, здійснювати контроль доступу до цього сервісу, збір статистики щодо його використання.

Головна відмінність між ними полягає в тому, що міжмережевий екран прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, міжмережеві екрани рівня з'єднання обслуговують велику кількість протоколів. Але попри все вони не можуть повністю гарантувати безпеку даних у локальних комп'ютерних мережах, тому що не можуть запобігти виникненню таких проблем як: віруси, що поширюються електронною поштою та фішингове шахрайство[6].

1.4 Cisco ASA

Еволюція глобальних робочих ресурсів і швидке поширення додатків і пристроїв привели до ускладнення мереж, вимагаючи від адміністраторів міжмережевих екранів вибору: дозволити доступ в будь-який час, з будь-якого місця і з будь-якого пристрою, що потрібно для підвищення продуктивності співробітників, або підтримувати певний рівень безпеки для захисту бізнесу.

Більшість міжмережевих екранів нездатні забезпечити ступінь прозорості, необхідну для прийняття обґрунтованих рішень в області безпеки, що змушує організації вибирати між можливостями персоналу і безпекою мережі.

Пристрій забезпечення безпеки з урахуванням контексту Cisco ASA CX вирішує цю проблему, розширюючи можливості платформи ASA за рахунок безпрецедентної прозорості та функцій контролю, що дозволяє підприємствам, нарешті, сказати «так» додаткам, пристроям та глобальним робочим ресурсам, що розвиваються.

Cisco ASA (Adaptive Security Appliance) - серія апаратних міжмережевих екранів, розроблених компанією Cisco Systems, вона є спадкоємцем наступних лінійок пристроїв:

- міжмережевих екранів Cisco PIX;
- Систем виявлення вторгнень Cisco IPS 4200;
- VPN-концентраторів Cisco VPN 3000.

Так як і PIX, ASA засновані на процесорах x86. Починаючи з версії 7.0 PIX і ASA використовують однакові образи операційної системи (але функціональність залежить від того, на якому пристрої вона запущена).

Функціональність залежить від типу ліцензії, який визначається введеним серійним номером. Інтерфейс командного рядка нагадує (але не повторює) інтерфейс Cisco IOS. Управляти пристроєм можна через telnet, SSH, веб-інтерфейс або за допомогою програми ASDM.



Рис.1.3. – Маршрутизатор Cisco ASA

Особливості та можливості:

- Міжмережне екранування з урахуванням стану з'єднань;
- Глибокий аналіз протоколів прикладного рівня;
- Трансляція мережесовіт адрес;

- IPsec VPN;
- SSL VPN (підключення до мережі через веб-інтерфейс);
- Протоколи динамічної маршрутизації (RIP, EIGRP, OSPF).
- ASA не підтримують протоколи тунелювання (такі, як GRE) і policy-based routing.

Програмне забезпечення Cisco Adaptive Security Appliance (ASA) є основною операційною системою для сімейства Cisco ASA. Він надає можливості брандмауера корпоративного класу для пристроїв ASA у безлічі форм-факторів - автономних пристроїв, блейдів та віртуальних пристроїв - для будь-якого розподіленого мережевого середовища[7].

ASA Software також інтегрується з іншими важливими технологіями безпеки, щоб забезпечити комплексні рішення, які відповідають потребам безпеки.

Програмне забезпечення Cisco ASA також підтримує стандарти шифрування наступного покоління, включаючи набір криптографічних алгоритмів Suite B. Він також інтегрується з рішенням Cisco Cloud Web Security, щоб забезпечити захист від загроз веб-класу.

Переваги Cisco ASA

Для початку будуть розібрані можливості Cisco ASA. Подані міжмережеві екрани призначені для забезпечення безпечної роботи невеликих офісів і організацій у вигляді філій. Для цього в них є:

- WSE, тобто функції інтернет-безпеки, які обмежують роботу в інтернеті і різних додатків;
- AVC - прозоре контролювання додатків, які регулюють особливе поведінки, обмежене дозволеними мікропріложеннями;
- незвичайні сервіси міжмережевих екранів, які є яскравими представниками наступного покоління;

- SIO - система, що забезпечує захист мережі, максимально різнопланову і глибоку, заснована на програмних забезпеченнях і хмарних технологіях;
- IPS - являє собою високоефективну систему запобігання вторгнень, що працює на основі технології глобальної кореляції;
- можливість використовувати практично постійний віддалений доступ і високопродуктивну мережу VPN.

Недоліки Cisco ASA

Йтиметься не лише про те, що потрібно періодична настройка firewall Cisco ASA. Існують більш істотні недоліки в роботі подаються міжмережевих екранів. Зокрема, Cisco ASA не підтримує надлишкові маршрути, хоча сама по собі вільно працює з такими протоколами, як RIPv1,2, OSPF, EIGRP. Тому в таблиці маршрутизації завжди можна побачити тільки один маршрут.

В Cisco ASA є route-map, яка часто використовується на маршрутизаторах, але тут вона виконує роль редистрибутива маршрутів.

Ще один критичний момент - відсутність віртуальних інтерфейсів, тому з Cisco ASA не вийде підтримувати тунелі GRE. З цієї причини стають недоступними зручні технології по типу DMVPN.

Cisco ASA блокує програму для використання динамічного перемикавання портів і протоколів (hopping), наприклад Skype і інші програми з одноранговим з'єднанням (P2P), що забезпечує більш ефективний захист в поєднанні з меншою кількістю встановлюваних політик.

Крім цього, пристрій ASA використовує більш ефективніший способів контролю над використанням соціальних мереж, ніж в інших міжмережевих екранах нового покоління. Він розпізнає більше 1 000 додатків і 75 000 мікрододатків, що дозволяє організаціям забезпечити доступ до конкретних компонентів програми (наприклад, Facebook для використання в ділових

цілях), одночасно забороняючи інші компоненти (гри Facebook). Встановлювані політики можуть передбачати управління як індивідуальним, так і груповим доступом до цих компонентів додатків[8].

Cisco ASA дозволяє бачити конкретний тип пристрою, який намагається отримати доступ до мережі, що працює на ньому, його операційну систему а також його місце розташування. Володіючи достовірною інформацією про те, які пристрої намагаються отримати доступ до мережевих ресурсів, адміністратори мають можливість впевнено дозволити доступ широкого кола пристроїв, в той же час підтримуючи високий рівень захисту мережі та її керованості.

Cisco ASA - це поєднання передових технологій забезпечення мережевої безпеки Cisco, інтегрованих в надійну апаратну платформу. Таке рішення протидіє мінливим загрозам безпеки і контролює трафік компанії.

Переваги для бізнесу:

Випуск брандмауера серії Cisco ASA 5500 забезпечує послуги безпеки та підключення, які допомагають вашому бізнесу:

Контрольований доступ до корпоративних ресурсів - запобігає несанкціонованому доступу до програм або інформаційних ресурсів, надаючи компаніям чіткий контроль за ідентифікацією чи мережею. Інтегрується з популярними службами автентифікації користувачів, такими як Microsoft Active Directory, полегшений протокол доступу до каталогу (LDAP), Kerberos та RSA SecurID[9].

Безпечне розгортання нових програм – дозволяє компаніям безпечно розгортати нові програми, надаючи розширені послуги захисту рівня додатків для широкого кола популярних програм, включаючи веб-програми, електронну пошту, передачу голосу через IP (VoIP), відео та мультимедіа додатків. Приховує адреси корпоративних мереж від Інтернету для додаткового рівня захисту від атак.

Захищений віддалений доступ до корпоративної мережі - забезпечує як SSL, так і IPsec методи підключення VPN, захищених від загроз, до віддалених сайтів, ділових партнерів та мобільних працівників.

Стійкість бізнесу - запобігає порушенню критично важливих додатків та служб через порушення безпеки шляхом впровадження брандмауера світового класу, VPN та мережевих технологій.

Можливості брандмауера серії Cisco ASA 5500 включають:

Найбільш довірена та розгорнута технологія брандмауера, спираючись на перевірені ринком можливості сімейства захисних пристроїв Cisco PIX®, серія Cisco ASA 5500 надає широкий спектр послуг для захисту сучасних мережевих середовищ. Гнучкі можливості політики запобігають несанкціонованому доступу до мережевих ресурсів або важливої корпоративної інформації. Розширені можливості управління програмами допомагають компаніям ефективно контролювати використання однорангового обміну файлами, обміну миттєвими повідомленнями та іншими некорпоративними програмами, таким чином покращуючи продуктивність праці співробітників та зменшуючи витрачену пропускну здатність Інтернету.

Захищений VPN-побудований на основі перевірених ринком можливостей VPN концентратора серії Cisco VPN 3000, брандмауер серії Cisco ASA 5500 забезпечує надійний доступ до сайту та віддаленого користувача до корпоративних мереж та служб. Це рішення пропонує компаніям максимальну гнучкість для безпечного підключення, поєднуючи підтримку рівнів захищених сокетів (SSL) та IP Security (IPsec) VPN в єдине, найкраще у своєму класі рішення. Використовуючи послуги, пропоновані виданням брандмауера Cisco ASA 5500 Series, компанії можуть застосовувати політику безпеки та мережі на основі ідентифікації до всього мережевого трафіку, дозволяючи таким чином підприємствам

пристосовувати привілеї доступу для кожної групи співробітників, підрядників та ділових партнерів.

Випуск брандмауера Cisco ASA серії 5500 може адаптуватися до змін бізнесу завдяки своєму унікальному модульному дизайну. Підприємства можуть легко розширити кількість пропонованих служб безпеки, додавши високопродуктивний спеціально створений модуль служб безпеки Cisco ASA серії 5500, такий як Модуль розширених служб контролю та запобігання (AIP SSM) для вдосконалених служб запобігання проникненню або Модуль служб безпеки та контролю вмісту (CSC SSM) для вдосконалених антивірусів, антиспаму та інших служб безпеки вмісту.

