ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

В.С. Балацька
О.І. Полотай
Н.І. Федінець
А.М. Ткаченко

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Навчальний посібник

(Лабораторний практикум)

Львів – 2025

УДК 004.056:004.7

Рецензенти: Іван ОПІРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Національного університету “Львівська Політехніка”
Назарій БУРАК, кандидат технічних наук, доцент, начальник кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності

Балацька В.С., Полотай О.І., Федінець Н.І., Ткаченко А.М. *Захист інформації в комп’ютерних мережах: навчальний посібник (лабор. практикум)* / Львівський державний університет безпеки життєдіяльності. Львів : ЛДУБЖД, 2025. 226 с.

Метою навчального посібника є формування у здобувачів вищої освіти цілісного уявлення про принципи, методи та засоби захисту інформації в комп’ютерних мережах, ознайомлення з класичними й сучасними підходами до забезпечення мережевої безпеки, а також розвиток практичних навичок із виявлення, аналізу та нейтралізації мережевих загроз і кібератак у процесі експлуатації інформаційних систем.

Матеріал подано у доступній та логічно структурованій формі з використанням прикладів, схем і рисунків. Лабораторні роботи, наведені у посібнику, дають змогу закріпити теоретичні знання на практиці, оволодіти сучасними інструментами захисту інформації в комп’ютерних мережах, навчитися налаштовувати мережеві політики безпеки, засоби контролю доступу, міжмережеві екрани, системи виявлення та запобігання вторгненням, а також застосовувати криптографічні методи захисту інформації.

Посібник призначений для здобувачів вищої освіти за освітньою програмою F5 «Кібербезпека та захист інформації» і спрямований на формування аналітичного мислення, системного підходу до оцінювання рівня захищеності комп’ютерних мереж та набуття практичних компетентностей у сфері інформаційної та кібербезпеки.

Рекомендовано рішенням Вченої ради Львівського
державного університету безпеки життєдіяльності
(Протокол № 5 від 17.12.2025 р.)

© Балацька В.С., 2025
© Полотай О.І., 2025
© Федінець Н.І., 2025
© Ткаченко А.М., 2025
© ЛДУ БЖД, 2025

ЗМІСТ

ВСТУП 4

ЛАБОРАТОРНА РОБОТА № 1 6

ЛАБОРАТОРНА РОБОТА № 2 21

ЛАБОРАТОРНА РОБОТА № 3 30

ЛАБОРАТОРНА РОБОТА № 4 71

ЛАБОРАТОРНА РОБОТА № 5 82

ЛАБОРАТОРНА РОБОТА № 6 119

ЛАБОРАТОРНА РОБОТА № 7 142

ЛАБОРАТОРНА РОБОТА № 8 170

ЛАБОРАТОРНА РОБОТА № 9 189

ЛАБОРАТОРНА РОБОТА № 10 199

СПИСОК ЛІТЕРАТУРИ 222

ВСТУП

Курс «Захист інформації в комп'ютерних мережах» є обов'язковим компонентом освітньої програми «Кібербезпека та захист інформації». Структуру та зміст курсу побудовано на основі використання моделей, методів та механізмів захисту інформації в комп'ютерних мережах.

Курс опирається на такі освітні компоненти: вища математика, технології програмування, WEB-програмування, інформатика.

Здобувачі освіти повинні опанувати застосування інформаційних технологій для захисту комп'ютерних мереж. Також є формування теоретичних знань та практичних навичок із побудови, керування, модернізації, моніторингу та аналізу продуктивності, діагностики та розв'язання проблем сучасних комп'ютерних мереж. Програму орієнтовано на формування професійних компетентностей у здобувачів вищої освіти щодо ефективного розв'язання різноманітних завдань майбутньої професійної діяльності в умовах інформаційного суспільства.

Процес вивчення дисципліни спрямований на формування елементів таких **компетентностей**:

загальних (ЗК):

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК4. Вміння виявляти, ставити на вирішувати проблеми за професійним спрямуванням.

ЗК9. Навики здійснення безпечної діяльності.

спеціальних/фахових (СК/ФК):

ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК4. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів).

ФК11. Здатність виконувати моніторинг процесів функціонування інформаційно-технологічних, інформаційно-телекомунікаційних (автоматизованих) систем згідно з встановленою політикою інформаційної та кібербезпеки.

Серед видів робіт здобувачів – лабораторні роботи. Лабораторні роботи з курсу «Захист інформації в комп'ютерних мережах» спрямовані на формування практичних навичок забезпечення безпеки даних і мережевої інфраструктури. Під час здобувачі вивчають основні загрози та вразливості комп'ютерних мереж, працюють із засобами сканування та аналізу безпеки. Вони знайомляться з криптографічними методами захисту інформації, реалізують шифрування та електронний цифровий підпис, а також налаштовують захищені канали зв'язку через VPN і SSL/TLS. Окрему увагу приділено автентифікації користувачів, управлінню доступом і політикам безпеки. Здобувачі вчаться налаштовувати міжмережеві екрани, системи виявлення та запобігання вторгненням, забезпечувати безпечну передачу електронної пошти за допомогою протоколів шифрування та цифрових підписів. Завершальні роботи присвячені моніторингу мережевого трафіка, аналізу журналів безпеки та реагуванню на інциденти. У результаті виконання лабораторних робіт здобувачі набувають практичного досвіду використання сучасних засобів і технологій для захисту інформації в комп'ютерних мережах.

ЛАБОРАТОРНА РОБОТА № 1

Тема: дослідження основних загроз інформаційної безпеки комп'ютерних мереж та засобів захисту від них.

Мета: формування у здобувачів вищої освіти знань про основні загрози інформаційній безпеці комп'ютерних мереж, типи комп'ютерних вірусів та шкідливого ПЗ, а також набуття практичних навичок добору та аналізу засобів захисту.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *Інформаційна безпека комп'ютерних мереж* – стан захищеності інформації та інфраструктури мережі від випадкових або навмисних впливів, що можуть порушити конфіденційність, цілісність або доступність даних.

Загроза інформаційній безпеці – потенційна подія або дія, яка може спричинити порушення нормального функціонування мережі та/або завдати шкоди інформаційним ресурсам.

Неавторизований доступ – отримання доступу до ресурсів мережі без належних прав або з порушенням установлених правил автентифікації та авторизації.

DoS/DDoS-атака – навмисне перевантаження мережевих ресурсів з метою порушення або повної зупинки їх функціонування.

Перехоплення даних (sniffing) – несанкціоноване прослуховування та аналіз трафіка, що передається мережею.

Комп'ютерний вірус – шкідлива програма, що здатна до саморозповсюдження та виконання деструктивних або небажаних дій без відома користувача.

Мережевий черв'як – різновид шкідливого ПЗ, що розповсюджується мережевими каналами без участі користувача.

Троянська програма – шкідливе ПЗ, яке маскується під корисне та виконує приховані небажані дії.

Антивірусне програмне забезпечення – сукупність програмних засобів для виявлення, блокування та видалення шкідливого ПЗ.

Мережевий екран (фаєрвол) – програмний або апаратний засіб, що контролює та фільтрає мережевий трафік відповідно до заданих правил безпеки.

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до мережі Інтернет; операційна система: Windows / Linux (за наявності – декілька ОС для порівняння); веббраузер для роботи з електронним курсом та пошуку інформації; текстовий редактор (MS Word / Google Docs або аналог); (за наявності) антивірусне ПЗ та/або демоверсії засобів захисту; доступ до електронного навчального курсу у віртуальному університеті та матеріалів мережевої академії Cisco.

План:

1. **Організаційні заходи**

- Повідомлення теми та мети лабораторного заняття.
- Мотивація навчальної діяльності: значення захисту комп'ютерних мереж в умовах зростання числа кіберзагроз.
- Ознайомлення з місцем розташування матеріалів лабораторної роботи в електронному навчальному середовищі «Віртуальний університет».
- Інструктаж з техніки безпеки під час роботи з комп'ютерною технікою та програмним забезпеченням.
- Пояснення порядку оформлення, подання та захисту звіту, критеріїв оцінювання.

2. **Контроль опорного рівня знань**

Вимоги до теоретичної готовності здобувачів: розуміння базових понять інформаційної безпеки; знання загальної структури комп'ютерних мереж; загальні уявлення про шкідливе програмне забезпечення, його призначення та наслідки впливу.

Перелік дидактичних одиниць для перевірки: класифікація загроз інформаційній безпеці мереж; поняття комп'ютерного вірусу та шкідливого ПЗ; основні підходи до захисту інформації в мережах; базові принципи роботи антивірусних засобів і фаєрволів.

Питання для усного опитування / самоконтролю:

1. Що таке загроза інформаційної безпеки комп’ютерної мережі?

2. Які основні групи загроз для мережевої інфраструктури можна виділити?

3. Чим відрізняється вірус, черв’як і троянська програма?

4. Які основні принципи побудови захисту комп’ютерних мереж?

5. Які функції виконують антивірусні програми та мережеві екрани?

3. Формування професійних вмінь та навичок

3.1. Теоретичні відомості

1. Основні види загроз інформаційної безпеки мереж, методи їх запобігання та вирішення:

1. Неавторизований доступ – можливість зловмисників отримати доступ до мережі чи її ресурсів без дозволу.

Рішення: Встановлення системи автентифікації, двофакторної автентифікації (2FA), використання VPN.

2. Атаки типу "відмова в обслуговуванні" (DoS/DDoS) – блокування або перевантаження мережевих ресурсів.

Рішення: Використання фаєрволів, систем запобігання DDoS атак, підвищення пропускної здатності каналів зв'язку.

3. Перехоплення даних (снифінг) – спостереження та захоплення інформації, що передається через мережу.

Рішення: Використання шифрування (SSL/TLS), VPN, заборона на використання незашифрованих протоколів (HTTP, FTP).

4. Вірусні атаки та шкідливе ПЗ – програмне забезпечення, яке шкодить або краде дані з комп'ютерних систем.

Рішення: Використання антивірусних програм, регулярне оновлення програмного забезпечення, фільтрація пошти.

5. Атаки типу "чоловік посередині" (MITM) – втручання між двома комунікуючими сторонами для маніпуляції інформацією.

