ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

студентки Яковлєвої Анастасії Ігорівни
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco".

2. Актуальність роботи зумовлено потребою у розробці та впровадженні у практику діяльності організації захищених комп'ютерних мереж.

3. Основний зміст пояснювальної записки роботи викладено на 73 сторінках тексту, записка містить 10 таблиць, 15 ілюстрацій, 2 додатки. Список використаних літературних джерел налічує 18 найменувань. Невід'ємною складовою роботи є реалізований у середовищі моделювання GNS3 проект мережі на базі обладнання Juniper та Cisco.

4. Пояснювальна записка складається з реферату, вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений теоретичним основам побудови захищених інформаційно-комунікаційних мереж. У розділі розглянуто загальні аспекти захисту інформаційно-комунікаційних мереж, особливості організації захисту інформації на базі обладнання Juniper та Cisco. Також у розділі виокремлено основні етапи розробки підсистеми захисту інформаційно-комунікаційної мережі.

Розділ 2 присвячений проектуванню захищеної інформаційно-комунікаційної мережі. У розділі розроблено проект структури інформаційно-комунікаційної мережі, схему адресації комп'ютерної мережі, підсистему захисту інформаційно-комунікаційної мережі.

Розділ 3 присвячений вибору обладнання та програмного забезпечення, налагодженню та тестуванню роботи підсистему захисту. У ньому, зокрема, обґрунтовано вибір використаних програмних та апаратних засобів, описано налаштування маршрутизаторів.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять опис технічних характеристик використовуваного обладнання, конфігураційні файли маршрутизаторів.

8. Таблиці та ілюстрації оформлені якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації загалом усунуто. Основне зауваження – неповна реалізація студенткою емуляції спроектованої мережі, передусім у зв'язку з обмеженими системними ресурсами.

11. Ставлення студентки до виконання випускної кваліфікаційної роботи – відповідальне.

12. У цілому у процесі написання випускної кваліфікаційної роботи студентка Яковлєва А. І. виявила здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Операційні системи», «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Теорія систем і системний аналіз». Також студентка Яковлєва А. І. показала вміння підібрати інформаційні джерела, аналізувати їх, виконати постановку задачі на розробку, розробити проект захищеної мережі, обрати відповідний інструментарій, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студентки Яковлєвої А. І. написана на належному рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «добре».

Науковий керівник
к.пед.н., доцент кафедри КІ та КБ О. С. Головня
19 червня 2020 року

РЕЦЕНЗІЯ

на кваліфікаційну роботу
студентки 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Яковлєвої Анастасії Ігорівни
на тему: „Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco"

Кваліфікаційну роботу студентки Яковлєвої А. І. "Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco" присвячено актуальній тематиці - розробленню підсистеми захисту комп'ютерної мережі.

Робота містить проект мережі на основі обладнання Cisco та Juniper, виконаний засобами GNS3 та VirtualBox. До складу пояснювальної записки входить вступ, три розділи основного тексту, висновки, список використаної літератури та додатки.

У першому розділі пояснювальної записки розглянуто загальні аспекти захисту інформаційно-комунікаційних систем, здійснено аналіз та порівняння можливостей обладнання Juniper та Cisco щодо захисту інформації, виокремлено основні етапи розробки підсистеми захисту інформаційно-комунікаційної мережі.

У другому розділі пояснювальної записки виконано проектування розроблено проект структури, схему адресації та підсистему захисту комп'ютерної мережі.

У третьому розділі пояснювальної записки обґрунтовано вибір обладнання та програмного забезпечення, описано налагодження базових засобів міжмережевої взаємодії, налаштування елементів підсистему захисту (на маршрутизаторах CISCO та Juniper). Здійснено тестування побудованої підсистеми захисту інформаційно-комунікаційної мережі.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на належному рівні. Тему роботи розкрито досить повно. Студенткою продемонстровано ґрунтовні теоретичні знання та практичні фахові навички. Пояснювальну записку сформовано логічно, науково й технічно грамотно. Функціонал проекту мережі загалом відповідає заявленому.

Позитивний бік роботи полягає у належному рівні теоретичного викладу (матеріал подано структуровано і повно, вибір використовуваних засобів та технологій обґрунтовано), а також у тому, що одержані результати може бути застосовано для налаштування реального обладнання мережі та для дослідження різноманітних атак на подібні мережі. Водночас, робота має недоліки, серед яких: земульованість лише частини проекту, мовленнєві та стилістичні помилки, недоліки оформлення (зокрема, пропущено посилання на джерела в основному тексті). Вказані недоліки у цілому не знижують досить високу якість і актуальність роботи.

У цілому кваліфікаційна робота студентки Яковлєвої А. І. "Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco" відповідає вимогам рівня вищої освіти "бакалавр" спеціальності 123 "Комп'ютерна інженерія" і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – "добре".

Рецензент,
старший викладач кафедри
БІ та Т
19 червня 2020 р.



Д. С. Морозов

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему:

«Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco»

Виконала: студентка 4-го курсу, групи КІ-2
спеціальності 123 «Комп'ютерна інженерія»
_____Яковлєва А. І
Керівник _к. пед. н., доцент кафедри КІ та КБ
_____Головня О. С.
Рецензент ст. викл. кафедри БІ та Т
_____Морозов Д. С.

Житомир – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії та
кібербезпеки
Єфіменко А. А.
«06» квітня 2020 року

ЗАВДАННЯ

на випускну кваліфікаційну роботу

Студентки **Яковлєвої Анастасії Ігорівни**

Тема роботи: **Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco.**

затверджена Наказом по університету від **«06» квітня 2020 року №98с**

Термін здачі студенткою закінченої роботи – **21 червня 2020 р.**

Вихідні дані для роботи:

1. Апаратне забезпечення: маршрутизатори, Juniper, Cisco.
2. Програмне забезпечення: GNS3, VBox, операційні системи: Jun OS, Cisco IOS.

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

Розділ	Консультант	Дата	
		Завдання видав	Завдання прийняв
1	Головня О. С.	16.02.2020	16.02.2020
2	Головня О. С.	06.03.2020	06.03.2020
3	Головня О. С.	04.05.2020	04.05.2020

Керівник _____ Головня О. С.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів	Примітка
1.	Аналіз вимог до програмного продукту	12 лютого 2020- 16 лютого 2020	виконано
2.	Аналіз літератури	20 лютого 2020 – 3 березня 2020	виконано
3.	Обгрунтування вибору рішення	04 березня 2020 – 06 березня 2020	виконано
4.	Збір даних	10 березня 2020 – 15 березня 2020	виконано
5.	Аналіз теоретичних основ побудови захищених інформаційно-комунікаційних мереж	25 березня 2020 – 04 квітень 2020	виконано
6.	Розробка проекту захищеної інформаційно- комунікаційної мережі	04 квітня 2020 – 27 квітня 2020	виконано
7.	Обґрунтування вибору обладнання та ПЗ, налагодження та тестування підсистеми захисту інформаційно-комунікаційної мережі	6 травня 2020 – 26 травня 2020	виконано
8.	Тестування роботи мережі	27 травня 2020	виконано
9.	Доопрацювання, оформлення і друк пояснювальної записки	30 травня 2020 – 15 червня 2020	виконано
11.	Оформлення презентації та друк додаткового матеріалу та графічної частини ПЗ	15 червня 2020 – 18 червня 2020	виконано
12.	Отримання рецензій від опонентів	20 червня 2020	виконано
13.	Захист	25 червня 2020	виконано

Студент_____ Яковлєва А.І.
(підпис) (прізвище та ініціали)

Керівник проекту (роботи)_____ Головня О. С.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку посилань, додатків і має 57 сторінок основного тексту, 15 рисунків, 10 таблиць, 16 сторінок додатків. Список використаних джерел містить 18 найменувань і займає 2 сторінки. Загальний обсяг роботи – 73 сторінки.

Метою дипломного проекту бакалавра є розробка проекту підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco.

Об'єктом дослідження є процес проектування підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco.

Предмет дослідження – підходи, моделі та методи побудови підсистеми захисту інформаційно-комунікаційної мережі.

В першому розділі дипломного проекту проведено дослідження теоретичних основ побудови захищених інформаційно-комунікаційних систем. В другому розділі розроблено проект структури інформаційно-комунікаційної мережі, систему адресації та підсистему захисту інформаційно-комунікаційної мережі. В третьому розділі було проведено вибір обладнання та програмного забезпечення, налагоджено підсистему захисту інформаційно-комунікаційної мережі.

Ключові слова: ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ МЕРЕЖІ, СИСТЕМА АДРЕСАЦІЇ, ПІДСИСТЕМА ЗАХИСТУ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, JUNIPER , CISCO.

Змн.	Арк.	№ докум.	Підпис	Дата	«Житомирська політехніка»		
Розроб.		Яковлєва А. І		23.06.20	Проект підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання Juniper, Cisco	Літ.	
Керівник		Головня О. С		23.06.20		Арк. 7	Аркушів 73
Реценз.		Морозов Д. С		23.06.20			
Н. Контр.		Єфіменко А. А		23.06.20			
Затверд.		Єфіменко А. А		23.06.20			

ЗМІСТ

ВСТУП 10
1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ 12
1.1 Загальні аспекти захисту інформаційно-комунікаційних мереж 12
1.2 Організація захисту інформації в інформаційно-комунікаційних мережах побудованих на базі обладнання Juniper, Cisco. 15
1.3 Виокремлення основних етапів розробки підсистеми захисту інформаційно-комунікаційної мережі. 31
ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ 33
2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ 34
2.1 Розробка проекту структури інформаційно-комунікаційної мережі 34
2.2 Розробка схеми адресації комп'ютерної мережі 39
2.3 Розробка підсистеми захисту інформаційно-комунікаційної мережі 46
ВИСНОВКИ З ДРУГОГО РОЗДІЛУ 48
3. ОБГРУНТУВАННЯ ВИБОРУ ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ 49
3.1 Обґрунтування вибору обладнання та програмного забезпечення. Налагодження базових засобів міжмережевої взаємодії 49
3.2 Налаштування елементів підсистеми захисту інформаційно-комунікаційної мережі 53
3.2.1 Налагодження маршрутизаторів Cisco 53
3.2.2 Налагодження маршрутизатора Juniper 55
ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ 57
ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 58
ДОДАТКИ 60
Додаток А 61
Додаток Б 66

ВСТУП

В умовах розвитку сучасного суспільства інформаційні технології глибоко проникають в життя людей. Зараз важко знайти сферу, в якій не використовуються інформаційні технології. Багато підприємств у світі переходять до використання широких можливостей Інтернет та електронного бізнесу. У таких умовах одним з найбільш цінних ресурсів організації є інформація.

Все більше систем, додатків і даних стає доступними з глобальної мережі, внаслідок чого організації стикаються зі зростаючим числом різних загроз для своєї інформаційної інфраструктури – несанкціонований доступ, вірусна небезпека, атаки типу «відмова в обслуговуванні» (DoS) і інші види вторгнення, мішенню для яких стають додатки, комп'ютерні мережі та інфраструктура ІС.

Тому застосування інформаційних технологій немислимо без підвищеної уваги до питань інформаційної безпеки. Одним з найбільш актуальних завдань, яке стоїть сьогодні перед розробниками і постачальниками інформаційних технологій, є рішення проблем інформаційної безпеки, пов'язаних з широким розповсюдженням Інтернет, інтранет та екстранет.

Реалізація рішень для електронного бізнесу повинна забезпечувати хороший захист, конфіденційність транзакцій, надавати захист цілісності виконання ділових операцій та даних замовників, а також гарантувати постійний доступ до даних. Інформація повинна бути доступна тільки тим, кому вона призначена, і прихована від сторонніх спостерігачів. Несанкціоноване використання інформації інформаційного ресурсу, його тимчасова недоступність або руйнування можуть завдати організації значний матеріальний збиток. Надійний захист інформаційних ресурсів підвищує ефективність всього процесу інформатизації, забезпечуючи безпеку важливої ділової інформації, що циркулює в локальних і глобальних інформаційних середовищах.

Використання Інтернет як глобальної публічної мережі означає для засобів безпеки підприємства не лише різке збільшення кількості зовнішніх користувачів і різноманітність типів комунікаційних зв'язків, але і співіснування з новими мережевими та інформаційними технологіями. Тому інформаційні ресурси та засоби здійснення електронних мережевих транзакцій потрібно захищати особливо надійно і якісно.

Об'єкт дослідження – захист інформаційно-комунікаційних мереж.

Предмет дослідження – застосування обладнання виробників Juniper і Cisco для побудови підсистеми захисту інформаційно-комунікаційної мережі.

Мета дослідження – розробка проекту підсистеми захисту інформаційно-комунікаційної мережі побудованої з використанням обладнання виробників Juniper, Cisco.

Метод дослідження – комп'ютерне моделювання, системний аналіз, методи декомпозиції, теорія передачі даних, методи комутації та маршрутизації, теорія кодування.

Для досягнення вказаної мети необхідно вирішити наступні завдання:

- розглянути загальні аспекти захисту інформаційно-комунікаційних систем;
- провести дослідження теоретичних основ організації захисту в інформаційно-комунікаційних системах на обладнанні виробників Cisco та Juniper;
- розробити проект структури інформаційно-комунікаційної мережі;
- розробити схему адресації інформаційно-комунікаційної мережі;
- розробити підсистему захисту інформаційно-комунікаційної мережі;
- провести вибір обладнання та програмного забезпечення для функціонування підсистеми захисту інформаційно-комунікаційної мережі, здійснити налагодження та тестування роботи мережі.

1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Загальні аспекти захисту інформаційно-комунікаційних мереж

Для побудови надійної системи захисту інформації в сучасних інформаційно-комунікаційних мережах та системах потрібно спочатку визначити ряд можливих загроз для інформаційних ресурсів.