Інтелектуальна мережева інтеграція та підвищення стійкості корпоративного класу на основі більш ніж 20-річного лідерства та інновацій у роботі Cisco, брандмауер серії Cisco ASA 5500 надає широкий спектр інтелектуальних мережевих послуг для безперебійної інтеграції в сучасні різноманітні мережеві середовища. Підприємства можуть максимізувати час безперебійної роботи та пропускну здатність, скориставшись багатьма послугами щодо стійкості та масштабованості, які може запропонувати це рішення, такими як Active / Active висока доступність, "оновлення програмного забезпечення з нульовим простоем" та інтегрованою кластеризацією VPN та балансуванням навантаження.

Простота розгортання та управління - набір управління та моніторингу Cisco забезпечує широкомасштабне розгортання та експлуатацію брандмауера серії Cisco ASA 5500. Cisco пропонує комплексне рішення, що охоплює управління та моніторинг. Також до цього рішення входить Cisco Adaptive Security Device Manager Manager (ASDM), який забезпечує потужний, але простий у використанні браузерний інтерфейс управління та моніторингу для окремих пристроїв безпеки[10].

Висновки до першого розділу

В даному розділі було розглянуто теоретичні відомості про захист комп'ютерної мережі та найбільш поширені загрози для інформаційних ресурсів організації. Було детально проаналізовано його функції та застосування.

Також було з'ясувано його застосування та основні функції та розглянули два типи міжмережевого екрану: апаратний і програмний та описали що вони являють собою.

Потім було розглянуто теоретичні відомості про міжмережевий екран та детальну інформацію про його використання.

Міжмережевий екран розділяють на три види:

- пакетні фільтри (packet filter);
- сервера прикладного рівня (application gateways);
- сервера рівня з'єднання (circuit gateways).

Виявлено переваги та недоліки кожного з видів мережевого екрану, В кінці підрозділу було визначено головні відмінності між видами міжмережевого екрану.

В останньому пункті розділу було розглянуто Cisco ASA. А саме про програмне забезпечення Cisco Adaptive Security Appliance (ASA), що є основною операційною системою для сімейства Cisco ASA, до того ж вона підтримує стандарти шифрування наступного покоління. А також виявлено основні переваги та недоліки користування Cisco ASA.

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

2.1. Визначення варіантів використання

Програмна підсистема периметрового захисту комп'ютерної мережі має певні цілі. Найголовнішою ціллю реалізації даної програми є, передусім, поглиблене вивчення роботи з комп'ютерними мережами, основні принципи роботи, способи реалізації та певні особливості. Перед нами постає реальна задача створення надійного захисту мережі організації. Реалізуючи програму буде можливим практично дослідити роботу периметрового захисту та завдяки дослідженню зробити певні висновки.

Варіантів використання периметрового захисту мережі безліч адже з кожним днем зростає кількість зломисників які намагаються викрасти інформацію заради власної вигоди. Кожна організація прагне захиститися від несанкціонованого доступу до їх серверів баз даних та інших внутрішніх структур.

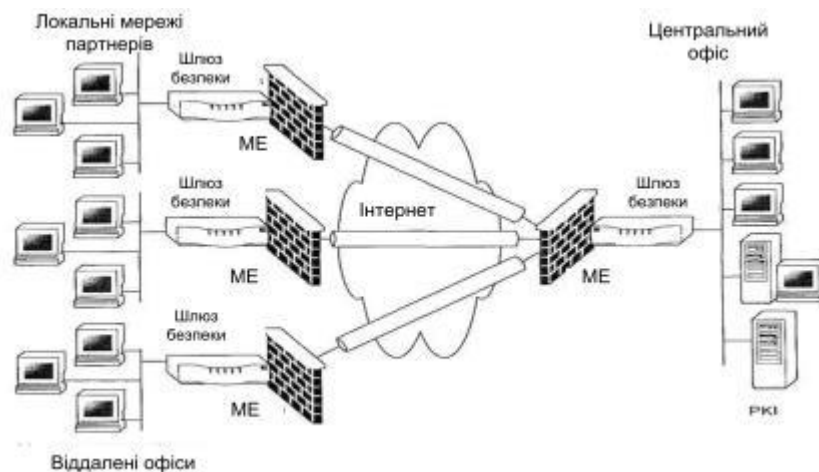


Рис.2.1. Захист мережі міжмережевими екранами

Можна виділити три варіанти вирішення проблеми.

Перший – побудувати у внутрішній мережі ще одну, створену із міркувань засобів безпеки. Багато виробників засобів захисту надають пропозиції для даного варіанту, включаючи в нього багато IPS сенсорів та мережевих екранів які будуть контролювати внутрішні мережеві потоки та

виявляти шкідливий код та заборонені додатки. Але такий варіант стикається з рядом складностей.

Не завжди існуючий дизайн мережі дозволяє реалізувати таке підключення. Мережа може працювати на швидкостях недоступних засобам безпеки. Або організація активно використовує віртуалізацію і засоби захисту не можуть ефективно контролювати трафік що не виходить за межі фізичного серверу.

Другий часто рекомендований варіант – встановлення засобів захисту на сервери та робочі станції, виявляючи і блокуючи несанкціоновану активність користувачів чи проти користувачів. Це правильно, але виникає питання що робити з рештою пристроїв, як то принтери, сканери, промислові контролери, ІР-системи відеоспостереження і контролю доступу. За ними користувачі не працюють (та їх не можна аутентифікувати традиційними методами) і на них не можна встановити ні антивірус ні інші засоби захисту.

Так склалось що часто ці пристрої, а їх може бути навіть більше ніж комп'ютерів користувачів, стають мішенню для зловмисників чи площею для подальшого просування по внутрішній мережі організації. А наявність обхідних каналів у вигляді незахищеного WiFi чи модему призведуть до того, що конфіденційні дані можуть витекти минаючи засоби захисту корпоративного периметра.

Третій варіант – перенести рішення на те у що вже інвестовано кошти, а саме на мережеву інфраструктуру. Маршрутизатори, комутатори і точки доступу, які можуть не лише передавати трафік з точки А в точку Б але й ефективно захищати цей трафік, виконуючи одночасно роль сенсору, захисної стіни та інструменту реагування на інциденти безпеки. Адже по суті кожен мережевий пристрій представляє собою сенсор системи захисту мережі – трафік проходить через нього, ідентифікується та класифікується, направляється в точку призначення.

Можна поставити питання розгляду кожного з цих пунктів з точки зору політики інформаційної безпеки. Ідентифікувати додаток на рівні

маршрутизатора чи комутатора, не доводячи трафік до міжмережевих екранів на периметрі. Власне ці можливості надає Cisco в своїй мережевій інфраструктурі, виступаючи не лише як сенсор системи захисту (Network as a Sensor), але і як система захисту (Network as a Enforcer) і система розслідування інцидентів ІБ (Інформаційної Безпеки).

В якості вихідних даних використовується протокол Netflow, який дає нам всі потрібні дані про що проходить трафіку, відповідають на всі важливі для політики ІБ питання – хто, що, коли, куди/звідки, як. За допомогою NetFlow можна класифікувати трафік, розпізнавати додатки, ідентифікувати атаки і витоки, виявляти використання недозволених додатків або появу сторонніх вузлів, проводити розслідування інцидентів та ідентифікувати точку входу зловмисників в мережу.

2.2 Розробка топології комп'ютерної мережі

Для проектування мережі було використано трирівневу ієрархічну модель мережі, яка містить в собі:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Проект даної мережі представлено на рисунку 2.2.

Для забезпечення продуктивності роботи мережі між рівнями розподілу та доступу використовуються високошвидкісні лінії зв'язку Gigabit Ethernet. Кінцеві вузли під'єднані до комутаційного обладнання за допомогою ліній Fast Ethernet.

В загальному у мережі використано 3 маршрутизатори та 7 комутаторів. Мережа складається з 4 підмереж.

Далі розглянемо детальніше кожен підмережу.

Від маршрутизатора R_1_1_1 виходить підмережа А, рис. 2.3.

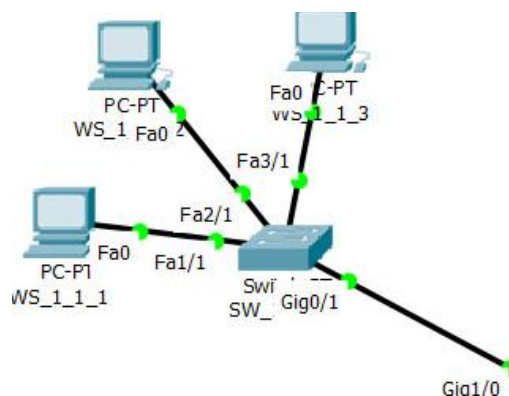


Рис. 2.4. Підмережа А

Підмережа А містить 1 комутатор, до якого можливо підключити 22 ПК. Маршрутизатор R_1_1_1 з'єднаний з комутатором SW_1_1_1 за допомогою витої пари Gigabit Ethernet.

Всі з'єднання в підмережі виконанні за допомогою витої пари технології Fast Ethernet.

Від маршрутизатора R_1_1_2 виходить під мережа В рис. 2.4.

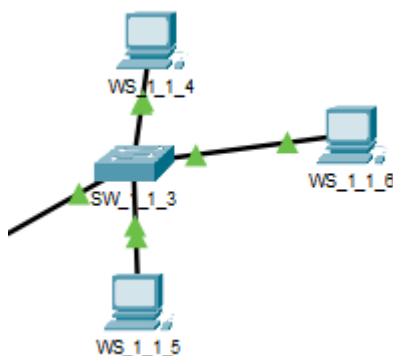


Рис. 2.5. Підмережа В

Підмережа В також містить 1 комутатор, до якого можливо підключити до 22 ПК.