Рішення: Використання криптографії (шифрування даних), автентифікація серверів, використання цифрових підписів.

6. Загроза витоку даних – ненавмисний або умисний вихід конфіденційної

інформації за межі організації.

Рішення: Використання систем управління доступом, моніторинг користувацької активності, шифрування даних.

7. Інсайдерські загрози – шкідливі або недбалі дії співробітників, що можуть призвести до компрометації інформації.

Рішення: Впровадження політики мінімальних прав доступу, аудит доступів, навчання співробітників.

8. Використання слабких паролів – паролі, які легко вгадати або зламати.

Рішення: Встановлення вимог до складності паролів, використання менеджерів паролів, впровадження багатофакторної автентифікації.

9. Фішинг – шахрайські спроби отримати конфіденційну інформацію за допомогою підроблених вебсайтів або листів.

Рішення: Навчання користувачів, використання фільтрів пошти, перевірка адреси вебсайтів.

10. Загроза маніпуляцій з даними – зміна або спотворення даних в процесі їх передачі.

Рішення: Використання механізмів контролю цілісності даних (наприклад, хеш-функцій, цифрових підписів).

11. Загроза несанкціонованого видалення даних – втрата важливої інформації через несанкціоновані дії.

Рішення: Регулярне резервне копіювання даних, використання систем збереження даних.

12. Вразливості програмного забезпечення – недоліки у коді, які можуть бути використані для атак.

Рішення: Оновлення програмного забезпечення, тестування на вразливості, патчинг.

13. Шкідливе програмне забезпечення, яке використовує вразливості пристроїв – атаки на фізичні пристрої, як-от USB-флешки.

Рішення: Використання антивірусних програм, обмеження доступу до USB-портів, перевірка підключених пристроїв.

14. Проблеми із сумісністю систем безпеки – різні системи безпеки не

можуть взаємодіяти належним чином.

Рішення: Впровадження стандартів безпеки, централізоване управління безпекою.

15. Неналежне використання ресурсів – неефективне використання мережевих ресурсів або зловживання ними.

Рішення: Моніторинг трафіка, обмеження доступу до певних ресурсів, впровадження політик щодо використання ресурсів.

2. Комп'ютерні віруси, їх властивості і класифікація

2.1. Властивості комп'ютерних вірусів

Зараз застосовуються персональні комп'ютери, в яких користувач має вільний доступ до всіх ресурсів машини. Саме це відкрило можливість для небезпеки, яка отримала назву комп'ютерного вірусу.

Що таке комп'ютерний вірус? Формальне визначення цього поняття до цих пір не придумане, і є серйозні сумніви, що його взагалі може бути дано. Численні спроби дати «сучасне» визначення вірусу не привели до успіху. Тому ми обмежимося розглядом деяких властивостей комп'ютерних вірусів, які дозволяють говорити про них як про деякий певний клас програм.

Перш за все, вірус – це програма. Таке просте твердження саме по собі здатне розвіяти безліч легенд про незвичайні можливості комп'ютерних вірусів. Вірус може перевернути зображення на вашому моніторі, але не може перевернути сам монітор. До легенд про віруси-вбивці, «що знищують операторів за допомогою виведення на екран смертельної колірної гами 25-м кадром» також не варто відноситися серйозно. На жаль, деякі авторитетні видання час від часу публікують «найсвіжіші новини з комп'ютерних фронтів», які при найближчому розгляді виявляються наслідком не цілком ясного розуміння предмету.

Вірус – програма, що здатна до самовідтворення. Така здатність є єдиним засобом, властивим всім типам вірусів. Але не тільки віруси здатні до самовідтворення. Будь-яка операційна система і ще безліч програм можуть створювати власні копії. Копії ж вірусу не тільки не зобов'язані повністю збігатися з оригіналом, але можуть взагалі з ним не збігатися!

Вірус не може існувати в «цілковитій ізоляції»: сьогодні не можна уявити собі вірус, який не використовує код інших програм, інформацію про файлову структуру або навіть просто імена інших програм. Причина зрозуміла: вірус повинен будь-яким способом забезпечити передачу собі управління.

2.2. Класифікація вірусів

На сьогодні відомі десятки тисяч вірусів, які в цілому мають конкретну класифікацію. Спробуємо детальніше розглянути основні групи, на які поділяються комп'ютерні віруси.

I. Поділ вірусів за середовищем їх розповсюдження:

— Завантажувальні віруси – це найбільш небезпечна група вірусів, що заражають Boot Record та Master Boot Record логічних та фізичних дисків. Про ці віруси ми вже говорили попередньо.

— Файлові віруси. Ці віруси поширюються, заражаючи файли різних типів, як вже було сказано, – найчастіше це виконуючі файли та файли оверлеїв. До цієї групи слід також віднести макровіруси, хоч інколи їх виділяють як окремий клас вірусів.

— Завантажувально-файлові віруси здатні вразити як код завантажувальних секторів, так і код файлів, як правило системних.

— Віруси сімейства Dir використовують інформацію про файлову структуру та вміст каталогів (див. попередній матеріал).

— Multipartition – віруси можуть вражати одночасно виконуючі файли, boot – сектор, MBR, FAT і каталоги і є найбільш небезпечними, особливо, якщо вони ще й володіють поліаморфними властивостями і елементами невидимості.

— Мережеві віруси – це віруси, що поширюються як сукупність машинного коду в комп'ютерних мережах.

— Поштові віруси – на сьогодні досить нова але надзвичайно поширена група вірусів, що розповсюджуються разом із поштовими повідомленнями у вигляді прикріплених до них файлів (Attachment) із програмним кодом. Як правило, такі віруси досить швидко розмножуються і час від часу викликають вірусні епідемії (згадати хоча б такі резонансні в останні роки віруси, як "I Love You" (LoveLetter), Melissa або "Anna Kournicova").

II. Класифікація комп'ютерних вірусів за алгоритмом роботи:

— Віруси "паразити" найпростіші віруси що використовують "тіло" інших файлів (виконуючих), записуючи туди себе. Вони можуть бути досить легко виявлені і знешкоджені.

— Віруси супутники створюють копію exe-файлу з розширенням com і записують туди себе. Коли з командного рядка DOS завантажують такий файл, то як правило розширення не вказують, а за правилами DOS, першим завантажується com файл, тобто вірус.

— Віруси "черв'яки" (віруси-реплікатори) не створюють собі файлу, а поширюються лише в комп'ютерних мережах та в оперативній пам'яті у вигляді певного машинного коду. Вони ніби черв'яки проникають в оперативну пам'ять ПК через комп'ютерну мережу, пронизуючи системи захисту. Найбільшгрізними представниками цього типу вірусів є Nimda (неодноразовий переможець рейтингів найнебезпечніших вірусів), Gigger та Redesi (здатні відформатувати диск C), Bumerang (здатний знищити FlashBIOS та таблиці файлової системи вінчестера), SirCam (найдзвичано швидкий у розповсюдженні та знищує інформацію на диска C), Кігау та Paukor (знищують всі файли із системних папок Windows).

— Студентські віруси – це віруси, які мають в собі багато помилок і написані, зазвичай, початківцями.

— Віруси "невидимки" (Stealth – віруси) фальсифікують інформацію, перехоплюючи звертання антивірусної програми, до заражених ділянок диска і спрямовуючи її на незаражені. Вірус перехоплює вектор переривання int 13h. Ця технологія використовується як у файлових, так і в завантажувальних вірусах.

— Віруси "мутанти" ("привиди") або поліаморфні (polimorphic) – не мають постійної сигнатури (машинного коду), за якою можна було б виявити вірус. Вони знінюють сигнатуру з кожною копією і тому з ними важко боротись. Виявляють такі віруси лише за допомогою еврістичного аналізу, коли антивірусна програма "прокручує" алгоритм роботи виконуючих файлів і в разі підозрілих операцій приймає це за вірус. Таким же чином антивірусні програми шукають невідомі ще їм віруси.

— Ретровіруси – це звичайні файлові віруси, які прагнуть заразити антивірусні програми, знищуючи їх або роблячи непрацездатними. Тому практично всі антивіруси в першу чергу перевіряють свої власні розміри і контрольну суму.

— "Троянські" віруси (Trojans) здійснюють шкідливі дії замість оголошених легальних функцій або разом з ними. Вони переважно не здатні на саморозповсюдження і передаються тільки при копіюванні користувачем. Часто ці віруси використовують в якості "шпигунів". Проникаючи по мережі на ПК, вони стараються "затаїтись" і "вкрасти" паролі користувача (особливо виходу в Internet) і передати їх господарю. Деякі троянські віруси готують ґрунт на зараженому ними ПК для проникнення без перешкод інших вірусів, що слідують за ними. Боротись з такими вірусами (особливо новими) досить важко, адже в їхньому коді немає ніякої диструктивної дії (не міняється розмір інших файлів, не форматуються диски), а навпаки вони стараються ніяк себе не проявити. Для боротьби з такими вірусами використовуються спеціальні програми FireWoll (файрволл) – мережеві екрани, які під час підключення до мережі слідкують чи не пробує якась програма на ПК вийти в Internet. Якщо така спроба відбулась, то вона блокується і виводиться повідомлення із запитом дозволу на таку операцію. Корисною функцією файрволл є те, що він може захистити не лише від троянських вірусів, але й від хакерських атак із зовні (з Internet). Потрібно відмітити, що існує багато відомих троянських вірусів, які не лише виступають в ролі "шпигунів" але й самі несуть досить високу деструктивну дію (наприклад TROJ_ZERAF знищує EXE і SYS файли та робить помилки в системному реєстрі).

— Віруси таймери очікують лише певної нагоди (години, дня і т.д.), і лише тоді спрацьовують.

III. Поділ вірусів за деструктивною дією:

— Нешкідливі віруси – це віруси, які не приносять жодної шкоди, а просто себе копіюють багато разів, заповнюючи диски або загромаджуючи оперативну пам'ять.

— Не небезпечні віруси схожі на попередні, але крім цього їх дія

супроводжується різними спецефектами (відео- та звуковими).

— Небезпечні віруси – це віруси дія яких призводить до серйозних збоїв в роботі ПК, таких як зависання комп'ютера і т.д.