Роль Інтернету у розвитку сучасного підприємництва зростає. Необхідною умовою використання світової мережі є захист інформації, розміщеної в ній. Однак однією з головних проблем процесу інформатизації є хакерські атаки на інформаційні системи, які наносять прямі матеріальні збитки не тільки розробникам інформаційних технологій, але й їхнім користувачам. Отже важливе питання захисту – це захист глобальної мережі.

Маршрутизатор – це "перша лінія оборони" корпоративної мережі, яка безпосередньо стикається з Internet. Вони часто застосовуються в якості ключових елементів в системах захисту мереж (наприклад, firewall для фільтрації пакетів та обмеження проходження певного IP-трафіку). Найбільш широко поширеним зараз є обладнання фірми Cisco Systems, яке завдяки різній реалізації своєї "фірмової" операційної системи Cisco IOS може набувати властивості, необхідні адміністраторам. Саме основою у виконанні дипломного проекту буде обладнання фірми Cisco і як додаткове буде використовуватися обладнання Juniper. У справі забезпечення інформаційної безпеки успіх може принести тільки комплексний підхід. Для захисту інформаційно-комунікаційних мереж необхідно поєднувати заходи наступних рівнів:

- законодавчого (нормативно-правовий);
- адміністративного (організаційного, накази та інші дії керівництва організацій, пов'язаних з інформаційними системами, що захищаються);
- процедурного (заходи безпеки, орієнтовані на людей);
- програмно-технічного (інженерно-технічний, апаратний, програмний).

З точки зору теми дипломного проекту будемо розглядати саме програмно-технічний захист інформаційно-комунікаційних мереж.

У інформаційно-комунікаційних мережах використовуються такі основні засоби мережевого захисту інформації:

- міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища. Вони управляють проходженням мережевого трафіка відповідно до правил безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;
- системи виявлення вторгнень (IDS – Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище. Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;
- засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації загроз інформації. Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Важливим для підприємства є резервне копіювання важливої інформації та створення копій образів системних дисків персональних комп’ютерів та

серверів у момент їх нормальної роботи. Поєднання цих заходів дозволяють відновити роботу в найкоротший термін.

Обмеження прав на зміну системної інформації, застосуванні автоматизованих правил захисту, планове оновлення та перевірка систем, своєчасний збір та аналіз інформаційної активності під час роботи користувача захистить від випадкових помилок у роботі інформаційної системи. Багато в чому правильні дії в цих напрямках залежать від кваліфікації адміністратора комп'ютерної мережі.

Комп'ютерні віруси, останнім часом, найчастіше проникають в систему через електронну пошту та заражені USB-носії інформації (флеш-карти та ін.).

Сучасний антивірусний захист не може обмежуватись лише встановленням антивірусної програми. Необхідним є застосування спеціалізованих програм одноразової перевірки, які оновлюються щоденно, та контроль автоматизованого запуску з USB-носіїв.

Для безпечної роботи в локальній та глобальній інформаційно-комунікаційній мережі Інтернет важливим є налаштування параметрів безпеки програми перегляду, а також спостереження за мережевою активністю комп'ютерів мережі з метою своєчасного виявлення та блокування мережевих загроз.

Для захисту від помилок користувачів під час роботи з важливими документами необхідно застосовувати засоби дозволів до окремих документів та інформації безпосередньо у документі. Це можливо досягти використовуючи можливості офісних програм: шаблони та захист.

Важливим фактором інформаційної безпеки є також використання ліцензійного та сертифікованого програмного забезпечення, що дозволяє отримувати своєчасні оновлення захисту та забезпечити стале функціонування та розвиток інформаційно-комунікаційної мережі підприємства.

1.2 Організація захисту інформації в інформаційно-комунікаційних мережах побудованих на базі обладнання Juniper, Cisco.

Для підтримання режиму інформаційної безпеки особливо важливі заходи програмно-технічного рівня, оскільки основна загроза комп'ютерним систем виходить від них самих: збої обладнання, помилки програмного забезпечення, промахи користувачів і адміністраторів та інше.

У рамках сучасних інформаційних систем повинні бути доступні принаймні наступні механізми безпеки:

- ідентифікація і автентифікація користувачів;
- управління доступом;
- протоколювання і аудит;
- криптографія;
- екранування;
- забезпечення високої доступності.

Ці механізми використовуються в технологіях, які розглянуті нижче, а саме технології VPN, міжмережеві екрани, системи виявлення та запобігання вторгнень, фільтрація URL, парольний захист, аутентифікація на канальному та мережевому рівнях, відключення сервісів для налагодження безпеки маршрутизаторів, списки управління доступом, віддалений доступ по ssh.

Існує така модель аутентифікації, авторизації і обліку (Authentication, Authorization and Accounting, AAA), яка є основою, що підтримує автентифікацію і облік у всій мережі. Вона вимагає підтримки іншого протоколу, зазвичай Radius або TACACS+. Radius є відкритим стандартом, підтримуваним широким спектром пристроїв і виробників. І Radius, і TACACS+ шифрують вразливі дані.

1.1.1 Технології VPN

VPN (Віртуальна приватна мережа, англ. Virtual Private Network) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через

загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

VPN класифікуються за наступними ознаками.

1. за типом використовуваного середовища:

- захищені – найпоширеніший варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених протоколів VPN є: Ipsec, OpenVPN і PPTP;
- довірчі – використовуються у випадках, коли передавальне середовище можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стануть неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol).

2. за способом реалізації:

- у вигляді спеціального програмно-апаратного забезпечення реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності;
- у вигляді програмного рішення – використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN;

- інтегроване рішення – функціональність VPN забезпечує комплекс, який займається також фільтрацією мережевого трафіку, організацією мережного екрану і забезпеченням якості обслуговування.

3. за призначенням:

- intranet VPN – використовують для об'єднання в єдину захищену мережу кількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку;
- remote access VPN – використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера, корпоративного ноутбука чи смартфона;
- extranet VPN – використовують для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти), яким обмежують доступ до особливо цінної, конфіденційної інформації;
- internet VPN – використовується для надання доступу до інтернету провайдерами, у випадку якщо по одному фізичному каналу підключаються декілька користувачів;
- client/server VPN – він забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі. Особливість даного варіанту в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність часто виникає в тих випадках, коли в одній фізичній мережі необхідно створити декілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, що звертаються до серверів, які знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку, використовується його шифрування.

1. за типом протоколу: існують реалізації віртуальних приватних мереж під TCP/IP, IPX і AppleTalk.
2. за рівнем мережевого протоколу: канальний, мережевий, транспортний.

Для створення мереж VPN розроблено безліч протоколів. Кожен з цих протоколів забезпечує певні можливості VPN. Наприклад, протокол IPSec, пропонує методи шифрування мережевого рівня, що забезпечують можливості аутентифікації і сервіс шифрування між кінцевими точками в загальнодоступних IP-мережах. Інші протоколи забезпечують підтримку певних можливостей VPN за допомогою тунелювання, тобто інкапсуляції даних або протоколів в інші протоколи.

Нижче перераховані деякі з найбільш популярних тунельних протоколів, використовуваних для створення мереж VPN [13, 17]:

- протокол GRE (Generic Routing Encapsulation – загальна інкапсуляція для маршрутизації). Розроблений Cisco тунельний протокол, що забезпечує інкапсуляцію багатьох типів протокольних пакетів в тунелі IP, створює віртуальний двоточковий зв'язок з маршрутизаторами Cisco у віддалених точках IP-мережі.
- протокол L2F (Layer 2 Forwarding – протокол пересилки рівня 2). Розроблений Cisco тунельний протокол, який дозволяє створити мережу VPDN (Virtual Private Dialup Network – віртуальна приватна комутована мережа) – систему, що забезпечує існування комутованих мереж, розповсюджуються на віддалені домашні офіси, які здаються при цьому безпосередньою частиною мережі підприємства.
- протокол PPTP (Point-to-Point Tunneling Protocol – протокол тунелювання двоточковим з'єднання). Розроблений Microsoft мережевий протокол, що забезпечує захищену передачу даних від віддаленого клієнта до приватного сервера підприємства за допомогою створення мережі VPN над IP-мережами. Протокол PPTP підтримує

маршрутизацію на вимогу, багатопротокольний обмін і віртуальні приватні мережі у відкритих мережах типу Internet.

- протокол L2TP (Layer 2 Tunnel Protocol – протокол тунелювання PPP-з'єднання рівня 2). Розроблений Cisco і Microsoft тунельний протокол, дозволяє створювати мережі VPDN. Протокол L2TP є розширенням протоколу PPP (Point-to-Point Protocol – протокол передачі від точки до точки), використовуваного для мереж VPN, і об'єднує кращі можливості тунельних протоколів PPTP і L2F.
- протокол MPPE (Microsoft Point-to-Point Encryption – протокол Microsoft шифрування двоточковим з'єднання). Засіб перекладу пакетів PPP в шифровану форму. Дозволяє створити захищену VPN-зв'язок через комутовану або віддалену мережу. Для забезпечення конфіденційності даних в рамках MPPE використовується алгоритм шифрування RSA типу RC4.
- протокол DMVPN (англ. Dynamic Multipoint Virtual Private Network – динамічна багатоточкова віртуальна приватна мережа) – технологія для створення віртуальних приватних мереж, розроблена Cisco Systems. Є подальшим розвитком VPN, і ґрунтується на спільній роботі протоколів дозволу шлюзу NHRP, протоколу тунелювання mGRE(GRE), шифрування IPSec і протоколів динамічної маршрутизації: OSPF, ODR, RIP, EIGRP, OSPF, BGP. Дана технологія забезпечує найефективніший спосіб реалізації масштабних віртуальних приватних мереж на базі IPSec.

Логічно DMVPN може бути реалізований в 2-х варіантах:

- spoke-to-spoke deployment – у цьому випадку на всіх маршрутизаторах віртуальні інтерфейси налаштовуються в режимі mGRE. У результаті, з точки зору передачі даних ми отримуємо full mesh мережу, в якій unicast трафік між spoke-вузлами йде напряму по динамічно установлених каналах. Для побудови динамічного тунелю spoke використовує отриману від hub-вузла NHRP таблицю. При цьому

постійно підтримуються і беруть участь в динамічній маршрутизації тільки тунелі до Hub-вузлів. До мінусів даного дизайну відноситься обмеження по QoS для Spoke-to-Spoke тунелів – що не надто сприятливо для медіа трафіку. Також подібний дизайн рідко виправданий логічно, тому що в 99% зв'язок використовується для доступу до центрального офісу компанії;

- hub-and-spoke deployment – віртуальні інтерфейси налаштовуються в режимі mGRE тільки на Hub маршрутизаторах. Всі інші налаштовуються в режимі p2p GRE. У результаті мережа поводиться як класичний point-to-multipoint Frame Relay. Весь трафік проходить через Hub маршрутизатори.

1.1.2 Міжмережеві екрани

Міжмережевий екран (Брандмауер, або Firewall) – це засіб фільтрації пакетного трафіку, що надходить із зовнішньої мережі по відношенню до даної локальної мережі чи комп'ютера.

Сучасна мережа передачі даних – це безліч віддалених високопродуктивних пристроїв, що взаємодіють один з одним на значній відстані. Одними з найбільш великомасштабних мереж передачі даних є комп'ютерні мережі, такі як мережа Інтернет. У ній одночасно працюють мільйони джерел і споживачів інформації по всьому світу. Широкий розвиток даної мережі дозволяє використовувати її не тільки приватним особам, але і великим компаніям для об'єднання своїх розрізнених пристроїв по всьому світу в єдину мережу. Разом з цим, загальний доступ до єдиних фізичних ресурсів відкриває доступ шахраям, вірусам і конкурентам можливість заподіяти шкоди кінцевим користувачам: викрасти, спотворити, підкинути або знищити збережену інформацію, порушити цілісність програмного забезпечення і навіть вивести апаратну частину кінцевої станції. Для запобігання даних небажаних впливів необхідно запобігти несанкціонованому доступу, для чого часто застосовується Firewall. Сама назва Firewall (wall - від англ. стіна) криє в собі

його призначення, тобто він служить стіною між локальною мережею, що захищається та Інтернетом або будь-якою іншою зовнішньою мережею і запобігає будь-які загрози. Окрім вищезгаданого міжмережевий екран також може виконувати й інші функції, пов'язані з фільтрацією трафіку від/до якогось ресурсу мережі Інтернет.

Firewall дозволяє настроювати фільтри, що відповідають за пропуск трафіку за наступними критеріями:

1. ip-адреса – будь-який кінцевий пристрій, що працює по протоколу IP повинен мати унікальну адресу, задавши якусь адресу або певний діапазон можна заборонити отримувати з них пакети, або навпаки дозволити доступ тільки з даних IP-адрес;
2. доменне ім'я – сайту в мережі Інтернет, точніше його IP-адресі може бути поставлене у відповідність буквено-цифрове ім'я, яке набагато простіше запам'ятати ніж набір цифр, таким чином, фільтр може бути налаштований на пропуск трафіку тільки до/від одного з ресурсів, або заборонити доступ до нього;
3. порт – дозволяє заборонити доступ з небажаних сервісів і додатків мережі, або навпаки дозволити доступ тільки до них;
4. протокол – firewall може бути налаштований на пропуск даних лише якогось одного протоколу, або заборонити доступ з його використанням.

Вище перераховані тільки основні параметри, за якими може бути проведене налаштування. Також можуть застосовуватися інші параметри для фільтрів, специфічні для даної конкретної мережі, залежно від виконуваних у ній завдань.

Таким чином, firewall надає комплексний набір завдань щодо запобігання несанкціонованого доступу, пошкодження або викрадення даних, або іншого негативного впливу, який може вплинути на працездатність мережі. Зазвичай міжмережевий екран використовується в сукупності з іншими засобами захисту, наприклад, антивірусне ПЗ.

