МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії (ЗФН)
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ Аліна САВЧЕНКО
«_____» _____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"МАГІСТР"

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ "КОМП'ЮТЕРНІ НАУКИ"

Тема: "Прикладний програмний інтерфейс для маршрутизатора Cisco"

Виконавець: Чайченко Олег Олегович

Керівник: к.т.н., доцент Савченко Аліна Станіславівна

Нормоконтролер: _____ Ігор РАЙЧЕВ

Київ — 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії (ЗФН)

Кафедра Комп'ютерних інформаційних технологій

Галузь знань, спеціальність, освітньо-професійна програма: 12 "Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології"

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Аліна САВЧЕНКО

"_____" _____ 2021 р.

ЗАВДАННЯ

на виконання дипломної роботи студента

Чайченко Олега Олеговича

(прізвище, ім'я, по батькові)

1. Тема проекту: «Прикладний програмний інтерфейс для маршрутизатора Cisco» затверджена наказом ректора від 12.10.2021 за № 2228/ст.

2. Термін виконання роботи: з 12.10.2021 по 31.12.2021.

3. Вихідні дані до роботи: Прикладний програмний інтерфейс для маршрутизатора Cisco.

4. Зміст пояснювальної записки: Вивчення прикладного програмного інтерфейсу для маршрутизатора Cisco. Опис та технологія використання прикладного програмного інтерфейсу в різних режимах, план, аналіз та розробка метода, висновок.

5. Перелік обов'язкового ілюстративного матеріалу: таблиці, схеми, графіки, презентація.

6. Календарний план-графік

№ п/п	Завдання	Термін виконання	Підпис керівника
1	Аналіз літератури та джерел за темою дипломного проекту.	12.10.2021 – 15.10.2021	
2	Розробка та затвердження плану дипломного проекту.	15.10.2021	
3	Проведення консультації з науковим керівником щодо створення першого розділ.	16.10.2021 – 19.10.2021	
4	Аналітичний огляд і постановка задачі.	20.10.2021 – 24.10.2021	
5	Порівняльний аналіз існуючих систем управління документами.	25.10.2021 – 31.10.2021	
6	Огляд технологій для розробки системи.	01.11.2021 – 07.11.2021	
7	Розробка компонентів системи.	08.11.2021 – 17.11.2021	
8	Висновки та оформлення пояснювальної записки дипломного проекту.	18.11.2021 – 01.12.2021	
9	Підписання необхідних документів у встановленому порядку.	02.12.2021 – 11.12.2021	
10	Підготовка до захисту та попередній захист дипломного проекту на випусковій кафедрі дипломного проекту	12.12.2021 – 20.12.2021	

7. Дата видачі завдання: 12.10.2021р.

Керівник дипломної роботи _____ Аліна САВЧЕНКО
(підпис керівника)

Завдання прийняв до виконання _____ Олег ЧАЙЧЕНКО
(підпис випускника)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Прикладний програмний інтерфейс для маршрутизатора Cisco» складається з 79 сторінок 18 малюнків 16 джерел

Об’єкт дослідження: процес контролю доступу до інформаційних ресурсів за допомогою маршрутизатора Cisco.

Предмет дослідження: блокування інформаційних доменів за допомогою прикладного програмного інтерфейсу маршрутизатора Cisco.

Мета роботи: дослідження прикладного програмного інтерфейсу Cisco та розробка методу блокування інформаційних доменів в сучасному інформаційному просторі України.

Отримані результати та їх новизна: проведено аналіз роботи маршрутизатора Cisco, та аналіз прикладного програмного інтерфейсу Cisco. Розглянуті стандартні рішення контролю доступу до інформаційних ресурсів , створення фаєрволу на маршрутизаторі Cisco, розроблено метод блокування інформаційних доменів.

Ключові слова: API, МАРШРУТИЗАТОР, CISCO, КОНТРОЛЬ ДОСТУПУ, GNS3.

ЗМІСТ

ВСТУП....6
РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ....8
1.1. Інтернет як складова сучасної соціальної реальності....8
1.1.1. Приклади цензури в Інтернеті....10
1.2. Право на доступ до Інтернету....14
1.3. Право на свободу вираження поглядів та інформації....14
1.4. Право на мирні зібрання, об'єднання та участь....16
1.5. Право на приватне життя і захист даних....17
1.6. Інтернет, та роль маршрутизатора в ньому....17
1.7. Принцип роботи....19
1.8. Таблиця маршрутизації....20
1.9. Застосування....21
1.10. Перенаправлення портів і віртуальні сервери....22
1.11. Безпека....23
1.11.1. Блокування запитів ping....23
1.11.2. Фільтрація змісту....23
1.11.3. Контроль доступу....24
1.11.4. Віртуальні приватні мережі....24
1.12. Висновки до розділу 1 та постановка задачі....26
РОЗДІЛ 2
2.1. Використання інтерфейсу командного рядка Cisco IOS....29
2.2. Огляд командних режимів CLI Cisco IOS....30
2.2.1. Режим користувача EXEC....32
2.2.2. Привілейований режим EXEC....34
2.2.3. Режим глобальної конфігурації....35
2.2.4. Режим конфігурування інтерфейсу....37
2.2.5. Режим конфігурування субінтерфейсу....38
2.2.6. Режим монітора ROM....40
2.3. Список завдань CLI Cisco IOS....44
2.3.1. Отримання контекстно-залежної довідки....44
2.3.2. Використання форм команд no та default....46
2.3.3. Використання історії команд....47
2.6. Висновки до розділу 2....55
РОЗДІЛ 3
РЕАЛІЗАЦІЯ МЕТОДУ....56
3.1. Знайомство з GNS3....56
3.2. Запуск GNS3 та емуляція мережі на базі маршрутизаторів CISCO C3745....58
3.2.1. Налаштування мережевих провайдерів....63
3.2.2. Налаштування таблиці маршрутизації....64
3.2.3. Перевірка працездатності мережі....65
3.3. Метод блокування інформаційних доменів. Реалізація....66
3.4. Блокування соціальної мережі Facebook за робочим провайдером....70
3.5. Перевірка методу....73
3.6. Висновки до розділу 3....74
Висновки:....75
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ....77

ВСТУП

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого регулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системної кібернетичної безпеки. Відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, та забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи. [1]

Також дана проблема актуальна і для компаній які мають обладнання яке підключене до мережі інтернет. Компанія, навряд чи буде задоволена якщо їх обладнання буде використано не за призначенням. Є заборони устніні, письмові, на законодавчому рівні, но що заважає компанії фізично заборонити доступ техніки до небажаних інформаційних ресурсів, такі як соціальні мережі, торенти, даркнету, локально на рівні компанії.

Враховуючи наведене вище, актуальним є дослідження прикладного програмного інтерфейсу маршрутизатора Cisco.

Метою дипломної роботи є дослідження прикладного програмного інтерфейсу маршрутизатора Cisco та розробка методу блокування інформаційних доменів в сучасному інформаційному просторі України.

Для досягнення поставленої мети необхідно проаналізувати та вирішити наступні задачі:

- Провести аналітичний огляд предметної області;
- Визначити критерії за якими буде відбуватися блокування ресурсу;
- Проаналізувати існуючі аналоги для блокування інформаційних ресурсів;
- Розробити метод прикладного програмування та спосіб його реалізації за допомогою прикладного програмного інтерфейсу маршрутизатора Cisco.

Функціонал запропонованого програмного методу реалізує такі можливості:

- Блокування використання інформаційних ресурсів в залежності від рівня заборони.
- Блокування доступу до певних інформаційних ресурсів з робочого обладнання, без втручання в особисте життя працівника

Перевагами проектованої запропонованого методу та його реалізації на маршрутизаторах Cisco є висока ефективність за рахунок:

- Простота впровадження;
- Швидкість обробки потоків даних та їх блокування у разі потреби;
- Можливість реалізації на рівні провайдера, без залучення спеціаліста в компанію.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Інтернет як складова сучасної соціальної реальності

Інтернет як складова сучасної соціальної реальності призвів до розвитку нових інституцій, які базуються на його можливостях і не мають прямих аналогів (електронні та «віртуальні» гроші, соціальні мережі, розраховані на багатьох користувачів онлайн-ігри), та змінює його. , запроваджує новий формат функціонування вже існуючих інститутів. У той же час користувачі Інтернет продовжують залишатися суб'єктом права, а суспільні відносини, що виникають між ними, потребують правового регулювання.

Винахідник Всесвітньої мережі «Інтернет» Тімоті Бернерс-Лі у книзі «Заснування Павутини» зазначає: «Мережа – це більше соціальне, ніж технічне явище». Задумував я її для досягнення результату – допомогти людям працювати разом, – а не як технічну іграшку. Найзагальніша мета Мережі – підтримка і поліпшення нашого існування у світі, яке саме багато в чому є мережевим». Інтернет, спочатку був розроблений як відкритий комунікаційний простір «для досягнення соціального результату допомогти людям працювати разом, а не як технічну іграшку» [2].

Сьогодні Інтернет охоплює майже всі сфери суспільного життя (бізнес, транспорт, охорону здоров’я, освіту, культуру, медіа, уряд, науку, особисту ідентичність, ігри тощо) і дозволяє вести прямий діалог між людьми, незалежно від їхнього фізичного місце знаходження.

Ерік Шмідт і Джерард Коен з компанії Google, прогнозують, що «кожна держава спробує регулювати Інтернет ... всі країни – від найбільш демократичних до авторитарних – намагаються спроектувати закони з реального світу на світ віртуальний» [3]. Ці тенденції простежуються в багатьох сучасних країнах (США, Великобританія, Німеччина, Ізраїль, Росія, Китай, Україна). Уряди цих країн почали посилювати свій контроль над кіберпростором і готові порушити комунікацію між користувачами в Інтернеті.

Управління використанням Інтернет охоплює як технічні питання, так і питання державної політики, і в ньому повинні брати участь всі зацікавлені сторони і відповідні міжурядові і міжнародні організації. У зв'язку з цим у «Декларації принципів побудови інформаційного суспільства – глобальне завдання в новому тисячолітті» (далі – Декларація) визнається, що: 1) політичні повноваження пов’язані з Інтернетом як частина державної політики є суверенним правом держав; 2) приватний сектор відіграє і повинен продовжувати відігравати важливу роль у розвитку Інтернету, як в технічній, так і в економічній сфері; 3) громадянське суспільство також відіграє важливу роль у сфері Інтернету, особливо на рівні громад, і повинно продовжувати відігравати таку роль; 4) міжурядові організації відіграють і повинні продовжувати відіграти роль у цьому питанні, що сприяє координації міждержавної політики у сфері Інтернет-відносин; 5) міжнародні організації також відіграють і повинні продовжувати відігравати важливу роль у розроблені технічних стандартів і відповідної політики у сфері Інтернету [14].

З метою забезпечення реалізації прав людини у 2011 році у доповіді Спеціального доповідача ООН із сприяння та захисту права на свободу думки та вираження Френка Ла Рю (далі – звіт) доступ до Інтернету визнав правом. Визнання цього права обґрунтоване тим, що «на відміну від будь-якого іншого засобу комунікації Інтернет дозволяє людям миттєво і недорого шукати, одержувати і поширювати інформацію та ідеї в транскордонному масштабі. Інтернет, значно розширюючи можливості людей здійснювати своє право на свободу думок та їх вільне вираження, є «активізатором» інших прав людини,

сприяє економічному, соціальному і політичному розвитку, а також розвитку людства в цілому» [4].

1.1.1. Приклади цензури в Інтернеті

Більшість членів Ради, серед яких і Україна, проголосували за схвалення документу. Водночас проти висловилися такі країни, як Росія, Китай, Саудівська Аравія, Південна Африка та Індія. Вони, зокрема, вимагали вилучити з тексту фрагмент, у якому йдеться про «засудження заходів з обмеження та блокування доступу до розміщеної в мережі інформації» [15].

Блокування – це захід, який використовується для запобігання доступу певного вмісту до кінцевого користувача. Серед них: блокування доступу користувачів до певних веб-сайтів, адрес Інтернет-протоколу та доменних зон, видалення веб-сайтів із веб-сервера, на якому вони розміщені, або використання технологій фільтрації, які запобігають відображенню сайтів, які можуть містити ключові слова, чи інший конкретний вміст. Механізми, що використовуються для управління інформацією та цензури Інтернету, стають технічно складнішими через використання багаторівневих систем контролю, часто прихованих від користувачів.

По суті, інформація, яку можна обмежити у всесвітній мережі, включає: дитячу порнографію (для захисту прав дітей), розпалювання ненависті (для захисту прав вразливих регіонів), наклеп (для захисту прав та репутації інших від протиправних нападі), пряме та публічне підбурювання до геноциду (для захисту прав інших), будь-які дії на користь національної, расової чи релігійної ворожнечі, що розпалюють дискримінацію, ворожнечу чи насильство (для захисту прав інших та їхнього права на життя).

«Якщо ви відкриєте вікно для свіжого повітря, ви повинні очікувати, що влітають мухи», – це фраза Ден Сяопіна, в якій розкрито суть «проекту Золотий Щит», також відомого як «Великий брандмауер Китаю» (The Golden Shield

Project) – система цензури і фільтрації Інтернету. Проект стартував у 2003 р. та є системою серверів на інтернет-каналі між провайдерами і міжнародними мережами передачі інформації, що фільтрує інформацію.

За словами Грега Уолтона з Міжнародного центру з прав людини та демократичного розвитку, в Китаї впроваджено найсучаснішу фільтрацію вмісту в Інтернеті, яка може ефективно фільтрувати вміст за допомогою різноманітних методів нормативного та технічного контролю (блокування IP-адресів і фільтрація вмісту; фільтрація DNS та URL-адрес); скидання підключення тощо).

До сайтів, які підлягають фільтрації у Китаї належать такі, що:

- створені забороненим групам у цій державі (waselpro.com, thecim.org) або сприяють обходу блокування сайтів (openvpn.net, strongvpn.com, purevpn.com);
- пов'язані з «ворожими» іноземними урядами, засобами масової інформації та іншими організаціями (time.com, economist.com, bbc.co.uk);
- пов'язані з релігійним і політичним контентом (waselpro.com), порнографічними матеріалами (drtuber.com, hardsextube.com) або сайти, які заохочують злочинну діяльність;
- сайти для блогів (urbansurvival.com, wretch.cc, fc2.com) [5].

Окремою групою заблокованих урядом Китаю сайтів є соціальні мережі (Google Plus; Twitter; Facebook; Instagram). Політика уряду в соціальних мережах полягає в тому, щоб блокувати міжнародні сайти та створювати виключно «китайські» цензурні соціальні мережі. Коли Google використовується в іншій частині світу, Baidu (www.baidu.com) працює в Китаї. Замість Twitter у них є Weibo (tw.weibo.com). Замість Facebook є Renren (www.renren.com). Замість Youtube у них є Tudou (www.tudou.com) або Youku (www.youku.com).

Фільтрація також стосується «ключових слів», які можуть бути заблоковані, коли місцеві користувачі шукають іноземні пошукові системи, а

інші можуть бути занесені в чорний список («демократія», «права людини», «диктатура», «гніт»). », «Червоний терор», «Далай-лама»).

У серпні 2016 року Кіберпростір Адміністрації Китаю ввів нові жорсткі вимоги щодо цензури для провайдерів, включаючи постійний моніторинг вмісту новин та особисту відповідальність головного редактора сайту за вміст.

Провайдери Інтернет-послуг зобов'язані блокувати веб-сайти та видаляти вміст відповідно до вказівок цензорів. Наприклад, у червні 2016 року заборона на самостійний збір або розповсюдження оригінальних новин була поширена на всі додатки соціальних мереж, тоді як у липні 2016 року китайська філія уряду Китаю ухвалила постанови, які забороняють китайським інтернет-порталам створювати оригінальні новини, обмежуючи до змісту, наданого невеликою кількістю авторизованих «офіційних» джерел. Керівництво новинного сайту повинно цілодобово перевіряти зміст нотаток і статей, щоб уникнути фактичних, стилістичних та інших помилок.