— Дуже небезпечні віруси – це віруси, дія яких супроводжується знищенням інформації (файлів, каталогів, форматування цілих дисків). В січні 1998 року, завдяки журналу "Virus Bulletin", з'явився термін WildList (список "диких вірусів"). Він регулярно поновлюється і публікується цим авторитетним міжнародним виданням.

IV. Класифікація вірусів за принципом дії:

— Резидентні – це віруси, що завантажуються в оперативну пам'ять і постійно там знаходяться, аж до виключення живлення чи перезавантаження ПК.

— Нерезидентні – це віруси, які короткочасно завантажуються в пам'ять, виконують потрібні їм дії і вивантажуються з пам'яті.

V. Поділ вірусів за місцем втілення у файли:

— На початку файлу.

— Всередині файлу.

— В кінці файлу.

2.3. Види файлів, які можуть бути заражені вірусом

Як правило, кожна конкретна різновидність вірусу може заразити тільки один або два типи файлів. На даний час частіше всього зустрічаються макровіруси, тоді як в 90-ті роки найпоширенішими були віруси, що заражали COM-файли, а на другому місці – EXE-файли.

Види файлів, які можуть бути заражені вірусом:

— виконуючі файли, тобто файли з розширеним ім'ям COM і EXE, а також оверлейні файли, завантажені іншими програмами. Вірус в заражених виконуючих файлах починає свою роботу при завантаженні тієї програми, в якій він знаходиться;

— файли документів та шаблонів, створених програмами Word, Excel, Access та іншими офісними програмами, а точніше макроси, що використовуються там. Цей тип вірусів порівняно молодий і називають його

макровірусами. Деякі з вірусів цього типу є надзвичайно шкідливими. Наприклад вірус W97M.Thus при активізації 13 грудня здатний знищити всі файли на диска С, зберігаючи при цьому структуру каталогів (папок).

— блок початкового завантаження операційної системи і головний завантажувальний запис жорсткого диска. Вірус, який заразив ці ділянки, як правило, складається з 2-х частин, оскільки на цих ділянках диска, важко розмістити програму вірусу в цілому. Частина вірусу, що не поміщається в них, розташована на іншій ділянці диска, який оголошується дефектним. Такий вірус починає свою роботу при початковому завантажуванні операційної системи і є резидентним, тобто постійно знаходиться в пам'яті комп'ютера. Відомі випадки, коли вірус форматує додаткову доріжку диска, куди і записує основну частину програми;

— таблиці файлової системи та каталоги. Як відомо, в кожен каталог записуються імена файлів, дата та час створення, номер першого кластера файлу, а також резервні байти, що ОС не використовуються. Віруси цього типу, записавшись в кластери, помічають їх як пошкоджені, а тоді реорганізовують файлову систему. При цьому інформація про перші кластери деяких виконуючих файлів записується у резервні біти, а на її місце поміщається посилання на тіло віруса. Тому, при спробі користувача завантажити відповідну програму – вірус отримує керівництво. Цей тип вірусів, з'явившись в 1991 році, викликав в росії справжню епідемію, яку можна порівняти із чумою.

— драйвери пристроїв, тобто файли, які здійснюють програмне керування зовнішнім пристроєм. Вірус, який знаходиться в цих файлах, починає свою роботу при кожному звертанні до відповідного пристрою;

— системні файли, тобто файли IO.SYS і MSDOS.SYS. Це досить небезпечно, оскільки вони, як і у випадку зараження блоків початкового завантаження дисків, починають діяти при кожному завантаженні ПК.

2.4. Шляхи проникнення вірусів в комп'ютер

Розглянемо, тепер, яким чином комп'ютерний вірус може потрапити на ПК звичайного користувача. На початку їх існування основним середовищем розповсюдження вірусів були переносні диски, переважно дискети. Пізніше, із

набуттям популярності CD-дисків, вони також стали зручним середовищем поширення вірусів (перш за все – це неліцензійні програмні продукти). В другій половині 2001 року комп'ютерні віруси проникли і на DVD (вірус Funvole).

В другій половині 90-х років основним середовищем розповсюдження комп'ютерних вірусів стали комп'ютерні мережі та електронна пошта. Це викликано надзвичайно бурхливим розвитком Internet, що дозволило фактично миттєво поширюватись новим вірусам на дуже великі території.

Прикладом може бути 2001 рік, визнаний відомими міжнародними антивірусними виданнями роком троянських вірусів та поштових черв'яків, а лідером серед вірусів став поштовий черв'як Nimda.

Варто пам'ятати про те, що розробники комп'ютерних вірусів не зупиняються на досягнутому і шукатимуть нові шляхи розповсюдження комп'ютерних вірусів. Так, наприклад, відомі вже випадки поширення вірусів через файли в форматі RTF, PDF та анімаційні файли, створені в Macromedia Flash (перший відомий вірус SWF/LFM-926).

2.5. Захист від комп’ютерних вірусів

Класифікація антивірусних програм:

Комп'ютерний вірус – це дуже неприємне шкідливе явище, побачити яке на своєму ПК не хотів би, напевне, жоден користувач. Застрахуватись від вірусів на сьогодні повністю неможливо, хіба що зовсім ізолювати ПК від обміну інформацією із навколишнім світом. Але робити це, звичайно, ніхто не буде, адже тоді ПК втратить багато своїх переваг.

Необхідно застосовувати спеціалізовані програми для захисту від вірусів. Ці програми можна поділити на кілька видів.

— детектори – дозволяють знайти файли, заражені яким-небудь одним, наперед відомим нам вірусом, або одним з багатьох відомих вірусів;

— вакцини (імунізатори) – модифікують (інфікують) програми і диски таким чином, що це не відображається на роботі програм. Після цього вірус, від якого виконується вакцинація, вважає ці програми або диски вже інфікованими і повторно їх не заражає;

— лікарі (фаги) – лікують заражені програми або диски "викусуючи" із

заражених програм тіло віруса, тобто відновлюючи програму в тому стані, в якому вона була до зараження вірусом;

— ревізори – спочатку запам'ятовують стан інформації (розмір, дату і час створення) і системних ділянок дисків, а потім порівнюють його з поточним. При виявленні невідповідностей про це повідомляється користувачу;

— лікарі-ревізори – це гібриди ревізорів і лікарів, тобто програми, які не тільки помічають зміни в файлах і системних ділянках дисків, але й можуть у випадку виявлення змін вилікувати заражені файли;

— фільтри (монітори) – резидентні програми для захисту від вірусів, які поміщаються резидентно в оперативній пам'яті комп'ютера і перехоплюють звернення вірусів до системних ділянок і файлів. Користувач може дозволити або заборонити виконання відповідних операцій;

— поліфаги – це найефективніша група програм, що поєднують в собі декілька вище приведених типів антивірусів, наприклад, фільтрів, детекторів та лікарів.

2.6. Огляд антивірусних засобів

Темі боротьби з комп’ютерними вірусами в світі приділяється значна увага. Багато великих та малих компаній займаються розробкою нових та ефективних програм для захисту ПК від вірусів. Найбільш впливовим і авторитетним показником ефективності антивірусних програм є рейтинг, який щомісяця проводить міжнародний комп'ютерний журнал Virus Bulettin (Англія). Проводяться тестування, при яких антивіруси встановлюються в однакових умовах на заражені різними типами вірусів комп'ютери і визначається відсоток виявлених та знешкоджених ними вірусів. Тестування проводиться по таких основних категоріях, як wild ("дикі"), макровіруси, поліморфні та стандартні. При тестуванні враховуються також такі параметри як швидкість роботи програми, її вартість та зручність інтерфейсу. Сама участь антивірусної програми в тестуванні вже є великим визнанням для неї.

3.2. Зміст лабораторної роботи

1. Ознайомитися з основними загрозами інформаційної безпеки в комп’ютерних мережах та їх класифікацією.

2. Вивчити основні методи та засоби захисту від загроз інформаційної безпеки в мережах.

3. Ознайомитися з основними типами комп'ютерних вірусів і шкідливого ПЗ, принципами їх роботи, поширення та впливу на системи.

4. Проаналізувати сучасні програмні засоби захисту від вірусів (антивірусне ПЗ, мережеві екрани тощо): принцип роботи, ефективність, функціональні можливості.

3.3. Рекомендації щодо виконання (хід роботи)

1. Опрацювати теоретичні відомості з курсу, конспекту та матеріалів у «Віртуальному університеті» (розділ про загрози мережевої безпеки та комп'ютерні віруси).

2. Обрати одну з основних загроз інформаційної безпеки в комп'ютерних мережах (згідно з варіантом або за погодженням з викладачем) та:

— детально описати сутність обраної загрози;

— навести приклади її реалізації;

— охарактеризувати можливі наслідки для мережі;

— запропонувати комплекс заходів із запобігання та реагування.

3. Обрати один із типів комп'ютерних вірусів / шкідливого ПЗ (наприклад, файловий вірус, мережевий черв'як, троянська програма, макровірус тощо) та:

— описати принцип роботи обраного типу;

— навести конкретні приклади (назви відомих представників);

— визначити характерні шляхи поширення;

— проаналізувати типові методи їх виявлення та видалення, вказавши назви програмних засобів, які їх підтримують.

4. Проаналізувати один або декілька антивірусних продуктів / засобів захисту**,** доступних у лабораторії або за відкритими джерелами:

— коротко описати функціональні можливості;

— визначити підтримувані методи виявлення;

— охарактеризувати переваги та обмеження (за відгуками, тестами,

документацією).

5. Оформити звіт відповідно до вимог (див. нижче) та подати його у встановленому викладачем форматі (друкований/електронний варіант).

6. Підготуватися до усного захисту роботи: відповіді на контрольні питання та обговорення зроблених висновків.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (структурований конспект з основних загроз, класифікації вірусів та засобів захисту – 1–2 сторінки).
4. Практичну частину, що включає:

— опис обраної загрози та запропонованих заходів захисту;

— опис обраного типу вірусів (властивості, приклади, шляхи розповсюдження, методи протидії);

— аналіз одного або декількох антивірусних/захисних продуктів.

5. Висновки, у яких відображаються:

— узагальнення щодо основних загроз та засобів захисту;

— отримані практичні навички;

— рекомендації щодо підвищення рівня безпеки комп’ютерних мереж.