1.1.3 Системи виявлення та запобігання вторгнень

Системи виявлення та запобігання вторгнень (англ. IPS/IDS – Intrusion Prevention/Detection System) – програми, які аналізують трафік в пошуках аномалій і відомих загроз і приймають рішення про їх блокування. До типових загроз, від яких може допомогти IPS, належать, наприклад, спроби сканування портів і визначення ОС, атаки мережевих черв'яків, відомі експлойти та інші види атак, виявлення яких вимагає глибокого аналізу трафіку.

Система виявлення вторгнень (англ. Intrusion Detection System (IDS)) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

IDS все частіше стають необхідним доповненням інфраструктури мережевої безпеки. На додаток до міжмережевих екранів (firewall), робота яких відбувається на основі політики безпеки, IDS служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які обійшли Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від IDS існує і не маленька.

Використання IDS допомагає досягти кількох цілей:

- виявити вторгнення або мережеву атаку;
- спрогнозувати можливі майбутні атаки і виявити вразливості для запобігання їх подальшого розвитку. Атакуючий зазвичай виконує ряд попередніх дій, таких як, наприклад, мережеве зондування (сканування) або інше тестування для виявлення вразливостей цільової системи;
- виконати документування існуючих загроз;
- забезпечити контроль якості адміністрування з точки зору безпеки, особливо у великих і складних мережах;

- отримати корисну інформацію про проникнення, які мали місце, для відновлення і коригування викликаних проникнення факторів;
- визначити розташування джерела атаки по відношенню до локальної мережі (зовнішні або внутрішні атаки), що важливо при прийнятті рішень про розташування ресурсів в мережі.

Система попередження вторгнень (англ. Intrusion Prevention System (IPS))– програмний або апаратний засіб, який здійснює моніторинг мережі або комп'ютерної системи в реальному часі з метою виявлення, запобігання або блокування шкідливої активності.

У цілому IPS за класифікацією і своїми функціями аналогічні IDS. Головна їх відмінність полягає в тому, що вони функціонують в реальному часі і можуть в автоматичному режимі блокувати мережеві атаки. Кожна IPS включає в себе модуль IDS.

1.1.4 Фільтрація URL

URL Фільтрація (URL Filtering) – це можливість блокування WEB-запитів за ключовим словом в адресі (а також можливість завдання "чорних" і "білих" списків WEB-сайтів). Кожен URL Filter складається з набору URL правил, кількість яких не обмежена. URL правило визначає адресу або частину адреси при знаходженні якого в адресі WEB-запиту, даний WEB-запит буде блокуватися.

URL фільтрація здійснюється в прозорому режимі (тобто немає необхідності використовувати будь-який проксі-сервер і спеціальним чином налаштовувати браузери на клієнтах). Технологія URL фільтрації аналізує кожен TCP пакет на предмет наявності в ньому заголовка HTTP-запиту. Якщо заголовок HTTP-запиту знайдено в пакеті і збігся шаблон URL правила для блокування сайту, то TMeter формує відповідну HTML-сторінку "доступ заборонено" і посилає її клієнту як би від імені WEB-сервера. На додаток, TMeter посилає TCP пакети з прапором FIN для закриття TCP-з'єднання.

1.1.5 Парольний захист

На маршрутизаторах Cisco існує можливість налагодити безпечний доступ для всіх видів підключень з використанням парольного захисту та шифрування трафіку. Для забезпечення парольного захисту на маршрутизаторах Cisco передбачено три типи паролів:

- пароль ліній (пароль для входу в користувацький режим);
- пароль входу в привілейований режим;
- паролі користувачів.

Перші два типи паролів встановлюються на пристрій в цілому і обмежують вхід до відповідних режимів. Паролі для користувачів можуть мати різний рівень привілей.

Інформація про паролі та користувачів зберігається у конфігураційному файлі пристрою. Для маршрутизаторів Cisco може використовуватися три види паролів:

- звичайний пароль;
- пароль типу 7;
- пароль типу 5.

Звичайні паролі (plain-text passwords) встановлюються за замовчуванням і зберігаються у конфігураційному файлі пристрою у відкритому вигляді, що є загрозою безпеці. Паролі типу 7 (type 7 passwords) використовують шифрування по алгоритму Віжінера (Vigenere). Паролі даного типу доволі легко розшифровуються, тому рекомендується використовувати паролі типу 5 (MD5 hash passwords), які мають найвищий рівень безпеки.

1.1.6 Аутентифікація на канальному та мережевому рівнях

Аутентифікація - процес перевірки належності суб'єкту прав доступу до інформаційних ресурсів системи, або веб-сайту, відповідно до пред'явленого ним ідентифікатора; підтвердження (встановлення) автентичності суб'єкта. Враховуючи ступінь довіри та інші властивості систем, перевірка що проводиться може бути односторонньою або взаємною. Зазвичай вона

проводиться за допомогою криптографічної обробки, що дозволяє захистити дані, що передаються від зловмисників.

Один із способів аутентифікації в комп'ютерній системі полягає у введенні користувацького ідентифікатора, простіше кажучи «логіну» і пароля.

Достовірна пара логін-пароль зберігається в спеціальній базі даних. Проста аутентифікація має наступний загальний алгоритм:

1. суб'єкт запитує доступ до системи і вводить особистий ідентифікатор та пароль;
2. введені унікальні дані надходять на сервер аутентифікації, де порівнюються з оригіналами;
3. при збігу даних з оригіналами, аутентифікація визнається успішною, при відмінності – суб'єкт переміщується до 1-го кроку.

Введений суб'єктом пароль може передаватися в мережі двома способами:

- у не зашифрованому або відкритому вигляді, на основі протоколу парольної аутентифікації (Password Authentication Protocol, PAP);
- з використанням шифрування або односпрямованих хеш-функцій. У цьому випадку унікальні дані, введені суб'єктом передаються по мережі захищено.

Бувають різні види аутентифікації. Для початку розглянемо взаємну аутентифікацію та її переваги. При налаштуванні, взаємна аутентифікація відбувається всякий раз, коли оновлення маршрутизації обмінюються між сусідніми маршрутизаторами. Дана перевірка справжності гарантує, що маршрутизатор отримує достовірну інформацію маршрутизації від надійного джерела.

Без взаємної аутентифікації, несанкціоноване або завідомо шкідливі оновлення маршрутів можуть поставити під загрозу безпеку мережевого трафіку. Злам безпеки може відбутися, коли ворожа сторона переадресовує або аналізує мережевий трафік. Наприклад, несанкціонований маршрутизатор може послати фіктивне відновлення маршрутизації, щоб «переконати»

маршрутизатор для відправки трафіку на неправильне призначення. Цей виток трафіку може бути проаналізований, щоб дізнатися конфіденційну інформацію про організацію, або просто використаний для зриву здатності ефективно спілкуватися, використовуючи мережі.

Принцип роботи взаємної аутентифікації наступний: коли взаємна маршрутизація була налаштована на маршрутизаторі, маршрутизатор аутентифікує джерело кожного з прийнятих пакетів. Це досягається шляхом обміну ключами аутентифікації.

Є два типи перевірки взаємної аутентифікації: звичайна аутентифікація тексту та Message Digest Algorithm Version 5 (MD5) аутентифікація. Обидві форми роботи загалом схожі, за винятком того що MD5 надсилає дайджест повідомлення, а не сам ключ аутентифікації. Дайджест повідомлення створюється за допомогою ключа і повідомлення, але сам ключ не передається, тим самим уникаючи можливість його зчитування під час передачі. Звичайна аутентифікація тексту надсилає сам ключ аутентифікації по мережі.

Наступною розглянемо текстову аутентифікацію. Кожен задіяний сусідній маршрутизатор повинен розділяти ключ аутентифікації. Цей ключ зазначений на кожному маршрутизаторі під час налагодження. Декілька ключів можуть бути зазначені зі спеціальними протоколами. Алгоритм аутентифікації наведений нижче:

1. маршрутизатор надсилає оновлення разом з ключем та відповідний номер ключа сусідньому маршрутизатору;
2. сусідній маршрутизатор перевіряє отриманий ключ з ключем, що зберігається у його пам’яті;
3. якщо ці два ключа співпадають, то маршрутизатор починає отримувати пакети оновлення, а якщо не співпадають, пакети оновлень не приймаються.

MD5 аутентифікація працює так само, як і звичайна аутентифікація тексту, за винятком того, що ключ не передається. Замість цього маршрутизатор створює дайджест повідомлення використовуючи алгоритм

MD5. Після його формування дайджест відправляється замість самого ключа. Це гарантує, що ніхто не зможе прослуховувати лінії зв'язку та шпигувати за мережею.

Також існують аутентифікації в таких протоколах маршрутизації:

- аутентифікації в протоколі RIP – аутентифікація може проводитися протоколом RIP 2 для обробки тільки тих повідомлень, які містять правильний аутентифікаційний код. При роботі в такому режимі перший 20 октетний елемент вектора відстаней, наступний безпосередньо за першим 32 бітовим словом RIP повідомлення, є сегментом аутентифікації. Він визначається за значенням поля «Address Family Identifier», рівному в цьому випадку 0xFFFF. Наступні 2 октети цього елементу визначають тип аутентифікації, а решта 16 октетів містять аутентифікаційний код. Таким чином, в RIP повідомленні з аутентифікацією може передаватися не 25, а тільки 24 елемента вектора відстаней, які слідують за сегментом аутентифікації. До теперішнього моменту надійного алгоритму аутентифікації для протоколу RIP не розроблено, стандартом визначена тільки аутентифікація за допомогою звичайного пароля (значення поля «Тип» дорівнює 2);
- аутентифікації в протоколі OSPF – існує можливість захистити обмін пакетами OSPF. Є два методи аутентифікації: простий і MD5. Аутентифікація OSPF відключена за замовчуванням. Аутентифікація конфігурується поінтерфейсно. Треба додати статичний запис OSPF інтерфейсу і вказати властивості аутентифікації, щоб забезпечити обмін інформацією OSPF;
- аутентифікація в протоколі маршрутизації EIGRP – використання аутентифікації дозволяє запобігти отримання шахрайських EIGRP-оновлень. За замовчуванням аутентифікація EIGRP-пакетів вимкнено. При включеній аутентифікації маршрутизатор перевіряє джерело

отриманих оновлень по ключах аутентифікації або паролів, відомих як передавальному, так і приймальному маршрутизаторів.

1.1.7 Відключення сервісів для налагодження безпеки маршрутизатора

Список основних команд для налагодження безпеки маршрутизатора Cisco:

- no cdp run – відключити управління маршрутизатором через cdp-протокол;
- no service tcp-small-servers, no service udp-small-servers – відключення аналогічних служб;
- no service finger – уникати поширення інформації про користувачів;
- service tcp-keepalives-in, service tcp-keepalives-out – ввімкнення служб keep-alive, для захисту від можливого перехоплення, наприклад, сесії telnet;
- no ip http server, no ip http secure-server – відключення доступу до маршрутизатора по протоколах http и https;
- no service dhcp – відключення динамічного присвоєння адрес.

1.1.8 Списки управління доступом

Список управління доступом (access control list, ACL) – це послідовний список правил, які використовуються для дозволу або заборони потоку пакетів всередині мережі на підставі інформації, наведеної всередині списку. Без списку доступу усі пакети всередині мережі дозволяються без обмежень для всіх частин мережі. Список доступу може бути використаний для контролю поширення та отримання інформації про зміну таблиць маршрутів та забезпечення безпеки. Політика безпеки включає захист від зовнішніх атак, обмеження доступу між відділами організації та розподіл завантаження мережі. Список доступу дозволяє використовувати маршрутизатор як міжмережевий екран для заборони або обмеження доступу до внутрішньої мережі з зовнішньої мережі, наприклад, Інтернет. Брандмауер поміщається в точках з'єднання між двома мережами.

1.1.9 Віддалений доступ по SSH

SSH (англ. Secure SHell – «безпечна оболонка») – мережевий протокол віддаленого доступу, який дає змогу здійснювати віддалене управління операційною системою будь-якого мережевого пристрою і безпечно передавати в незахищеному середовищі будь-який інший мережевий протокол (наприклад, здійснювати тунелювання TCP-з'єднань для передачі файлів). За функціональністю схожий на протоколи Telnet, rlogin, rsh, але на відміну від них, шифрує увесь трафік, що передається, зокрема і паролі. Окрім шифрування може також здійснювати стиснення даних. SSH, як і решта протоколів віддаленого управління побудований з використанням клієнт-серверного підходу. SSH-клієнти та SSH-сервери доступні для більшості мережевих операційних систем.

SSH належить до прикладного рівня моделі OSI та прикладного рівня стеку TCP/IP. Для організації інформаційного обміну використовує 22 порт TCP. Існує дві версії протоколу: SSH-1 (1995 р.) та SSH-2 (1996 р.). Версія SSH-2 є більш безпечною в порівнянні з SSH-1, тому набула більшого поширення. На сьогодні коли йде мова про протокол SSH, то мається на увазі саме SSH-2. Як стандарт Інтернета SSH був затверджений IETF у 2000 р.

Архітектурно в протоколі SSH виділяють три рівні:

- транспортний рівень;
- рівень аутентифікації користувача;
- рівень з'єднання.

Протокол транспортного рівня забезпечує аутентифікацію сервера, конфіденційність і цілісність даних з гарною естафетною передачею. Додатково може підтримуватися стиснення даних. Протокол аутентифікації користувача дає змогу серверу аутентифікувати клієнта. Протокол з'єднання мультиплексує шифрований тунель, створюючи в ньому кілька логічних каналів.