ПК під'єднані до комутаторів за допомогою витोї пари технології FastEthernet.

Комутатори з'єднані з маршрутизатором за допомогою потужних каналів зв'язку витої пари Gigabit Ethernet.

Від маршрутизатора R_1_1_3 виходить підмережа С рис. 2.5.

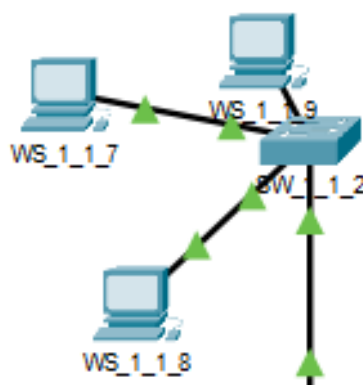


Рис. 2.6. Підмережа С

Підмережа С містить 1 комутатор, до якого можливо підключити 22 ПК. Всі з'єднання в підмережі були виконанні за допомогою витої пари Fast Ethernet.

Рівень розподілу представляє собою набір з трьох міжмережевих екранів Cisco ASA 5506, що під'єднані до ядра мережі. З'єднання з ядром мережі виконано за допомогою каналів зв'язку витої пари Gigabit Ethernet. Маршрутизатори рівня ядра були з'єднані між собою за допомогою каналів зв'язку Serial.

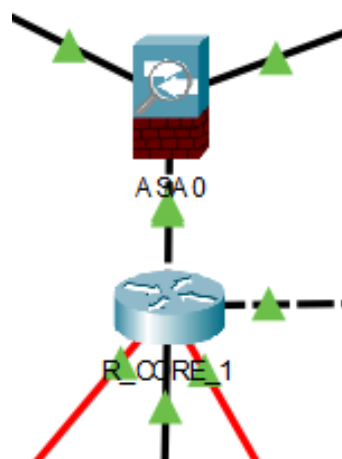


Рис. 2.7. Рівень розподілу ASA 0

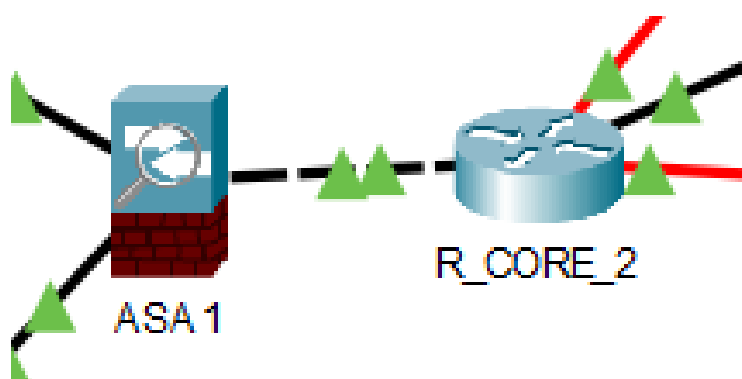


Рис. 2.8. Рівень розподілу ASA 1

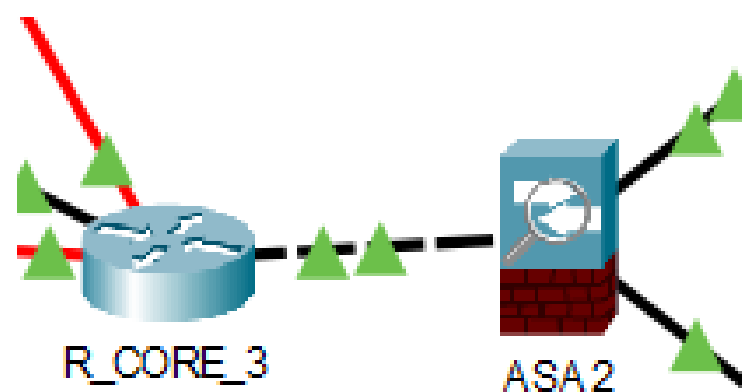


Рис. 2.9. Рівень розподілу ASA 2

2.3 Розробка схеми адресації пристроїв

Після того, як було визначено топологію комп'ютерної мережі, необхідно розробити схему адресації комп'ютерної мережі.

Далі наведені таблиці, в яких описано підмережі та їх адресація, а саме: діапазони, маски, префікси, зарезервовані адреси.

Для рівня ядра мережі розподіл адрес по діапазону проводився таким чином, щоб використати мінімальну кількість IP-адрес, забезпечивши при цьому потреби підключених вузлів. Розрахунок приведено нижче:

R_CORE_1 – R_CORE_2 – 200.1.1.8 /30

R_CORE_2 – R_CORE_3 – 200.1.1.16 /30

R_CORE_3 – R_CORE_1 – 200.1.1.12 /30

Таблиця 2.1

Адресація підмережі O

<i>Призначення</i>	<i>IP-адреса</i>
Адреса мережі	200.1.1.0
Маска мережі	255.255.255.252 /30
Інвертована маска	0.0.0.7
Мінімальна адреса	200.1.1.1
Максимальна адреса	200.1.1.6
Широкомовна адреса	200.1.1.7

Для зв'язку між рівнем ядра та рівнем розподілу було використано 3 підмережі:

Таблиця 2.2

Адресація підмережі A

<i>Призначення</i>	<i>IP-адреса</i>
Адреса мережі	192.1.1.0
Маска мережі	255.255.255.0 /24

Інвертована маска	0.0.0.255
Мінімальна адреса	192.1.1.1
Максимальна адреса	192.1.1.254
Широкомовна адреса	192.1.1.255

Таблиця 2.3

Адресація підмережі В

<i>Призначення</i>	<i>IP-адреса</i>
Адреса мережі	193.1.1.0
Маска мережі	255.255.255.248 /29
Інвертована маска	0.0.0.7
Мінімальна адреса	193.1.1.1
Максимальна адреса	193.1.1.6
Широкомовна адреса	193.1.1.7

Таблиця 2.4

Адресація підмережі С

<i>Призначення</i>	<i>IP-адреса</i>
Адреса мережі	194.1.1.0
Маска мережі	255.255.255.248 /29
Інвертована маска	0.0.0.7
Мінімальна адреса	194.1.1.1
Максимальна адреса	194.1.1.6
Широкомовна адреса	194.1.1.7

Таблиця 2.5

Адресація підмережі SER

<i>Призначення</i>	<i>IP-адреса</i>
Адреса мережі	200.1.1.20
Маска мережі	255.255.255.252 /30

Інвертована маска	0.0.0.3
Мінімальна адреса	200.1.1.21
Максимальна адреса	200.1.1.22
Широкомовна адреса	200.1.1.23
Шлюз по замовчуванню	200.1.1.22

Висновки до другого розділу

В даному розділі було розглянено варіанти використання данної переиметрованої мережі а також виділено три основні методи захисту себе та орзганізації від несанкціонованого доступу третім особам.

Спроектовано топологію комп'ютерної мережі. Було розглянуто підмережі, пристрої, використані у них, з'єднання між пристроями, а також було визначено основні складові підмережі. Ми визначили кількість підмереж та їх призначення.

Також було розроблено адресацію даної глобальної комп'ютерної мережі. Було розглянуто кожну підмережу і пристрій окремо, а саме їх: інтерфейс, ір- адреса, маска та префікс, визначено ІР-адреси для маршрутизаторів, детально описано адресацію для кожної з підмереж.

РОЗДІЛ 3. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Вибір обладнання для побудови мережі

При виборі моделі маршрутизатора необхідно враховувати як він маршрутизує пакети в складній мережі з різними видами топологій.

Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

На рівні розподілу нам потрібний маршрутизатор який би підтримував технологію FastEthernet та протокол OSPF та EIGRP, та містив додаткові функції налаштування. Маршрутизатор CiscoSystems CISCO ASA 5506-X рисунок 3.1, найбільш оптимальний варіант для великої мережі організації.



Рис.3.1. Маршрутизатор Cisco ASA 5506-X

Серія маршрутизаторів з інтегрованими сервісами Cisco ASA 5506 відповідає вимогам сучасних офісів, володіючи гнучкістю конструкції для впровадження нових додатків.

Модульна архітектура призначена для підтримки зростаючих вимог клієнтів, збільшення пропускнуєї спроможності і установки модулів для розподілу потужності.



Рис.3.2. Маршрутизатор Cisco ASA 5506

Можливості пристрою:

Звичайно, знати що таке обладнання Cisco це добре, але необхідно також знати і всі його допустимі можливості. Сенс даних екранів полягає в захисті від вірусних або дрібних гіператак, які відбуваються з метою крадіжки фінансів, будь-яких даних.

Також однією з додаткових можливостей є підтримка віддалених підключень. Ця функція відповідає за розширення радіусу можливого підключення точка-точка, якщо сказати простою мовою, то його використовують для збільшення дальності сигналу при підключенні по Wi-Fi. До того ж присутній моніторинг вірусних пакетів, підвищення продуктивності мережі, а також багато інших функцій.

Технічні характеристики обладнання:

Пристрій моделі 5506 в порівнянні зі своїми попередниками - є більш міцною в корпусі, має два високошвидкісних просторових потоку з метою обслуговування клієнтів в своєму діапазоні. Можливий монтаж на стіні, столі і стійці. Що стосується начинки, то тут трохи простіше: 4 гігабайти на жорсткому диску і 8 гігабайт на флеш-пам'яті.

Також це обладнання обладнано вісьмома мережевими інтерфейсами введення-виведення і багато інших елементів, які немає сенсу описувати.