6. Список використаних джерел згідно з вимогами до оформлення бібліографічних посилань.

4. Підбиття підсумків заняття

— обговорення виявлених загроз та запропонованих шляхів їх нейтралізації;

— аналіз правильності класифікації та опису обраних типів вірусів;

— оцінювання повноти та якості звітів, уміння аргументувати вибір засобів захисту;

— формулювання узагальнених висновків щодо значення комплексного підходу до забезпечення інформаційної безпеки комп’ютерних мереж.

5. Список рекомендованої літератури

Основна:

1. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. К., 2013. 435 с.

2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ, 2013. 476 с.

4. Полотай О., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи**.** Зб. тез III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.

Додаткова:

1. Кавун С. В., Смірнов О. А., Столбов В. Ф. Основи інформаційної безпеки. Кіровоград : Вид. КНТУ, 2012. 414 с.

2. Гарасимчук О. І., Дудикевич В. Б., Ромака В. А. Комплексні системи санкціонованого доступу : навч. посіб. Л. : Вид-во Львів. політехніки, 2010. 212 с.

Інформаційні ресурси:

1. Віртуальний університет ЛДУБЖД : електронне навчальне середовище. URL: https://virt.ldubgd.edu.ua

2. Офіційний сайт мережевої академії Cisco: http://www.netacad.com

ЛАБОРАТОРНА РОБОТА № 2

Тема: налаштування контролю доступу до мережевих служб на основі механізмів автентифікації та авторизації.

Мета: формування у здобувачів вищої освіти знань про механізми AAA (Authentication, Authorization, Accounting) та їх застосування для захисту мережевих служб, а також набуття практичних навичок налаштування контролю доступу до бездротових мереж, служб електронної пошти та FTP.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *Автентифікація* – процес перевірки належності користувача до заявленої ідентичності (логін/пароль, токен, сертифікат тощо).

Авторизація – процес надання або обмеження прав доступу до ресурсів після успішної автентифікації.

AAA (Authentication, Authorization, Accounting) – концепція централізованого управління автентифікацією, авторизацією та обліком дій користувачів у мережі.

RADIUS-сервер – мережевий сервер, що реалізує функції AAA та взаємодіє з мережевими пристроями (маршрутизаторами, комутаторами, точками доступу) для перевірки облікових даних та прав доступу.

Контроль доступу – сукупність механізмів, що регулюють, хто і до яких ресурсів має право доступу у мережі.

Служба електронної пошти – сервіс обміну електронними повідомленнями, що базується на протоколах SMTP (відправлення) і POP3/IMAP (отримання).

FTP (File Transfer Protocol) – протокол передавання файлів між клієнтом і сервером із використанням облікових записів та прав доступу.

Привілеї доступу (R, W, D, N, L) – набір дозволів для користувача FTP: Read (читання), Write (запис), Delete (видалення), Rename (перейменування), List (перегляд вмісту каталогу).

Обладнання та програмне забезпечення: персональні комп’ютери / ноутбуки з доступом до мережі; операційна система: Windows / Linux (на розсуд викладача); симулятор мережі Cisco Packet Tracer; веббраузер для роботи з електронним курсом та мережевими сервісами; текстовий редактор (MS Word /

Google Docs або аналог); електронний навчальний курс у віртуальному університеті; мережеві сервіси в Packet Tracer: AAA-сервер, поштовий сервер (SMTP/POP3), FTP-сервер.

План:

1. **Організаційні заходи**

— Повідомлення теми та мети лабораторного заняття.

— Мотивація навчальної діяльності: значення контролю доступу до мережевих служб для зменшення кількості мережевих атак.

— Ознайомлення з місцем розташування матеріалів лабораторної роботи в електронному навчальному середовищі «Віртуальний університет».

— Інструктаж з техніки безпеки під час роботи з комп'ютерною технікою та програмним забезпеченням.

— Пояснення порядку оформлення, подання та захисту звіту, критеріїв оцінювання.

2. **Контроль опорного рівня знань**

Вимоги до теоретичної готовності здобувачів: знання базових понять мережевої безпеки; уявлення про клієнт-серверну модель та мережеві служби (e-mail, FTP, Wi-Fi); розуміння ролі облікових записів користувачів і паролів.

Перелік дидактичних одиниць для перевірки: поняття автентифікації, авторизації, обліку (AAA); призначення RADIUS-сервера; основи роботи SMTP/POP3 та FTP; базові принципи захисту бездротових мереж.

Питання для усного опитування / самоконтролю:

1. У чому відмінність між автентифікацією та авторизацією?
2. Що таке AAA і які функції вона виконує?
3. Які ризики пов'язані з використанням служб електронної пошти та FTP?
4. Які способи захисту бездротових мереж ви знаєте?
5. Для чого потрібні облікові записи користувачів на серверах AAA, Mail, FTP?

3. Формування професійних вмінь та навичок

3.1. Теоретичні відомості

(Коротко, 1–1,5 сторінки – опис AAA, RADIUS, контролю доступу до Wi-Fi, e-mail, FTP; можна взяти з попереднього варіанта або з конспекту – тут у методичці ти вставиш свій текст, як у ЛР №1.)

3.2. Зміст лабораторної роботи

1. Частина 1: налаштування та використання облікових даних автентифікації AAA для доступу до бездротової мережі.

2. Частина 2: налаштування та використання служб електронної пошти (SMTP/POP3) для обміну повідомленнями між користувачами.

3. Частина 3: налаштування та використання служб FTP, створення облікових записів з різними правами доступу та перевірка їх дії.

У процесі виконання роботи здобувачі освіти повинні:

— налаштувати AAA-сервер і облікові записи користувачів;

— забезпечити автентифікацію користувачів при підключенні до бездротової мережі;

— налаштувати поштовий сервер та клієнтів електронної пошти;

— виконати обмін повідомленнями між користувачами;

— налаштувати FTP-сервер, створити облікові записи з різними привілеями;

— перевірити можливості читання, запису, видалення та перейменування файлів для різних користувачів.

3.3. Рекомендації до виконання (хід роботи)

Довідкова інформація / сценарій

Автентифікація та авторизація – це окремі процеси безпеки у сфері керування ідентифікацією та доступом (Identity and Access Management – IAM). Автентифікація використовує паролі та інші методи ідентифікації, аби пересвідчитися, що користувач є тим, за кого себе видає. Натомість авторизація визначає дозволи на користування ресурсами для тих, хто має доступ. У цьому завданні у Packet Tracer (PT) ви налаштуєте автентифікацію та авторизацію для користування мережевими службами, зокрема, бездротовим зв’язком, електронною поштою та послугами FTP.

Примітка: ця лабораторна робота відкривається у Фізичному режимі. Проте, її можна виконувати також у Логічному режимі. Більшість завдань у цій вправі буде оцінено. За необхідності можна скористатися функцією **Check Results** для перевірки правильності налаштувань.

Частина 1. Налаштування та використання облікових даних автентифікації AAA

Крок 1. Налаштування облікових записів користувачів на сервері AAA

1. Перейдіть у приміщення Headquarters (HQ), а потім до комутаційної шафи, клацнувши на Wiring Closet (висока чорна серверна стійка в нижньому лівому куті).

2. На стійці Rack справа клацніть на сервері AAA-RADIUS. Відкрийте вкладку Services, у розділі SERVICES оберіть AAA.

3. Увімкніть службу AAA (перемикач On).

4. У розділі User Setup додайте такі облікові записи:

   user1 / PASSuser1!

   user2 / PASSuser2!

Крок 2. Налаштування автентифікації для бездротового доступу на HQ-Laptop-1

1. Поверніться до приміщення HQ та клацніть на HQ-Laptop-1 (розташований на дві кімнати правіше від комутаційної шафи).

2. Перейдіть на вкладку Config, у розділі INTERFACE оберіть Wireless0.

3. У полі SSID введіть: HQ-INT.

4. У розділі Authentication встановіть режим WPA2.

5. У полі User ID вкажіть user1, у полі Password – PASSuser1!.

6. У розділі IP Configuration оберіть DHCP. Дочекайтесь отримання параметрів IP-адресації.

7. Переконайтесь що HQ-Laptop-1 отримав адресу з мережі 192.168.50.0/24.

Примітка: за необхідності перемкніться між режимами Static/DHCP, а також скористайтеся Check Results для актуалізації параметрів у Packet Tracer.

Крок 3. Налаштування автентифікації для бездротового доступу на HQ-Laptop-2

1. Клацніть на HQ-Laptop-**2** (у верхньому правому куті HQ).
2. Аналогічно до HQ-Laptop-1 налаштуйте інтерфейс Wireless0, використовуючи облікові дані:

User ID: user2

Password: PASSuser2!

3. Увімкніть отримання IP-адрес через DHCP та переконайтесь, що HQ-Laptop-2 отримав адресу з мережі 192.168.50.0/24**.**

Частина 2. Налаштування та використання служб електронної пошти

Крок 1. Активація служб і налаштування облікових записів користувачів електронної пошти

1. Перейдіть до комутаційної шафи Wiring Closet.
2. На полиці Rack справа клацніть на сервері Mail. Відкрийте вкладку Services, оберіть EMAIL у розділі SERVICES.
3. Увімкніть служби SMTP та POP3.
4. У полі доменного імені задайте: mail.cyberhq.com.
5. У розділі User Setup додайте такі облікові записи (натискаючи + для кожної пари логін/пароль):

HQuser1 / Cisco123!

HQuser2 / Cisco123~

BRuser1 / Cisco123-

BRuser2 / Cisco123+

Крок 2. Налаштування e-mail клієнтів

1. Поверніться до HQ та клацніть на PC 1-1 (у нижньому куті).
2. Відкрийте вкладку Desktop > Email (вікно Configure Mail).
3. Заповніть поля:

Your Name: Suk-Yi

Email Address: HQuser1@mail.cyberhq.com

Incoming & Outgoing Email Server(s): mail.cyberhq.com

User Name: HQuser1

Password: Cisco123!

Натисніть Save.