Для аутентифікації сервера в SSH використовується протокол аутентифікації сторін на основі алгоритмів електронно-цифрового підпису RSA або DSA. Для аутентифікації клієнта також може використуватися ЕЦП RSA

або DSA, але допускається також аутентифікація за допомогою паролю (режим зворотної сумісності з Telnet) і навіть за IP-адресою вузла (режим зворотної сумісності з rlogin). Аутентифікація за паролем найбільш поширена і безпечна, оскільки пароль передається по зашифрованому віртуальному каналу. Аутентифікація за IP-адресою небезпечна, цю можливість, як правило, відключають. Для створення загального секрету (сеансового ключа) використовується алгоритм Діффі-Хеллмана. Для шифрування переданих даних викокористовується симетричне шифрування, алгоритми IDEA, AES, Blowfish, DES або 3DES. Цілісність передачі даних перевіряється за допомогою CRC32 в SSH1 або HMAC-SHA1/HMAC-MD5 в SSH2.

Для стиснення даних може використовуватися алгоритм LempelZiv (LZ77), який забезпечує такий же рівень стиснення, що і архіватор ZIP. Стиснення в SSH активується лише за запитом клієнта, і на практиці рідко використовується. На ринку програмного забезпечення наявна велика кількість як комерційних, так і вільнорозповсюджуваних серверів та клієнтів SSH для різних операційних систем.

Широкого використання протокол SSH набув для віддаленого доступу та адміністрування мережевих пристроїв. Більшість виробників мережевого обладнання (в т.ч. Cisco, Juniper, Vyatta, Huawei та ін.) включають реалізації SSH-серверів та клієнтів в мережеві операційні системи комутаторів, маршрутизаторів та інших пристроїв і саме його рекомендують використовувати.

Рекомендації щодо безпеки використання SSH:

1. заборона віддаленого доступу під паролем основного адміністратора (root-доступу);
2. заборона підключення з пустим паролем або відключення входу по паролю;
3. вибір нестандартного порта для SSH-сервера;
4. використання довгих SSH2 RSA-ключів (як мінімум 1024, бажано 2048 біт і більше);

5. обмеження списку IP-адрес, з яких дозволений доступ;
6. заборона доступу з потенційно небезпечних адрес;
7. відмова від використання поширених або широко відомих системних логінів для доступу по SSH;
8. регулярний перегляд повідомлень про помилки аутентифікації;
9. установка систем виявлення вторгнень;
10. використання засобів-пасток, які підроблюють SSH-сервіс (honeypots).

Зведену інформацію про набір можливостей в обладнанні виробників Cisco, Juniper наведено в таблиці 1.1.

Таблиця 1.1 – Набір можливостей в обладнанні виробників Cisco, Juniper

Можливості	Cisco	Juniper
Технологія VPN Site-to-site	+	+
Підтримка протоколу VPN PPTP	+	+
Підтримка протоколу VPN L2TP	+	+
Підтримка протоколу VPN DMVPN	+	-
Міжмережеві екрани	+	+
Системи IPS/IDS	+	+
Фільтрація URL	+	+
Парольний захист	+	+
Аутентифікація на канальному та мережевому рівнях	+	+
Відключення сервісів	+	-
Списки управління доступом	+	+
Віддалений доступ	+	+

1.3 Виокремлення основних етапів розробки підсистеми захисту інформаційно-комунікаційної мережі.

У першому розділі дипломного проекту уже сформоване уявлення про теоретичні основи побудови захищених інформаційно-комунікаційних систем.

Далі потрібно розробити проект захищеної інформаційно-комунікаційної мережі. Для цього потрібно для початку розробити проект структури мережі, попередньо проаналізувавши моделі побудови інформаційно-комунікаційних мереж і вибрати ту, яка найбільше підходить, детально розглянути кожну з підмереж. Як результат аналізу підмереж представити дані з використанням пристроїв в кожній з підмереж, враховуючи кількість використаних пристроїв. На наступному етапі для забезпечення міжмережевої взаємодії необхідно розробити схему адресації фізичних та логічних з'єднань інформаційно-комунікаційної мережі, враховуючи оптимальне використання адресного простору. Показати даний розрахунок на прикладі однієї підмережі для кращого розуміння. Навести адресації для підмереж та інших фізичних та логічних з'єднань. Також необхідно розробити підсистему захисту інформаційно-комунікаційної мережі, посилаючись на теоретичні основи, які були розглянуті. Потрібно розробити добре захищену мережу, адже наступним етапом буде її реалізація.

В третьому розділі необхідно зробити вибір обладнання та програмного забезпечення в залежності від вимог та обґрунтувати свій вибір, налаштувати базові засоби міжмережевої взаємодії та зробити перевірку. На завершальному етапі налагодити елементи підсистеми захисту інформаційно-комунікаційної мережі та зробити тестування даних налагоджень.

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

В першому розділі розглянуто загальні аспекти захисту інформаційно-комунікаційних систем, в результаті чого визначено основні засоби захисту інформаційно-комунікаційних систем, а саме: віртуальні приватні мережі, міжмережеві екрани, системи виявлення вторгнень та засоби аналізу захищеності.

Проведено аналіз теоретичних основ організації захисту інформації в інформаційно-комунікаційних системах з використанням обладнання виробників Juniper, Cisco. В результаті аналізу побудована таблиця з набором можливостей для кожної з фірм, які використовуються в дипломному проекті.

Розглянуто постановку задачі досліджень для розробки підсистеми захисту інформаційно-комунікаційної мережі.

2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Розробка проекту структури інформаційно-комунікаційної мережі

Сучасні мережі будуються з використанням різних моделей, але за основу побудови мереж в дипломному проекті візьмемо саме трирівневу ієрархічну модель компанії Cisco. Адже за допомогою ієрархії можна впорядкувати всі компоненти в легко аналізованої моделі. Причому, модель буде диктувати характеристики кожного ієрархічного рівня. Ієрархічна модель Cisco допомагає в розробці, впровадженні й обслуговуванні масштабованих, надійних і ефективних у вартісному вираженні об’єднаних мереж. Компанія Cisco визначила три ієрархічних рівня, на кожному з яких виконуються специфічні мережеві функції.

В моделі визначені такі рівні:

1. базовий рівень;
2. рівень розподілу;
3. рівень доступу.

Базовий рівень формує ядро мережі. Цей рівень відповідає за швидку і надійну пересилку великих об’ємів трафіку. Єдиним призначенням базового рівня є швидка комутація трафіку. Трафік передається на базовому рівні спільно для декількох користувачів. Однак на рівні розподілу обробляються дані користувача, що може призвести до додаткових запитів в базовий рівень. Якщо відбувається помилка на базовому рівні, то вона впливає на всіх користувачів. Отже, вельми важливо забезпечити високу надійність на базовому рівні. На цьому рівні обробляються великі об'єми трафіку, тому не менш важливо враховувати швидкість і затримки.

Рівень розподілу іноді називають рівнем робочих груп. Він розташований між базовим рівнем і рівнем доступу. Основні функції рівня поширення полягають у маршрутизації, фільтрації та доступі до регіональних мереж, а

також (якщо необхідно) у визначенні правил доступу пакетів до базового рівня. Рівень розподілу зобов’язаний встановлювати найбільш швидкий спосіб обробки запитів до служб (наприклад, метод файлового звернення до сервера). Після визначення на рівні поширення найкращого шляху доступу, запит може бути переданий на базовий рівень, де реалізовано швидкісний транспорт запиту до потрібної служби. На рівні розподілу встановлюється політика мережі, а також забезпечуються можливості гнучкого опису мережевих операцій.

На рівні доступу реалізовано управління користувачами і робочими групами при зверненні до ресурсів об’єднаної мережі. Іноді рівень доступу називають рівнем настільних систем. Найбільша частина необхідних користувачам мережевих ресурсів повинна бути доступна локально. На рівні розподілу виконується перенаправлення трафіку до віддалених служб.

Існує можливість об'єднання деяких рівнів, можуть бути об’єднанні рівень ядра та розподілу або рівень розподілу та доступу. Для дипломного проекту доцільно використати саме об’єднанні рівень ядра та розподілу. На цьому рівні функціонують інтерфейси Gigabit Ethernet. Маршрутизатори з’єднуються з підмережами за допомогою Fast Ethernet та Gigabit Ethernet.

Рівень доступу призначений для підключення кінцевих користувачів і надання їм різних сервісів. На рівні доступу використовуються комутатори, які з’єднуються між собою за допомогою Fast Ethernet та Gigabit Ethernet. В основному Gigabit Ethernet використовується для з’єднання головного комутатора з додатковими та з серверами і в деяких випадках з маршрутизаторами. А Fast Ethernet використовується для під’єднання робочих станцій до комутаторів.

До головного маршрутизатора Router_1 під’єднані маршрутизатори Router_8 На рисунку 2.1 можна побачити загальний проект структури інформаційно-комунікаційної мережі.

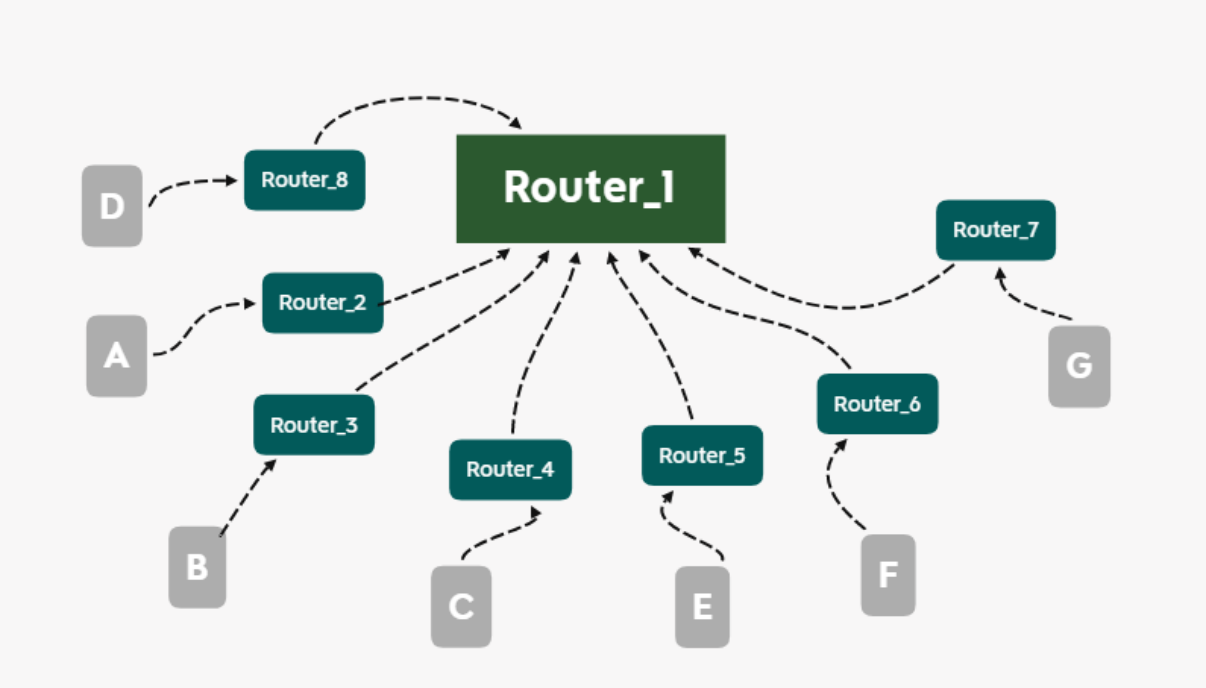


Рисунок 2.1 – Загальна схема мережі

На рівні доступу підключаються локальні підмережі з різною кількістю вузлів. Для кожної із цих підмереж розробимо топологію, враховуючи кількість вузлів.

Існують типові комутатори:

- на 48 порти Fast Ethernet + 2 високошвидкісних порти Gigabit Ethernet;
- на 24 порти Fast Ethernet + 2 високошвидкісних порти Gigabit Ethernet;
- на 24 високошвидкісних порти Gigabit Ethernet;
- на 12 порти Fast Ethernet + 2 високошвидкісних порти Gigabit Ethernet;
- на 12 високошвидкісних порти Gigabit Ethernet;
- на 8 портів Fast Ethernet + 1 високошвидкісний Gigabit Ethernet.

Отже, на основі даних про типові комутатори підберемо види і кількість комутаторів для кожної з підмереж.

Підмережа А складається з 41 вузла (1 з яких сервер). В цій підмережі використаємо один коммутатор на 48+2 порти, один порт з яких задіяний для підключення сервера за допомогою Gigabit Ethernet, 40 портів для підключення персональних комп'ютерів за допомогою Fast Ethernet та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу за допомогою Fast

Ethernet. На головному комутаторі залишиться вільних 7 портів Fast Ethernet та 1 порт Gigabit Ethernet. Вільні порти можуть використовуватися для розширення мережі.

Підмережа B складається з 125 вузлів (3 з яких сервери). Головний комутатор використаємо на 12 портів, 5 портів з яких задіяно для під'єднання 5 комутаторів на 24+2 порти, 1 порт для під'єднання комутатора на 8+1 портів, 3 порти задіяні для підключення серверів та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу. Всі задіяні порти головного комутатора підключаються за допомогою Gigabit Ethernet. На головному комутаторі залишиться вільних 2 порти Gigabit Ethernet для розширення мережі. До комутаторів на 24+2 порти та на 8+1 порти підключено робочі станції за допомогою Fast Ethernet. До комутаторів на 24+2 порти підключено по 23 робочі станції, а до комутаторів на 8+1 порти підключено 7 робочих станцій. У комутаторів на 24+2 порти залишиться вільних 1 порт Fast Ethernet та 1 порт Gigabit Ethernet, а в комутатора на 8+1 порт залишиться вільним 1 порт Fast Ethernet. Всі вільні порти можуть використовуватися для розширення мережі.