В ряді країн сформувалася тенденція до тимчасового блокування з метою позбавлення користувачів можливості отримувати та розповсюджувати інформацію в політичні періоди, такі як вибори, соціальні протести або історичних подій або святкування річниці важливих політичних. У цей час блокуються сайти опозиційних партій, незалежних медіа та засобів масової інформації та соціальних мереж, таких як «Facebook» і«Twitter», як це було в період протестів у країнах «Арабської весни» у 2010-2011 рр. та під час військового перевороту в Туреччині у липні 2016 р.

Е. Шмідт і Дж. Коен прогнозують розвиток блокування доступу до комунікацій та Інтернету, відзначаючи, що авторитарні країни не будуть замислюватися над тим, як заборонити або контролювати однорангові комунікації. Але демократії будуть діяти помірковано, перш ніж застосовувати обмеження в цій сфері. Під час заворушень у Великобританії в серпні 2011 року протестувальники вимагали справедливості у справі Марка Деггана, застреленого поліцією в Тоттенхемі. Через кілька днів протести переросли у сутички, в результаті яких загинуло п'ятеро людей і було пошкоджено майно на

суму 300 мільйонів фунтів стерлінгів. За даними британського уряду, це сталося в основному через такі засоби комунікації, як Facebook, Twitter, BlackBerry. Коли протести припинилися, британський Прем'єр-Міністр Девід Кемерон виступив у парламенті та повідомив про можливість блокування цих соціальних сервісів в певних ситуаціях, зокрема тоді, «коли відомо, що люди задумують розбій, безпорядки та злочини» [6].

Виходячи з вищесказаного, слід зазначити, що використання державами технологій блокування чи фільтрації часто порушує їхні зобов'язання щодо забезпечення права на свободу вираження поглядів, наприклад:

- Підстави для блокування законодавчо не закріплені, або вони є надзвичайно широкими та нечіткими в законах, створюючи загрозу довільного та надмірного блокування;
- Блокування не здійснюється для цілей, зазначених у статті 19 пункт 3 Міжнародного пакту про громадянські та політичні права, і списки заблокованих сайтів зазвичай не оприлюднюються, що ускладнює оцінку того, чи є обмеження доступу до вмісту законними;
- Навіть якщо заходи блокування виправдані, вони є непотрібними та непропорційними заявленій меті, оскільки часто є ненавмисними та призводять до блокування доступу до більшої кількості вмісту, ніж вважається незаконним;
- Вміст часто блокується без проходження судового або незалежного органу чи перегляду рішень цих органів.

1.2. Право на доступ до Інтернету

Доступ до Інтернету є важливим інструментом для реалізації ваших прав і свобод та участі в демократичних процесах. Тому заборонити доступ до Інтернету проти вашої волі можна лише за рішенням суду. У деяких випадках надання послуг може бути припинено згідно з умовами договору, але це може не відбутися до тих пір, поки не будуть вичерпані всі інші засоби. Доступ до інтернету має надаватися за розумну ціну і бути недискримінаційним, та не бути пропагандним.

Під час взаємодії з державними установами, постачальниками Інтернет-послуг і постачальниками Інтернет-контенту або послуг, або іншими користувачами чи групами користувачів, ви не повинні зазнавати дискримінації за будь-якою ознакою, як раса, колір шкіри, стать, мова, релігія чи переконання, національність або соціальне походження, належність до національної меншини, політичні чи інші переконання, майновий стан, походження або будь-який інший статус, зокрема за ознакою етнічної приналежності, віку чи сексуальної орієнтації.

1.3. Право на свободу вираження поглядів та інформації

Особа має право шукати, отримувати та поширювати інформацію та ідеї на свій вибір без втручання та незалежно від кордонів.

Це означає що:

- Право вільно висловлюватися в Інтернеті та мати доступ до інформації, думок і висловлювань інших. Сюди входять політичні заяви, релігійні переконання, погляди та заяви, які розглядаються як прихильні або образливі, а також заяви, які можуть образити, шокувати або засмутити інших.

- Можуть бути накладені обмеження на заяви, які розпалюють дискримінацію, ненависть або насильство. Такі обмеження мають бути законними, цілеспрямованими та виконуватися під наглядом суду.
- Право на вільне створення, повторне використання та розповсюдження Інтернет-контенту, пов'язаного з правом на захист інтелектуальної власності, включаючи авторське право.
- Використовуйте псевдонім замість справжнього імені.

Державні установи можуть вжити заходів для оприлюднення вашої особи. Органи державної влади зобов'язані поважати та захищати індивідуальну свободу вираження поглядів та інформації. Будь-яке обмеження цієї свободи не повинно бути свавільним і повинно переслідувати законну мету відповідно до вимог Європейської конвенції з прав людини, таких як захист національної безпеки або громадського порядку, здоров’я чи моралі, а також відповідно до прав людини.

Інтернет-провайдер та провайдер Інтернет-контенту і послуг мають корпоративні зобов’язання поважати права особи та забезпечувати механізми розгляду скарг. Водночас, провайдери Інтернет-послуг, такі як соціальні мережі, можуть обмежувати окремі види контенту і поведінку у зв’язку з їхньою політикою щодо контенту. Користувача повинні повідомляти про можливі обмеження для того, щоб особа могла прийняти свідоме рішення щодо користування послугою [7].

1.4. Право на мирні зібрання, об’єднання та участь

Людина має право на мирні зустрічі та спілкування з іншими в Інтернеті. На практиці це означає, що:

- Право вільно обирати будь-який сайт, додаток чи будь-яку іншу послугу з метою створення груп, приєднання, мобілізації та участі в будь-якій соціальній групі та об’єднанні незалежно від їхнього офіційного визнання з боку органів державної влади. Право передбачає можливість використовувати Інтернет для реалізації свого права на створення профспілок та приєднання до них.
- Право на мирний протест в Інтернеті. Однак дії не повинні призводити до блокування, перебоїв у надання послуг та (або) завдавати шкоду майну інших осіб.
- Право вільно користуватися доступними онлайновими можливостями для участі в місцевих, національних і глобальних публічних політичних дебатах, законодавчих ініціативах, контролі за прийняттям рішення, зокрема, право підписувати петиції та брати участь у розробці політики, пов’язаної з управлінням Інтернетом [7].

1.5. Право на приватне життя і захист даних

Людина має право на приватне та сімейне життя в Інтернеті, включаючи захист персональних даних та повагу до конфіденційності листування та спілкування.

Це означає, що:

- персональні дані повинні оброблятися лише у передбачених законом випадках або за умови надання згоди. Особі повинні повідомляти про те, які саме персональні дані обробляються та (або) передаються третім сторонам, а також про те, коли, ким та з якою метою здійснюється така обробка.
- на особу не повинні поширюватися заходи загального спостереження чи перехоплення інформації. Втручання у приватне життя щодо персональних даних дозволяється лише за виняткових обставин, передбачених законом, наприклад, у разі здійснення кримінального провадження.
- право на конфіденційність електронної кореспонденції та спілкування, заборона спостереження та(або) моніторингу [7].

1.6. Інтернет, та роль маршрутизатора в ньому

Інтернет є основою мережі (the Web), технічною інфраструктурою, завдяки якій існує Всесвітня Павутина. За своєю суттю інтернет - дуже велика мережа комп'ютерів, які можуть взаємодіяти один з одним. Основним вузлом взаємодії є маршрутизатор, розглянемо базові принципи роботи маршрутизатора.

Враховуючи стрімкий розвиток Інтернету в останні роки, все актуальнішою стає проблема обмеження доступу до певних інформаційних ресурсів. Необхідність контролювати доступ співробітників до певних ресурсів

часто зумовлений корпоративною політикою компанії щодо заборони доступу до розважальних ресурсів у робочий час.

На сьогодні існує значна кількість програмно-апаратних рішень, що забезпечують доступ до інформаційних ресурсів Інтернету на різних рівнях (навіть, безпосередньо на робочому місці користувача, на стороні провайдера, в точках обміну навантаженням операторів телекомунікацій тощо).

Найчастіше такі програмно-апаратні рішення включають в себе налаштування активного комунікаційного обладнання, зокрема, маршрутизаторів, для фільтрації та обмеження у разі необхідності певних інформаційних потоків.

Маршрутизатор, або роутер (англ. router) — електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Для звичайного користувача маршрутизатор – це мережевий пристрій, який з’єднує локальну мережу з Інтернетом. Часто маршрутизатор не обмежується лише передачею даних між інтерфейсами, а виконує й інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до Інтернет-ресурсів, розподіляє IP-адреси, шифрує трафік тощо.

Маршрутизатори працюють на рівні мережі моделі OSI: вони можуть пересилати пакети з однієї мережі в іншу. Маршрутизатор використовує таблицю маршрутизації, збережену в пам'яті, щоб направити пакети в потрібному напрямку. Таблицю маршрутизації можна побудувати за допомогою статичної або динамічної маршрутизації.

Крім того, маршрутизатори можуть здійснювати трансляцію адреси відправника й одержувача (англ. NAT, Network Address Translation), фільтрацію

транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/дешифрування передаваних даних тощо.

Маршрутизатори не можуть здійснювати передачу широкомовних повідомлень, таких як ARP-запит.

Маршрутизатором може виступати як спеціалізований пристрій, так і звичайний комп'ютер, що виконує функції простого маршрутизатора.

Зазвичай маршрутизатор використовує адресу одержувача, вказану в пакетах даних, і визначає за таблицею маршрутизації шлях, за яким слід передати дані. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, пакет відкидається.

Існують і інші способи визначення маршруту пересилки пакетів, коли, наприклад, використовується адреса відправника, використовувані протоколи верхніх рівнів і інша інформація, що міститься в заголовках пакетів мережевого рівня. Нерідко маршрутизатори можуть здійснювати трансляцію адрес відправника і одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/дешифрування переданих даних тощо [8].

1.7. Принцип роботи

Маршрутизатор використовує адресу одержувача, зазначену в пакетах даних, і визначає з таблиці маршрутизації шлях, через який дані повинні бути відправлені. Якщо в таблиці маршрутизації для адреси не описано жодного маршруту, пакет відхиляється.

Існують і інші способи визначення маршруту пересилки пакетів, коли, наприклад, використовується адреса відправника, використовувані протоколи верхніх рівнів і інша інформація, що міститься в заголовках пакетів мережевого рівня. Нерідко маршрутизатори можуть здійснювати трансляцію адрес

відправника і одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування/дешифрування переданих даних тощо [8].

1.8. Таблиця маршрутизації

Таблиця маршрутизації містить інформацію про маршрут, який визначає рішення про пересилання пакетів. Таблиця, що складається з кількох записів - маршрутів, кожен з яких містить адресу мережі одержувача, адресу наступного університету, мережу aera одержувача, адресу наступного університету та записи метрики в таблиці. обчислення найкоротших шляхів до різних приймачів. Залежно від моделі маршрутизатора та використовуваних протоколів маршрутизації, таблиця може містити деяких додаткових співробітників. Наприклад (рис. 1.1.):

```
2513#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 171.70.24.0 to network 171.70.0.0

 *   171.70.0.0/16 is variably subnetted, 2 subnets, 2 masks
S*      171.70.0.0/16 [1/0] via 171.70.24.0
S       171.70.24.0/24 [1/0] via 131.108.99.2
    161.44.0.0/24 is subnetted, 1 subnets
C       161.44.192.0 is directly connected, Ethernet0
    131.108.0.0/24 is subnetted, 1 subnets
C       131.108.99.0 is directly connected, Serial0
S*   198.10.1.0/24 [1/0] via 161.44.192.2
```

Рис. 1.1. Приклади виводу маршрутів

Таблиця маршрутизації може складатися двома способами:

- статична маршрутизація — коли записи в таблиці вводяться і змінюються вручну. Такий спосіб вимагає втручання адміністратора щоразу, коли відбуваються зміни в топології мережі. З іншого боку, він є найстабільнішим і таким, що вимагає мінімуму апаратних ресурсів маршрутизатора для обслуговування таблиці.
- динамічна маршрутизація — коли записи в таблиці оновлюються автоматично за допомогою одного або кількох протоколів маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, і ін. Крім того, маршрутизатор будує таблицю оптимальних шляхів до мереж призначення на основі різних критеріїв — кількості проміжних вузлів, пропускної спроможності каналів, затримки передачі даних тощо. Критерії обчислення оптимальних маршрутів найчастіше залежать від протоколу маршрутизації, а також задаються конфігурацією маршрутизатора. Такий спосіб побудови таблиці дозволяє автоматично тримати таблицю маршрутизації в актуальному стані і обчислювати оптимальні маршрути на основі поточної топології мережі. Проте динамічна маршрутизація надає додаткове навантаження на пристрої, а висока нестабільність мережі може приводити до ситуацій, коли маршрутизатори не встигають синхронізувати свої таблиці, що приводить до суперечливих відомостей про топологію мережі в різних її частинах і втраті передаваних даних [8].

1.9. Застосування

Маршрутизатори допомагають зменшити перевантаження мережі, розділяючи її на конфліктуючи домени та широкомовні домени, а також фільтруючи пакети. В основному вони використовуються для об’єднання різних типів мереж, часто несумісних за архітектурою та протоколами, наприклад для поєднання локальних мереж Ethernet і WAN з’єднань за допомогою xDSL, PPP, ATM, Frame Relay тощо. Часто маршрутизатор використовується для

забезпечення доступу з локальної мережі до всесвітньої мережі, виконуючи функції трансляції адрес і брандмауера.

Маршрутизатором може бути спеціалізований апаратний пристрій (зазвичай продукти Cisco) або звичайний комп'ютер, який виконує роль маршрутизатора. Існує кілька програмних пакетів (зазвичай заснованих на ядрі Linux), які можна використовувати для перетворення ПК на потужний і багатофункціональний маршрутизатор, наприклад GNU Zebra.

1.10. Перенаправлення портів і віртуальні сервери

Перенаправлення портів і віртуальні сервери (англ. Port Mapping, Port Forwarding, Virtual Server) Функція дозволяє перенаправляти звернення до вказаних портів зовнішнього інтерфейсу маршрутизатора на пристрої, підключені до внутрішнього інтерфейсу. Необхідність перенаправлення може виникнути, наприклад, при розміщенні всередині мережі різних серверів (Web, FTP). При використанні перенаправлення слід звернути увагу на брандмауер: деякі пристрої автоматично створюють відповідні перенаправленню портів правила брандмауера, проте в більшості випадків вирішувати проходження трафіку доведеться самостійно. Відзначимо також, що існує декілька способів перенаправлення портів:

- **Статичне перенаправлення окремих портів** (Static) — простий випадок, при якому задаються відповідності між протоколом (TCP/UDP) і портами зовнішнього інтерфейсу і протоколом і портами внутрішнього, а також адресами пристроїв внутрішньої мережі. Робота такого перенаправлення дозволить зробити сервер, розташований у внутрішній мережі доступним із зовнішньої мережі.
- **Статичне перенаправлення груп портів**. Відрізняється від статичного перенаправлення окремих портів лише тим, що для перенаправлення можна вказувати не окремі порти, а їхні групи (список окремих портів або діапазон). Вся група перенаправляється на одну адресу. Таке

перенаправлення дозволяє забезпечити роботу таких застосунків, як ігри і аудіо/відеоконференції.

- Динамічне перенаправлення портів (Dynamic, Triggered Mapping, Special Application). Основна відмінність від статичного перенаправлення портів полягає в тому, що один номер порту можна перенаправити на декілька внутрішніх IP-адрес (але не одночасно). Використання динамічного перенаправлення актуальне для застосунків, що використовують короткочасні передачі даних, які не займають порт надовго. Слід зазначити, що подія, що ініціює динамічне перенаправлення, повинна відбуватися у внутрішньому сегменті мережі, що накладає істотні обмеження на використання цього типу перенаправлення при хостингу служб [8].