Переваги використання:

Що ж стосується переваг то тут все просто. Цей прилад досить недорогий в порівнянні з його суперниками, але не поступається рівнем захисту і забезпечення безпеки інформації від вірусних та гіператак. Також кількість споживання електроенергії не велика, а якщо розглядати примхливість до навколишнього середовища, то і тут все добре.

Серія Cisco Firepower 5500 - це сімейство з шести платформ безпеки NGFW, орієнтованих на загрози, які забезпечують стійкість бізнесу завдяки чудовій системі захисту від загроз. Він пропонує виняткову стійку роботу, коли ввімкнені розширені функції загроз.

Платформи серії ASA 5500 можуть запускати як брандмауер Cisco ASA, так і захист Cisco Firepower Threat Defense (FTD).

Принциповою відмінністю Cisco 5506 від попередніх продуктів компанії є інтеграція технологій захисту від вторгнень і вірусних атак Sourcefire з платформою Cisco ASA 5500-X. Вийшло рішення Firepower for ASA є неперевершеним по ширині спектра розв'язуваних завдань безпеки.

- Багаторівневий захист нового покоління

Міжмережеві екрани Cisco ASA 5506 практично не залишають вразливих місць в захисті мереж. Ефективність боротьби з різного виду атаками, можливості використання засобів боротьби з погрозами дозволяють гнучко і оперативно реагувати на інциденти. Реалізовано нові можливості роботи з мережами VPN і функцій детального контролю та моніторингу, поліпшені засоби фільтрації URL-адрес, контролю дій будь-якого джерела мережевої активності.

- Контроль функціонування мережі.

Централізація на базі консолі Cisco FireSIGHT, можливості якої

надають повний контроль службам безпеки над будь-якими діями в мережі.

Під час вибору моделі маршрутизатора необхідно звертати увагу на те як він маршрутизує пакети в складній мережі з різними топологіями. Маршрутизатор має містити достатню кількість портів та забезпечувати просте розширення мережі, забезпечувати швидкість передачі даних, яка вам потрібна та швидкість їх опрацювання.

На рівні ядра нам потрібний маршрутизатор який би підтримував технологію FastEthernet та протокол OSPF та EIGRP, та містив додаткові функції налаштування. Для даних критеріїв підходить маршрутизатор Cisco Systems CISCO2911-K9, рис. 3.3, найбільш оптимальний варіант для великої мережі підприємства чи офісу.



Рис.3.3. Маршрутизатор Cisco Systems CISCO1941-K9

Маршрутизатори з інтегрованими сервісами CISCO1941 відповідають вимогам сучасних закладів, володіючи гнучкістю конструкції для додавання нових додатків. Модульна архітектура, яка призначена для підтримки вимог клієнтів, збільшення пропускної спроможності і встановлення модулів для розподілу потужності.

3.2 Налагодження обладнання мережі

Спочатку налаштуємо адресацію маршрутизаторам, комутаторам та серверам. Лістинг коду налаштування буде представлений на скріншотах нижче, рисунки 3.4 – 3.9.

```

R_CORE_1(config)#interface GigabitEthernet 0/0
R_CORE_1(config-if)#ip address 201.1.1.4 255.255.255.248
R_CORE_1(config-if)#no shutdown

R_CORE_1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R_CORE_1(config-if)#exit
R_CORE_1(config)#interface GigabitEthernet 1/0
R_CORE_1(config-if)#ip address 200.1.1.1 255.255.255.248
R_CORE_1(config-if)#no shutdown

R_CORE_1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

R_CORE_1(config-if)#exit
R_CORE_1(config)#interface Serial 2/0
R_CORE_1(config-if)#ip address 200.1.1.1 255.255.255.252
R_CORE_1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down

R_CORE_1(config-if)#exit
R_CORE_1(config)#interface Serial 3/0
R_CORE_1(config-if)#ip address 200.1.1.2 255.255.255.252
R_CORE_1(config-if)#no shutdown

```

Рис. 3.4. Базове налагодження маршрутизатора R_CORE_1

```

R_CORE_2(config)#interface GigabitEthernet 0/0
R_CORE_2(config-if)#ip address 201.1.1.5 255.255.255.2
R_CORE_2(config-if)#no shutdown

R_CORE_2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R_CORE_2(config-if)#exit
R_CORE_2(config)#interface GigabitEthernet 1/0
R_CORE_2(config-if)#ip address 200.1.1.5 255.255.255.2
R_CORE_2(config-if)#no shutdown

R_CORE_2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up

R_CORE_2(config-if)#exit
R_CORE_2(config)#interface Serial 2/0
R_CORE_2(config-if)#ip address 200.1.1.4 255.255.255.2
R_CORE_2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down

R_CORE_2(config-if)#exit
R_CORE_2(config)#interface Serial 3/0
R_CORE_2(config-if)#ip address 200.1.1.3 255.255.255.2
R_CORE_2(config-if)#no shutdown

```

Рис. 3.5. Базове налагодження маршрутизатора R_CORE_2

```

R_CORE_3(config)#interface GigabitEthernet 0/0
R_CORE_3(config-if)#ip address 201.1.1.6 255.255.255.2
R_CORE_3(config-if)#no shutdown

R_CORE_3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed

%LINEPROTO-5-UPDOWN: Line protocol on Interface Gigabi

R_CORE_3(config-if)#exit
R_CORE_3(config)#interface GigabitEthernet 1/0
R_CORE_3(config-if)#ip address 200.1.1.6 255.255.255.2
R_CORE_3(config-if)#no shutdown

R_CORE_3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed

%LINEPROTO-5-UPDOWN: Line protocol on Interface Gigabi

R_CORE_3(config-if)#exit
R_CORE_3(config)#interface Serial 2/0
R_CORE_3(config-if)#ip address 200.1.1.7 255.255.255.2
R_CORE_3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to
R_CORE_3(config-if)#exit
R_CORE_3(config)#interface Serial 3/0
R_CORE_3(config-if)#ip address 200.1.1.8 255.255.255.2
R_CORE_3(config-if)#no shutdown

```

Рис. 3.6. Базове налагодження маршрутизатора R_CORE_1

Рис. 3.7. Базове налагодження робочої станції WS_1_1_1

Рис. 3.8. Базове налагодження робочої станції WS_1_1_7

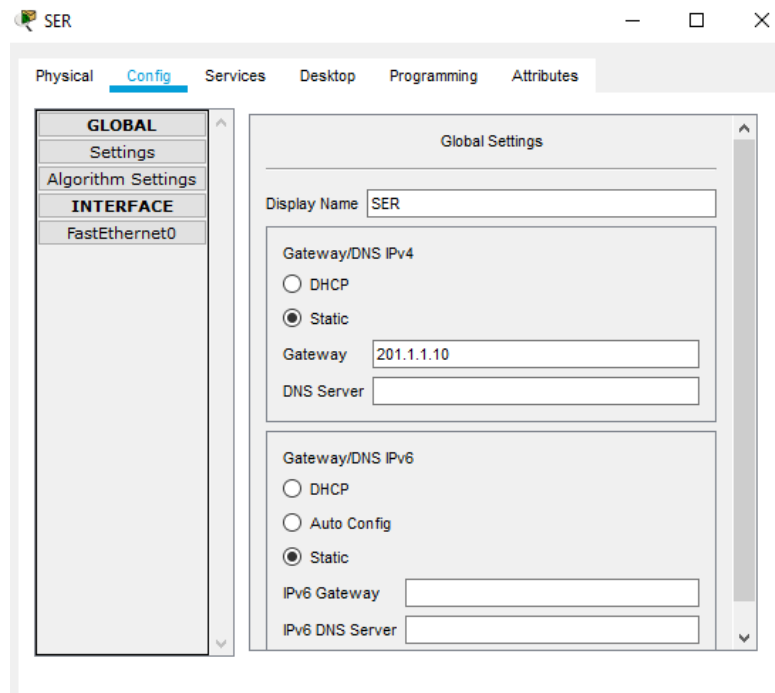


Рис. 3.9. Базове налагодження серверу SER

Всі інші комутатори та маршрутизатори налаштовуються аналогічно, але в залежності від комутатора змінюється його ір-адреса, маска, ір-адреса за замовчуванням та ір-мережа.

Далі налаштуємо міжмережеві інтерфейси Cisco ASA 5506

```
ASA0(config-if)#int gl/1
ASA0(config-if)#ip address 201.1.1.4 255.255.255.252
ASA0(config-if)#nameif outside
ASA0(config-if)#security-level 0
ASA0(config-if)#no shutdown
```

Рис. 3.10. Базове налагодження міжмережевого інтерфейсу ASA0

```
ASA0(config-if)#int mal/1
ASA0(config-if)#ip address 192.1.1.1 255.255.255.0
ASA0(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA0(config-if)#security-level 100
ASA0(config-if)#no shutdown
```

Рис. 3.11. Базове налагодження міжмережевого інтерфейсу ASA0

Всі інші маршрутизатори налаштовуються аналогічно, але в залежності від маршрутизатора змінюється мережа та адреси, які ми вилучаємо з обліку.

Далі було налаштовано DHCP на відповідних маршрутизаторах.

```
ASA0(config)#dhcp address 192.1.1.1-192.1.1.10 inside
ASA0(config)#dhcp dns 201.1.1.4
ASA0(config)#dhcpd option 3 ip 192.1.1.1
ASA0(config)#dhcpd enable inside
```

Рис. 3.12. Налашдування DHCP на міжмережевому інтерфейсі ASA0

Всі інші маршрутизатори налаштовуються аналогічно, але в залежності від маршрутизатора змінюється мережа та адреси, які ми вилучаємо з обліку.

Тепер на маршрутизаторах налаштуємо можливість віддаленого доступу за допомогою протоколу ssh.