Підмережа C складається з 30 вузлів (1 з яких сервер). Використаємо один комутатор на 48+2, з яких 1 порт задіяний для підключення сервера за допомогою Gigabit Ethernet, 29 портів для підключення робочих станцій за допомогою Fast Ethernet та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу за допомогою Fast Ethernet. На головному комутаторі залишається вільних 18 портів Fast Ethernet та 1 порт Gigabit Ethernet для розширення мережі.

Підмережа D складається з 59 вузлів (2 з яких сервери). В даній підмережі задіяно 2 комутатори, 1 з яких на 48+2 порти, інший на 24+2 порти. В комутатора на 48+2 порти 1 порт задіяний для підключення сервера та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу за допомогою Gigabit Ethernet, а також 40 портів для підключення робочих станцій за допомогою Fast Ethernet. На даному комутаторі залишиться вільних 8 портів

Fast Ethernet. В комутатора на 24+2 порти 1 порт задіяний для підключення сервера та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу за допомогою Gigabit Ethernet, а також 17 портів для підключення робочих станцій за допомогою Fast Ethernet. На цьому комутаторі залишається вільних 7 портів Fast Ethernet. Всі вільні порти можуть використовуватися для розширення мережі.

Підмережа E складається з 720 вузлів (4 з яких сервери). Головний коммутатор на 24 порти, 15 портів задіяно для під'єднання 15 комутаторів на 48+2 порти, 1 порт для під'єднання комутатора на 12+2 портів, 4 порти задіяні для підключення серверів та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу. Всі задіяні порти головного комутатора підключаються за допомогою Gigabit Ethernet. На головному комутаторі залишається вільних 3 порти Gigabit Ethernet для розширення мережі. До комутаторів на 48+2 порти та на 12+2 порти підключені робочі станції за допомогою Fast Ethernet. До комутаторів на 48+2 порти підключено по 47 робочих станцій, а до комутатора на 12+2 порти підключено 11 робочих станцій. На цих комутаторах залишається вільних 1 порт Gigabit Ethernet та 1 порт Fast Ethernet для розширення мережі.

Підмережа F складається з 198 вузлів (3 з яких сервери). Головний комутатор на 12 портів, 4 порти задіяно для під'єднання 4 комутаторів на 48+2 порти, 1 порт для під'єднання комутатора на 8+1 портів, 3 порти задіяні для підключення серверів та 1 порт для під'єднання до маршрутизатора рівня розподілу. Всі задіяні порти головного комутатора підключаються за допомогою Gigabit Ethernet. На головному комутаторі залишається вільних 3 порти Gigabit Ethernet для розширення мережі. До комутаторів на 48+2 порти та на 8+1 порти підключені робочі станції за допомогою Fast Ethernet. До комутаторів на 48+2 порти підключено по 47 робочих станцій, а до комутаторів на 8+1 порти підключено 7 робочих станцій. На цих комутаторах залишається вільних 1 порт Gigabit Ethernet та 1 порт Fast Ethernet для розширення мережі. Підмережа G складається з 35 вузлів (1 з яких сервер).

Використовується один коммутатор на 48+2 порти, з яких 1 порт задіяний для підключення сервера за допомогою Gigabit Ethernet, 34 портів для підключення робочих станцій за допомогою Fast Ethernet та 1 порт для під'єднання до маршрутизатора рівня ядра та розподілу за допомогою Fast Ethernet. На головному комутаторі залишається вільних 13 портів Fast Ethernet та 1 порт Gigabit Ethernet для розширення мережі.

Зведена інформація по використанню комутаторів в різних підмережах наведена в таблиці 2.1.

Таблиця 2.1 – Використання комутаторів в підмережах

Піжмережа	Комутатори на:					
	48+2	24+2	24	12+2	12	8+1
A	1	0	0	0	0	0
B	0	5	0	0	1	1
C	1	0	0	0	0	0
D	1	1	0	0	0	0
E	15	0	1	1	0	0
F	4	0	0	0	1	1
G	1	0	0	0	0	0

Отже, з даної таблиці чітко видно які комутатори використовуються в кожній підмережі.

2.2 Розробка схеми адресації комп'ютерної мережі

2.1.1 Розрахунок адресації підмереж та вузлів на прикладі однієї підмережі

Для забезпечення міжмережевої взаємодії проведемо розрахунок фізичних та логічних з'єднань, враховуючи оптимальне використання фізичного простору.

Розглянемо розрахунок адресації на прикладі підмережі А. Враховуючи кількість вузлів, в даному випадку – 41, кількість комутаторів – 1, порт

маршрутизатора, адресу мережі та широкомовну адресу потрібно розрахувати адресацію для N=45.

Отже, потрібно обрати маску, яка б дозволяла адресувати 45 адрес (0 – 44 адрес). Розрахуємо її. Для цього переведемо 44 в двійкову форму : $44_2=101100_2$ (використовується 6 бітів для адресації вузлів і 26 бітів для зазначення номера підмережі.)

Маска в двійковій системі числення: **11111111.11111111.11111111.11**000000.

Маска в десятковій системі числення: 255.255.255.192.

Адреса мережі : 192.12.5.0 (**11000000.00001100.00000101.00**000000).

Інверсія маски: 0.0.0.127 (**00000000.00000000.00000000.00**111111).

Min IP: 192.12.5.1 (**11000000.00001100.00000101.00**000001).

Max IP: 192.12.5.62 (**11000000.00001100.00000101.00**111110).

Широкомовна адреса:192.12.5.63 (**11000000.00001100.00000101.00**111111).

Шлюз по замовчуванню (інтерфейс маршрутизатора)=192.12.5.1.

Для IP-адресації комп'ютерів виділимо діапазон адрес: 192.12.5.2 – 192.12.5.42.

Для адресації коммутатора виділимо адресу: 192.12.5.43.

Діапазон вільних IP-адрес, які можна використовувати в подальшому для розширення підмережі А: 192.12.5.44 – 192.12.5.62.

Розраховані значення для даної підмережі представлено у вигляді таблиці для зручності перегляду і користування, яка наведена в таблиці 2.2.

2.2.2 Адресація кожної з підмереж

Аналогічно прикладу розрахунку прораховуються всі інші підмережі, тому всі подальші налаштування адресації представлено лише у вигляді таблиць.

Таблиця 2.2 – Параметри адресації підмережі А

Призначення	IP-адреса
Адреса підмережі	192.12.5.0
Маска	255.255.255.192(26)
Інвертована маска	0.0.0.63
Мінімальна адреса	192.12.5.1
Максимальна адреса	192.12.5.62
Широкомовна адреса	192.12.5.63
Шлюз по замовчуванню	192.12.5.1
Діапазон адрес комп’ютерів	192.12.5.2 – 192.12.5.42
Діапазон адрес комутаторів	192.12.5.43
Діапазон вільних адрес	192.12.5.44 – 192.12.5.62

Розрахунок адресації підмережі B наведений в таблиці 2.3.

Таблиця 2.3 – Параметри адресації підмережі B

Призначення	IP-адреса
Адреса підмережі	192.12.6.0
Маска	255.255.255.0(24)
Інвертована маска	0.0.0.255
Мінімальна адреса	192.12.6.1
Максимальна адреса	192.12.6.254
Широкомовна адреса	192.12.6.255
Шлюз по замовчуванню	192.12.6.1
Діапазон адрес комп’ютерів	192.12.6.2 – 192.12.6.126
Діапазон адрес комутаторів	192.12.6.127 – 192.12.6.133
Діапазон вільних адрес	192.12.6.134 – 192.12.6.254

Розрахунок адресації підмережі C наведений в таблиці 2.4.

Таблиця 2.4 – Параметри адресації підмережі C

Призначення	IP-адреса
Адреса підмережі	192.12.7.0
Маска	255.255.255.192(26)
Інвертована маска	0.0.0.63
Мінімальна адреса	192.12.7.1
Максимальна адреса	192.12.7.62
Широкомовна адреса	192.12.7.63
Шлюз по замовчуванню	192.12.7.1
Діапазон адрес комп'ютерів	192.12.7.2 – 192.12.7.31
Діапазон адрес комутаторів	192.12.7.32
Діапазон вільних адрес	192.12.7.33– 192.12.7.62

Розрахунок адресації підмережі D наведений в таблиці 2.5.

Таблиця 2.5 – Параметри адресації підмережі D

Призначення	IP-адреса
Адреса підмережі	200.93.12.0
Маска	255.255.255.128(25)
Інвертована маска	0.0.0.127
Мінімальна адреса	200.93.12.1
Максимальна адреса	200.93.12.126
Широкомовна адреса	200.93.12.127
Шлюз по замовчуванню	200.93.12.1
Діапазон адрес комп'ютерів	200.93.12.2 – 200.93.12.60
Діапазон адрес комутаторів	200.93.12.61 – 200.93.12.62
Діапазон вільних адрес	200.93.12.63 – 200.93.12.126

Розрахунок адресації підмережі E наведений в таблиці 2.6.

Таблиця 2.6 – Параметри адресації підмережі E

Призначення	IP-адреса
Адреса підмережі	192.12.0.0
Маска	255.255.252.0(22)
Інвертована маска	0.0.3.255
Мінімальна адреса	192.12.0.1
Максимальна адреса	192.12.3.254
Широкомовна адреса	192.12.3.255
Шлюз по замовчуванню	192.12.0.1
Діапазон адрес комп’ютерів	192.12.0.2 – 192.12.2.209
Діапазон адрес комутаторів	192.12.2.210 – 192.12.2.226
Діапазон вільних адрес	192.12.2.227 – 192.12.3.254

Розрахунок адресації підмережі F наведений в таблиці 2.7.

Таблиця 2.7 – Параметри адресації підмережі F

Призначення	IP-адреса
Адреса підмережі	192.12.8.0
Маска	255.255.255.0(24)
Інвертована маска	0.0.0.255
Мінімальна адреса	192.12.8.1
Максимальна адреса	192.12.8.254
Широкомовна адреса	192.12.8.255
Шлюз по замовчуванню	192.12.8.1
Діапазон адрес комп’ютерів	192.12.8.2 – 192.12.8.199
Діапазон адрес комутаторів	192.12.8.200 – 192.12.8.205
Діапазон вільних адрес	206. – 192.12.8.254

Розрахунок адресації підмережі G наведений в таблиці 2.8.

Таблиця 2.8 – Параметри адресації підмережі G

Призначення	IP-адреса
Адреса підмережі	192.12.4.0
Маска	255.255.255.192(26)
Інвертована маска	0.0.0.63
Мінімальна адреса	192.12.4.1
Максимальна адреса	192.12.4.62
Широкомовна адреса	192.12.4.63
Шлюз по замовчуванню	192.12.4.1
Діапазон адрес комп'ютерів	192.12.4.2 – 192.12.4.36
Діапазон адрес комутаторів	192.12.4.37
Діапазон вільних адрес	192.12.4.38– 192.12.4.62

Оскільки в розробленій схемі мережі використовуються інші пристрої, які не входять в жодну з підмереж, наведемо їх адресацію. До таких пристроїв відносяться Router_1, Router_2, Router_3, Router_4, Router_5, Router_6, Router_7, Router_8 та Інтернет-провайдер. Між маршрутизаторами Router_1 та Router_2, Router_3, Router_4, Router_5, Router_6, Router_7 встановлені доточкові з'єднання, які виступають тунелями між цими маршрутизаторами. Отже наведемо адресацію даних пристроїв в таблиці 2.9.

Таблиця 2.9 – Адресація інших пристроїв

Router_1	
З'єднання між Router_1 та Інтернет	195.93.12.1/30
З'єднання між Router_1 та Router_8	199.93.12.1/30
Інтернет	
З'єднання між Інтернет та Router_1	195.93.12.2/30
З'єднання між Інтернет та Router_2	196.93.12.1/30
З'єднання між Інтернет та Router_3	197.93.12.1/30
З'єднання між Інтернет та Router_4	198.93.12.1/30
З'єднання між Інтернет та Router_5	202.93.12.1/30
З'єднання між Інтернет та Router_6	203.93.12.1/30

З’єднання між Інтернет та Router_7	204.93.12.1/30
Router_2	
З’єднання між Router_2 та Інтернет	196.93.12.2/30
З’єднання між Router_2 та підмережею A	192.12.5.1/26
Router_3	
З’єднання між Router_3 та Інтернет	197.93.12.2/30
З’єднання між Router_3 та підмережею B	192.12.6.1/24
Router_4	
З’єднання між Router_4 та Інтернет	198.93.12.2/30
З’єднання між Router_4 та підмережею C	192.12.7.1/26
Router_5	
З’єднання між Router_5 та Інтернет	202.93.12.2/30
З’єднання між Router_5 та підмережею E	192.12.0.0/22
Router_6	
З’єднання між Router_6 та Інтернет	203.93.12.2/30
З’єднання між Router_6 та підмережею F	192.12.8.1/24
Router_7	
З’єднання між Router_7 та Інтернет	204.93.12.2/30
З’єднання між Router_7 та підмережею G	192.12.4.1/26
Router_8	
З’єднання між Router_8 та Router_1	199.93.12.2/30
З’єднання між Router_8 та підмережею D	200.93.12.1/30
Tunnel 0	
IP-адреса(на стороні Router_1)	201.93.12.1/28
IP-адреса(на стороні Router_2)	201.93.12.2/28
IP-адреса(на стороні Router_3)	201.93.12.3/28
IP-адреса(на стороні Router_4)	201.93.12.4/28
IP-адреса(на стороні Router_5)	201.93.12.5/28
IP-адреса(на стороні Router_6)	201.93.12.6/28

IP-адреса(на стороні Router_7)	201.93.12.7/28

На даному етапі сформована повна інформація про схему мережі, про підмережі та їх адресацію і адресацію всіх інших пристроїв мережі.

2.3 Розробка підсистеми захисту інформаційно-комунікаційної мережі

Під захистом інформації в ІКМ розуміють діяльність, спрямовану на забезпечення безпеки оброблюваної в ІКМ інформації й ІКМ у цілому, що дає змогу запобігти реалізації загроз або унеможливити її, та зменшити ймовірність завдання збитків від реалізації загроз.