1.11. Безпека

1.11.1. Блокування запитів ping

Віддалений блок запиту Ping, Ігнорувати WAN Ping, Невидимий режим. Оскільки запити ping часто використовуються для визначення доступності сайту в Інтернеті, комп’ютер приховує свою присутність у мережі, не відповідаючи на такий запит. Багато роутери дозволяють блокувати запити ping, точніше, блокувати відповіді на ці запити, приховуючи їх присутність в мережі.

1.11.2. Фільтрація змісту

Фільтрація вмісту призначена для обмеження доступу користувачів локальної мережі до Інтернет-ресурсів із сумнівним вмістом. Залежно від версії ви можете створити чорний або білий список URL-адрес або IP-адрес або використовувати списки фільтрів сторонніх розробників. Слід зазначити, що фільтрацію вмісту можна застосувати до всіх комп’ютерів у локальній мережі або лише кількох, причому часто можна встановити розклад цих списків.

1.11.3. Контроль доступу

Контроль доступу, фільтрація портів. Багато невеликих організацій мають обмежений доступ до послуг Інтернету. Одним із варіантів такого обмеження може бути використання маршрутизатора. Так, деякі користувачі мають доступ лише до електронної пошти, інші можуть отримувати доступ до веб-сторінок і додавати ICQ, а треті мають необмежений доступ до всіх послуг. Щоб спростити налаштування, маршрутизатори дозволяють створювати групи локальних користувачів, для яких ви можете вирішити, чи забороняти доступ. Крім того, більшість маршрутизаторів дозволяють активувати обмеження за розкладом.

Також є цікаві відмінності в діях роутера при блокуванні несанкціонованого трафіку. Деякі просто блокують, створюючи у користувача враження, що сервіс недоступний і не відображається, інші надсилають користувачеві повідомлення та реєструють спроби доступу до системного журналу маршрутизатора.

1.11.4. Віртуальні приватні мережі

Віртуальна приватна мережа (VPN) є дуже популярною темою, пов’язаною з безпекою комп’ютерної мережі. Технології VPN зробили можливим використання загальнодоступних небезпечних мереж, таких як Інтернет, для безпечної передачі даних, використовуючи можливості шифрування та цифрового підпису. Це підключення дозволяє користувачеві працювати з ресурсами віддаленої мережі так само, як і з ресурсами локальної мережі. Багато виробників маршрутизаторів почали випускати моделі, які підтримують VPN, від простого проходження через тунелі VPN до повноцінних вбудованих серверів PPTP або IPSec. Для створення VPN використовуються такі

протоколи: IPSec (безпека Інтернет-протоколу), PPTP (протокол тунелювання «точка-точка»), L2TP (протокол тунелювання рівня 2), SSL.

VPN pass-through дозволяє тунелям VPN проходити через маршрутизатор; Наявність цієї функції стало де-факто стандартом, хоча раніше не всі пристрої могли встановити VPN-з'єднання.

Клієнт VPN дозволяє підключатися до сервера VPN. Він представляє інтерес для абонентів провайдерів, які надають доступ до мережі через VPN (часто за протоколом PPTP), а також для філій підприємств, які потребують безпечного підключення до центрального офісу.

Сервер VPN дозволяє вам приймати підключення, ініційовані клієнтом. Часто використовується в штаб-квартирі компанії для підключення філій і співробітників.

Підтримка VPN-тунелів (VPN Endpoint). Створення віртуального тунелю між мережевими маршрутизаторами часто передбачає використання протоколів IPSec, які дозволяють шифрувати і дешифрувати дані, що надсилаються, а також перевіряти їх цілісність і обмінюватися ключами. Саме цей сценарій сьогодні найбільш активно використовується для об’єднання різноманітних зовнішніх мереж.

1.12. Висновки до розділу 1 та постановка задачі.

Сучасний і досить вільний світ, принаймні його цивілізована частина, рухається все далі до демократії, віддаючи на відповідальність робітників все більше аспектів їхньої роботи, процеси виконання якої, раніше знаходилися «під контролем» керівництва. Соціальні мережі все частіше стають перешкодою для гармонійного перебігу деяких сторін життя. Ця звичка людства також впливає на роботу та робочий процес.

Незадоволеність керівництва вільним доступом робітників компаній до соціальних мереж, не випадкова, й численні заборони компаній на користування цим прошарком інтернет середовища під час робочого дня, цілком обумовлена. Науковими дослідженнями, висновки яких отримали практичне підтвердження згодом, було доведено, що надто сильна залежність людини від користування соціальними мережами, не аби як негативне впливає на її життя та роботу. Щодо останньої, то «зависання» у соцмережах, забирає забагато часу, що проектується на об’ємах та якості результатів роботи співробітників [9].

Наприклад, в Україні респонденти виявили, що кожен десятий співробітник погано зосереджений на правильних завданнях, оскільки кілька разів на день звертає увагу на соціальні мережі, легко і швидко переглядає оновлену стрічку новин.

Заборона на такі відволікання на роботі – вже звичайна практика. Оскільки працівник проводить свій час на роботі, керівництво слідкує щоб працівник працював, а не витрачав свій час на такі подразники як телефон, електронна пошта, месенджери та Інтернет.

Про певні заборони в соцмережах або можливість стежити за листуванням співробітників світові компанії повідомляють заздалегідь, тож, якщо останніх спіймають на цьому, шансів уникнути звільнення майже немає.

Українське трудове законодавство у цьому питанні не конкретизоване й в Кодексі законів про працю немає окремих вказівок, щодо таких причин, що відволікають робітника від належного виконання його обов’язків. Проте, все

більше українських компаній прописують заборону користування соціальними мережами у трудових договорах, чи, принаймні, повідомляють про такі вимоги «під розпис». У такому випадку, бути звільненим через відволікання саме на соціальні мережі цілком можливо [9].

Також важливим є — заборона використання робочого обладнання, на якому знаходиться критична інформація, до небажаних інформаційних доменів.

На жаль, заборони усної, письмової мало. Тому можна зробити фізичну заборону в вигляді заборони доступу з робочого обладнання, або з робочої мережі. Для того щоб не відволікались працівники, або не використовували робоче обладнання для не робочих методів, тому актуальним є розробка методів блокування інформаційних ресурсів.

Для досягнення поставленої мети роботи необхідно вирішити наступні задачі:

- проаналізувати предметну область;
- розглянути особливості маршрутизатора Cisco;

Враховуючи наведене вище, актуальною є дослідження прикладного програмного інтерфейсу Cisco та розробка методу блокування інформаційних доменів в сучасному інформаційному просторі України.

Таким чином, метою дипломної роботи є дослідження прикладного програмного інтерфейсу Cisco та розробка методу блокування інформаційних доменів в сучасному інформаційному просторі України. Для досягнення поставленої мети необхідно проаналізувати та вирішити наступні задачі:

- Провести аналітичний огляд предметної області;
- Визначити критерії оцінки їх ефективності;
- Розробити метод прикладного програмування для застосування розробленої технології.

Функціонал запропонованого програмного методу реалізує такі можливості:

- Блокування використання інформаційних ресурсів в залежності від рівня заборони.
- Блокування доступу до небажаних інформаційних ресурсів з робочого обладнання, без втручання в особисте життя працівника.
-
- Перевагами проектованої системи є висока ефективність за рахунок:
- Простота;
- Швидкість;
- Можна зробити на рівні провайдера, без залучення спеціаліста в компанію.

РОЗДІЛ 2
CLI CISCO API

2.1. Використання інтерфейсу командного рядка Cisco IOS

Інтерфейс командного рядка (CLI) Cisco IOS — це основний інтерфейс, який використовується для конфігурування, моніторингу та обслуговування пристроїв Cisco. Цей інтерфейс користувача дозволяє безпосередньо виконувати команди Cisco IOS за допомогою консолі маршрутизатора, терміналу або з використанням віддаленого доступу.

У цьому розділі описано основні функції CLI Cisco IOS та порядок їх застосування. Теми, що розглядаються, включають введення в режими команд Cisco IOS, функції навігації та редагування, функції довідки та історії команд.

Додаткові інтерфейси користувача – це режим установки (використовується при початковому запуску), веб-браузер Cisco та меню користувача, що налаштовуються системним адміністратором. Інформацію про режим установки викладено в розділі "Конфігурування за допомогою процедур налаштування та автоматичної установки". Інформація про виконання команд у середовищі веб-браузера Cisco наведена у розділі "Використання інтерфейсу користувача веб-браузера Cisco". Інформація про меню користувача наведена у розділі "Управління підключеннями, меню та системними банерами" [10].

2.2. Огляд командних режимів CLI Cisco IOS

Щоб полегшити конфігурацію пристроїв Cisco, інтерфейс командного рядка Cisco IOS поділений на окремі режими команд. У кожному командному режимі передбачено власний набір команд для конфігурування, обслуговування та моніторингу роботи маршрутизатора та мережі. Сукупність доступних у певний момент команд залежить від поточного командного режиму. Введення знаку запитання (?) після системного запрошення дозволяє вивести список доступних команд для кожного командного режиму.

Застосування певних команд забезпечує перехід від одного режиму командного до іншого. Стандартний порядок, в якому користувачеві слід здійснювати доступ до режимів, такий: режим користувача EXEC, привілейований режим EXEC; режим глобальної конфігурації; режими спеціальної конфігурації, підрежими конфігурації та підрежими конфігурації 2-го рівня.

Сеанс на маршрутизаторі зазвичай починається в режимі користувача EXEC, який являє собою один з двох рівнів доступу режиму EXEC. З метою безпеки в режимі користувача EXEC доступне лише обмежене підмножина команд EXEC. Цей рівень доступу призначений для завдань, які не змінюють конфігурацію маршрутизатора, наприклад визначення статусу маршрутизатора.

Для отримання доступу до всіх команд необхідно перейти до привілейованого режиму EXEC, який забезпечує другий рівень доступу до режиму EXEC. Зазвичай для входу в привілейований режим EXEC необхідно ввести пароль. У привілейованому режимі EXEC можна вводити будь-яку команду EXEC, так як він передбачає набір команд, розширений по відношенню до режиму користувача EXEC.

Більшість команд режиму EXEC є "одноразовими" командами, наприклад команди show або more, які показують статус поточної конфігурації, і команди clear, що скидають лічильники або інтерфейси. Команди режиму EXEC не зберігаються після перезавантаження маршрутизатора.

З привілейованого режиму EXEC можна перейти до режиму глобальної конфігурації. У цьому режимі можливе введення команд, які дозволяють конфігурувати загальні характеристики системи. Режим глобальної конфігурації можна використовувати також для переходу до специфічних режимів конфігурації. Режими конфігурації, включаючи режим глобальної конфігурації, дозволяють вносити зміни до поточної конфігурації. Якщо конфігурація пізніше зберігається, ці команди зберігаються після перезавантаження маршрутизатора.

З режиму глобальної конфігурації можна перейти до багатьох режимів конфігурації, специфічних для конкретного протоколу або функції. Ієрархія CLI передбачає, що вхід у ці специфічні режими конфігурування провадиться лише з режиму глобальної конфігурації. Як приклад у цьому розділі описаний один із зазвичай використовуваних режимів конфігурування - режим конфігурування інтерфейсу.

З режимів конфігурації можна перейти до режимів конфігурації. Підрежими конфігурування використовуються для налаштування певних функцій у межах даного режиму конфігурування. Як приклад у цьому розділі описаний режим конфігурування субінтерфейсу, який є підлеглим щодо режиму конфігурування інтерфейсу.

Режим монітора ROM — це окремий режим, який використовується в тому випадку, якщо маршрутизатор не завантажується належним чином. Якщо система (маршрутизатор, комутатор або сервер доступу) не знаходить правильний образ системи, що завантажується в процесі запуску, система переходить в режим монітора ROM. У режим монітора ROM (ROMMON) можна увійти також переривання послідовності завантаження під час запуску [10] .

У наступних розділах наведено докладні відомості про ці командні режими:

- Режим користувача EXEC
- Привілейований режим EXEC
- Режим глобальної конфігурації
- Режим конфігурації інтерфейсу
- Режим конфігурації субінтерфейсу
- Режим монітора ROM

2.2.1. Режим користувача EXEC

Після реєстрації в маршрутизаторі користувач входить у режим користувача команд EXEC (за винятком тих випадків, коли система налаштована на негайний вхід у привілейований режим EXEC). Зазвичай під час реєстрації в системі потрібно ввести ім'я користувача та пароль. Дозволяється ввести пароль тричі, після чого у спробах підключення буде відмовлено.

Команди EXEC, доступні на рівні користувача, є підмножиною команд, доступних на привілейованому рівні. Зазвичай команди EXEC дозволяють підключитися до віддалених пристроїв, тимчасово змінити параметри абонентської лінії, виконати основні тести і отримати відомості про систему.

Для виведення списку доступних команд користувача EXEC використовується наступна команда:

Команда	*Призначення*
Router> ?	Виведення списку команд користувача EXEC.

Для виведення списку доступних команд режиму користувача EXEC введіть знак запитання (?), як показано в наведеному нижче прикладі:

Router>? Exec commands:	
<1-99>	Session number to resume
connect	Open a terminal connection
disconnect	Disconnect an existing telnet session
enable	Turn on privileged commands
exit	Exit from Exec mode
help	Description of the interactive help system
lat	Open a lat connection
lock	Lock the terminal
login	Log in as a particular user
logout	Exit від Exec mode and log out
menu	Start a menu-based user interface
mbranch	Trace multicast route for branch of tree
mrbranch	Trace reverse multicast route to branch of tree
mtrace	Trace multicast route to group
name-connection	Name an existing telnet connection
pad	Open a X.29 PAD connection
ping	Send echo messages
resume	Resume an active telnet connection
show	Show running system information

systat	Display information o terminal lines
telnet	Open a telnet connection
terminal	Set terminal line parametersss
tn3270	Open a tn3270 connection
trace	Trace route to destination
where	List active telnet connections
x3	Set X.3 parameters on PAD

Список команд може змінюватись в залежності від використовуваної платформи маршрутизатора та набору функціональних можливостей програмного забезпечення.

2.2.2. Привілейований режим EXEC

Зважаючи на те, що багато команд привілейованого режиму EXEC встановлюють робочі параметри, щоб уникнути несанкціонованого використання доступ привілейованого рівня повинен бути захищений паролем. Набір привілейованих команд EXEC включає команди режиму користувача EXEC. Привілейований режим EXEC забезпечує доступ до режимів конфігурації за допомогою команди configure та включає команди розширеного тестування, наприклад, debug.

Запрошення привілейованого режиму EXEC складається з імені пристрою як вузла мережі, за яким слідує знак фунта (#), як показано в наступному прикладі:

```
Router#
```

Для входу в привілейований режим EXEC використовується така команда:

Команда	*Призначення*
Router> enable	Увімкнення привілейованого режиму EXEC. •При запиті необхідно ввести пароль.

Слід пам'ятати, що привілейований режим EXEC іноді називають "режим enable", оскільки входу до нього використовується команда enable.

Якщо в системі встановлено пароль, перед тим, як буде дозволено доступ до привілейованого режиму EXEC, з'явиться запит на введення пароля. Пароль не відображається на екрані та вводиться з урахуванням регістру символів. Якщо пароль привілейованого режиму не встановлено, вхід у привілейований режим EXEC можливий лише з консолі маршрутизатора (терміналу, підключеного до консольного порту). Для встановлення пароля, що обмежує доступ до привілейованого режиму, системний адміністратор може скористатися командами глобальної конфігурації enable secret або enable password.

Для повернення в режим користувача EXEC використовується наступна команда:

Команда	*Призначення*
Router# disable	Вихід із привілейованого режиму EXEC і повернення в режим користувача EXEC.

2.2.3. Режим глобальної конфігурації

Термін "глобальний" використовується для позначення характеристик або функціональних можливостей щодо системи в цілому. Режим глобальної конфігурації використовується для конфігурування системи глобально або для переходу до спеціальних режимів конфігурації, що забезпечують налаштування

специфічних елементів, наприклад, інтерфейсів або протоколів. Для входу в режим глобальної конфігурації використається команда привілейованого режиму EXEC configure terminal.