Протокол SSH дає змогу здійснювати віддалене управління операційною системою будь-якого мережного пристрою і безпечно передавати у незахищеному середовищі повідомлення будь-якого іншого мережного протоколу. Даний протокол шифрує увесь трафік, що передається, зокрема і паролі. Окрім шифрування може також здійснювати стиснення даних.

```
R_CORE_1(config)#username admin privilege 15 secret cisco
R_CORE_1(config)#username user privilege 1 secret cisco
R_CORE_1(config)#enable secret cisco
R_CORE_1(config)#ip domain-name cisco.net
R_CORE_1(config)#crypto key generate rsa
The name for the keys will be: R_1_1_1.cisco.net
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK]

R_CORE_1(config)#ip ssh version 2
R_CORE_1(config)#ip ssh time-out 60
R_CORE_1(config)#ip ssh authentication-retries 5
R_CORE_1(config)#line vty 0 4
R_CORE_1(config-line)#login local
R_CORE_1(config-line)#transport input ssh
R_CORE_1(config-line)#transport output ssh
R_CORE_1(config-line)#logging synchronous
R_CORE_1(config-line)#exit
```

Рис. 3.13. Налаштування протоколу SSH на R_CORE_1

```

ASA0(config)#domain-name security.com
ASA0(config)#username cisco password cisco
ASA0(config)#aaa autenticstion ssh console locsl
      ^
% Invalid input detected at '^' marker.

ASA0(config)#aaa authentication ssh console locsl
      ^
% Invalid input detected at '^' marker.

ASA0(config)#aaa authentication ssh console locsl
      ^
% Invalid input detected at '^' marker.

ASA0(config)#aaa authentication ssh console local
ASA0(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ASA0(config)#ssh 192.1.1.0 255.255.255.0 inside
ASA0(config)#ssh timeout 10

```

Рис. 3.14. Налаштування протоколу SSH на ASA0

```

ASA1(config)#domain-name security.com
ASA1(config)#username cisco password cisco
ASA1(config)#aaa authentication ssh console local
ASA1(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ASA1(config)#ssh 193.1.1.0 255.255.255.0 inside
ASA1(config)#ssh timeout 10

```

Рис. 3.14. Налаштування протоколу SSH на ASA1

```

ASA2(config)#domain-name security.com
ASA2(config)#username cisco password cisco
ASA2(config)#aaa authentication ssh console local
ASA2(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ASA2(config)#ssh 194.1.1.0 255.255.255.0 inside
ASA2(config)#ssh timeout 10

```

Рис. 3.14. Налаштування протоколу SSH на ASA2

На всіх інших маршрутизаторах мережі налаштування ssh проводиться аналогічним чином. Також було налаштовано ssh на міжмережевих екранах.

Далі налаштуємо NTP. Протокол NTP – мережевий протокол для синхронізації часу. Який був розроблений Девідом Міллсом., професором Делаверського університету, в 1985 році.

← червень 2019 →						
Пн	Вт	Ср	Чт	Пт	Сб	Нд
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Рис. 3.15. Налаштування NTP на SER_NTP

```
ASA1(config)#domain-name security.com
ASA1(config)#username cisco password cisco
ASA1(config)#aaa authentication ssh console local
ASA1(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-
Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ASA1(config)#ssh 192.1.1.0 255.255.255.0 inside
ASA1(config)#ssh timeout 10
```

Рис. 3.16. Налаштування NTP на R_CORE_1

На всіх інших маршрутизаторах мережі налаштування NTP аналогічні. Всі маршрутизатори одночасно будуть і NTP-клієнтами та NTP-серверами.

```
ASA0(config)#object network INSIDE-NET
ASA0(config-network-object)#subnet 192.1.1.0 255.255.255.0
ASA0(config-network-object)#nat (inside)?
% Unrecognized command
ASA0(config-network-object)#nat (inside,outside) dynamic interface
ASA0(config-network-object)#exit
```

Рис. 3.17. Налаштування NAT на ASA0

```
ASA1(config)#object network INSIDE-NET
ASA1(config-network-object)#subnet 193.1.1.0 255.255.255.0
ASA1(config-network-object)#nat (inside)?
% Unrecognized command
ASA1(config-network-object)#nat (inside,outside) dynamic interface
ASA1(config-network-object)#exit
```

Рис. 3.18. Налаштування NAT на ASA1

На всіх інших міжмережєвих екранах мережі налаштування NAT аналогічні, але в залежності змінюється мережа та адреси, які ми вилучаємо з обліку.

```
ASA0(config)#policy-map global_policy
ASA0(config-pmap)#class inspection_default
ASA0(config-pmap-c)#inspect icmp
ASA0(config-pmap-c)#inspect http
```

Рис. 3.19. Дозволяємо протоколи ICMP та HTTP на ASA0

```
ASA1(config)#policy-map global_policy
ASA1(config-pmap)#class inspection_default
ASA1(config-pmap-c)#inspect icmp
ASA1(config-pmap-c)#inspect http
```

Рис. 3.20. Дозволяємо протоколи ICMP та HTTP на ASA1

```
ASA2(config)#policy-map global_policy
ASA2(config-pmap)#class inspection_default
ASA2(config-pmap-c)#inspect icmp
ASA2(config-pmap-c)#inspect http
```

Рис. 3.21. Дозволяємо протоколи ICMP та HTTP на ASA2

3.3 Перевірка працездатності мережі

В попередньому пункті було налаштована повністю дану мережу. В даному пункті перевіримо налаштування.

Для початку перевіримо налаштування NAT. На рисунку 3.18, 3.19 видно, що NAT налаштоване коректно.

```
ASA0#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NET interface
   translate_hits = 0, untranslate_hits = 0
```

Рис. 3.20. Виконання команди show nat

```
ASA1#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NET interface
   translate_hits = 0, untranslate_hits = 0
```

Рис. 3.21. Виконання команди show nat

Далі перевіримо налаштування маршрутів, за допомогою команди show route, рис.3.22.

```

ASA0(config)#show route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
        i - IS-IS, 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

Gateway of last resort is 201.1.1.225 to network 0.0.0.0

    201.1.1.0/30 is subnetted, 2 subnets
C      201.1.1.0 255.255.255.252 is directly connected, outside,
GigabitEthernet1/1
C      201.1.1.4 255.255.255.252 is directly connected, outside,
GigabitEthernet1/1
S*    0.0.0.0/0 [1/0] via 201.1.1.225

```

Рис. 3.22. Виконання команди show route

Тепер перевіримо налаштування NTP на маршрутизаторах. Перевірка буде за допомогою команди – show ntp status, рис. 3.23.

```

R_CORE_1>enable
R_CORE_1#show ntp status
Clock is synchronized, stratum 2, reference is 200.1.1.21
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz,
precision is 2**19
reference time is E0862E62.00000295 (06:21:22.661 UTC Fri Jun 14
2019)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.

```

Рис. 3.23. Виконання команди show ntp status на R_CORE_1

Далі перевіримо результати виконання налаштувань маршрутизації та резервних статичних плаваючих маршрутів за допомогою команди show ip route на маршрутизаторах.

```

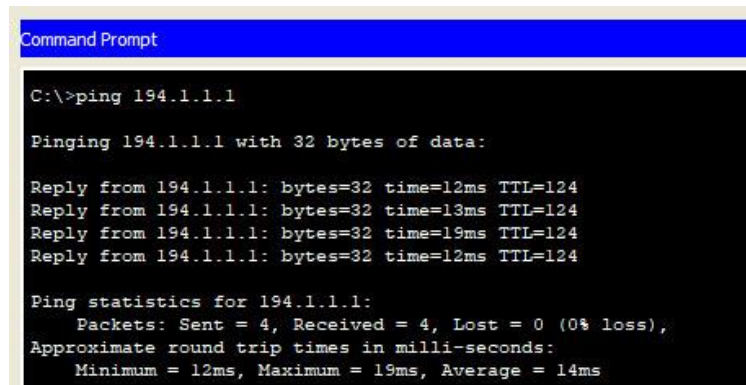
R_CORE_1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, 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

Gateway of last resort is not set

S    192.1.1.0/24 [1/0] via 201.1.1.1
    193.1.1.0/25 is subnetted, 2 subnets
S      193.1.1.0 [1/0] via 201.1.1.2
S      193.1.1.128 [1/0] via 201.1.1.2
S    194.1.1.0/24 [1/0] via 201.1.1.3
    200.1.1.0/24 is variably subnetted, 5 subnets, 2 masks
C      200.1.1.0/29 is directly connected, GigabitEthernet1/0
C      200.1.1.8/30 is directly connected, Serial2/0
C      200.1.1.12/30 is directly connected, Serial3/0

```

Рис. 3.24. Виконання команди show ip route на R_CORE_1



```

Command Prompt

C:\>ping 194.1.1.1

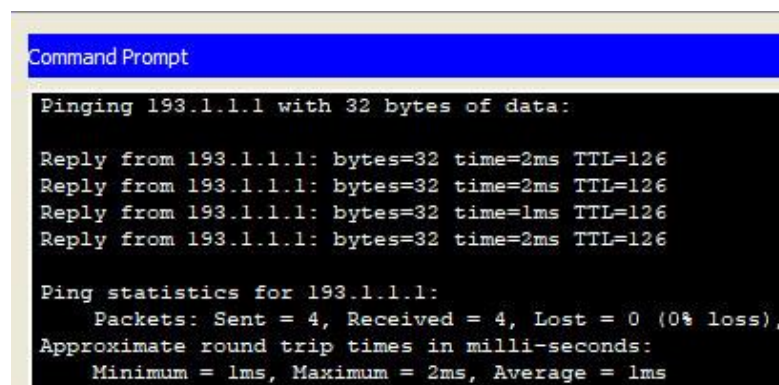
Pinging 194.1.1.1 with 32 bytes of data:

Reply from 194.1.1.1: bytes=32 time=12ms TTL=124
Reply from 194.1.1.1: bytes=32 time=13ms TTL=124
Reply from 194.1.1.1: bytes=32 time=19ms TTL=124
Reply from 194.1.1.1: bytes=32 time=12ms TTL=124

Ping statistics for 194.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 19ms, Average = 14ms