Захист інформаційно-комунікаційної мережі може бути як базовий так і додатковий, отже розглянемо кожен з них.

Як базовий захист в дипломному проекті будемо використовувати технологію VPN, криптографічні перетворення, базове налаштування безпеки, парольний захист пристроїв та списки доступу.

Маршрутизатори Router_1, Router_2, Router_3, Router_4, Router_5, Router_6, Router_7 будуть функціонувати по протоколу DMVPN, на кожен з цих маршрутизаторів встановлюємо парольний захист і застосовуємо шифрування паролів. Також відключаємо сервіси для базового налаштування захисту. На маршрутизаторах Router_2, Router_3, Router_4, Router_5, Router_6, Router_7 встановлюємо списки доступу таким чином, щоб підмережі, які під’єднуються до цих маршрутизаторів не могли взаємодіяти між собою.

Як додатковий захист в дипломному проекті будемо використовувати технологію ssh, аутентифікацію канального рівня, міжмережеві екрани, Radius-server.

На маршрутизаторі Router_8 налаштуємо технологію ssh і міжмережевий екран, який буде дозволяти тільки визначеним користувачам з визначеним ip-адресом підключатися до маршрутизатора по протоколу ssh.

Між маршрутизаторами Router_1, Router_2, Router_3, Router_4, Router_5, Router_6, Router_7 налаштуємо аутентифікацію канального рівня, а саме аутентифікацію по протоколу маршрутизації.

На маршрутизаторах, які підключаються до підмереж A, B, C, E, F, G налаштовуємо функціонування radius-server для аутентифікації на зовнішньому сервері і в кожній з підмереж на одному з ПК налаштовуємо radius-server і відповідно на кожному з цих маршрутизаторів налаштовуємо технологію ssh. Таким чином тільки визначені користувачі зможуть підключатися по ssh до маршрутизатора.

ВИСНОВКИ З ДРУГОГО РОЗДІЛУ

Нами розроблено проект структури мережі, розглянуто ієрархічну модель Cisco, яка допомагає в розробці, впровадженні й обслуговуванні масштабованих, надійних і ефективних у вартісному вираженні об’єднаних мереж, розглянуто кожен рівень цієї моделі та визначено застосування даної моделі до проекту структури мережі.

Детально розглянуто кожну з підмереж, особливості її побудови, підключення пристроїв на рівні доступу, вибір використання з’єднання.

Розглянуто розрахунок адресації на прикладі однієї підмережі, з чого чітко прослідковуються всі моменти розрахунку. Наведені адресації всіх підмереж у вигляді таблиць. Також наведена адресація тих пристроїв, які не використовуються в даних підмережах.

В результаті розробки захищеної інформаційно-комунікаційної мережі сформоване уявлення про схему мережі, про підмережі, які вона включає та про її захист.

3. ОБГРУНТУВАННЯ ВИБОРУ ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПІДСИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору обладнання та програмного забезпечення. Налагодження базових засобів міжмережевої взаємодії

В даній частині дипломного проекту необхідно обрати та обґрунтувати свій вибір мережевого обладнання для побудови мережі.

Оскільки технічні можливості ПК не дають можливості емулювати проект повністю для тестування будемо емулювати частину проекту. В реалізації даної топології обрано обладнання фірми Cisco та Juniper, які являються провідними компаніями з виготовлення мережевого обладнання.

Компанія Cisco Systems є абсолютним лідером на ринку маршрутизаторів (займає близько 70% ринку, на другому місці Juniper – 21%). Cisco пропонує моделі від найпростіших маршрутизаторів для малого офісу (серія 800) до мультигігабітних пристроїв, які розміщуються у ядрі Інтернету (серія 12000). Всі маршрутизатори Cisco працюють під управлінням операційної системи Cisco IOS. Для кожної моделі маршрутизатора пропонуються кілька різновидів IOS.

Компанія Juniper Networks є світовим лідером з виробництва високопродуктивних мережевих рішень. Компанія пропонує високопродуктивну мережеву інфраструктуру, яка створює швидкореагуюче і надійне середовище для прискорення розгортання віртуалізованних настільних систем, серверів і додатків в одній мережі.

В якості маршрутизаторів, які з’єднуються з Інтерне-провайдером та формують віртуальні з’єднання по протоколу DMVPN обираємо обладнання фірми Cisco, оскільки обладнання саме цієї фірми підтримує протокол DMVPN.

Отже для забезпечення функціонування мережі потрібні маршрутизатори з наявністю таких портів:

- 1 маршрутизатор Cisco, який має 4 порти Gigabit Ethernet – маршрутизатор Internet;
- 1 маршрутизатор Cisco, який має 3 порти Gigabit Ethernet – маршрутизатор R_2_26_1;
- 1 маршрутизатор Cisco, який має 2 порти Gigabit Ethernet – маршрутизатор RS_2_26_3, підключається до підмережі B;
- 2 маршрутизатори Cisco, які мають 1 порт Gigabit Ethernet та 1 порт Fast Ethernet – маршрутизатор RS_2_26_2 та RS_2_26_4, підключаються до підмереж A та C.

Ще однією умовою є те, що ці маршрутизатори мають підтримувати технологію DMVPN та відповідні протоколи шифрування, які використовуються.

Аналіз пошуку показав, що даним вимогам підлягає аналог реального обладнання маршрутизатор моделі Cisco 3825. Він має 2 порти Gigabit Ethernet, тому в деяких випадках потрібно використовувати додатково модулі. В даний маршрутизатор можна включити до 6 модулів. Отже будемо використовувати модуль розширення Cisco HWIC-1FE для підключення Fast Ethernet там де це потрібно, і модуль Cisco HWIC-1GE-SFP для підключення Gigabit Ethernet. Технічні характеристики даного маршрутизатора та модулів наведені в додатку А.

Також потрібен маршрутизатор Juniper, який матиме 3 порти Gigabit Ethernet. Такій вимозі підлягає маршрутизатор Juniper MX80. Технічні характеристики даного маршрутизатора наведені в додатку А.

Рівень доступу в спроектованій схемі мережі представлений сукупністю комутаторів, робочих станцій та серверного обладнання. Оскільки конфігурації робочих станцій та серверного обладнання постійно змінюються, то не має сенсу їх описувати і вибирати. Лише слід відмітити, що вузли повинні мати мережеві карти з підтримкою відповідних підключень.

В дипломному проекті використовуються комутатори на 48 порти + 2 додаткові порти з підтримкою технології Gigabit Ethernet. Аналогом реального

обладнання було обрано комутатор Catalyst WS-C2950G-48-EI фірми Cisco з інтерфейсами Fast Ethernet і Gigabit Ethernet, технічні характеристики якого наведені в додатку А.

Також використовуються комутатори на 24 порти + 2 додаткові порти з підтримкою технології Gigabit Ethernet. Аналогом реального обладнання було обрано комутатор Catalyst WS-C2950G-24 фірми Cisco з інтерфейсами Fast Ethernet і Gigabit Ethernet, технічні характеристики якого наведені в додатку А.

Для побудови підмережі В задіяний комутатор на 12 портів в яких усі порти підтримують технологію Gigabit Ethernet, тому аналогом було обрано комутатор моделі Catalyst WS-C3550-12T фірми Cisco на 12 портів. Для цієї ж підмережі задіяний комутатор на 8 портів Fast Ethernet + 1 додатковий комбо-порт. Аналогом реального обладнання було обрано комутатор Huawei S2309TP-EI-AC.

Для побудови підмережі D використовуються комутатори на 48+4 та на 24+4 порти. Аналогами реального обладнання були обрані такі комутатори Juniper EX3300-48T та Juniper EX2200-24P.

В додатку А наведено детальні технічні характеристики обраного обладнання.

Оскільки мережеве обладнання відсутнє, то емуляцію спроектованої мережі будемо проводити в GNS3.

Основні переваги GNS3:

- Повний функціонал емульованого пристроїв - тобто запустивши той же маршрутизатор Cisco, нам будуть доступні практично всі функції, які працюють на реальному маршрутизаторі. Якщо згадати Cisco Packet Tracer, то там значна частина функціоналу недоступна, тому що це всього лише симулятор.
- Можливість побудови гетерогенних мереж - ми можемо зібрати схему де будуть не тільки пристрої Cisco, а й Juniper, Mikrotik, CheckPoint і т.д. Це зручно у побудові емуляції мережі, тому що в реальному житті рідко зустрічається організація, де вся мережа

побудована на обладнанні одного виробника.

- Додавання в мережу повноцінних робочих станцій і серверів – у Cisco Packet Tracer в якості кінцевих пристроїв були доступні клієнтські комп'ютери або сервери з дуже обмеженим функціоналом. У GNS3 ми можемо додати повноцінний комп'ютер з Windows або Ubuntu.

GNS3 ефективно функціонує з програмним комплексом VirtualBox, який орієнтується на віртуалізацію операційних систем Microsoft Windows, Linux, FreeBSD, Solaris/OpenSolaris, ReactOS, DOS та інших.

Для налаштування базових засобів міжмережевої взаємодії потрібно налаштувати ip-адреси на інтерфейсах маршрутизаторів згідно таблиць, які були розроблені в другому розділі та протокол маршрутизації. Для реалізації функціонування мережі обираємо протокол маршрутизації OSPF.

Також щоб всі компоненти системи взаємодіяли між собою потрібно налаштувати ip-адресацію на кінцевих пристроях, а саме на робочих станціях та серверному обладнанні. Для зручності було налаштовано функціонування DHCP-сервера на маршрутизаторах, які підключені до під мереж A, B та C, а в підмережі A для S_2_26_2 налаштовано DHCP-сервер з прив’язкою до MAC-адреси.

Щоб переконатися в правильності налаштувань виконаємо первірку за допомогою команди ping між підмережами A та D. Результати виконання даної команди приведені на рисунку 3.1.

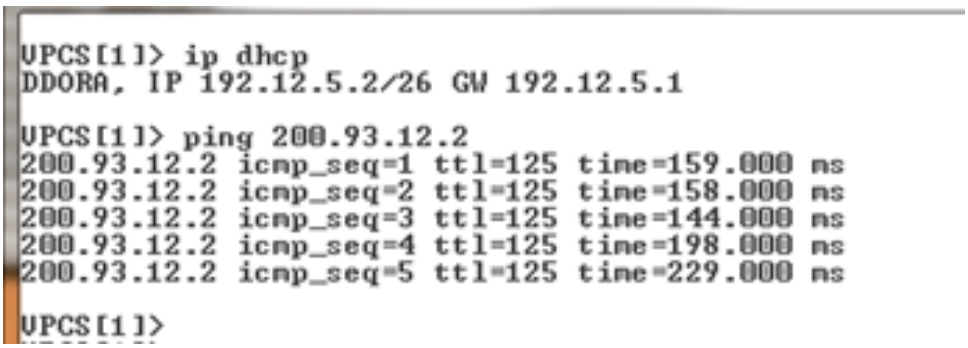


Рисунок 3.1 – Виконання команди ping між підмережами A та D

3.2 Налаштування елементів підсистеми захисту інформаційно-комунікаційної мережі

3.2.1 Налагодження маршрутизаторів Cisco

Наступним етапом налаштування було налаштування між маршрутизаторами R_2_26_1, RS_2_26_2, RS_2_26_3 та RS_2_26_4 протоколу DMVPN. Для правильного функціонування DMVPN спочатку проводимо налаштування mGRE інтерфейсів на R_2_26_1, RS_2_26_2, RS_2_26_3, RS_2_26_4. Для адресації тунелів виділена мережа 201.93.12.0/24, всі тунелі знаходяться в одній мережі.

Для прикладу наведемо сценарій налаштування на прикладі маршрутизатора R_2_26_1:

```
R_2_26_1 (config)#interface Tunnel0
R_2_26_1 (config-if)#ip add 201.93.12.1 255.255.255.0
R_2_26_1 (config-if)#ip mtu 1400
R_2_26_1 (config-if)#ip nhrp map multicast dynamic
R_2_26_1 (config-if)#ip nhrp network-id 1
R_2_26_1 (config-if)#ip nhrp holdtime 400
R_2_26_1 (config-if)#ip tcp adjust-mss 1360
R_2_26_1 (config-if)#tunnel source f0/1
R_2_26_1 (config-if)#tunnel mode gre multipoint
R_2_26_1 (config-if)#tunnel path-mtu-discovery
```

На наступному етапі налаштовуємо динамічну маршрутизацію eigrp.

Наступним пунктом буде налаштування IPsec, перша фаза цього налаштування полягає в налагоджені IKE. Друга фаза – налагодження IPsec-профілю.

Для прикладу покажемо процес налаштувань на маршрутизаторі R_2_26_1:

```
R_2_26_1 (config)#crypto keyring DMVPN
R_2_26_1 (conf-keyring)#local-address f0/1
```

R_2_26_1 (conf-keyring)#pre-shared-key address 0.0.0.0 0.0.0.0 key secret

R_2_26_1 (conf-keyring)#crypto isakmp policy 10

R_2_26_1 (config-isakmp)#encr 3des

R_2_26_1 (config-isakmp)#authentication pre-share

R_2_26_1 (config-isakmp)#group 2

R_2_26_1 (config-isakmp)#crypto isakmp invalid-spi-recovery

R_2_26_1 (config)#crypto isakmp keepalive 10 periodic

R_2_26_1 (config)#crypto isakmp profile DMVPN

R_2_26_1 (conf-isa-prof)#keyring DMVPN

R_2_26_1 (conf-isa-prof)#match identity address 0.0.0.0

R_2_26_1 (conf-isa-prof)#local-address f0/1

R_2_26_1 (conf-isa-prof)# crypto ipsec transform-set ESP-3DES-SHA-HMAC esp-3des esp-sha-hmac

R_2_26_1 (cfg-crypto-trans)#crypto ipsec profile DMVPN

R_2_26_1 (ipsec-profile)#set transform-set ESP-3DES-SHA-HMAC

R_2_26_1 (ipsec-profile)#set isakmp-profile DMVPN

R_2_26_1 (ipsec-profile)#int Tunnel0

R_2_26_1 (config-if)#tunnel protection ipsec profile DMVPN

На маршрутизаторах RS_2_26_2, RS_2_26_3, RS_2_26_4 налаштовано списки доступу таким чином, щоб користувачі з різних підмереж, а саме з A, B та C не могли взаємодіяти між собою.