Для отримання доступу до режиму глобальної конфігурації використовується наступна команда EXEC привілейованого режиму:

Команда	*Призначення*
Router# configure terminal	Перехід із привілейованого режиму EXEC у режим глобальної конфігурації.

Слід звернути увагу, що системне запрошення змінюється, показуючи тим, що користувач перебуває у режимі глобальної конфігурації. Запрошення режиму глобальної конфігурації складається з імені пристрою як вузла мережі, за яким слідує (config) і знак фунта (#). Щоб вивести список команд, доступних у привілейованому режимі EXEC, введіть ? після запрошення системи.

Команди, що вводяться в режимі глобальної конфігурації, змінюють поточну конфігурацію. Іншими словами, зміни конфігурації набирають чинності при кожному натисканні Enter або Return після введення правильної команди. Проте ці зміни не зберігаються у файлі конфігурації запуску, доки не буде введена команда режиму EXEC copy running-config startup-config. Така поведінка пояснюється докладніше в цьому документі.

Як показано у прикладі, системний діалог пропонує закінчити сеанс конфігурування (вийти з режиму конфігурування) шляхом одночасного натискання клавіш Ctrl та "z"; Якщо натиснути ці клавіші, на екрані відображається ^Z. Насправді можна завершити сеанс конфігурування шляхом натискання клавіш Ctrl-Z, за допомогою команди end або використовуючи клавіш Ctrl-C. Рекомендується використовувати команду end, щоб вказати системі на закінчення поточного сеансу конфігурування.

Крім того, для повернення з режиму глобальної конфігурації в режим EXEC можна скористатися командою exit, але вона працює лише в режимі

глобальної конфігурації. Натискання Ctrl-Z або введення команди end завжди викликають повернення в режим EXEC незалежно від поточного режиму або підрежиму конфігурування.

Для виходу з командного режиму глобальної конфігурації та повернення до привілейованого режиму EXEC використовується така команда:

Команда	*Призначення*
Router(config)#end або Router(config)# ^Z	Завершення поточного сеансу конфігурування та повернення до привілейованого режиму EXEC.
Router(config)# exit	Вихід із поточного командного режиму та повернення до попереднього режиму. Наприклад, вихід із режиму глобальної конфігурації у привілейований режим EXEC.

З режиму глобальної конфігурації можливий перехід у безліч режимів конфігурування, специфічних для конкретного протоколу, конкретної платформи чи функціональної можливості. Відомості про специфічні режими представлені у контексті відповідних конкретних завдань у комплекті документації на програмне забезпечення Cisco IOS.

Режим конфігурування інтерфейсу, що описується в наступному розділі, є прикладом режиму конфігурування, в який можна перейти з режиму глобальної конфігурації.

2.2.4. Режим конфігурування інтерфейсу

Одним із прикладів специфічного режиму конфігурування, перехід у який виробляється з режиму глобальної конфігурації, є режим конфігурування інтерфейсу.

Він дозволяє включити багато функціональних можливостей, що залежать від конкретного інтерфейсу. Команди конфігурування інтерфейсу змінюють функціонування інтерфейсу (наприклад, Ethernet, FDDI чи послідовного порту). Командам конфігурування інтерфейсу завжди передує команда режиму глобальної конфігурації interface, що визначає тип інтерфейсу.

Для отримання доступу до команд конфігурування інтерфейсу та виведення їх списку використовується така команда:

Команда	*Призначення*
Router(config)# interface номер	Вказує інтерфейс, що конфігурується, і вхід у режим конфігурування інтерфейсу.

Для виходу з режиму конфігурування інтерфейсу та повернення до режиму глобальної конфігурації необхідно ввести команду exit.

Підрежими конфігурування є режимами конфігурування, перехід до яких здійснюється з інших режимів конфігурування (крім режиму глобальної конфігурації). Підрежими конфігурування призначені для конфігурування специфічних елементів у режимі конфігурування. Один із прикладів підрежиму конфігурування є режим конфігурування субінтерфейсу, який описується в наступному розділі.

2.2.5. Режим конфігурування субінтерфейсу

З режиму конфігурування інтерфейсу можна перейти до режиму конфігурування субінтерфейсу. Режим конфігурування субінтерфейсу є підлеглим стосовно режиму конфігурування інтерфейсу. У режимі конфігурування субінтерфейсу можна задавати параметри множини віртуальних інтерфейсів (вони називаються субінтерфейсами) на єдиному фізичному інтерфейсі. Різним протоколам субінтерфейси представляються як окремі фізичні інтерфейси. Наприклад, мережі Frame Relay надають безліч з'єднань

"точка-точка", які називаються "постійне віртуальне з'єднання" (PVC). PVC можуть бути згруповані в рамках окремих субінтерфейсів, які, своєю чергою, конфігуруються на єдиному фізичному інтерфейсі. З точки зору з'єднань з підтримкою протоколу spanning-tree, кожен субінтерфейс є окремим портом моста, і кадр, що надходить на один субінтерфейс, може бути на виході спрямований на інший субінтерфейс.

Субінтерфейси також підтримують множинну інкапсуляцію протоколів в один фізичний інтерфейс. Наприклад, маршрутизатор або сервер доступу може прийняти IPX-пакет (пакет міжмережевого пакетного обміну) зі структурою ARPA (Агентство з перспективних дослідницьких проектів) і випустити його за тим самим фізичним інтерфейсом як IPX-пакет зі структурою SNAP (протокол доступу до підмереж).

Докладніші відомості про конфігурування субінтерфейсів можна знайти в комплекті документації на програмне забезпечення Cisco IOS. у відповідному модулі документації з описом конкретного протоколу.

Для отримання доступу до режиму конфігурування субінтерфейсу використовується наступна команда режиму конфігурування інтерфейсу:

Команда	*Призначення*
Router(config-if)# interface тип номер	Вказує конфігурований віртуальний інтерфейс і вхід у режим конфігурування субінтерфейсу.

У наступному прикладі задаються параметри субінтерфейсу для послідовної лінії 2, яка налаштована для інкапсуляції Frame Relay. Субінтерфейс отримує позначення "2.1", що вказує на те, що це субінтерфейс послідовної 1 лінії 2. Нове запрошення hostname(config-subif)#, вказує на режим конфігурування субінтерфейсу. Субінтерфейс можна налаштувати для підтримки одного або декількох постійних віртуальних з'єднань (PVC) мережі Frame Relay.

```
Router(config)# interface serial 2
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 2.1
Router(config-subif)#
```

Для виходу з режиму конфігурування субінтерфейсу та повернення до режиму конфігурування інтерфейсу використовується команда exit. Щоб завершити сеанс конфігурації та повернутися до режиму EXEC, натисніть Ctrl-Z або введіть команду end.

2.2.6. Режим монітора ROM

Режим монітора ROM (ROMMON) запускається зі спеціалізованого способу програмного забезпечення і призначений для того, щоб вручну знайти правильний образ системного програмного забезпечення для завантаження системи (режим монітора ROM іноді називається також "режим завантаження").

Якщо система (маршрутизатор, комутатор або сервер доступу) не знаходить правильний образ системи для завантаження, система переходить в режим монітора ROM. У режим монітора ROM можна увійти також переривання послідовності завантаження під час запуску. З режиму монітора ROM можна завантажити пристрій або виконати діагностичні тести.

На більшості систем можна ввійти в режим ROM, якщо ввести команду EXEC reload і потім протягом перших 60 секунд процедури запуску видати команду Break. Команда Break видається шляхом натискання клавіші Break на клавіатурі або за допомогою клавіш Break (сполучення клавіш Break за замовчуванням – Ctrl-C).

Щоб перейти в режим ROM з режиму EXEC, виконайте такі дії:

• Крок 1 У режимі EXEC введіть reload. Після введення цієї команди та відповіді (за потребою) на системні запрошення система почне перезавантаження образу системного програмного забезпечення.

• Крок 2 Протягом перших 60 секунд процедури запуску видайте команду Break. Команда Break видається за допомогою клавіш Break або поєднання клавіш Break. (Поєднання клавіш Break за замовчуванням - Ctrl-C, але можливе завдання іншої комбінації). При видачі команди Break послідовність завантаження переривається і відбувається перехід у режим монітора ROM.

Інший спосіб переходу в режим монітора ROM - Встановлення значення регістру конфігурації, що забезпечує автоматичний перехід маршрутизатора в режим монітора ROM у процесі завантаження. Інформацію про встановлення значення регістру конфігурації.

У режимі монітора ROM як запрошення командного рядка використовується кутова дужка (>). На деяких пристроях Cisco запрошення на монітор ROM виглядає як (rommon >). Список команд монітора ROM відображається під час введення команди ? чи команди help. У цьому прикладі показано, як може виглядати цей список команд:

alias	set and display aliases command
boot	boot up an external process
break	set/show/clear the breakpoint
confreg	configuration register utility
cont	continue executing a downloaded image

context	display the context of a loaded image
cpu_card_type	display CPU card type
dev	list the device table
dir	list files in file system
dis	disassemble instruction stream
frame	print out a selected stack frame
help	monitor builtin command help
history	monitor command history
meminfo	main memory information
repeat	repeat a monitor command
reset	system reset
set	show all monitor variables
stack	produce a stack trace
sync	write monitor environment to NVRAM
sysret	print out info from last system return
unalias	unset an alias
unset	unset a monitor variable

Зведення основних командних режимів Cisco IOS

Таблиця відображає інформацію про основні командні режими, що використовуються в інтерфейсі командного рядка Cisco IOS.

Командний режим	Спосіб доступу	? Запрошення	Спосіб виходу
Режим користувача EXEC	Вхід в систему	Router >	Команда logout.
Привілейований режим EXEC	У режимі EXEC використовується команда EXEC	Router#	Для виходу в режим користувача EXEC використовується команда

	enable.		disable. Для входу в режим глобальної конфігурації використається команда привілейованого режиму EXEC configure terminal.
Глобальна конфігурація	У привілейованому режимі EXEC використається команда configure terminal.	Router(config)#	Для виходу в привілейований режим EXEC введіть end або натисніть Ctrl-Z. Щоб перейти до режиму конфігурації інтерфейсу, введіть команду конфігурації interface.
Налаштування інтерфейсу	У режимі глобальної конфігурації вкажіть інтерфейс команді interface.	Router(config-if)#	Щоб вийти в режим глобальної конфігурації, введіть команду exit. Для виходу в привілейований режим EXEC введіть end або натисніть Ctrl-Z. Для входу в режим конфігурування субінтерфейсу вкажіть субінтерфейс команді interface.
Конфігурація субінтерфейсу	У режимі конфігурування інтерфейсу вкажіть інтерфейс команді interface. (Доступність цього режиму залежить від платформи.)	Router(config-subif)#	Щоб вийти в режим глобальної конфігурації, введіть команду exit. Для виходу в привілейований режим EXEC введіть end або натисніть Ctrl-Z.
Монітор ROM	У привілейованому режимі EXEC введіть	>	Якщо вхід у режим монітора ROM здійснено шляхом

	команду EXEC reload. Натисніть клавішу Break протягом перших 60 секунд процедури завантаження системи.	або boot> або rommon>	переривання процесу завантаження, можна вийти з режиму монітора ROM та відновити завантаження за допомогою команд continue.

2.3. Список завдань CLI Cisco IOS

Щоб познайомитися з функціональними можливостями інтерфейсу командного рядка Cisco IOS, виконайте будь-яке із завдань, описаних у наступних розділах:

- Отримання контекстно-залежної довідки.
- Використання форм команд no та default.
- Використання історії команд.
- Використання функцій редагування CLI та клавіш.
- Пошук та фільтрація виводу CLI.

2.3.1. Отримання контекстно-залежної довідки

Введення знаку запитання (?) після запрошення системи дозволяє вивести список команд, доступних у кожному командному режимі. За допомогою функції контекстно-залежної довідки також можна отримати список аргументів і ключових слів для будь-якої команди.

Для отримання довідки, специфічної для командного режиму, імені команди, ключового слова чи аргументу, використовується будь-яка з наступних команд:

Команда	Призначення
(запрошення)# help	Відображає короткий опис системи довідки.
(запрошення) # скорочене введення команди?	Вивод списку команд поточного режиму, що починаються з певного символьного рядка.
(запрошення)# скорочене введення команди <>	Доповнення часткового імені команди.
(Запрошення) #?	Вивод списку всіх команд, доступних у командному режимі.
(запрошення) # команда?	Виведення списку доступних синтаксичних опцій (аргументів та ключових слів) для команди.
(запрошення)# команда ключове слово?	Виведення списку наступних синтаксичних опцій для команди

Слід пам'ятати, що системне запрошення змінюватиметься залежно від поточного режиму конфігурації.

При використанні контекстно-залежної довідки наявність або відсутність пробілу перед знаком питання (?) є важливим. Для отримання списку команд, що починаються з певної послідовності символів, введіть ці символи та відразу після них введіть знак запитання (?). Не вводіть пробіл. Ця форма довідки називається довідка за словом, оскільки вона доповнює слово користувача. Подальшу інформацію див. у розділі "Додаток частково введеного імені команди" в цьому розділі.

Щоб вивести список ключових слів або аргументів, введіть знак запитання (?) замість ключового слова або аргументу. Увімкніть пробіл перед ?. Ця форма довідки називається довідка за синтаксисом команди, тому що вона

показує можливі ключові слова або аргументи на основі вже введених команд, ключових слів та аргументів.

Можна скорочувати команди та ключові слова до кількості символів, що забезпечує унікальність скорочення. Наприклад, можна скоротити команду configure terminal до config t. Завдяки унікальності скороченої форми команди маршрутизатор прийме скорочену форму і виконає команду.

При введенні команди help, доступної в будь-якому командному режимі, буде виведено такий опис довідки:

```
Router# help
```

Як зазначено у виведенні команди help, знак питання (?) може використовуватися для доповнення частково введеного імені команди (часткова довідка), а також для отримання списку аргументів або ключових слів, що доповнюють поточну команду.

2.3.2. Використання форм команд no та default

Багато команд конфігурування допускають використання форми no. Форма no служить заборони функціональної можливості чи функції. Щоб повторно дозволити заборонену функціональну можливість або дозволити функціональну можливість заборонену за замовчуванням, використовується команда без ключового слова no . Наприклад, IP-маршрутизація за замовчуванням дозволена. Для заборони IP-маршрутизації використається форма no ip routing команди ip routing. Для повторного її вирішення використовується проста форма ip routing.

Довідник по командах програмного забезпечення Cisco IOS описує функцію форми команд no незалежно від доступності форми no.

Багато команд CLI мають також форму default. Шляхом введення команди default команда_ім'я можна налаштувати команду на її установки за замовчуванням. Довідник по командах програмного забезпечення Cisco IOS

зазвичай описує функцію форми default команди у випадках, коли форма default виконує іншу функцію, відмінну від простої форми команди та форми no. Щоб побачити, які стандартні команди доступні в системі, введіть default ? у відповідному командному режимі.

2.3.3. Використання історії команд

Інтерфейс командного рядка Cisco IOS надає історію запису введених команд. Ця функціональна можливість є особливо корисною для повторного виклику довгих або складних команд або фрагментів введення, включаючи списки доступу.

2.4. Використання CLI Cisco IOS: приклади

CLI забезпечує локалізацію помилки як покажчика помилки — символу вставки (^). Символ ^ з'являється там командного рядка, де користувач ввів неправильну команду, ключове слово або аргумент.