```

Рис. 3.25. Перевірка зв'язку між пристроями віддалених під мереж



```

Command Prompt

Pinging 193.1.1.1 with 32 bytes of data:

Reply from 193.1.1.1: bytes=32 time=2ms TTL=126
Reply from 193.1.1.1: bytes=32 time=2ms TTL=126
Reply from 193.1.1.1: bytes=32 time=1ms TTL=126
Reply from 193.1.1.1: bytes=32 time=2ms TTL=126

Ping statistics for 193.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

```

Рис. 3.26. Перевірка зв'язку між пристроями віддалених підмереж

Наступним кроком перевіримо налаштування DHCP, рис.3.25.

```

dhcpd dns 201.1.1.4
dhcpd option 3 ip 192.1.1.1
!
dhcpd address 192.1.1.1-192.1.1.10 inside
dhcpd enable inside

```

Рис. 3.27. Налаштування DHCP на ASA0

IP Configuration	
IP Configuration	
☒ DHCP	☐ Static DHCP request successful.
IP Address	192.1.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.1.1.254
DNS Server	8.8.8.8

Рис. 3.28. Налаштування DHCP на робочій станції

IP Configuration	
IP Configuration	
☒ DHCP	☐ Static DHCP request successful.
IP Address	194.1.1.2
Subnet Mask	255.255.255.0
Default Gateway	
DNS Server	8.8.8.8

Рис. 3.29. Налаштування DHCP на робочій станції

Кінцевою перевіркою правильності налаштування нашої мережі буде виконання команди `show running` на міжмережевих екранах Cisco ASA

```

object network INSIDE-NET
  subnet 192.1.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 201.1.1.225 1
!
!
!
object network INSIDE-NET
  nat (inside,outside) dynamic interface
!
!
!
!
class-map inspection_default
  match default-inspection-traffic
!
policy-map global_policy
  class inspection_default
    inspect http
    inspect icmp
!
service-policy global_policy global
!

```

Рис. 3.30. Виконання команди show running на ASA0

А також на робочій станції виконання команди ssh -l (user) (ip-address)

```

C:\>ssh -l cisco 192.1.1.1
Open
[Connection to 192.1.1.1 closed by foreign host]

```

Рис. 3.31. Виконання команди ssh -l cisco 192.1.1.1 на робочій станції WS_1_1_1

```

C:\>ssh -l cisco 193.1.1.1
Open
[Connection to 193.1.1.1 closed by foreign host]

```

Рис. 3.32. Виконання команди ssh -l cisco 193.1.1.1 на на робочій станції WS_1_1_5

Висновки до третього розділу

В даному розділі було визначено пристрій який найбільше підходить до нашої комп'ютерної мережі на яких буде вона побудована. Вияснено його технічні характеристики і можливості пристрою. Та визначено що Cisco ASA має такі функції як контроль функціонування мережі та багаторівневий захист нового покоління. Також було знайдено основні переваги у

використанні даного пристрою та його недоліки.

В наступному пункті було повністю налагоджено комп'ютерну мережу. Налаштовано IP-адресацію, DHCP, віддалений доступ за допомогою SSH, технологію NAT, а також мережевий протокол NTP. В останньому пункті було перевірено налаштування та коректність роботи даної мережі.

ВИСНОВКИ

Під час роботи над кваліфікаційною роботою було спроектовано та реалізовано проект підсистеми периметрового захисту на базі Cisco ASA 5506, для цього було вирішено наступні завдання:

1. Виявлено актуальність данної системи для організацій, компаній та інших структур.
2. Було розглянуто теоретичні відомості про захист комп'ютерної мережі та найбільш поширені загрози для інформаційних ресурсів організації.
3. Також з'ясовано призначення міжмережевого екрану та основні функції і розглянуто два його типи: апаратний і програмний та описано що вони являють собою. Потім було розглянуто теоретичні відомості про міжмережевий екран та детальну інформацію про його використання. Далі розглянуто, що міжмережевий екран розділяється на три види:
 - пакетні фільтри (packet filter);
 - сервера прикладного рівня (application gateways);
 - сервера рівня з'єднання (circuit gateways).

Було виявлено переваги та недоліки кожного з видів мережевого екрану та головні відмінності між видами міжмережевого екрану.

4. Далі розглянуто Cisco ASA. А саме, про його історію та функціональність. З'ясувано про програмне забезпечення Cisco Adaptive Security Appliance (ASA), що є основною операційною системою для сімейства Cisco ASA, до того ж вона підтримує стандарти шифрування наступного покоління. А також виявлено основні переваги та недоліки користування Cisco ASA.
5. В другому розділі дипломної роботи було розглянено варіанти використання данної периметрової мережі а також виділено декілька основних методів захисту себе та організації від неавторизованого доступу третім особам.

6. Після виконаної теоретичної підготовки була почата робота над топологією комп'ютерної мережі. А саме розглянуто підмережі, пристрої, використані у них, з'єднання між пристроями, а також визначено основні складові підмережі. Ми визначили кількість використаних підмереж та їх призначення.
7. По закінченню роботи над топологією мережі було розроблено адресацію глобальної мережі, розглянуто кожну з підмереж, їх інтерфейс, ір-адресу префікс та маску, детально описано адресацію для кожної підмережі.
8. Далі було визначено пристрої які найбільше підходять для данної комп'ютерної мережі. Дізналися їх технічні характеристики і можливості. Визначили недоліки на переваги.
9. Потім після остаточного вибору обладнання було налаштовано комп'ютерну мережу, а саме її ір-адресацію, віддалений доступ SSH, протокол синхронізації внутрішнього годинника NTP, технологію трансляції мережних адрес NAT та DHCP для кожної з підмереж.
10. Кінцевим завданням була перевірка роботи данної комп'ютерної мережі.

В результаті проведеної роботи було вирішено поставлену задачу та розроблено систему захисту комп'ютерної мережі на базі Cisco ASA.

Реалізований проект підсистеми мережі має необхідний функціонал для захисту цієї мережі. В даному випадку проект розроблений для невеликої організації, проте в подальшому планується робота над розширеннями його можливостей та функціонуванням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захист периметра мережі [Електронний ресурс] – Режим доступу: <http://integritysys.com.ua/security/utm/>
2. Безпека периметра корпоративної мережі [Електронний ресурс] – Режим доступу: <https://goobkas.com/g80295191-bezpeka-perimetra-korporativnoyi>
3. ОРГАНІЗАЦІЯ ПЕРИМЕТРОВОГО ЗАХИСТУ ДЛЯ СУЧАСНИХ МЕРЕЖ [Електронний ресурс] – Режим доступу: <https://conf.ztu.edu.ua/wp-content/uploads/2021/01/23-2.pdf>
4. Міжмережевий екран [Електронний ресурс] – Режим доступу: <https://www.yaklass.ru/materiali?mode=cht&chtid=462>
5. Екранування [Електронний ресурс] – Режим доступу: <https://studfile.net/preview/5367404/page:5/>
6. Межсетевой экран Cisco ASA 5506-X [Електронний ресурс] – Режим доступу: https://internet-lab.ru/cisco_asa_5506_x
7. Cisco Adaptive Security Appliance (ASA) [Електронний ресурс] – Режим доступу: [https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Cisco_Adaptive_Security_Appliance_\(ASA\)](https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Cisco_Adaptive_Security_Appliance_(ASA))
8. Хабр [Електронний ресурс] – Режим доступу: <https://habr.com/ru/post/80414/>
9. Cisco Asa. Основы. Доступ в интернет. [Електронний ресурс] – Режим доступу: <https://deltaconfig.ru/cisco-asa-internet-access/>
10. Устройства обеспечения безопасности Cisco (ASA) серии 5500 [Електронний ресурс] – Режим доступу: <https://www.hp-pro.net/Netshop/network-cisco/security/ASA-5500/>
11. Методи захисту комп'ютерних мереж [Електронний ресурс] – Режим доступу: <http://km.ptngu.com/lections/17.html>
12. Cisco ASA 5505 Firewall [Електронний ресурс] – Режим доступу: <https://www.secureitstore.com/ASA-5505>

13. Cisco Packet Tracer [Електронний ресурс] – Режим доступу:
https://ru.wikipedia.org/wiki/Cisco_Packet_Tracer
14. С.В. Толюпа. Захист від несанкціонованого доступу в масштабах організації за допомогою використання можливостей мережевої інфраструктури на прикладі cisco // Сучасний захист інформації №2, 2016 УДК 004.056.5(045). - с. 17-28 [Електронний ресурс] – Режим доступу: <http://journals.dut.edu.ua/index.php/dataprotect/article/view/685>
15. NTP [Електронний ресурс] – Режим доступу:
<https://uk.wikipedia.org/wiki/NTP>
16. Cisco ASA 5500 Series Data Sheet [Електронний ресурс] – Режим доступу:
<https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html#CiscoASA5500Seriesappliances>
17. Cisco ASA 5506-X [Електронний ресурс] – Режим доступу:
<https://linkas.ru/services/cisco-asa-5506-x/>
18. Cisco 1941 Series [Електронний ресурс] – Режим доступу:
https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html

ДОДАТКИ

					КБ.КР.Б – 125 – 20 – ПЗ	Арк.
						59

Виконання команд show running-config на пристроях:

R_MAIN#show running-config	interface Ethernet0/2
Building configuration...	no ip address
Current configuration : 2543 bytes	shutdown
Last configuration change at 11:06:08 UTC Wed Jan 27 2021	interface Ethernet0/3
	no ip address
	shutdown
version 15.5	
service timestamps debug datetime msec	interface Ethernet1/0
service timestamps log datetime msec	no ip address
no service password-encryption	shutdown
hostname R_MAIN	interface Ethernet1/1
	no ip address
boot-start-marker	shutdown
boot-end-marker	
	interface Ethernet1/2
enable secret 5 \$1\$3/Zt\$97XWxgsw5dCls926yjqCV/	no ip address
	shutdown
no aaa new-model	
	interface Ethernet1/3
bsd-client server url	no ip address
https://cloudsso.cisco.com/as/token.oauth2	shutdown
mmi polling-interval 60	
no mmi auto-configure	interface Serial2/0
no mmi pvc	ip nat inside
mmi snmp-timeout 180	ip virtual-reassembly in
	serial restart-delay 0
no ip icmp rate-limit unreachable	
	interface Serial2/1
ip domain name cisco.net	ip nat inside
ip cef	ip virtual-reassembly in
no ipv6 cef	serial restart-delay 0
multilink bundle-name authenticated	interface Serial2/2
	no ip address
cts logging verbose	shutdown
	serial restart-delay 0
username admin privilege 15 secret 5	
\$1\$7fKU\$nD5OKUmqvbKYboEm1Kn2F/	interface Serial2/3
username user secret 5	no ip address
\$1\$5IUd\$z4s4i/xzqhJyZavvmyWLV/	shutdown
	serial restart-delay 0
redundancy	
	interface Serial3/0
ip tcp synwait-time 5	no ip address
ip ssh time-out 60	shutdown
ip ssh authentication-retries 5	serial restart-delay 0
ip ssh version 2	
	interface Serial3/1
interface Ethernet0/0	no ip address
ip address 192.168.1.4 255.255.255.0	shutdown
ip nat outside	serial restart-delay 0
ip virtual-reassembly in	
	interface Serial3/2
interface Ethernet0/1	no ip address
no ip address	shutdown
shutdown	serial restart-delay 0

```
interface Serial3/3
no ip address
shutdown
serial restart-delay 0

ip default-gateway 192.168.1.1
ip forward-protocol nd

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
logging synchronous
login local
transport input ssh
transport output ssh

end

R_CORE_1#show running-config
Building configuration...
Current configuration : 2569 bytes

Last configuration change at 10:54:02 UTC Wed Jan
27 2021

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R_CORE_1

boot-start-marker
boot-end-marker

enable secret 5 $1$naNE$Jf7LP4xE78sOB0097l/24/

no aaa new-model

bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180

no ip icmp rate-limit unreachable

no ip domain lookup
ip domain name cisco.net
ip cef
no ipv6 cef

multilink bundle-name authenticated
```

```
cts logging verbose

username admin privilege 15 secret 5
$1$F4Ec$F8Xmh.e3kw0OYsnGY/PwL/
username user secret 5
$1$A4Y0$P KTDIHemA VxNYzosnndqG0

redundancy

ip tcp synwait-time 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2

interface Ethernet0/0
ip address 201.1.1.1 255.255.255.248
ip nat inside
ip virtual-reassembly in

interface Ethernet0/1
no ip address
shutdown

interface Ethernet0/2
no ip address
shutdown

interface Ethernet0/3
no ip address
shutdown

interface Ethernet1/0
no ip address
shutdown

interface Ethernet1/1
no ip address
shutdown

interface Ethernet1/2
no ip address
shutdown

interface Ethernet1/3
no ip address
shutdown

interface Serial2/0
ip nat outside
ip virtual-reassembly in
serial restart-delay 0

interface Serial2/1
no ip address
shutdown
serial restart-delay 0
ip virtual-reassembly in
serial restart-delay 0

interface Serial2/3
no ip address
shutdown
serial restart-delay 0
```

```

interface Serial3/0
no ip address
shutdown
serial restart-delay 0

interface Serial3/1
no ip address
shutdown
serial restart-delay 0

interface Serial3/2
no ip address
shutdown
serial restart-delay 0

interface Serial3/3
no ip address
shutdown
serial restart-delay 0

router ospf 1
network 201.1.1.0 0.0.0.7 area 0

ip forward-protocol nd

no ip http server
no ip http secure-server
ip nat inside source static 201.1.1.1

control-plane

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh

end

R_CORE_2#show running-config
Building configuration...

Current configuration : 2570 bytes

Last configuration change at 10:56:27 UTC Wed Jan
27 2021

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R_CORE_2

boot-start-marker
boot-end-marker

enable secret 5
$1$C0vQ$8EX39uYKTbnaOc0ChpBNs0

no aaa new-model

bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180

no ip icmp rate-limit unreachable

no ip domain lookup
ip domain name cisco.net
ip cef
no ipv6 cef

multilink bundle-name authenticated

cts logging verbose

username admin privilege 15 secret 5
$1$aQTu$0AbptdH1PFxJ9092sDNue1
username user secret 5
$1$JVaW$G/XxMK4VBVkSrgZLPOK85/

redundancy

ip tcp synwait-time 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2

interface Ethernet0/0
ip address 200.1.1.1 255.255.255.248
ip nat inside
ip virtual-reassembly in

interface Ethernet0/1
no ip address
shutdown

interface Ethernet0/2
no ip address
shutdown

interface Ethernet0/3
no ip address
shutdown

interface Ethernet1/0
no ip address
shutdown

interface Ethernet1/1
no ip address
shutdown

```

```

interface Ethernet1/2
no ip address
shutdown

interface Ethernet1/3
no ip address
shutdown

interface Serial2/0
no ip address
shutdown
serial restart-delay 0

interface Serial2/1
ip address 202.1.1.6 255.255.255.252
ip nat outside
ip virtual-reassembly in
serial restart-delay 0

interface Serial2/2
ip address 202.1.1.10 255.255.255.252
ip nat inside
ip virtual-reassembly in
serial restart-delay 0

interface Serial2/3
no ip address
shutdown
serial restart-delay 0

interface Serial3/0
no ip address
shutdown
serial restart-delay 0

interface Serial3/1
no ip address
shutdown
serial restart-delay 0

interface Serial3/2
no ip address
shutdown
serial restart-delay 0

interface Serial3/3
no ip address
shutdown
serial restart-delay 0

router ospf 1
network 200.1.1.0 0.0.0.7 area 0

ip forward-protocol nd

no ip http server
no ip http secure-server
ip nat inside source static 200.1.1.1
ip nat inside source static 202.1.1.10

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
logging synchronous
login local
transport input ssh
transport output ssh

end

R_1_1_1#show running-config
Building configuration...

Current configuration : 2602 bytes

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R_1_1_1

boot-start-marker
boot-end-marker

enable secret 5 $1$xS1I$moZ9.7tjvWfAbJZwFX66O/

no aaa new-model

bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180

no ip icmp rate-limit unreachable

ip domain name cisco.net
ip cef
no ipv6 cef

multilink bundle-name authenticated
vpdn enable

username admin privilege 15 secret 5
$1$rEnH$WmlfHBXBf0c8LZO19sIJ0
username user secret 5
$1$q.Yc$cg7yXrcGu/VEY2j3X.Gro0
username Bohdana password 0 cisco

redundancy

ip tcp synwait-time 5
ip ssh time-out 60
ip ssh authentication-retries 5

```

```

ip ssh version 2

interface Ethernet0/0
ip address 201.1.1.2 255.255.255.248
ip nat outside
ip virtual-reassembly in

interface Ethernet0/1
ip nat inside
ip virtual-reassembly in

interface Ethernet0/2
no ip address
shutdown

interface Ethernet0/3
no ip address
shutdown

interface Ethernet1/0
no ip address
shutdown

interface Ethernet1/1
no ip address
shutdown

interface Ethernet1/2
no ip address
shutdown

interface Ethernet1/3
no ip address
shutdown

interface Serial2/0
no ip address
shutdown
serial restart-delay 0

interface Serial2/1
no ip address
shutdown
serial restart-delay 0

interface Serial2/2
no ip address
shutdown
serial restart-delay 0

interface Serial2/3
no ip address
shutdown
serial restart-delay 0

interface Serial3/0
no ip address
shutdown
serial restart-delay 0

interface Serial3/1
no ip address
shutdown

serial restart-delay 0

interface Serial3/2
no ip address
shutdown
serial restart-delay 0

interface Serial3/3
no ip address
shutdown
serial restart-delay 0

interface Virtual-Template1
ip unnumbered Ethernet0/1
peer default ip address dhcp-poolNetwork_F
ppp authentication chap ms-chap ms-chap-v2

router ospf 1
network 201.1.1.0 0.0.0.7 area 0

ip forward-protocol nd

no ip http server
no ip http secure-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
logging synchronous
login local
transport input ssh
transport output ssh

end

R_1_1_2#show running-config
Building configuration...

Current configuration : 2837 bytes

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R_1_1_2

boot-start-marker
boot-end-marker

enable secret 5 $1$EUqz$gENSz1qmxkgU2tyPip1EZ.

no aaa new-model

```

```
bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
```

```
no ip domain lookup
ip domain name cisco.net
ip cef
no ipv6 cef
```

```
multilink bundle-name authenticated
vpdn enable
```

```
username admin privilege 15 secret 5
$1$U5d.$Pyo26vn9BhiSSeMUUYT6O0
username user secret 5
$1$3/yC$qwa1rLnFT9WjeucEQVseR0
username Bohdana password 0 cisco
```

```
redundancy
```

```
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2
```

```
interface Ethernet0/0
ip address 201.1.1.3 255.255.255.248
ip nat outside
ip virtual-reassembly in
```

```
interface Ethernet0/1
interface Ethernet0/3
no ip address
shutdown
```

```
interface Ethernet1/0
no ip address
shutdown
```

```
interface Ethernet1/1
no ip address
shutdown
```

```
interface Ethernet1/2
no ip address
shutdown
```

```
interface Ethernet1/3
no ip address
shutdown
```

```
interface Serial2/0
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial2/1
no ip address
```

```
shutdown
serial restart-delay 0
```

```
interface Serial2/2
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
```

```
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
```

```
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
logging synchronous
login local
transport input ssh
transport output ssh
```

```
end
```

```
R_1_1_3#show running-config
Building configuration...
```

```
Current configuration : 3016 bytes
```

```
Last configuration change at 11:49:44 UTC Wed Jan
27 2021
```