Також була налаштована аутентифікація протокола маршрутизації EIGRP.

Для прикладу наведено налаштування на маршрутизаторі Internet:

На всіх маршрутизаторах були відключені сервіси для налагодження безпеки маршрутизатора.

Оскільки сервер S_2_26_2 не може напряму взаємодіяти з Internet, то було проведено налаштування підключення по ssh спочатку до RS_2_26_2 і вже через нього до маршрутизатора Internet, парольний доступ. Було вибрано підключення по ssh, адже пароль в конфігураційному файлі знаходиться в

зашифрованому вигляді.

Налагоджено маршрутизатор RS_2_26_2 для аутентифікації на зовнішньому сервері, приклад налаштування:

RS_2_26_2 (config)#aaa new-model

RS_2_26_2 (config)#aaa authentication login default radius

RS_2_26_2 (config)#radius-server host 192.12.5.2 auth-port 1812 acct-port 1813

RS_2_26_2 (config)#radius-server key testing123

Для шифрування паролів (встановлення паролів типу 7) на маршритузаторах Cisco використовується команда service password-encryption.

Конфігураційні файли цих маршрутизаторів наведені в додатку Б.

3.2.2 Налагодження маршрутизатора Juniper

На маршрутизаторі налаштовуємо протокол ssh, створюємо користувача, забороняємо підключатися користувачу root, встановлюємо кількість одночасних підключень – 10, а також кількість спроб вводу паролю за 1 хвилину – 4.

Приклад налаштувань:

set system services ssh

set system services ssh protocol-version v2

set system login user Lavryk class super-user authentication plain-text-password

set system services ssh root-login deny

set system services ssh connection-limit 10

set system services ssh rate-limit 4

Також на цьому маршрутизаторі налаштовано firewall, а саме доступ по ssh відкритий тільки для однієї IP-адреси.

Наведемо приклад налаштування:

edit firewall filter deny-ssh

set term 1 from source-address 0/0

set term 1 from source-address 200.93.12.2

set term 1 from destination-port ssh

set term 1 from then log discard

set term 2 then accept

set interfaces lo0 unit 0 family inet filter input deny-ssh

Конфігураційний файл цього маршрутизатора наведений в додатку Б.

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

Був проведений вибір обладнання в залежності від того, які інтерфейси використовуються, яка швидкість інтерфейсів, які технології та протоколи використовуються.

Обгрунтовано вибір GNS та VBox для емуляції схеми мережі. Налаштовано базові засоби міжмережевої взаємодії, а також проведена перевірка.

Налаштовано елементи підсистеми захисту інформаційно-комунікаційної мережі, наведено приклади налаштувань, проведено тестування функціонування побудованої підсистеми захисту інформаційно-комунікаційної мережі.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Анин Б. Защита компьютерной информации / Б. Анин. – СПб.: БХВ-Петербург, 2000. – 384 с.
2. Бабак В. П. Теоретичні основи захисту інформації : Підручник / В. П. Бабак. – К.: НАУ, 2008. – 752 с.
3. Бабак В. П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В. П. Бабак, О. Г. Корченко. – К.: НАУ, 2003. – 670 с.
4. Белов Е. Б. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
5. Браун С. Виртуальные частные сети / С. Браун. – Лори, 2001. – 503 с.
6. Богуш В. М. Інформаційна безпека від А до Я / В. М. Богуш, А. М. Кусин. – К.: МОУ, 1999. – 456 с.
7. Васильчук М. В. та ін. Основи охорони праці / М. В. Васильчук. – К.: Просвіта, 1997. – 208 с.
8. Гайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
9. Гайкович В. Ю. Информационная безопасность компьютерных сетей. Технологии электронных коммуникаций / В. Ю. Гайкович, П. В. Дорошкевич , В. К. Левин. – М. 1993. т.5. –128 с.
10. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебное пособие / В. И. Завгородний. – М.: Логос, 2001. – 264 с.
11. Запечников С. В. Основы построения виртуальных частных сетей / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. – М.: Телеком, 2003. – 248 с.

12. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452с.
13. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб.: В НУ, 2000. – 356 с.
14. Конахович Г. Ф. Захист інформації в мережах передачі даних: Підручник / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдін. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с.
15. Лукацкий А.В. VPN – старые песни о главном / А. В. Лукацкий // Компьютер-Пресс. – 2001. № 5. – 107 с.
16. Малюк А. А. Введение в защиту информации в автоматизированных системах: Учеб. Пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – М.: Горячая линия – Телеком, 2005. – 147 с.
17. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика; Электронинформ, 1997. – 368с.
18. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, И. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 1999. – 328 с.

ДОДАТКИ

Додаток А

Технічні характеристики обладнання

Маршрутизатор Cisco 3825



Рисунок Б.1 – Загальний вигляд маршрутизатора Cisco 3825

Опис: 2 порти Gigabit Ethernet (10/100/1000Base-T), один порт SFP, 2 слота NME, 4 слота HWIC (підтримка VIC, VWIC і WIC модулів), і два слота AIM.

Серія багатосервісних маршрутизаторів Cisco 3800 побудована на базі потужної серії багатофункціональних маршрутизаторів серії Cisco 3700. Дана серія призначена, перш за все, для завдань по забезпеченню безпеки і голосових сервісів, а також інших типів додатків. Достатньо потужне рішення на базі Cisco 3800 (від 350 до 500 Kpps) дозволяє вирішувати завдання на базі декількох інтерфейсів Fast Ethernet на одному слоті, вирішувати завдання по об'єднанню мереж, що працюють за принципом time-division multiplexing (TDM), а також забезпечувати інтеграцію технології IEEE 802.3af Power over Ethernet (PoE) в існуючих мережах.

Серія Cisco 3800, завдяки Cisco IOSR Software Advanced Security Feature Set, може виконувати функції із забезпечення мережної безпеки, серед яких варто відзначити firewall, intrusion prevention, IPSec VPN, Secure Shell (SSH) 2.0 і SNMP v3, network admissions control (NAC), Voice and Video Enabled VPN (V3PN), Dynamic Multipoint VPN (DMVPN) і Easy VPN. Маршрутизатори серії Cisco 3800 можуть легко інтегруватися в корпоративні мережі великого рівня для забезпечення сервісів IP на базі однієї платформи. Так, наприклад, рішення на базі інтегрованого Cisco CallManager Express (CME) забезпечує задачу по забезпечення VoIP сервісів з використанням до 240 Cisco IP-phones (на Cisco 3825 можливо організація рішення до 168 IP-телефонів).

Модуль Cisco HWIC-1FE



Рисунок Б.2 – Загальний вигляд модуля Cisco HWIC-1FE

Опис: 1 порт 10/100BaseT для маршрутизаторів серії 1800, 2800, 3800.

Технічні характеристики:

- розміри (ширина x глибина x висота), см: 7.82 x 12.03 x 1.93;
- вага, кг: 0.063;
- тип інтерфейсу: HWIC;
- інтерфейсні порти: 1 x RJ-45;
- швидкість передачі даних: 100 Мбіт / с;
- типи кабелів: кабель RJ-45.

Мережеві особливості:

1. особливості Ethernet і VLAN:

- IEEE802.3 with IEEE802.2 Service Advertising Protocol (SAP);
- IEEE802.3 with IEEE802.2 and Subnetwork Access Protocol (SNAP);
- IEEE 802.1Q VLAN tagging;
- Auto-MDIX;
- унікальна MAC-адреса;
- підтримка Simple Network Management Protocol (SNMP).

2. додаткові особливості:

- Cisco Group Management Protocol and Internet Group Management Protocol (IGMP) для багатоадресної передачі;
- High availability, supporting Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP);
- особливості MPLS, в залежності від платформи;

- Generic routing encapsulation (GRE);
- IPv6;
- IP Security (IPsec) (crypto map);
- Layer 2 Tunneling Protocol Version 3 (L2TPv3) tunnel termination;
- Dynamic Host Configuration Protocol (DHCP) client and server;
- Network Address Translation (NAT);
- Generic Traffic Shaping (GTS);
- Media Gateway Control Protocol (MGCP) bind;
- особливості IBM;
- Point-to-Point Protocol over Ethernet (PPPoE) client;
- Bridging.

Модуль Cisco HWIC-1GE-SFP



Рисунок Б.3 – Загальний вигляд модуля Cisco HWIC-1GE-SFP

Опис: Високопродуктивний модуль Cisco Gigabit Ethernet High-Speed WAN Interface Card (HWIC) дає можливість використовувати з'єднання Gigabit Ethernet маршрутизаторам Cisco 2800 і 3800 серій для прискорення таких додатків, як доступ Metro Ethernet, маршрутизація у віртуальних мережах, і високошвидкісне з'єднання з LAN-комутаторами.

Технічні характеристики:

- розміри (ширина x глибина x висота), см: 7.9 x 12.2 x 2.1;
- тип інтерфейсу: HWIC;
- інтерфейсні порти: 1 x SFP;
- швидкість передачі даних: 1 Гбіт / с;
- типи кабелів: кабель SFP.

Мережеві особливості:

1. особливості Ethernet і VLAN:

- IEEE802.3 with IEEE802.2 Service Advertising Protocol (SAP);
- IEEE802.3 with IEEE802.2 and Subnetwork Access Protocol (SNAP);
- IEEE 802.1Q VLAN tagging;
- Flow control (802.3x);
- Gigabit EtherChannel для надмірності з'єднання.

2. додаткові особливості:

- підтримка Jumbo frame до 9576 байт;
- Cisco Group Management Protocol and Internet Group Management Protocol (IGMP) for multicasting;
- High availability, supporting Hot Standby Router Protocol (HSRP), Virtual Router Redundancy. Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP);
- Hot insertion and removal for SFPs on all platforms;
- відображення типу (Media або SFP) через інтерфейс командного рядка (CLI).

Маршрутизатор Juniper MX80



Рисунок Б.4 – Загальний вигляд маршрутизатора Juniper MX80

Опис: 4 порти 10GE (XFP), 2 слота для встановлення MIC модулів.

Основні особливості:

- 4,000,000 IPv4 prefixes in the RIB;
- 1,000,000 IPv4 prefixes in the FIB;
- підтримка протоколів третього рівня: BGP, IS-IS, OSPF, MPLS-TE, l2/l3 vpn, VPLS, Multicast VPN, RSVP/LDP;

- підтримка механізмів комутації пакетів на другому рівні: dot1q vlan switching, QnQ tunneling, і.т.д.;
- Inline jflow (за наявності ліцензії);
- Subscriber Management (BRAS функціонал, за наявності ліцензії);
- відсутня підтримка NAT;
- підтримка механизом QoS/H-QoS, bandwith policing/shaping;
- немає підтримки MIC карт на 4 порти 10 Гбіт/сек.

Комутатор Juniper EX3300-48T



Рисунок Б.5 – Загальний вигляд комутатора Juniper EX3300-48T

Опис: комутатор Layer 3, 48 портів 10/100/1000Base-T, 4 порти 1000Base-X (SFP +).
Основні особливості:

- розмір таблиці MAC-адрес: 16000;
- кількість VLAN: 4096;
- протоколи маршрутизації: RIP v1/v2, OSPF, BGP;
- кількість активних unicast-маршрутів: 8000;
- функція BFD;
- функція віртуальних маршрутизаторів (VRF);
- функція Dynamic ARP Inspection;
- функція IP Source Guard;
- функція Virtual Chassis;
- функція Cable Diagnostic;
- підключення зовнішнього БП, через спеціальний роз'єм;
- гаряча заміна блоків вентиляції та швидка заміна блоку живлення.

Комутатор Juniper EX2200-24P



Рисунок Б.6 – Загальний вигляд комутатора Juniper EX2200-24P

Опис: комутатор Layer 2 +, 24 порти 10/100/1000Base-T з підтримкою PoE, 4 порти 1000Base-X (SFP).
Основні особливості:

- розмір таблиці MAC-адрес: 16000;
- кількість VLAN: 1024;
- протоколи маршрутизації: RIP v1/v2, OSPF (v1/v2 за наявності ліцензії, до 4 інтерфейсів);
- кількість активних unicast-маршрутів: 6500;
- функція Dynamic ARP Inspection;
- функція IP Source Guard;
- функція Cable Diagnostic;
- стекування (Junos OS 12.2, за наявності ліцензії);
- PoE.