У наступному прикладі, припустимо, необхідно встановити годинник. Щоб визначити правильний синтаксис для встановлення годинника, використовується контекстно-залежна довідка.

```
Router # clock?
  set Set time and date
Router# clock
```

Виведення довідки показує, що потрібне ключове слово set. Визначимо синтаксис для встановлення часу:

```
Router# clock set?
hh:mm:ss Current time
Router# clock set
```

Введемо поточний час:

```
Router# clock set 13:32:00
% Incomplete command.
```

Система вказує на необхідність введення додаткових аргументів для завершення команди. Натисніть Ctrl-P або клавішу "Стрілка вгору", щоб автоматично повторити попереднє введення команди. Потім додамо пробіл і знак запитання (?), щоб показати додаткові аргументи:

```
Router# clock set 13:32:00 ?
  <1-31> Day of the month
  January Month of the year
  February
  March
  April
  May
  June
  July
  August
  September
  Жовтень
  November
  December
Router#
Router#
Router# clock set 13:32:00 23 November 2021
```

2.5. Пошук та фільтрація виводу CLI: приклади

Нижче приклад наведено фрагмент виведення команди привілейованого режиму EXEC **more nvram:startup-config | begin**, яка починає нефільтрований висновок з першого рядка, що містить регулярний вираз ip. Після запрошення --More-- користувач визначає фільтр, який виключає рядки, що містять регулярне вираження ip.

```
Router# more nvram:startup-config | begin ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 192.168.48.48
ip name-server 172.16.2.132
!
isdn switch-type primary-5ess
.
interface Ethernet1
 ip address 10.5.5.99 10.255.255.0
 --More--
-ip
filtering...
 media-type 10BaseT
!
interface Serial0:23
 encapsulation frame-relay
 no keepalive
 dialer string 4001
 dialer-group 1
 isdn switch-type primary-5ess
 no fair-queue
```

Далі для прикладу наведено фрагмент виведення команди привілейованого режиму EXEC **more nvram:startup-config | include**. Він відображає лише рядки, що містять регулярний вираз ip.

```
Router# more nvram:startup-config | include ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 1192.168.48.48
ip name-server 172.16.2.132
```

Далі для прикладу наведено фрагмент виведення команди привілейованого режиму EXEC more nvram:startup-config | exclude. З нього виключені рядки, що містять регулярний вираз service. Після запрошення --More-- користувач задає фільтр із регулярним виразом Dialer1. При заданні цього фільтра висновок поновлюється з першого рядка, що містить підрядок Dialer1.

```
Router# more nvram:startup-config | exclude service
!
version 12.2
!
hostname router
!
boot system flash
no logging buffered
!
ip subnet-zero
ip domain-name cisco.com
.
--More--
/Dialer1
filtering...
interface Dialer1
 no ip address
 no ip directed-broadcast
 dialer in-band
 no cdp enable
```

Далі для прикладу наведено фрагмент виведення команди користувальницького або привілейованого режиму EXEC show interface із зазначенням пошуку в потоці виводу. При вказівці після символу каналу ключових слів begin Ethernet нефільтрований висновок починається з першого рядка, що містить регулярний вираз Ethernet. Після запрошення --More-- користувач задає фільтр, який відображає лише рядки, що містять регулярний вираз Serial.

```
Router# show interface | begin Ethernet
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Description: ip address is 172.1.2.14 255.255.255.0
  Internet address is 172.1.2.14/24
.
.
.
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
--More--
+Serial
filtering...
Serial1 is up, line protocol is up
Serial2 is up, line protocol is up
Serial3 is up, line protocol is down
Serial4 is down, line protocol is down
Serial5 is up, line protocol is up
Serial6 is up, line protocol is up
Serial7 is up, line protocol is up
```

Далі приклад наведено фрагмент виведення команди show buffers | exclude. З нього виключені рядки, що містять регулярний вираз 0 міс. Після запрошення --More-- користувач визначає пошук, який продовжує фільтрований висновок, починаючи з першого рядка, що містить підрядок Serial0.

```
Router# show buffers | exclude 0 Misses

Buffer elements:
    398 in free list (500 max allowed)
Public buffer pools:
Малі buffers, 104 байт (тотал 50, permanent 50):
    50 in free list (20 min, 150 max allowed)
    551 hits, 3 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
    49 in free list (5 min, 150 max allowed)
Very Big buffers, 4520 bytes (total 10, permanent 10):
.
Huge buffers, 18024 bytes (total 0 permanent 0):
    0 in free list (0 min, 4 max allowed)
--More--
/Serial0
filtering...
Serial0 buffers, 1543 bytes (total 64, permanent 64):
    16 in free list (0 min, 64 max allowed)
    48 hits, 0 fallbacks
```

Далі для прикладу наведено фрагмент виведення команди користувача або привілейованого режиму EXEC show interface | include . При вказівці після символу каналу (|) ключових слів include (is) команда відображає лише рядки, що містять регулярний вираз (is). Дужки забезпечують включення прогалин до і після is. Завдяки використанню дужок у висновок включаються лише ті рядки, в яких міститься підрядок is з пробілами до та після неї (при цьому виключається, наприклад, слово "disconnect").

```
router# show interface | include (is)

ATM0 is administratively down, line protocol is down
  Hardware is ATMizer BX-50
Dialer1 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  DTR is pulsed for 1 seconds on reset
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Internet address is 172.21.53.199/24
Ethernet1 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.639c (bia 0060.837c.639c)
  Internet address is 10.5.5.99/24
Serial0:0 is down, line protocol is down
  Hardware is DSX1
.
 --More--
```

Після запрошення --More-- користувач задає пошук, який продовжує фільтрований висновок, починаючи з першого рядка, що містить підрядок Serial0:13:

```
/Serial0:13
filtering...
Serial0:13 is down, line protocol is down
  Hardware is DSX1
  Internet address is 10.0.0.2/8
    0 output errors, 0 collisions, 2 interface resets
  Timeslot(s) Used:14, Transmitter delay is 0 flag
```

2.6. Висновки до розділу 2

Одним із ефективних рішень для обмеження доступу до небажаних інформаційних ресурсів в мережі Інтернет є використання програмно-апаратних рішень, які включають в себе налаштування активного комунікаційного обладнання, зокрема, маршрутизаторів.

Налаштування маршрутизатора відбувається через інтерфейс командного рядка (CLI). Cisco IOS — це основний інтерфейс, який використовується для конфігурування, моніторингу та обслуговування пристроїв Cisco. Цей інтерфейс користувача дозволяє безпосередньо виконувати команди Cisco IOS за допомогою консолі маршрутизатора, терміналу або з використанням віддаленого доступу.

В розділі 2 розглянуто принцип дії CLI API Cisco, та проаналізовано основні команди. Вивчено можливості реалізації обмеження доступу до інформаційних ресурсів у мережі. Підібрані команди для реалізації методу по блокування інформаційних доменів.

API відносно прості але вимагають базової підготовки та навичок мережевого адміністрування, та розуміння принципу дії мережі Інтернет по моделі tcp/ip.

РОЗДІЛ 3

РЕАЛІЗАЦІЯ МЕТОДУ

Використання прикладного програмного інтерфейсу для маршрутизатора Cisco для блокування соціальних мереж.

3.1. Знайомство з GNS3

Для наглядного використання використано емулятор GNS3 (рис. 3.1).

Рис. 3.1. GNS3 – графічний емулятор мережі

Що таке GNS3?

Graphical Network Simulator. Якщо перекласти дослівно – графічний емулятор мережі. Він дозволяє створювати різні мережеві топології прямо на вашому комп'ютері. Найчастіше GNS використовується як лабораторний стенд, де можна перевірити ту чи іншу технологію або схему [11].

Емулятор дозволяє створити модель комп'ютера або іншого пристрою і запустити в ньому оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, включаючи пам’ять, процесор, інтерфейси, та пристрої вводу/виводу. У випадку Cisco, емулятор створює модель маршрутизатора і запускає справжню операційну систему Cisco IOS всередині. Таким чином ми отримуємо повністю обладнаний роутер.

Чому GNS3?

- Першою і головною причиною є повна функціональність емульованих пристроїв. Тобто. використовуючи той самий маршрутизатор Cisco, ми можемо отримати доступ майже до всіх функцій, які працюють на реальному маршрутизаторі.

- Можливість побудови гетерогенних мереж. Мається на увазі, що ми можемо зібрати схему, де будуть не тільки пристрої Cisco, але і Juniper, Mikrotik, CheckPoint і т.д.

- Додавання до мережі повноцінних робочих станцій і серверів. У GNS3 ми можемо додати повноцінний комп'ютер із Windows 7 або Ubuntu.

- Безкоштовність! GNS3 знаходиться у вільному доступі і не має жодних обмежень щодо використання.

Недоліки GNS3

- Відсутність можливості емуляції комутаторів. Справа в тому, що справжні комутатори мають велику кількість мікросхем ASIC, які поки не можна емулювати на звичайному комп'ютері. Саме ці чіпи ASIC забезпечують величезну швидкість обробки пакетів. Але в основі роутерів лежить процесор, який дуже схожий на процесор звичайного комп’ютера, а іноді такий самий. Тому проблем з емуляцією роутера немає. Однак процесор набагато повільніше, ніж чіпи ASIC.
- Високі вимоги до системних ресурсів.

3.2. Запуск GNS3 та емуляція мережі на базі маршрутизаторів CISCO C3745

Запустимо GNS3 та створимо мережу з декількома маршрутизаторами CISCO. Буде використано емуляцію маршрутизатора CISCO C3745 (рис. 3.2).

Рис. 3.2. CISCO C3745

Емулюємо інтернет (рис. 3.3):

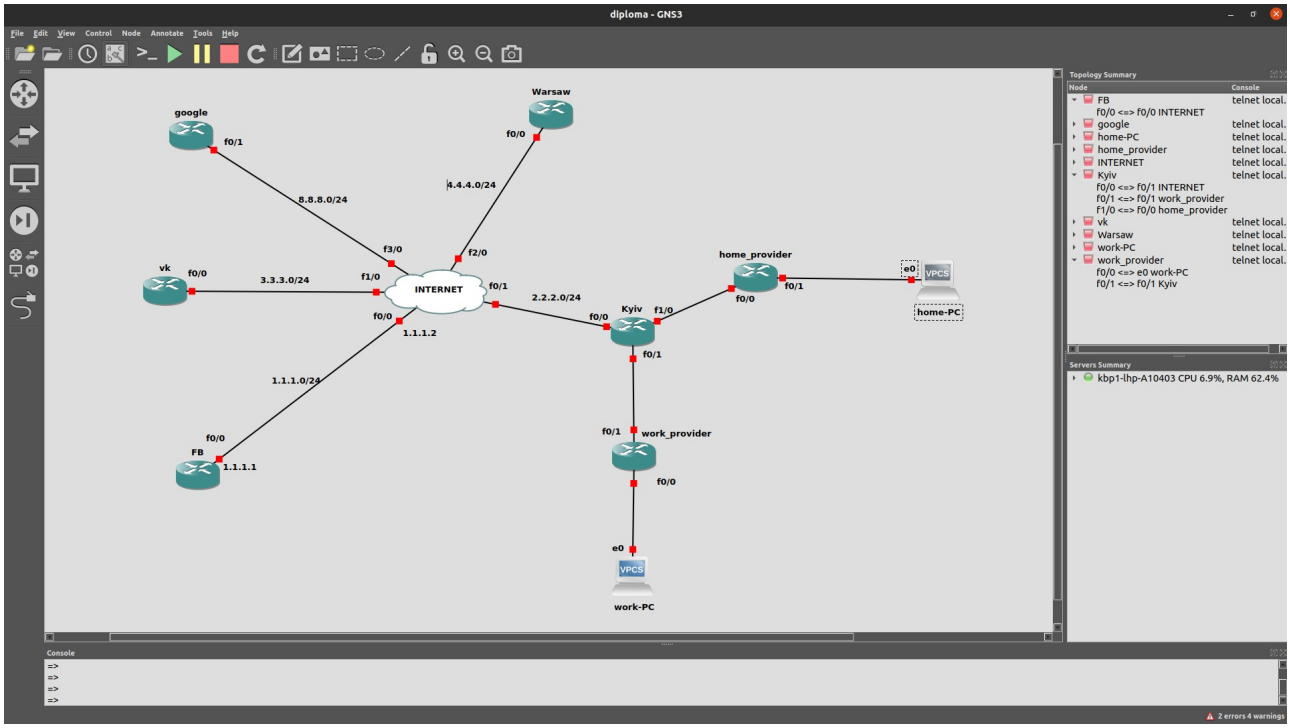

Рис. 3.3. Емуляція інтернету

Поставимо в стенд декілька маршрутизаторів CISCO, створимо спрощену схему інтернет без комутаторів l2 рівня. Створюємо step-by-step контрольний маршрутизатор Warsaw, маршрутизатор Kyiv, сервер соціальних мереж для google.com , vk.ru , facebook.com, провайдерів для робочих та домашніх ПК.

Наступним кроком буде поетапне включення серверів (рис. 3.4), та налаштування їх за допомогою CLI API CISCO.

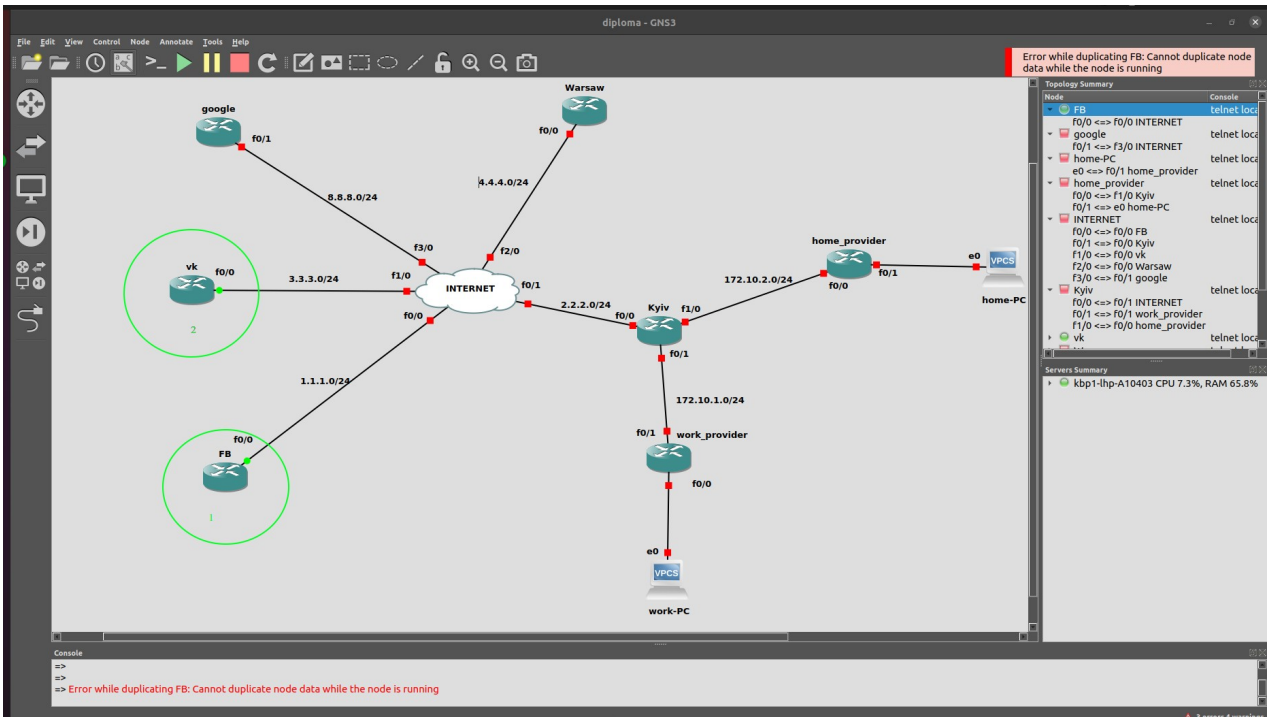

Рис. 3.4. Поетапне підключення серверів

Розглянемо приклад підключення серверу vk (рис. 3.5), всі наступні налаштування відбуваються за подібною схемою:

- Вхід до привілегованого режиму.
- Налаштування мережевого інтерфейсу для виходу в інтеренет.
- Пропис default gateaway.
- Збереження конфігурації.
- Перевірка доступу до “internet” (тест буде провалено – оскільки сервер “internet” на даному етапі ще не введено в мережу)

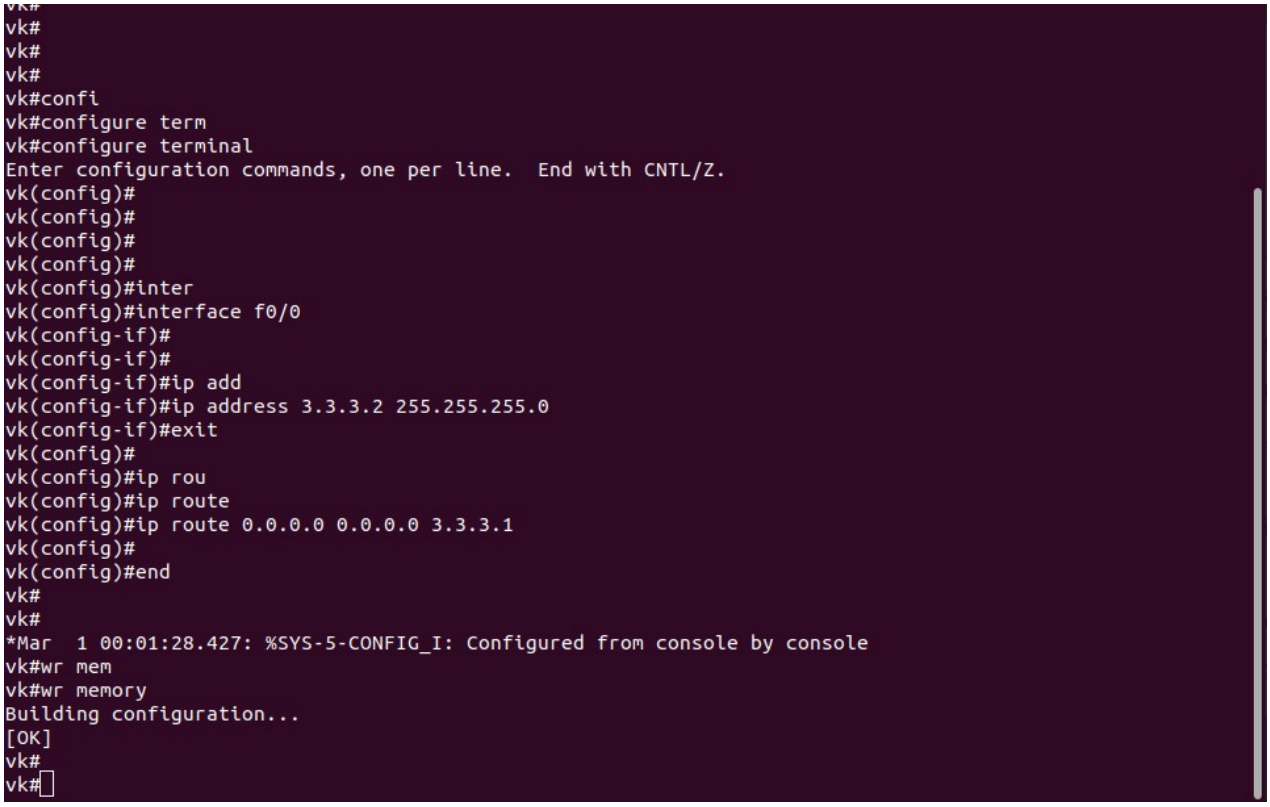

Рис. 3.5. Підключення серверу vk

На Маршрутизаторі INTERNET використано наступні CLI API CISCO:

```
!
interface FastEthernet0/0
 no shutdown
 ip address 1.1.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no shutdown
 ip address 2.2.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no shutdown
 ip address 3.3.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no shutdown
 ip address 4.4.4.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet3/0
 no shutdown
 ip address 8.8.8.1 255.255.255.0
 duplex auto
 speed auto
!
```

3.2.1. Налаштування мережевих провайдерів.

Налаштуємо мережеві провайдери для домашнього ПК, та робочого ПК, по принципу описаного налаштування для сервера VK (рис 3.6, рис 3.7).

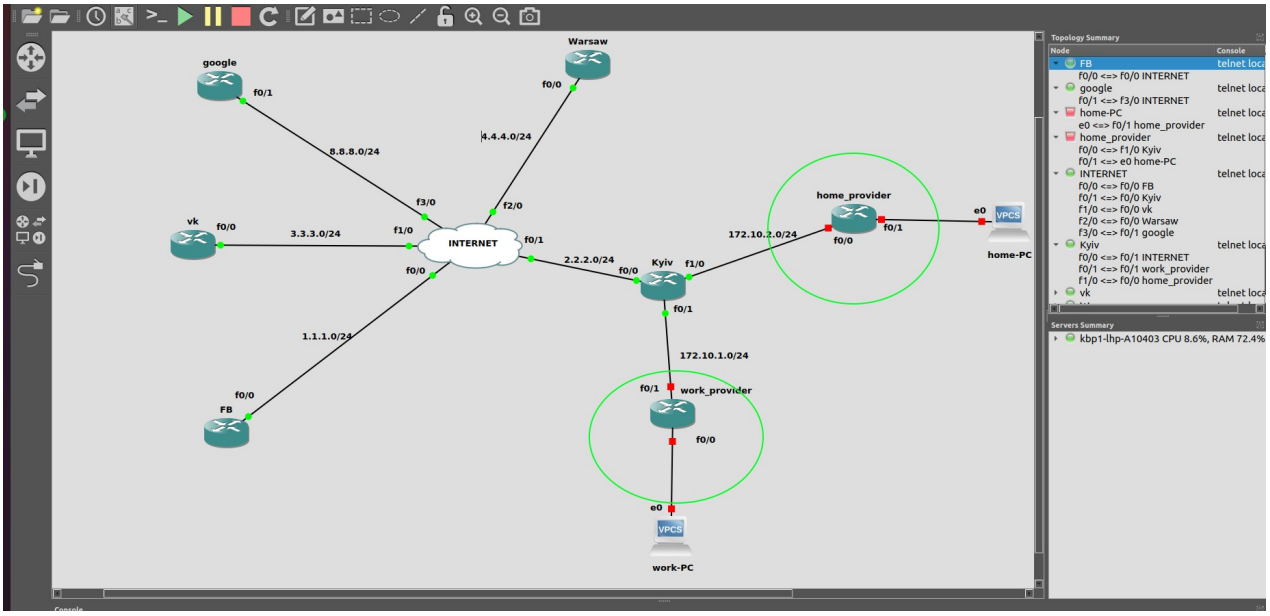

Рис. 3.6. Поетапне підключення маршрутизаторів work_provider та home_provider

```
INTERNET(config)#
INTERNET(config)#interf
INTERNET(config)#interface f2/0
INTERNET(config-if)#
INTERNET(config-if)#
INTERNET(config-if)#no shutdown
INTERNET(config-if)#ip address 8.8.8.1 255.255.255.0
*Mar  1 00:02:13.903: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Mar  1 00:02:14.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to u
p
INTERNET(config-if)#ip address 4.4.4.1 255.255.255.0
INTERNET(config-if)#
INTERNET(config-if)#
INTERNET(config-if)#
INTERNET(config-if)#exit
INTERNET(config)#
INTERNET(config)#
INTERNET(config)#inter
INTERNET(config)#interface f0/1
INTERNET(config-if)#
INTERNET(config-if)#
INTERNET(config-if)#no shut
INTERNET(config-if)#no shutdown
INTERNET(config-if)#
*Mar  1 00:03:08.883: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:03:09.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to u
p
INTERNET(config-if)#ip add
INTERNET(config-if)#ip address 2.2.2.1 255.255.255.0
INTERNET(config-if)#
INTERNET(config-if)#
INTERNET(config-if)#
```

Рис. 3.7. Підключення маршрутизатора INTERNET

3.2.2. Налаштування таблиці маршрутизації.

Коли ми назначили всі адреса мереж, можемо прописати таблицю маршрутизації на відповідних маршрутизаторах (рис. 3.8).

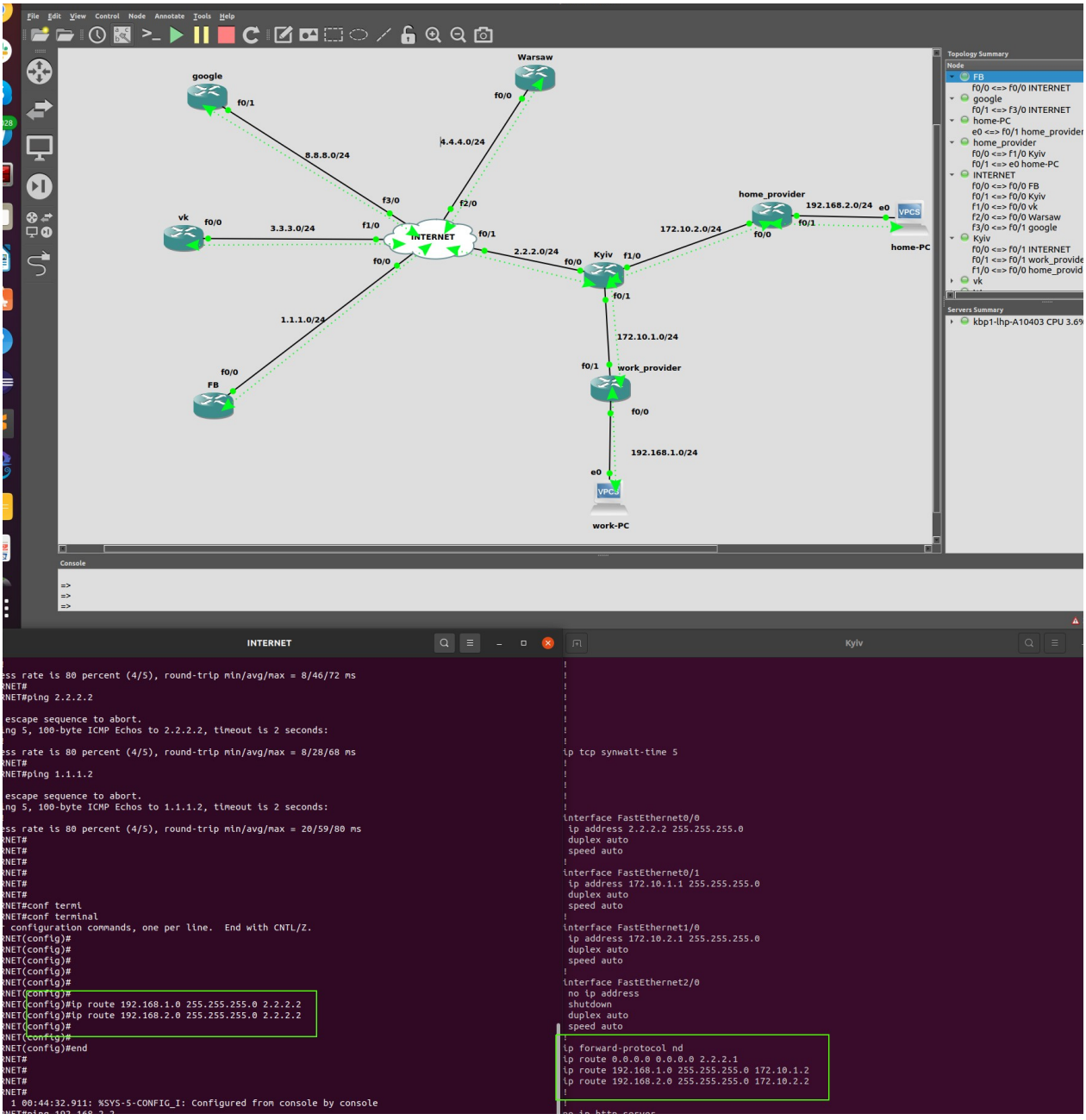

Рис. 3.8. Пропис таблиці маршрутизації

3.2.3. Перевірка працездатності мережі.

Після налаштування маршрутів, перевіримо стандартними утилітами ping та traceroute.

Ping використовується, щоб визначити, чи може служба успішно спілкуватися з віддаленим хостом. Ping створює Send, який намагається надіслати повідомлення із запитом на перевірку зв'язку ICMP на зовнішню IP-адресу та отримує з неї відповідне повідомлення про перевірку зв'язку ICMP.

ICMP — мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як ping та traceroute [12].

Перевірка доступу до серверу VK за допомогою ping та trace (traceroute) (рис. 3.9):

```
work-PC>
work-PC> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=252 time=34.474 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=252 time=36.396 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=252 time=37.241 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=252 time=37.100 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=252 time=37.770 ms

work-PC> trace 8.8.8.8 -P 1
trace to 8.8.8.8, 8 hops max (ICMP), press Ctrl+C to stop
 1   192.168.1.1   9.755 ms  9.055 ms  9.538 ms
 2   172.10.1.1   20.125 ms  20.238 ms  19.865 ms
 3   2.2.2.1   39.574 ms  39.928 ms  39.532 ms
 4   8.8.8.8   50.580 ms  49.983 ms  50.265 ms

work-PC>
work-PC>
work-PC> trace

trace HOST [OPTION ...]
  Print the path packets take to the network HOST. HOST can be an ip address or
  name.
    Options:
      -P protocol    Use IP protocol in trace packets
                       1 - icmp, 17 - udp (default), 6 - tcp
      -m ttl         Maximum ttl, default 8

  Notes: 1. Using names requires DNS to be set.
         2. Use Ctrl+C to stop the command.

work-PC>
```

Рис. 3.9. ping vk з work-PC

Емуляція інтернету завершена.

3.3. Метод блокування інформаційних доменів. Реалізація

Блокування російських інтернет-сервісів в Україні (також відоме як блокування російських соцмереж) — обмеження інтернет-провайдерами доступу до низки російських інтернет-сайтів. Юридичним приводом для блокування стало введення додаткових санкцій України щодо Росії указом Президента України Петра Порошенка № 133/2017 від 15 травня 2017 року про введення в дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Особливістю нових санкцій стала вимога блокування інтернет-провайдерами доступу до веб-ресурсів інтернет-компаній ВКонтакті, Однокласники, «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web», офіційного дистриб'ютора «1С» на території України тощо строком на 3 роки.

Треба розробити метод, який буде блокувати трафік з VK, та не шкодити іншому доступу до мережі.