4. Аналогічно налаштуйте поштові клієнти на інших ПК/ноутбуках:

Пристрій	Your Name	Email Address	User Name	Password
PC 2-3	Ajulo	BRuser1@mail.cyberhq.com	BRuser1	Cisco123-
HQ-Laptop-1	Malia	BRuser2@mail.cyberhq.com	BRuser2	Cisco123+
Net-Admin	Cisco	HQuser2@mail.cyberhq.com	HQuser2	Cisco123~

Крок 3. Тестування обміну електронною поштою

1. На PC 1-1 (Suk-Yi) у вікні Email натисніть Compose.

2. Створіть лист до Ajulo за адресою BRuser1@mail.cyberhq.com. Введіть довільну тему та текст листа. Натисніть Send.

Примітка: Packet Tracer може займати кілька секунд, перш ніж показати повідомлення Send Success.

3. Перейдіть на PC 2-3 **(**Ajulo**)**, відкрийте Desktop > Email**.**

4. Натисніть Receive і переконайтесь, що лист від Suk-Yi отримано та його вміст відображається коректно.

Частина 3. Налаштування та використання служб FTP

Крок 1. Активація служби FTP

1. Перейдіть до комутаційної шафи Wiring Closet.

2. На полиці Rack клацніть на сервері **FTP**. Відкрийте вкладку **Services**, оберіть FTP у розділі SERVICES.

3. Увімкніть службу FTP (перемикач On).

Крок 2. Створення облікових записів користувачів FTP

1. У розділі User Setup додайте користувачів з відповідними паролями та привілеями:

sukyi / cisco123 / RWDNL (Write, Read, Delete, Rename, List)

ajulo / cisco321 / RWDNL (Write, Read, Delete, Rename, List)

malia / cisco123 / RWNL (Write, Read, Rename, List – без Delete)

2. Перевірте правильність введених даних та закрийте налаштування сервера.

Крок 3. Передавання файлів між Net-Admin і FTP-сервером

1. На ПК Net-Admin перейдіть до Desktop > Command Prompt.
2. Виконайте команду:

   ftp 192.168.75.2

та пройдіть автентифікацію з обліковими даними:

   Username: sukyi

   Password: cisco123

3. Введіть команду dir для перегляду вмісту каталогу на FTP-сервері.
4. Завантажте файл aMessage.txt командою:

   get aMessage.txt

5. Завершіть сеанс FTP командою bye (або quit).
6. Вийдіть з Command Prompt, відкрийте Desktop > Text Editor, оберіть File > Open і відкрийте файл aMessage.txt.
7. Занотуйте у звіті, яке повідомлення містить файл.
8. Створіть новий файл: File > New, введіть довільний текст.
9. Збережіть його як aMessage_new.txt (File > Save), закрийте Text Editor.
10. Знову відкрийте Command Prompt, виконайте підключення до FTP-сервера як sukyi, та завантажте новий файл на сервер командою:

    put aMessage_new.txt

11. Завершіть FTP-сеанс.

Крок 4. Перевірка дії прав доступу користувачів FTP

1. На HQ-Laptop-1 відкрийте Desktop > Command Prompt**.**
2. Підключіться до FTP-сервера командою:

   ftp 192.168.75.2

— З обліковими даними:

   Username: malia

   Password: cisco123

3. Спробуйте виконати команду видалення файлу:

   delete aMessage_new.txt

— У звіті дайте відповідь: чи вдалося видалити файл? Чому?

4. Виконайте команду перейменування файлу:

rename aMessage_new.txt aMessage_rename.txt

— У звіті вкажіть: чи вдалося перейменувати файл? Поясніть, як на це впливають встановлені привілеї користувача malia.

5. Завершіть FTP-сеанс та закрийте вікно HQ-Laptop-1.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (AAA, автентифікація/авторизація, e-mail, FTP – 1-2 сторінки).
4. Практичну частину, що включає:

— опис налаштування AAA-сервера (створені користувачі, скріншоти/схематичні рисунки);

— опис налаштування бездротового доступу на HQ-Laptop-1, HQ-Laptop-2 та отриманих IP-адрес;

— опис налаштування поштового сервера та клієнтів, приклад надісланого й отриманого листа;

— опис налаштування FTP-сервера, створених облікових записів та результатів виконання команд get/put/delete/rename для різних користувачів.

5. Висновки:

— узагальнення щодо ролі AAA та контролю доступу у захисті мережевих служб;

— отримані практичні навички;

— рекомендації щодо побудови безпечної архітектури доступу до Wi-Fi, e-mail та FTP.

6. Список використаних джерел згідно з вимогами до оформлення бібліографічних посилань.

4. Підбиття підсумків заняття

— обговорення результатів налаштування AAA, поштових та FTP-служб;

— аналіз правильності реалізації прав доступу користувачів;

— оцінювання повноти та якості звітів, уміння пояснювати вплив налаштувань на безпеку;

— формулювання узагальнених висновків щодо значення комплексного підходу до контролю доступу в мережі.

5. Список рекомендованої літератури

Основна:

1. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. К., 2013. 435 с.

2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.

3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навчальний посібник. Х. : Вид. ХНЕУ, 2013. 476 с.

4. Полотай О., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.

Додаткова:

1. Кавун С. В., Смірнов О. А., Столбов В. Ф. Основи інформаційної безпеки. Кіровоград : Вид. КНТУ, 2012. 414 с.

2. Гарасимчук О. І., Дудикевич В. Б., Ромака В. А. Комплексні системи санкціонованого доступу : навч. посіб. Л. : Вид-во Львів. політехніки, 2010. 212 с.

Інформаційні ресурси:

1. Віртуальний університет ЛДУБЖД : електронне навчальне середовище. URL: https://virt.ldubgd.edu.ua

2. Офіційний сайт мережевої академії Cisco: http://www.netacad.com

ЛАБОРАТОРНА РОБОТА № 3

Тема: вивчення та налаштування міжмережевого екрана.

Мета: формування у здобувачів вищої освіти цілісного уявлення про принципи роботи міжмережевих екранів, їх типи та архітектури; набуття практичних навичок налаштування правил фільтрації трафіка, контролю доступу та моніторингу мережевої активності; відпрацювання навичок застосування міжмережевих екранів (у т.ч. ZPF Cisco IOS та брандмауера ОС Windows) для забезпечення безпеки локальних та корпоративних мереж.

Місце проведення: згідно з розкладом.

Час: 8 годин.

Основні поняття: *Міжмережевий екран (брандмауер, фаєрвол)* – програмно-апаратний або чисто програмний засіб, що реалізує політику контролю доступу між мережами, фільтраючи трафік за заданими правилами.

Фільтрація пакетів (packet filtering) – перевірка заголовків пакетів (IP-адреси, порти, протокол, прапорці), на основі чого приймається рішення «дозволити/заборонити».

Stateless firewall – брандмауер без збереження стану, що аналізує кожен пакет окремо, не враховуючи контекст з'єднання.

Stateful firewall – брандмауер зі збереженням стану, який веде таблицю станів з'єднань і дозволяє зворотний/пов'язаний трафік.

Проксі-брандмауер (Application Gateway Firewall) – брандмауер, що працює на рівні прикладних протоколів, виступає посередником між клієнтом і сервером.

Брандмауер наступного покоління (Next-Generation Firewall, NGFW) – міжмережевий екран із розширеними функціями: IPS, контроль додатків, інтеграція з сервісами загроз тощо.

DMZ (demilitarized zone) – демілітаризована зона мережі, сегмент із проміжним рівнем довіри, де зазвичай розташовують публічні сервери.

Зона безпеки (security zone) – логічна група інтерфейсів з однаковим рівнем довіри (INSIDE, OUTSIDE, DMZ тощо).

Zone-Based Policy Firewall (ZPF) – модель брандмауера Cisco IOS, у якій політика безпеки застосовується до трафіка між зонами, а не до окремих інтерфейсів.

Class-map – об’єкт, у якому описується, який трафік вважається «цікавим» (за ACL, протоколами тощо).

Policy-map – політика, що визначає дію над трафіком, відібраним class-map (inspect, drop, pass).

Zone-pair – односпрямована зв’язка «джерело–призначення» між зонами, до якої прив’язується policy-map.

Self zone – спеціальна зона Cisco IOS, яка представляє сам маршрутизатор (IP-адреси його інтерфейсів, трафік керування).

ICMP (Internet Control Message Protocol) – протокол обміну службовими повідомленнями, що, зокрема, використовується командою ping.

Брандмауер Windows (Windows Firewall) – вбудований у ОС Windows засіб фільтрації вхідного/вихідного трафіка.

Обладнання та програмне забезпечення: персональні комп’ютери / ноутбуки з ОС Windows (ПК-А, ПК-В, а також хости у топологіях Cisco Packet Tracer). Операційна система: Windows 10 / 11. Програмне забезпечення: Cisco Packet Tracer (версія згідно з вимогами курсу). Віртуальний університет (електронний курс дисципліни). Веббраузер (для доступу до web-сервера та мережевої академії Cisco). Текстовий редактор (MS Word / Google Docs / LibreOffice Writer) для оформлення звіту.

План

1. **Організаційні заходи:**

— повідомлення теми, мети та завдань лабораторної роботи;

— мотивація навчальної діяльності (роль брандмауерів у забезпеченні мережевої безпеки);

— ознайомлення з матеріалами в «Віртуальному університеті».

2. **Усний контроль опорного рівня знань:**

— базові поняття мережної безпеки, моделі OSI;

— принципи фільтрації трафіка, поняття статичного/динамічного брандмауера;

— основи роботи ACL та брандмауера Windows.

3. **Формування професійних умінь та навичок:**

— налаштування брандмауера Windows (ICMP/Inbound Rules);

— базова конфігурація Zone-Based Policy Firewall (ZPF) у Packet Tracer;

— розширена конфігурація ZPF з декількома зонами (INSIDE, CONFROOM, INTERNET).

4. Пояснення порядку оформлення та подання звіту, критеріїв оцінювання.

5. Захист лабораторної роботи, аналіз результатів, формулювання висновків.

3. Формування професійних умінь та навичок

3.1. Теоретичні відомості

Міжмережевий екран/брандмауер/фаєрвол – це система фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки.

Брандмауер – це система або група систем, яка забезпечує політику контролю доступу між мережами.