Комутатор Cisco Catalyst WS-C2950G-48-EI



Рисунок Б.7 – Загальний вигляд комутатора Cisco Catalyst WS-C2950G-48-EI

Опис: Layer2, 48 портів 10/100Base-TX і 2 порти 1000BaseX (фільтрація L2-L4)
Основні функції:

- підтримка MVR (multicast vlan registration), DHCP opt.82 insertion, QoS mark/remark, DHCP snooping;

- повнофункціональна фільтрація Layer3 і Layer4 (ACL - access control list). Обмеження доступу по IP (layer 3) і номером порту tcp/udp (layer 4);
- керований дуплекс на всіх портах (авто, напівдуплексний і повнодуплексний режими);
- можливість автоматичного або примусового переходу на 10base-T і 100base-Tx на всіх мідних портах;
- високошвидкісна внутрішня комутація;
- повна підтримка VLAN включаючи 802.1q (256 active VLANs, 4094 Vlan ID);
- підтримка Voice VLAN і 802.1x;
- підтримка транкового технології Fast EtherChannel для створення єдиного логічного з'єднання з пропускною здатністю 800 Мб/сек;
- підтримка протоколу Cisco Group Management Protocol (CGMP);
- розвинені функції щодо забезпечення безпеки;
- вбудоване програмне забезпечення Cisco IOS забезпечує найбільші функціональні можливості для кінцевої інтеграції активного устаткування, включаючи створення високошвидкісних магістралей;
- наявність flash-пам'яті і конфігурації за умовчанням дозволяє включати комутатори в роботу з мінімальною кількістю змін, а також дозволяє зберігати конфігурацію пристрою при відключенні живлення;
- режим автоконфігурірованія полегшує процес введення в експлуатацію нових комутаторів. Це забезпечується копіюванням конфігурації на кілька комутаторів по мережі з одного завантажувального сервера;
- протокол Cisco Discovery Protocol (CDP) дозволяє станції мережевого управління з програмним забезпеченням CiscoWorks автоматично розпізнавати комутатор в складі обчислювальної системи;
- підтримка чотирьох груп RMON;
- управління пристроєм через платформу CiscoWorks Windows дозволяє використовувати єдиний інтерфейс керування для всіх пристроїв Cisco (маршрутизаторів, комутаторів, концентраторів) в складі обчислювальної системи;
- вбудований web-сервер для управління;
- пріоритезація трафіку (802.1p);
- можливість об'єднання комутаторів Cisco Catalyst серій 2900-XL, 3500-XL, 2950, 1900 в кластер;
- режим security - прив'язка до 132 MAC-адрес до порту вручну;
- управління потоками трафіку за стандартом 802.3x;
- підтримка протоколу Spanning Tree – збільшення надійності використовуючи надлишкову топологію;
- можливість об'єднувати порти в транки для збільшення швидкості;
- можливість оновлення прошивки.

Комутатор Cisco Catalyst WS-C2950G-24



Рисунок Б.8 – Загальний вигляд комутатора Cisco Catalyst WS-C2950G-24

Опис: Layer2, 24 порту 10/100Base-TX і 2 порти 1000BaseX (фільтрація L2-L4).

Основні функції:

- підтримка MVR (multicast vlan registration), DHCP opt.82 insertion, QoS mark/remark, DHCP snooping;
- повнофункціональна фільтрація Layer3 і Layer4 (ACL – access control list);
- обмеження доступу по IP (layer 3) і номером порту tcp / udp (layer 4);
- керований дуплекс на всіх портах (авто, напівдуплексний і повнодуплексний режими);
- можливість автоматичного або примусового переходу на 10base-T і 100base-Tx на всіх мідних портах;
- високошвидкісна внутрішня комутація;
- повна підтримка VLAN включаючи 802.1q (256 active VLANs, 4094 Vlan ID);
- підтримка Voice VLAN і 802.1x;
- підтримка транкової технології Fast EtherChannel для створення єдиного логічного з'єднання з пропускною здатністю 800 Мб/сек;
- підтримка протоколу Cisco Group Management Protocol (CGMP);
- розвинені функції щодо забезпечення безпеки;

- вбудоване програмне забезпечення Cisco IOS забезпечує найбільші функціональні можливості для кінцевої інтеграції активного устаткування, включаючи створення високошвидкісних магістралей;
- наявність flash-пам'яті і конфігурації за умовчанням дозволяє включати комутатори в роботу з мінімальною кількістю змін, а також дозволяє зберігати конфігурацію пристрою при відключенні живлення;
- режим автоконфігурірованія полегшує процес введення в експлуатацію нових комутаторів. Це забезпечується копіюванням конфігурації на кілька комутаторів по мережі з одного завантажувального сервера;
- протокол Cisco Discovery Protocol (CDP) дозволяє станції мережевого управління з програмним забезпеченням CiscoWorks автоматично розпізнавати комутатор в складі обчислювальної системи;
- підтримка чотирьох груп RMON;
- управління пристроєм через платформу CiscoWorks Windows дозволяє використовувати єдиний інтерфейс керування для всіх пристроїв Cisco (маршрутизаторів, комутаторів, концентраторів) в складі обчислювальної системи;
- вбудований web-сервер для управління;
- можливість об'єднання комутаторів Cisco Catalyst серій 2900-XL, 3500 XL, 2950, 1900 в кластер;
- режим security – прив'язка до 132 MAC-адрес до порту вручну;
- управління потоками трафіку за стандартом 802.3x;
- підтримка протоколу Spanning Tree – збільшення надійності використовуючи надлишкову топологію;
- можливість об'єднувати порти в транки для збільшення швидкості;
- можливість оновлення прошивки.

Комутатор Cisco Catalyst WS-C3550-12T



Рисунок Б.9 – Загальний вигляд комутатора Cisco Catalyst WS-C3550-12T

Опис: Layer3, 2 порти 1000BaseX, 10 портів 1000BaseTX.

Основні особливості:

- підтримка IP Unnumbered for VLAN-SVI interfaces, IP Source Guard, DHCP Snooping, IEEE 802.1Q and Layer 2 Protocol Tunneling;
- високошвидкісна маршрутизація трафіку: завдяки технології Cisco Express Forwarding (CEF) серія Catalyst 3550 забезпечує високопродуктивну маршрутизацію трафіку IP. Програмне забезпечення SMI підтримує статичну, RIPv1 і RIPv2 маршрутизацію, а EMI - ще й OSPF, IGRP, EIGRP, а також маршрутизацію multicast-трафіку (PIM, DVMRP, IGMP snooping);
- висока безпека: підтримка протоколу 802.1x, функціональність Identity Based Networking Services (IBNS), списки доступу для трафіку, комутованого на другому рівні (VLAN ACL), на третьому і четвертому рівнях (Router ACL), а також Port-based ACLs (PACL). Для забезпечення безпеки при адмініструванні підтримуються протоколи SSH і SNMPv3, а також централізована аутентифікація на TACACS + і RADIUS серверах;
- висока доступність: для захисту від збоїв внутрішніх блоків живлення комутатори Catalyst 3550 підтримують ре-зервной системи живлення Cisco Redundant Power System 300 (RPS 300) і 675 (RPS 675), протоколи 802.1D, 802.1s, 802.1w, функціональність UplinkFast, CrossStack UplinkFast (CSUF), HSRP, UDLD, Aggressive UDLD, Switch port Auto-recovery;
- підтримка якості обслуговування (QoS): класифікація трафіку по полям DSCP або 802.1p (CoS), стандартні і розширені списки доступу для виділення заданого типу трафіка, WRED, черговість Strict Priority, Weighted Round Robin.;
- існує можливість визначення максимальної смуги для певного виду трафіку, а також виділення гарантованої смуги CIR;
- відмінна керованість: запроваджене в комутатор ПЗ Cisco CMS, підтримка управління за допомогою SNMP-плат-форм, таких як CiscoWorks, підтримка SNMP версій 1, 2, 3, Telnet, RMON, SPAN, RSPAN, NTP, TFTP;
- комутатори забезпечують одночасну роботу всіх портів на швидкості каналу.

Додаток Б

Конфігураційні файли маршрутизаторів

Файл конфігурації маршрутизатора Juniper:

```
    }
    services {
        ssh {
            root-login deny;
            protocol-version v2;
            connection-limit 10;
            rate-limit 4;
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    em1 {
        unit 0 {
            family inet {
                address 199.93.12.2/30;
            }
        }
    }
```

```
    em2 {
        unit 0 {
            family inet {
                address 200.93.12.1/25;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input deny-ssh;
                }
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface all;
        }
    }
}
firewall {
    filter deny-ssh {
        term 1 {
            from {
                source-address {
                    0.0.0.0/0;
                    200.93.12.2/32 except;
                }
                destination-port ssh;
            }
            then {
                log;
                discard;
            }
        }
        term 2 {
            then accept;
        }
    }
}
```

Файл конфігурації маршрутизатора R_2_26_1:

```
Current configuration : 2458 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2_26_1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
key chain priv
 key 1
   key-string 393
!
archive
 log config
  hidekeys
!
crypto keyring DMVPN
  local-address FastEthernet0/1
  pre-shared-key address 0.0.0.0 0.0.0.0 key secret
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 0.0.0.0
   local-address FastEthernet0/1
!
crypto ipsec transform-set ESP-3DES-SHA-HMAC esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set ESP-3DES-SHA-HMAC
 set isakmp-profile DMVPN
!
interface Tunnel0
 ip address 201.93.12.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 400
 ip tcp adjust-mss 1360
```

```
 ip ospf network broadcast
 ip ospf priority 2
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 ip address 194.93.12.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 195.93.12.1 255.255.255.252
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 priv
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 199.93.12.1 255.255.255.252
 duplex auto
 speed auto
!
router eigrp 1
 network 195.93.12.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet1/0
 no passive-interface Tunnel0
 network 194.93.12.0 0.0.0.3 area 0
 network 199.93.12.0 0.0.0.3 area 0
 network 201.93.12.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Файл конфігурації маршрутизатора RS_2_26_2:

```
Current configuration : 3048 bytes
!
```

```
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RS_2_26_2
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa authentication login default group radius
!
aaa session-id common
memory-size iomem 5
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.12.5.44 192.12.5.62
!
ip dhcp pool NastyaY
   network 192.12.5.0 255.255.255.192
   default-router 192.12.5.1
!
no ip domain lookup
ip domain name lavrik
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
username NastyaY privilege 15 password 7 09604B0718
archive
 log config
  hidekeys
!
crypto keyring DMVPN
  local-address FastEthernet0/0
  pre-shared-key address 0.0.0.0 0.0.0.0 key secret
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 0.0.0.0
   local-address FastEthernet0/0
!
crypto ipsec transform-set ESP-3DES-SHA-HMAC esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set ESP-3DES-SHA-HMAC
 set isakmp-profile DMVPN
!
ip ssh authentication-retries 5
!
interface Tunnel0
```

```
 ip address 201.93.12.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 201.93.12.1 195.93.12.1
 ip nhrp map multicast 195.93.12.1
 ip nhrp network-id 1
 ip nhrp holdtime 400
 ip nhrp nhs 201.93.12.1
 ip tcp adjust-mss 1360
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 ip address 196.93.12.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.12.5.1 255.255.255.192
 ip access-group 1 out
 duplex auto
 speed auto
!
router eigrp 1
 network 196.93.12.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Tunnel0
 network 192.12.5.0 0.0.0.63 area 0
 network 201.93.12.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 1 deny   192.12.6.0 0.0.0.255
access-list 1 deny   192.12.7.0 0.0.0.63
access-list 1 permit any
no cdp run
!
radius-server host 192.12.5.2 auth-port 1812 acct-port 1813
radius-server key 7 044F0E151B284249584B56
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
```

```
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 login local
 transport input ssh
 transport output ssh
!
end
```

Файл конфігурації маршрутизатора RS_2_26_3:

```
Current configuration : 2534 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RS_2_26_3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.12.6.134 192.12.6.254
!
ip dhcp pool NastyaU
   network 192.12.6.0 255.255.255.0
   default-router 192.12.6.1
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto keyring DMVPN
  local-address FastEthernet0/0
  pre-shared-key address 0.0.0.0 0.0.0.0 key secret
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 0.0.0.0
   local-address FastEthernet0/0
!
crypto ipsec transform-set ESP-3DES-SHA-HMAC esp-3des esp-sha-hmac
```

```
!
crypto ipsec profile DMVPN
 set transform-set ESP-3DES-SHA-HMAC
 set isakmp-profile DMVPN
!
interface Tunnel0
 ip address 201.93.12.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 201.93.12.1 195.93.12.1
 ip nhrp map multicast 195.93.12.1
 ip nhrp network-id 1
 ip nhrp holdtime 400
 ip nhrp nhs 201.93.12.1
 ip tcp adjust-mss 1360
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 ip address 197.93.12.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.12.6.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
router eigrp 1
 network 197.93.12.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Tunnel0
 network 192.12.6.0 0.0.0.255 area 0
 network 201.93.12.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 1 deny   192.12.5.0 0.0.0.63
access-list 1 deny   192.12.7.0 0.0.0.63
access-list 1 permit any
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Файл конфігурації маршрутизатора RS_2_26_4:

```
Current configuration : 2536 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RS_2_26_4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.12.7.33 192.12.7.62
!
ip dhcp pool NastyaI
   network 192.12.7.0 255.255.255.192
   default-router 192.12.7.1
!
no ip domain lookup
ip domain name lab.local
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto keyring DMVPN
  local-address FastEthernet0/0
  pre-shared-key address 0.0.0.0 0.0.0.0 key secret
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 0.0.0.0
   local-address FastEthernet0/0
!
crypto ipsec transform-set ESP-3DES-SHA-HMAC esp-3des esp-sha-hmac
!
crypto ipsec profile DMVPN
 set transform-set ESP-3DES-SHA-HMAC
```

```
 set isakmp-profile DMVPN
!
interface Tunnel0
 ip address 201.93.12.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 201.93.12.1 195.93.12.1
 ip nhrp map multicast 195.93.12.1
 ip nhrp network-id 1
 ip nhrp holdtime 400
 ip nhrp nhs 201.93.12.1
 ip tcp adjust-mss 1360
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel path-mtu-discovery
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 ip address 198.93.12.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.12.7.1 255.255.255.192
 ip access-group 1 out
 duplex auto
 speed auto
!
router eigrp 1
 network 198.93.12.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Tunnel0
 network 192.12.7.0 0.0.0.63 area 0
 network 201.93.12.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 1 deny   192.12.6.0 0.0.0.255
access-list 1 deny   192.12.5.0 0.0.0.63
access-list 1 permit any
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
```

```
 login
!
end
```