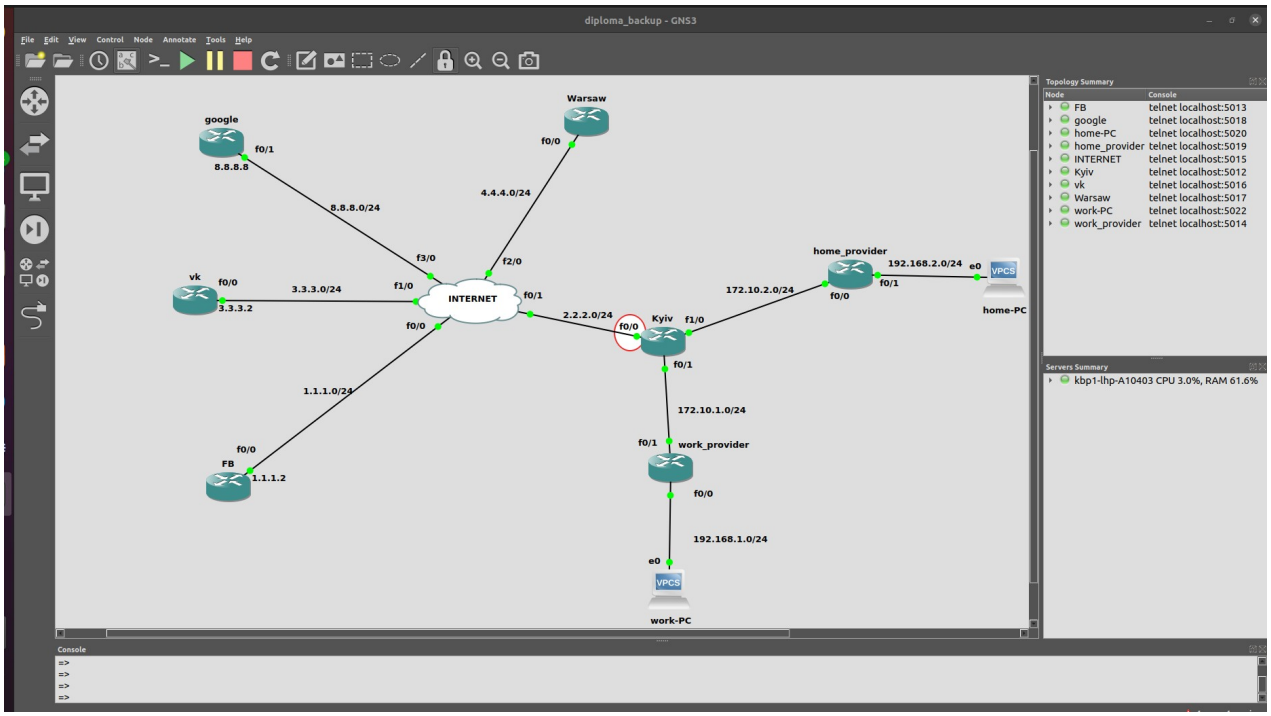

Рис. 3.10. Блокування інтерфейсу, який іде до інтернету

В нашому емульованому інтернеті, є мережа Вконтакті (VK), зробимо блокування на рівні Kyiv маршрутизатора в нашому емульованому інтернеті за допомогою CLI API CISCO:

- Додамо access-list BLOCK_VK.
- В даному емульованому інтернеті нам відомий ip VK, додамо ip соціальної мережі вконтакте до access-list BLOCK_VK, та заборонимо доступ до неї.
- В кожному access-list є остання неявне правило `deny any any`, кожний пакет проходить по access-list зверху вниз, і доходячи до останнього неявного правила — блокується. Додамо до останнього неявного правила, наше явне правило `permit ip any any` (рис 3.11).
- Додамо access-list BLOCK_VK до інтерфейсу який виходить до "інтернету" (рис 3.10).

```
Kyiv#
Kyiv#
Kyiv#
Kyiv#
Kyiv#
Kyiv#
Kyiv#
Kyiv#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Kyiv(config)#
Kyiv(config)#
Kyiv(config)#
Kyiv(config)#ip access-list extended BLOCK_VK
Kyiv(config-ext-nacl)#
Kyiv(config-ext-nacl)#
Kyiv(config-ext-nacl)#
Kyiv(config-ext-nacl)#
Kyiv(config-ext-nacl)#deny ip any 3.3.3.2 0.0.0.255
Kyiv(config-ext-nacl)#permit any any
                      ^
% Invalid input detected at '^' marker.

Kyiv(config-ext-nacl)#permit ip any any
Kyiv(config-ext-nacl)#
Kyiv(config-ext-nacl)#exit
Kyiv(config)#inte
Kyiv(config)#interface f0/0
Kyiv(config-if)#ip access-group BLOCK_VK out
Kyiv(config-if)#
```

Рис. 3.11. Створення access-list

Перевіримо доступ до заблокованої мережі вконтакті зі сторони користувача за Kyiv маршрутизатором. Перевіряємо доступ до соціальних мережі вконтакті, за домогою утиліти ping з ПК.

```
# ping 3.3.3.2
```

Прийшла відповідь з кодом 13 (Communication Administratively Prohibited)

TTL — 254.

Time to live (TTL) в обчислювальні техніці та комп'ютерних мережах — максимальний період часу або кількість ітерацій або переходів, за який набір даних (пакет) може існувати до свого зникнення.

В IPv4 TTL є 8-бітним полем IP-заголовка. Воно знаходиться у дев'ятому октеті з двадцяти. Значення TTL може розглядатися як верхня межа часу існування IP-датаграми в мережі. Поле TTL встановлюється відправником датаграми, і зменшується з кожним вузлом (наприклад, маршрутизатором) на шляху його слідування, згідно з часом перебування у даному пристрої або згідно з протоколом обробки.

Якщо поле TTL стає рівним нулю до того, як датаграма дістанеться пункту призначення, то вона відкидається і відправнику відсилається ICMP-пакет з кодом 11 — «Перевищення інтервалу».

Відкидання пакетів із часом життя який закінчився дозволяє уникнути ситуацій, коли датаграми, що не можуть бути доставлені, і «вічно» циркулюють в системі Інтернет, перевантажуючи мережу (наприклад, у разі виникнення циклічних маршрутів через некоректну маршрутизацію).

За стандартом RFC791, час життя вимірюється в секундах, але кожен вузол, крізь який проходить датаграма, має зменшити значення TTL принаймні на одиницю. На практиці, якщо обробка займає менше секунди, поле TTL зменшується на одиницю на кожному хопі. Для того щоб відобразити це, в протоколі IPv6 поле було перейменовано в «hop limit». Також в деяких

реалізаціях IP-протоколу TTL вимірюється в кількості кроків (хопів), у цьому разі маршрутизатор зменшує значення TTL рівно на одиницю.[29]

В якості контрольного тесту використано ping сервера google.com 8.8.8.8 — доступ є (рис 3.12).

```
# ping 8.8.8.8
```

Для контролю так же використано утиліту trace, яка показує кількість пройдених “хопів”. Прапор “-P 1” як бачимо з опису команди — використовувати icmp протокол (рис 3.12).

```
# trace 8.8.8.8 -P 1
```

Як бачимо trace обривається на ip Київського провайдера (рис 3.13).

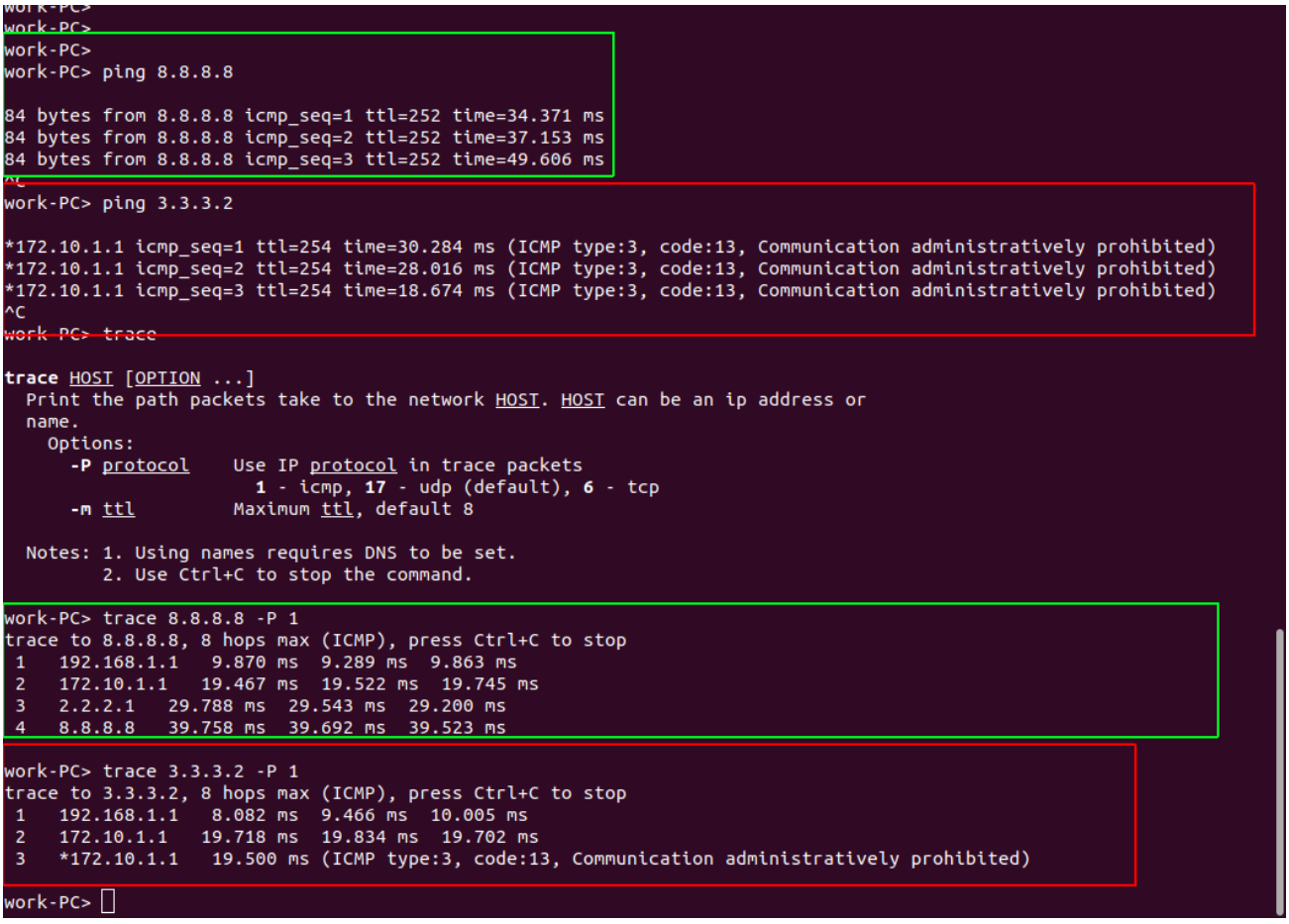

Рис. 3.12. Перевірка access-list

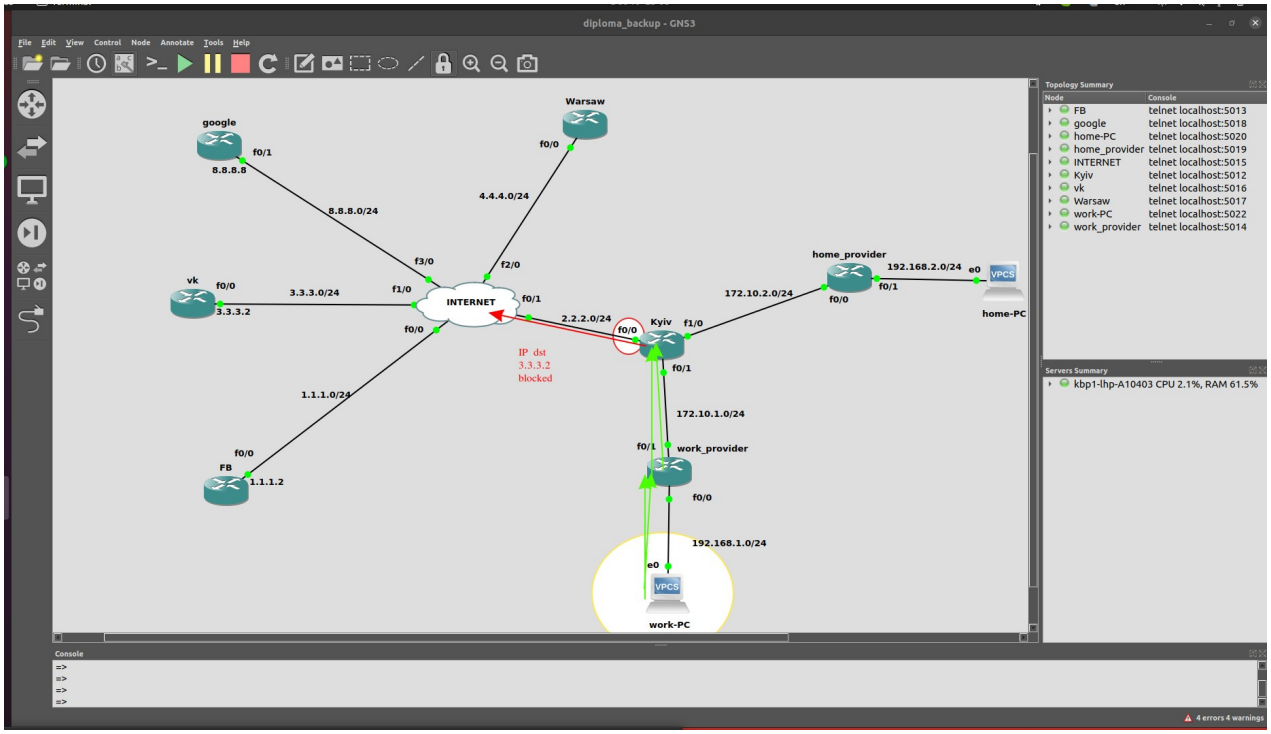

Рис. 3.13. Перевірка access-list на графіку

3.4. Блокування соціальної мережі Facebook за робочим провайдером

В нашому емульованому інтернеті, є мережа Facebook (FB), зробимо блокування на рівні work_provider (рис. 3.14) маршрутизатора в нашому емульованому інтернеті за допомогою CLI API CISCO:

- Додамо access-list BLOCK_FB.
- В даному емульованому інтернеті нам відомий ip FB, додамо ip соціальної мережі facebook до access-list BLOCK_FB, та заборонимо доступ до неї.
- В кожному access-list є остання неявне правило `deny any any`, кожний пакет проходить по access-list зверху вниз, і доходячи до останнього неявного правила — блокується. Додамо до останнього неявного правила, наше явне правило `permit ip any any`.

- Додамо access-list BLOCK_FB до інтерфейсу який виходить до робочого ПК

Перевіряємо доступ до соціальної мережі вконтакті, за допомогою утиліти ping з ПК (рис. 3.14, рис. 3.15).

```
# ping 1.1.1.2
```

Прийшла відповідь з кодом 13 (Communication Administratively Prohibited) TTL — 255.