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
```

no service password-encryption

hostname R_1_1_3

boot-start-marker

boot-end-marker

enable secret 5

\$1\$LN\$s\$\$SQubAdlp2UOivdILpW VIC.

aaa new-model

aaa authentication ppp default local

no ip domain lookup

ip domain name cisco.net

ip cef

no ipv6 cef

multilink bundle-name authenticated

vpdn enable

username admin privilege 15 secret 5

\$1\$NKFs\$3buAw54HUW VoA3vyE.cfU.

username user secret 5

\$1\$yulN\$uCISbku8iJq LsMuzzWgTG0

username Bohdana password 0 cisco

redundancy

ip tcp synwait-time 5

ip ssh time-out 60

ip ssh authentication-retries 5

ip ssh version 2

interface Ethernet0/0

ip address 200.1.1.2 255.255.255.248

ip nat outside

ip virtual-reassembly in

ip nat inside

ip virtual-reassembly in

interface Ethernet0/2

no ip address

shutdown

interface Ethernet0/3

no ip address

shutdown

interface Ethernet1/0

no ip address

shutdown

interface Ethernet1/1

no ip address

shutdown

interface Ethernet1/2

no ip address

shutdown

interface Ethernet1/3

no ip address

shutdown

interface Serial2/0

no ip address

shutdown

serial restart-delay 0

interface Serial2/1

no ip address

shutdown

serial restart-delay 0

interface Serial2/2

no ip address

shutdown

serial restart-delay 0

interface Serial2/3

no ip address

shutdown

serial restart-delay 0

interface Serial3/0

no ip address

shutdown

serial restart-delay 0

interface Serial3/1

no ip address

shutdown

serial restart-delay 0

interface Serial3/2

no ip address

shutdown

serial restart-delay 0

interface Serial3/3

no ip address

shutdown

serial restart-delay 0

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

logging synchronous

transport input ssh

transport output ssh

end

R_1_1_4#show running-config

Building configuration...

Current configuration : 3251 bytes

Last configuration change at 11:44:45 UTC Wed Jan 27 2021

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname R_1_1_4

boot-start-marker
boot-end-marker

enable secret 5 $1$Zxij$hm4o2OApQHgl9xknvTdOH/

aaa new-model

aaa authentication ppp default local

aaa session-id common

bsd-client server url
https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180

no ip icmp rate-limit unreachable

ip dhcp excluded-address 199.1.1.1 199.1.1.2
ip dhcp excluded-address 199.1.1.129 199.1.1.130

ip dhcp pool Network_K
network 199.1.1.0 255.255.255.128
default-router 199.1.1.1
dns-server 8.8.8.8

ip dhcp pool Network_L
network 199.1.1.128 255.255.255.128
default-router 199.1.1.129
dns-server 8.8.8.8

no ip domain lookup
ip domain name cisco.net
ip cef
no ipv6 cef

multilink bundle-name authenticated
vpdn enable

username admin privilege 15 secret 5
$1$qfko$P7wVX56e.vavIRscouA7f1
username user secret 5
$1$.zf8$dBpfSxPIHkon2hSgi8JQ00
username Bohdana password 0 cisco

redundancy

ip tcp synwait-time 5
```

```
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh version 2

interface Ethernet0/0
ip address 200.1.1.3 255.255.255.248
ip nat outside
ip virtual-reassembly in

interface Ethernet0/3
no ip address
shutdown

interface Ethernet1/0
no ip address
shutdown

interface Ethernet1/1
no ip address
shutdown

interface Ethernet1/2
no ip address
shutdown

interface Ethernet1/3
no ip address
shutdown

interface Serial2/0
no ip address
shutdown
serial restart-delay 0

interface Serial2/1
no ip address
shutdown
serial restart-delay 0

interface Serial2/2
no ip address
shutdown
serial restart-delay 0

interface Serial2/3
no ip address
shutdown
serial restart-delay 0

interface Serial3/0
no ip address
shutdown
serial restart-delay 0

interface Serial3/1
no ip address
shutdown
serial restart-delay 0

interface Serial3/2
no ip address
shutdown
serial restart-delay 0
```

```

interface Serial3/3
no ip address
shutdown
serial restart-delay 0

privilege level 15
logging synchronous
line aux 0

no nameif
no security-level
no ip address
shutdown

interface Management1/1
management-only
nameif inside
security-level 100
ip address 192.1.1.1 255.255.255.0

object network INSIDE-NET
subnet 192.1.1.0 255.255.255.0

route outside 0.0.0.0 0.0.0.0 201.1.1.225 1

object network INSIDE-NET
nat (inside,outside) dynamic interface

class-map inspection_default
match default-inspection-traffic

policy-map global_policy
class inspection_default
inspect http
inspect icmp

service-policy global_policy global

telnet timeout 5
ssh timeout 5

dhcpd dns 201.1.1.4
dhcpd option 3 ip 192.1.1.1

dhcpd address 192.1.1.1-192.1.1.10 inside
dhcpd enable inside

ASA0(config)#policy-map type inspect dns
preset_dns_map
ASA0(config-pmap)#message-length maximum 512
^
% Invalid input detected at '^' marker.
ASA0(config-pmap)#parameters
ASA0(config-pmap-p)#message-length maximum 512
^
% Invalid input detected at '^' marker.
ASA0(config-pmap-p)#message-length maximum 512
ASA0(config-pmap-p)#exit
ASA0(config-pmap)#policy-map global_policy
^
% Invalid input detected at '^' marker.

exec-timeout 0 0
privilege level 15
logging synchronous

line vty 0 4
logging synchronous
transport input ssh
transport output ssh

ASA0(config-pmap)#policy-map global_policy
ASA0(config-pmap)#class inspection_default
ASA0(config-pmap-c)#inspect dns preset_dns_map
ASA0(config-pmap-c)#exit
ASA0(config)#show running
: Saved
:
ASA Version 9.6(1)

hostname ASA0
names

interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 201.1.1.4 255.255.255.252

interface GigabitEthernet1/2
no nameif
no security-level
ip address 202.1.1.1 255.255.255.248

interface GigabitEthernet1/3
no nameif
no security-level
no ip address
shutdown

interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown

interface GigabitEthernet1/5
no nameif
no security-level
no ip address
shutdown

interface GigabitEthernet1/6
no nameif
no security-level
no ip address
shutdown

interface GigabitEthernet1/7
no nameif
no security-level
no ip address
shutdown

interface GigabitEthernet1/8

```

```

no nameif
no security-level
no ip address
shutdown
interface Management1/1
management-only
nameif inside
security-level 100
ip address 192.1.1.1 255.255.255.0

object network INSIDE-NET
subnet 192.1.1.0 255.255.255.0

route outside 0.0.0.0 0.0.0.0 201.1.1.225 1

object network INSIDE-NET
nat (inside,outside) dynamic interface

class-map inspection_default
match default-inspection-traffic

policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect http
inspect icmp
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512

service-policy global_policy global

telnet timeout 5
ssh timeout 5

dhcpd dns 201.1.1.4
dhcpd option 3 ip 192.1.1.1

dhcpd address 192.1.1.1-192.1.1.10 inside
dhcpd enable inside

ASA0(config)#domain-name security.com
ASA0(config)#username cisco password cisco
ASA0(config)#aaa autenticstion ssh console locsl
^
% Invalid input detected at '^' marker.
ASA0(config)#aaa authentication ssh console locsl
^
% Invalid input detected at '^' marker.
ASA0(config)#aaa authentication ssh console locsl
^
% Invalid input detected at '^' marker.

```

```

ASA0(config)#aaa authentication ssh console local
ASA0(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined
named <Default-RSA-Key>.

```

```

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
ASA0(config)#ssh 192.1.1.0 255.255.255.0 inside
ASA0(config)#ssh timeout 10
ASA0(config)#%IP-4-DUPADDR: Duplicate address
201.1.1.4 on GigabitEthernet1/1, sourced by
0001.64DB.EBB4
%IP-4-DUPADDR: Duplicate address 201.1.1.4 on
GigabitEthernet1/1, sourced by 0001.64DB.EBB4
%IP-4-DUPADDR: Duplicate address 201.1.1.4 on
GigabitEthernet1/1, sourced by 0001.64DB.EBB4
%IP-4-DUPADDR: Duplicate address 201.1.1.4 on
GigabitEthernet1/1, sourced by 0001.64DB.EBB4
%IP-4-DUPADDR: Duplicate address 201.1.1.4 on
GigabitEthernet1/1, sourced by 0001.64DB.EBB4
%IP-4-DUPADDR: Duplicate address 201.1.1.4 on
GigabitEthernet1/1, sourced by 0001.64DB.EBB4

```

```

%LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet1/2, changed state to down

```

```

ASA0(config)#
ASA0(config)#show running
: Saved
:
ASA Version 9.6(1)

```

```

hostname ASA0
domain-name security.com
names

```

```

interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 201.1.1.4 255.255.255.252

```

```

interface GigabitEthernet1/2
no nameif
no security-level
ip address 202.1.1.1 255.255.255.248

```

```

interface GigabitEthernet1/3
no nameif
no security-level
no ip address

```