Переваги використання брандмауера в мережі:

— Вони запобігають доступу до ненадійних користувачів чутливих хостів, ресурсів і програм.

— Вони очищають потік протоколу, що запобігає використанню недоліків протоколу.

— Вони блокують шкідливі дані з серверів і клієнтів.

— Вони зменшують складність управління безпекою, перевантажуючи більшу частину контролю доступу до мережі на декілька брандмауерів у мережі.

Брандмауери мають обмеження:

— Неправильно налаштований брандмауер може мати серйозні наслідки для мережі, наприклад, стати єдиною точкою збою.

— Дані з багатьох програм не можуть бути надійно передані через брандмауери.

— Користувачі можуть активно шукати шляхи обійти брандмауер для

отримання заблокованого матеріалу, що піддає мережу потенційній атаці.

— Продуктивність мережі може сповільнитися.

— Несанкціонований трафік можна тунелювати або приховати як законний трафік через брандмауер.

Типи брандмауерів

1. Брандмауери фільтрації пакетів (stateless). Брандмауери фільтрації пакетів зазвичай є частиною брандмауера маршрутизатора, який дозволяє або забороняє трафік на основі інформації рівня 3 і рівня 4. Це брандмауери без стану, які використовують просту таблицю політики, яка фільтрає трафік за певними критеріями.

Наприклад, SMTP-сервери слухають порт 25 за усталеним налаштуванням. Адміністратор може налаштувати брандмауер фільтрації пакетів, щоб блокувати порт 25 з певної робочої станції, щоб запобігти поширенню вірусу електронної пошти.

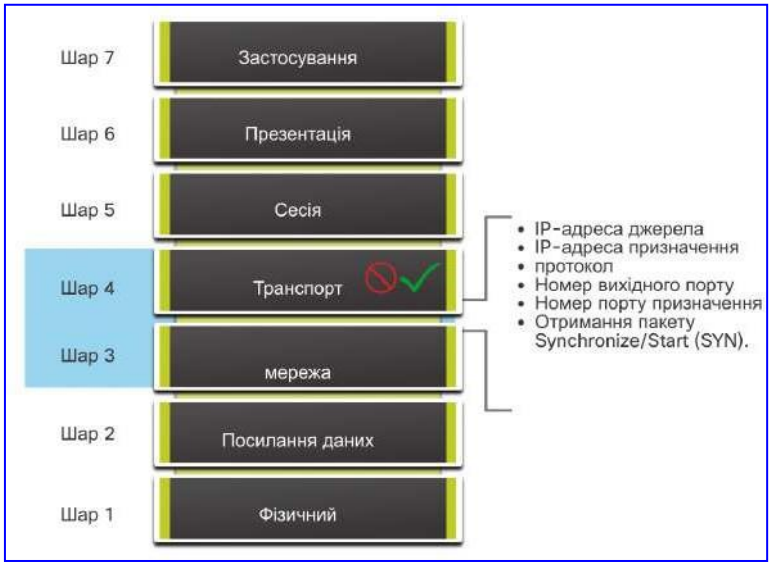


Рисунок 1. Логічна схема рівнів OSI та параметри транспортного шару (SYN, порти, IP-адреси)

2. Брандмауери зі збереження стану (stateful). Брандмауери зі збереження стану (statefull) є найбільш універсальними та найпоширенішими технологіями брандмауера. Брандмауери, що зберігають стан, забезпечують фільтрацію пакетів із збереженням стану, використовуючи інформацію про з'єднання, яка зберігається в таблиці станів. Фільтрація за станом – це архітектура брандмауера,

яка класифікується на мережевому рівні. Він також аналізує трафік на рівнях 4 і 5 OSI.

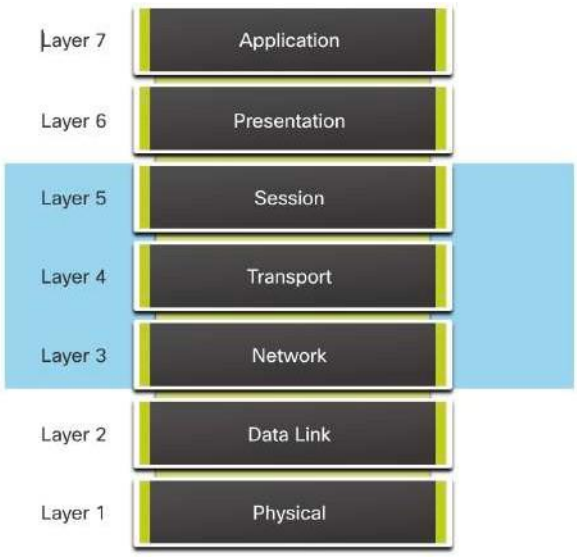


Рисунок 2. Логічна модель взаємодії мережевих протоколів OSI

3. **Брандмауер шлюзу програми (проксі-брандмауер) (application gateway firewall).** Брандмауер шлюзу програми фільтрає інформацію на рівнях 3, 4, 5 і 7 еталонної моделі OSI. Більшість контролю та фільтрації брандмауера здійснюється програмно. Коли клієнту потрібно отримати доступ до віддаленого сервера, він підключається до проксі-сервера. Проксі-сервер підключається до віддаленого сервера від імені клієнта. Тому сервер бачить лише з'єднання з проксі-сервера.

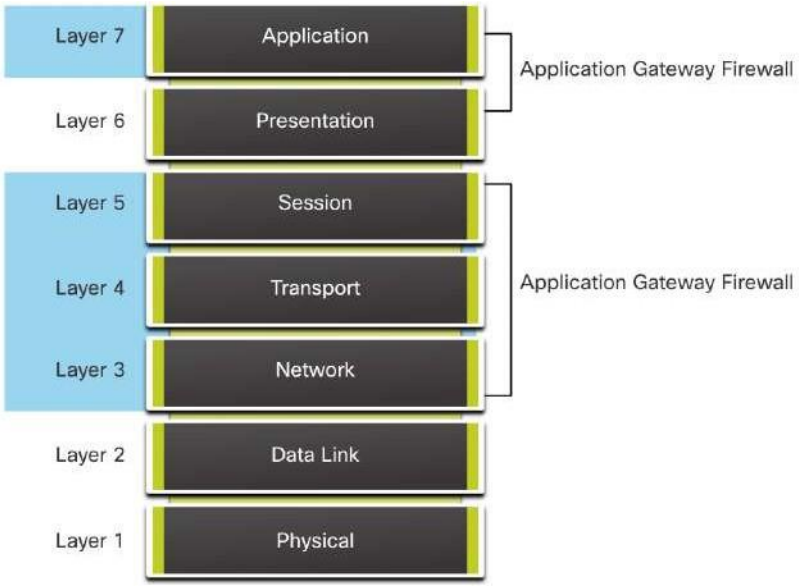


Рисунок 3. Область роботи Application Gateway Firewall у моделі OSI

4. **Брандмауери наступного покоління (NGFW).** Брандмауери наступного покоління (NGFW) виходять за межі брандмауерів із визначенням стану, забезпечуючи:

— Комплексне запобігання вторгненню.

— Обізнаність і контроль додатків для перегляду та блокування ризикованих програм.

— Оновити шляхи, щоб включити майбутні інформаційні канали.

— Методи боротьби з загрозами безпеки, що розвиваються.

Поширені конструкції брандмауера:

1. **Приватне і публічне (Private and public)**

Як показано на малюнку, публічна мережа (або зовнішня мережа) не є надійною, а приватна мережа (або внутрішня мережа) є довіреною. Як правило, брандмауер з двома інтерфейсами налаштовується таким чином:

— Трафік із приватної мережі дозволений та перевіряється, коли він рухається до мережі загального користування. Дозволено перевірений трафік, що повертається із загальнодоступної мережі та пов’язаний з трафіком, що походить із приватної мережі.

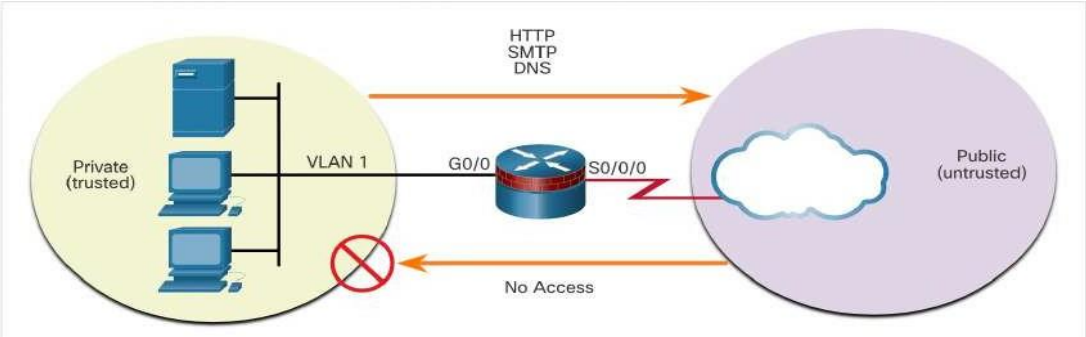


Рисунок 4. Схема фільтрації трафіка між приватною та публічною мережею

— Трафік, що надходить із загальнодоступної мережі та прямує до приватної мережі, як правило, заблокований.

2. **Демілітаризована зона (DMZ)**

Демілітаризована зона (DMZ) – це конструкція брандмауера, де зазвичай є один внутрішній інтерфейс, підключений до приватної мережі, один зовнішній інтерфейс, підключений до загальнодоступної мережі, і один інтерфейс DMZ, як показано на рисунку.