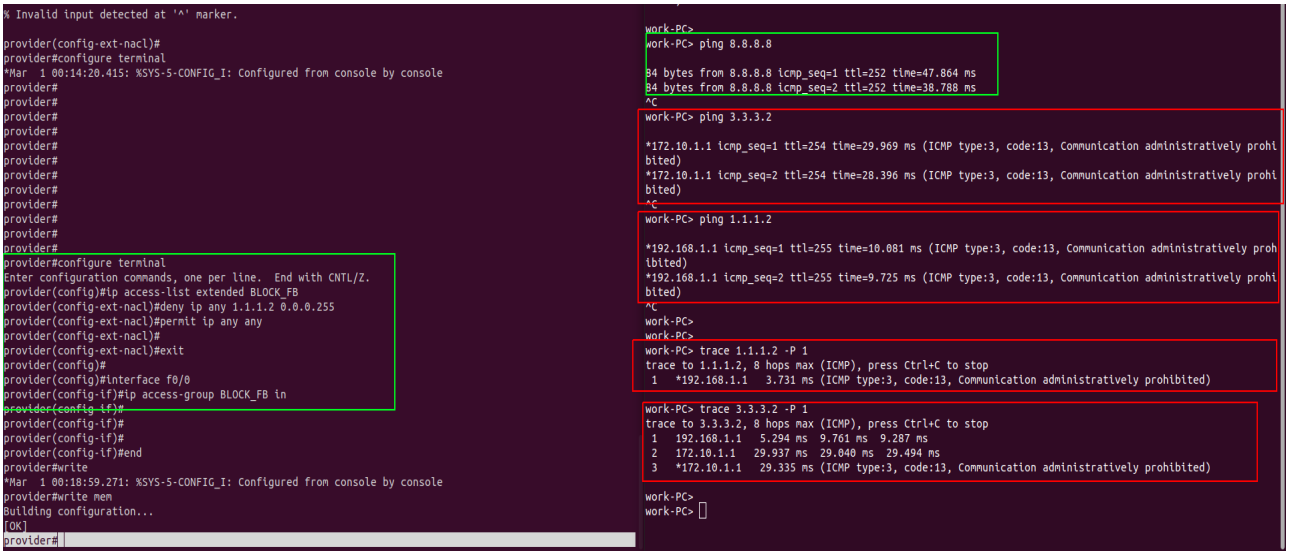

Рис. 3.14. Перевірка доступа до VK та FB

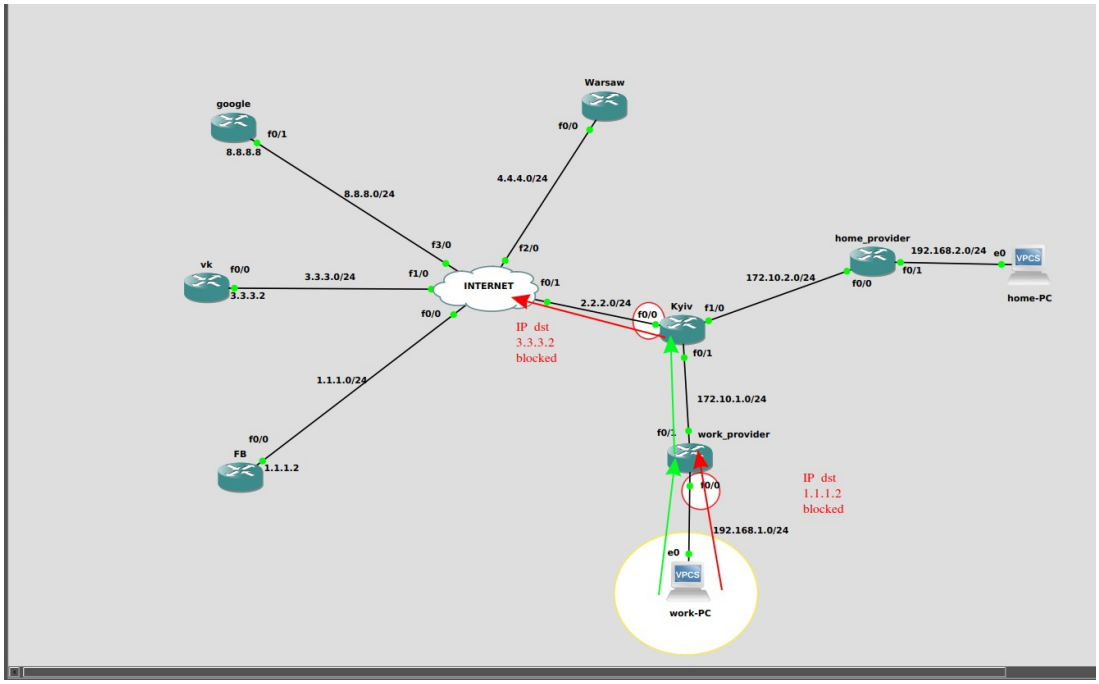

Рис. 3.15. Перевірка доступа до VK та FB на графіку

Перевірка доступу до соціальної мережі Facebook з робочого-ПК та домашнього-ПК (рис. 3.16).

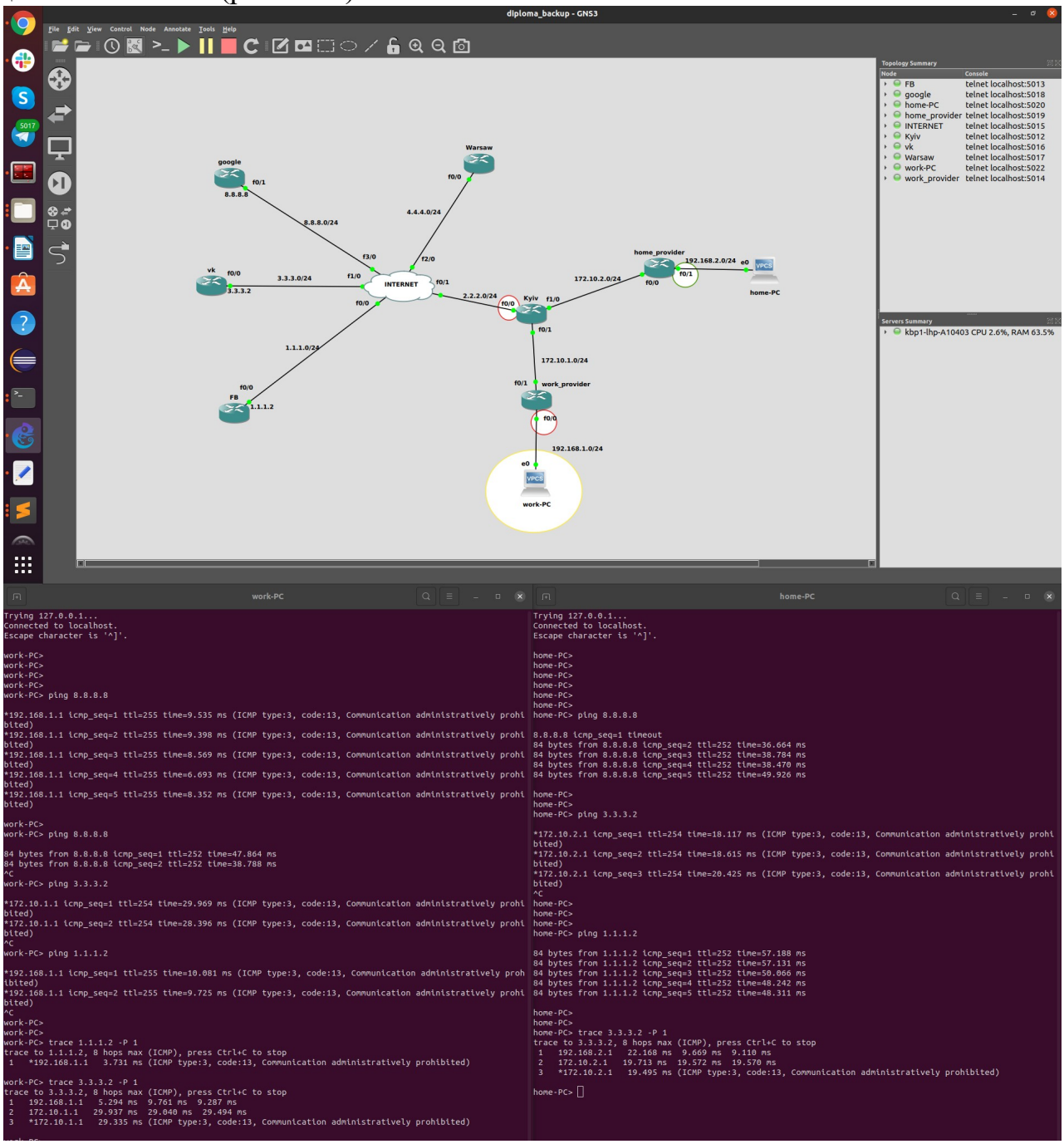

Рис. 3.16. Перевірка доступа до VK та FB на з домашнього PC та робочого PC

3.5. Перевірка методу

Перевірка доступу до соціальної мережі Facebook, Вконтакте, Google.com з Варшавського (рис. 3.17) Маршрутизатору — доступ вільний.

Перевірка доступу до соціальної мережі Facebook, Вконтакте

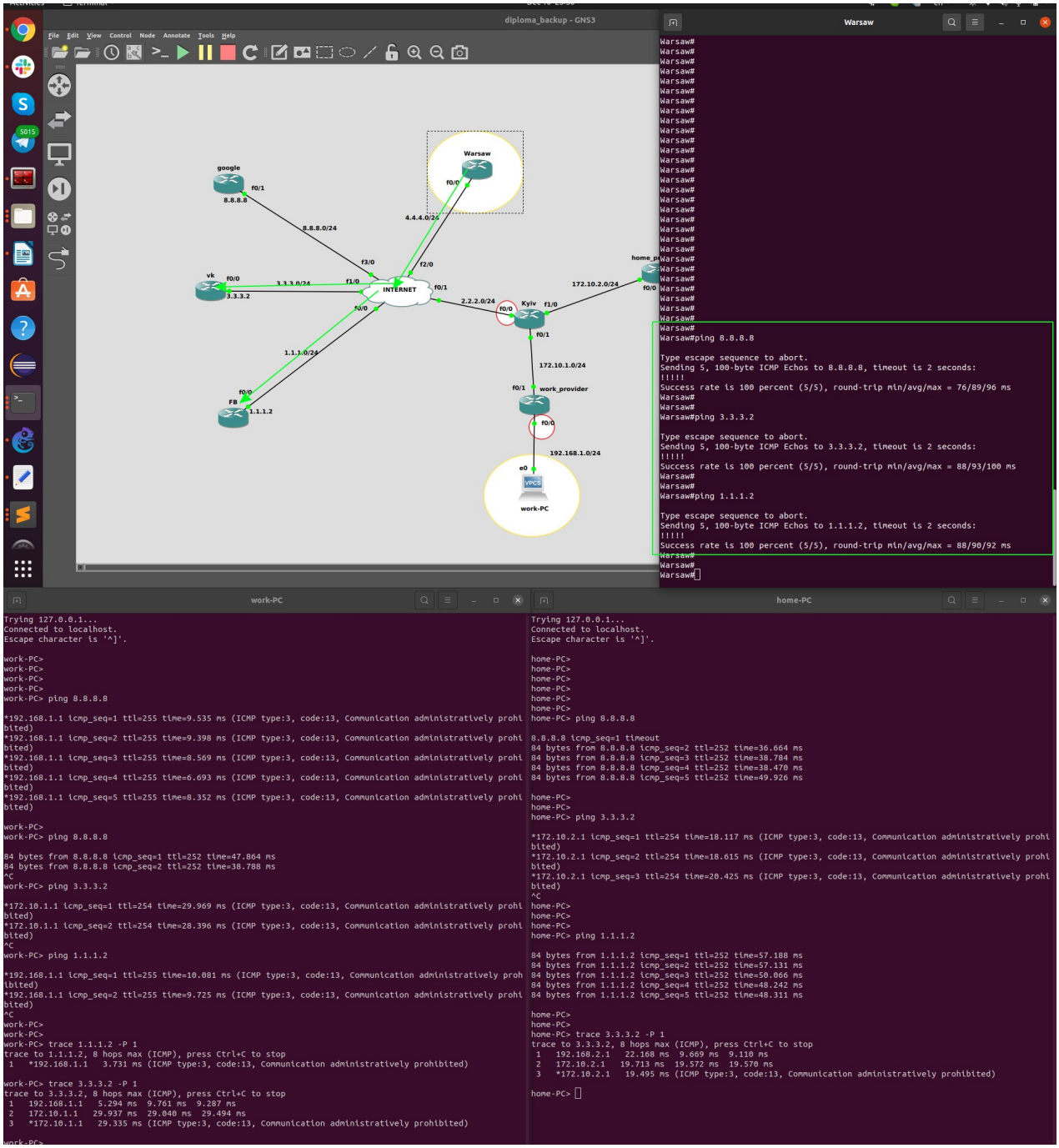

Рис. 3.17. Перевірка доступа до VK та FB на з домашнього PC та робочого PC

3.6. Висновки до розділу 3

Був розглянутий простий та ефективний метод, за допомогою CLI API Cisco, для блокування інформаційних ресурсів зі сторони Маршрутизатора Cisco.

Для огляду та верифікації було використано:

- GNS3
- Образ маршрутизатора Cisco C3745
- Стандартні інтернет утиліти ping, traceroute

На базі емулятора GNS3 було перевірено та використано блокування інформаційних доменів з різних рівнів ієрархії інтернет маршрутизації. Для верифікації блокування, використовувалися утиліти який використовують протокол ICMP (ping, traceroute). Також для контролю було використано окремий маршрутизатор, який не підпадає під каскад заборон на рівні досліджуваних маршрутизаторів.

Висновки:

З задачею заборони доступ до певних інформаційних доменів, можна зіштовхнутися на різних рівнях, на рівні держави (заборона доступу до ВКонтакті, «Mail.ru», Однокласники, «Яндекс», «Dr.Web», «Лабораторія Касперського» в 2017 році), заборона на рівні трудового контракту (заборона витрачання робочого часу на соц мережі, або використання обладнання до доступу до небажаних інтернет порталів: торенти, соціальні мережі, новостні ресурси).

Одним із ефективних рішень для обмеження доступу до небажаних інформаційних ресурсів в мережі Інтернет є використання програмно-апаратних рішень, які включають в себе налаштування активного комунікаційного обладнання, зокрема, маршрутизаторів. Налаштування маршрутизатора відбувається через інтерфейс командного рядка (CLI). Cisco IOS — це основний інтерфейс, який використовується для конфігурування, моніторингу та обслуговування пристроїв Cisco. Інтерфейс користувача дозволяє безпосередньо виконувати команди Cisco IOS за допомогою консолі маршрутизатора, терміналу або з використанням віддаленого доступу.

Дана робота була присвячена розробці методу, який залучає програмно-апаратне рішеня та містить у собі практичний підхід до впровадження за допомогою CLI API Cisco заборони доступу до інформаційних ресурсів на різних рівнях.

Дана робота була присвячена розробці методу, який містить у собі практичний підхід до впровадження за допомогою CLI API Cisco заборони доступу до інформаційних ресурсів на рівні IP маршрутизації. В третьому розділі даної роботи було описано принцип використання методу за допомогою програми GNS3.

В незалежності від рівня поставленої задачі (держава, компанія або домашній провайдер) даний метод покаже себе:

- Простим.
- Швидким.
- Дешевим (не треба в штаті тримати мережевого адміністратора, можно звернутися до провайдера з заявою на заборону доступу до певних інформаційних доменів)

Із явних мінусів:

- Потрібні базові навички та розуміння в API Cisco.
- Права доступу до консолі маршрутизатора.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека: освіта, наукаб техніка №1 (9), 2020 .

http://oaji.net/articles/2020/8096-1601616947.pdf (дата звернення 10.10.2021)

2. Безнерс-Лі Т. Заснування Павутини: з чого все починалося і до чого прийде Всесвітня Мережа / Т. Бернерс-Лі, М. Фічетті; Пер. з англ. А. Ішенка. – К.: Вид. Дім “Києво-Могилянська академія”, 2007. – 207 с. Сторінка 107.

3. Шмідт Е. Коен Дж. Новий цифровий світ / Пер. з англ. Ганна Ленів. – Л,: Літопис, 2015. – 368 с. Сторінка 91.

4. Декларація принципів Побудови інформаційного суспільства. http://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата звернення: 17.11.2021)

5. Чи є блокування інтернету "порушенням прав людини"? ООН вирішила, що так. – Електронний ресурс. – Режим доступу: http://ua.euronews.com/2016/07/05/un-denounces-disruption-of-internet-access-as-human-rights-violation (дата звернення: 17.11.2021)

6. Шмідт Е. Коен Дж. Новий цифровий світ / Пер. з англ. Ганна Ленів. – Л,: Літопис, 2015. – 368 с.

7. https://wiki.legalaid.gov.ua/index.php/Захист_прав_в_Інтернеті (дата звернення: 17.11.2021)

8. https://uk.wikipedia.org/wiki/Маршрутизатор (дата звернення: 17.11.2021)

9. https://jobs.ua/articles/chi-mayut-pravo-spvrobtniki-koristuvatis-sotsalnimi-merejami-na-robochomu-msts-13634 (дата звернення: 17.11.2021)

10. https://www.cisco.com/c/ru_ru/td/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book/cf_cli-basics.html (дата звернення: 24.11.2021)

11. https://www.gns3.com/ (дата звернення: 30.11.2021)

12. https://uk.wikipedia.org/wiki/ICMP (дата звернення 10.10.2021)

13. https://uk.wikipedia.org/wiki/Time_to_live (дата звернення 11.10.2021)

14. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 16 May2011:

http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (дата звернення 10.10.2021)

15. Pierluigi Paganini. The business of Censorship. Golden Shield Project, but not only

http://securityaffairs.co/wordpress/204/cyber-crime/business-of-censorship-golden-shield-project-but-not-only.html (дата звернення 10.10.2021)

16. www.uk.wikipedia.org/wiki/Блокування_російських_інтернет-сервісів_в_Україні (дата звернення 11.11.2021)