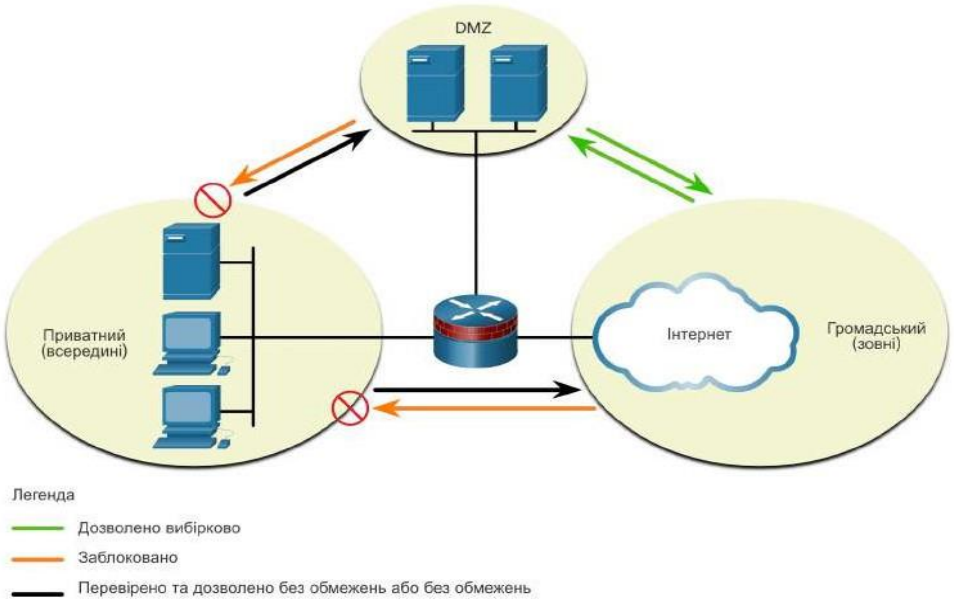


Рисунок 5. Архітектура мережі з DMZ та політиками фільтрації трафіка

— Трафік, що надходить із приватної мережі, перевіряється, коли він рухається до загальнодоступної мережі або мережі DMZ. Цей рух дозволено з невеликими обмеженнями або без них. Перевірений трафік, що повертається з DMZ або загальнодоступної мережі в приватну мережу, дозволено.

— Трафік, що надходить із мережі DMZ і прямує до приватної мережі, зазвичай блокується.

— Трафік, що надходить із мережі DMZ і прямує до мережі загального користування, вибірково дозволяється відповідно до вимог обслуговування.

— Трафік, що йде від мережі загального користування та прямує до DMZ, вибірково дозволяється та перевіряється. Цей тип трафіка, як правило, є трафіком електронної пошти, DNS, HTTP або HTTPS. Зворотний трафік із DMZ до загальнодоступної мережі динамічно дозволений.

— Трафік, що надходить із загальнодоступної мережі та прямує до приватної мережі, заблоковано.

3. **Брандмауери на основі зон (ZPF)**

Брандмауери на основі зон (ZPF) використовують концепцію зон для забезпечення додаткової гнучкості. Зона – це група з одного або кількох інтерфейсів, які мають подібні функції чи функції. Зони допомагають визначити, де має застосовуватися правило або політика брандмауера Cisco IOS. На малюнку політики безпеки для LAN 1 і LAN 2 подібні і можуть бути згруповані в зону для конфігурації брандмауера. За усталеним налаштуванням трафік між інтерфейсами в одній зоні не підпадає під політику і проходить вільно. Проте весь міжзонний рух заблоковано. Щоб дозволити рух між зонами, потрібно налаштувати політику, що дозволяє або перевіряє трафік.

Концепція ZBPF – це зона, яка групує різні інтерфейси, що мають однакові атрибути безпеки або однаковий рівень довіри. Дозволи на пересилання трафіка надаються між зонами або всередині зони, а не між фізичними інтерфейсами.

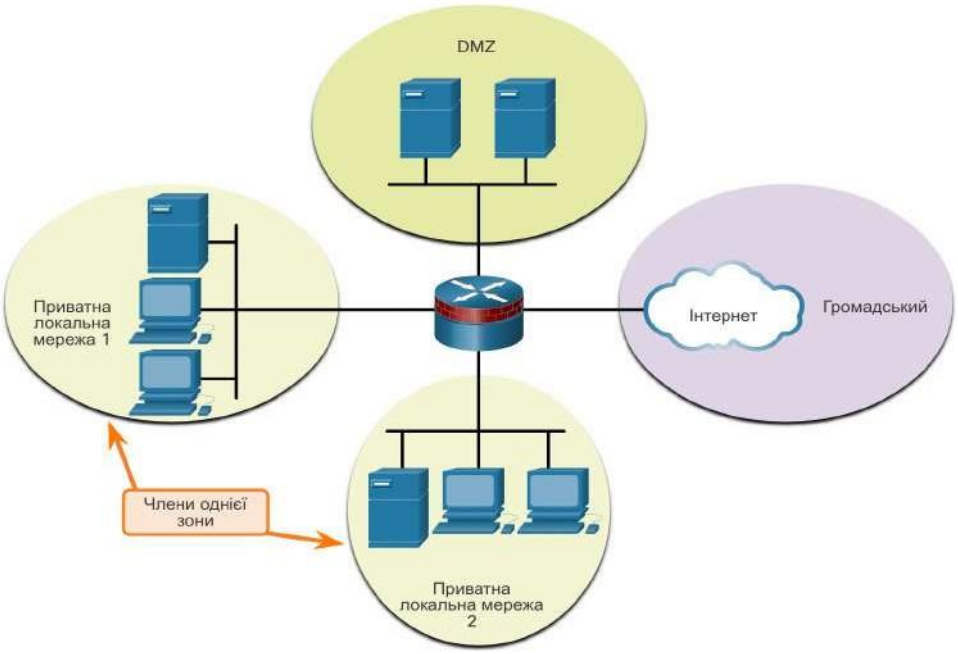


Рисунок 6. Архітектура мережі з двома приватними локальними мережами та DMZ

Єдиним винятком із цієї політики заборони за усталеним налаштуванням є власна зона маршрутизатора (self zone). Власна зона (self zone) – це сам маршрутизатор і включає всі IP-адреси інтерфейсу маршрутизатора. Конфігурації політики, які включають зону self, застосовуватимуться до трафіка, призначеного маршрутизатору та отриманого з нього. За усталеним

налаштуванням для цього типу трафіка немає політики. Трафік, який слід враховувати при розробці політики для самої зони, включає в себе трафік площини керування та рівня керування, наприклад SSH, SNMP та протоколи маршрутизації.

Існує дві моделі конфігурації для брандмауера Cisco IOS:

— Класичний брандмауер – традиційна модель конфігурації, в якій політика брандмауера застосовується до інтерфейсів.

— Брандмауер політики на основі зони (ZPF) – модель конфігурації, в якій інтерфейси призначаються зонам безпеки, а політика брандмауера застосовується до трафіка, що переміщується між зонами.

Переваги ZPF. Основними мотивами переходу на модель ZPF фахівців із мережевої безпеки є структура та простота використання. Структурований підхід корисний для документації та спілкування. Простота використання робить реалізації мережевої безпеки більш доступною для більшої спільноти професіоналів у сфері безпеки.

Проектування ZPF включає кілька кроків:

Крок 1. Визначення зони. Адміністратор зосереджується на поділі мережі на зони. Зони встановлюють кордони безпеки мережі. Зона визначає межу, де трафік піддається обмеженням політики, коли він перетинає інший регіон мережі.

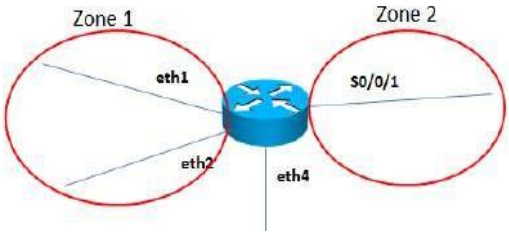


Рисунок 7. Приклад поділу інтерфейсів маршрутизатора на мережеві зони

Наприклад, загальнодоступна мережа буде однією зоною, а внутрішня мережа – іншою. Як бачите, інтерфейси eth1 і 2 належать до зони 1, інтерфейс s0/0/0 належить до зони 2, а інтерфейс eth3 не належить жодному інтерфейсу. Політика за усталеним налаштуванням або користувацька політика буде використовуватися, якщо потік трафіка між інтерфейсом у зоні 1 і інтерфейсом

у зоні 2. Політика не використовуватиметься, якщо потік трафіка між інтерфейсом у зоні 1 та іншим інтерфейсом у зоні 1. Між інтерфейсом у зоні 1 або 2 і інтерфейсом, який не належить жодній зоні, не буде дозволено жодне з'єднання та потік трафіка.

Зона безпеки – це група інтерфейсів, до яких можна застосувати політику. Групування інтерфейсів у зони включає дві процедури:

— Створення зони, щоб до неї можна було приєднати інтерфейси.

— Налаштування інтерфейсу як члена певної зони.

Є два типи зон, про які потрібно знати:

— Налаштовується користувачем: ви створюєте та налаштовуєте.

— «self»: одна зона за усталеним налаштуванням, створена та попередньо налаштована системою.

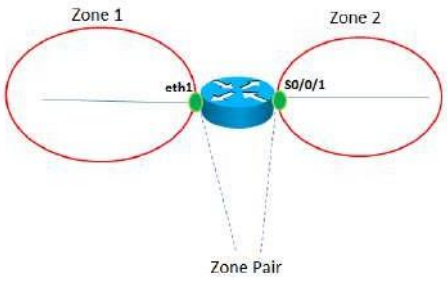


Рисунок 8. Приклад створення Zone Pair для контролю трафіка між зонами

У кожному маршрутизаторі є одна зона за усталеним налаштуванням, відома як self, яка охоплює власні IP-адреси маршрутизатора. Трафік із цієї зони в будь-яку іншу зону дозволений за усталеним налаштуванням, щоб забезпечити трафік на площині керування та на площині керування. Однак ви можете застосувати явну двонаправлену політику між власною зоною та будь-якою іншою налаштованою зоною, щоб керувати трафіком, створеним маршрутизатором або маршрутизатором. Після створення та визначення ваших зон і інтерфейсів до якої зони, ми повинні створити пару зон.

Пари зон. Пара зон дозволяє вказати політику односпрямованого брандмауера між двома зонами безпеки. Щоб дозволити певні потоки трафіка між двома різними зонами безпеки, ви повинні визначити пару зон і застосувати

політику використання за усталеним налаштуванням або використовувати політику перевірки до цієї пари.

Крок 2. Встановлення політики між зонами. Для кожної пари зон «джерело-призначення» (наприклад, від внутрішньої мережі до зовнішнього Інтернету) визначте сеанси, які клієнти в вихідних зонах можуть запитувати від серверів у зонах призначення. Найчастіше це сеанси TCP і UDP, але також можуть бути сеанси ICMP, наприклад ICMP echo. Для трафіка, який не заснований на концепції сеансів, адміністратор повинен визначити односпрямовані потоки трафіка від джерела до призначення і навпаки. Політики є односпрямованими і визначаються на основі вихідних і цільових зон, які відомі як пари зон.

Крок 3. Розроблення фізичної інфраструктури. Після того, як зони були визначені та задокументовані вимоги до трафіка між ними, адміністратор повинен спроектувати фізичну інфраструктуру. При проектуванні фізичної інфраструктури адміністратор повинен враховувати вимоги безпеки та доступності. Це включає в себе диктування кількості пристроїв між найбільш безпечними та найменш захищеними зонами та визначення резервних пристроїв.

Крок 4. Визначте підмножини в межах зон і об'єднайте вимоги до трафіка. Для кожного пристрою брандмауера в проекті адміністратор повинен визначити підмножини зон, які підключені до його інтерфейсів, і об'єднати вимоги до трафіка для цих зон.

3.2. Зміст лабораторної роботи

Лабораторна робота складається з таких логічних частин:

— Частина 1. Налаштування та використання облікових даних автентифікації AAA.

— Частина 2. Налаштування та використання служб електронної пошти.

— Частина 3. Налаштування та використання служб FTP.

Під час виконання роботи здобувачі налаштовують механізми автентифікації та авторизації доступу до мережевих ресурсів, електронної пошти та FTP-сервера з використанням програмного середовища Packet Tracer.

3.3. Рекомендації щодо виконання (хід роботи)

Довідкова інформація / Сценарій

Автентифікація та авторизація – це окремі процеси безпеки у сфері керування ідентифікацією та доступом (Identity and Access Management – IAM).

Автентифікація використовує паролі та інші методи ідентифікації для підтвердження особи користувача.

Авторизація визначає дозволи на користування ресурсами для автентифікованих користувачів.

У цій лабораторній роботі в середовищі Packet Tracer здійснюється налаштування автентифікації та авторизації для користування:

— бездротовим доступом;

— електронною поштою;

— FTP-службою.

Примітка. Лабораторна робота відкривається у Фізичному режимі, але її також можна виконувати у Логічному режимі.

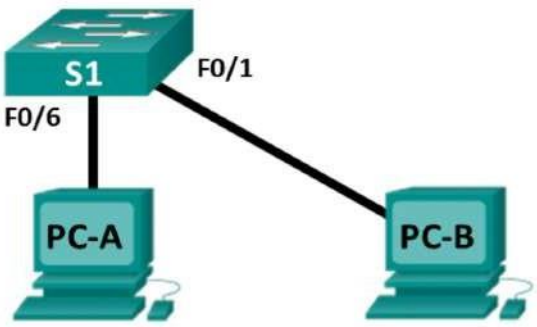
Примітка. Більшість завдань підлягають автоматичному оцінюванню через кнопку Check Results у розділі Assessment Items.

Робота складається з трьох кількох частин:

1. Частина 1. Налаштування параметрів брандмауера
2. Частина 2. Конфігурація ZPF
3. Частина 3. Налаштування ZPF

Частина 1. Налаштування параметрів брандмауера

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Рисунок 9. Топологія підключення двох ПК до комутатора

Мета:

— Навчитися налаштовувати і додавати нові правила брандмауер Windows.

— Створити правило брандмауера, щоб дозволити запити ping.

— Видалити нове правило брандмауера, щоб повернути налаштування до попереднього стану.

Крок 1. Переконайтеся, що брандмауер Windows активний і блокує запити ICMP.

a. Клацніть правою кнопкою миші Пуск. Виберіть «Мережеві підключення» (Network Connections).

b. Клацніть правою кнопкою миші потрібний мережевий адаптер і виберіть Властивості (Properties).

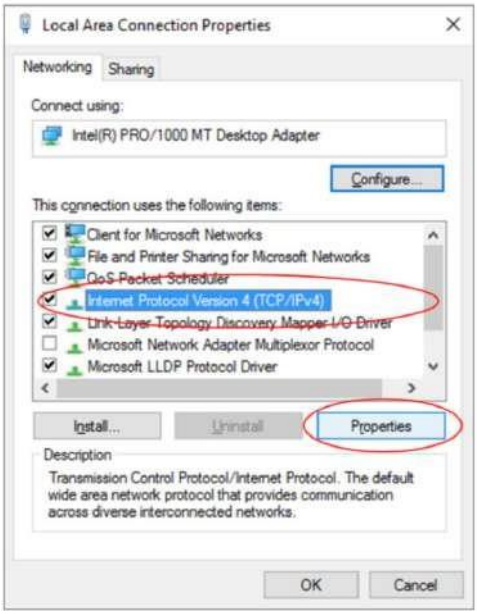


Рисунок 10. Вікно налаштувань мережевого адаптера в Windows: вибір протоколу IPv4

c. Виберіть Internet Protocol Version 4 (TCP/IPv4). Натисніть «Властивості», щоб налаштувати два ПК зі статичними IP-адресами, показаними в таблиці адресації. Для шлюзу за усталеним налаштуванням або DNS-сервера в цій лабораторній роботі не потрібна конфігурація, оскільки обидва ПК знаходяться в одній IP-мережі і використовуватимуть IP-адреси замість доменних імен.

Відкрийте вікно командного рядка на PC-A, клацнувши правою кнопкою миші Пуск > Командний рядок (Start > Command Prompt). Спробуйте пінгувати IP-адресу, призначену для PC-B.

Команда ping повинна бути невдалою. Повторіть команду ping на ПК-B, намагаючись відправити ping на адресу ПК-A. Команди ping з обох комп'ютерів не повинні виконуватися, що вказує на те, що брандмауер Windows активний і блокує запити ping ICMP.

Примітка: Якщо ping успішно виконано на будь-якому комп'ютері, переконайтеся, що брандмауер Windows активний на обох комп'ютерах.

Крок 2. Створіть нове правило для вхідного доступу, яке дозволить трафік ICMP через брандмауер.

a. Налаштуйте параметри брандмауера на PC-A. Натисніть кнопку Пуск і введіть Брандмауер (Firewall). Виберіть Брандмауер Windows.



Рисунок 11. Вікно налаштувань Windows Firewall: доступ до розширених параметрів

b. На лівій панелі вікна брандмауера Windows натисніть кнопку Додаткові параметри (Advanced settings).

c. У вікні «Розширений захист» (Advanced Security) виберіть параметр Inbound Rules на лівій бічній панелі, а потім натисніть « Нове правило…» (New Rule…) на правій бічній панелі.

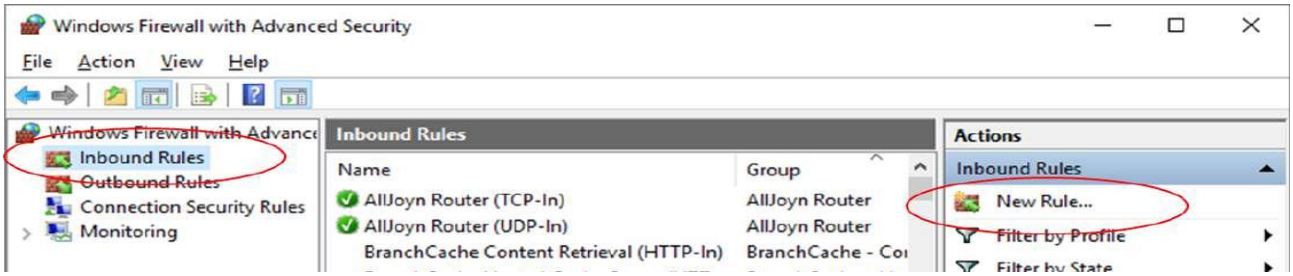


Рисунок 12. Створення нового правила вхідного трафіка у Windows Firewall

d. При натисканні пункту меню Нове правило запускається майстер створення нового правила для входу. На екрані «Тип правила» клацніть перемикач Custom і натисніть «Далі».

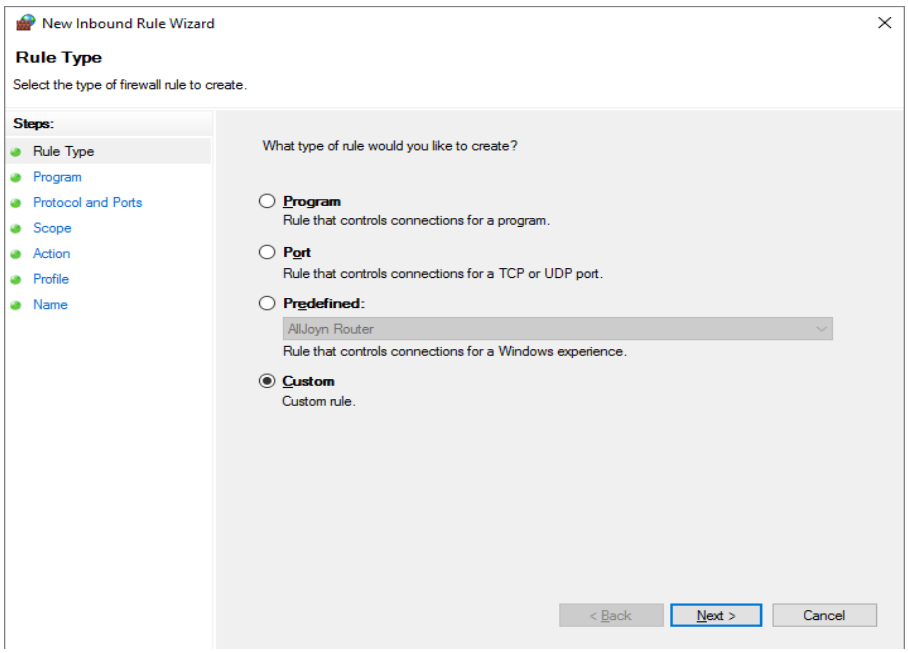


Рисунок 13. Вибір типу правила під час створення нового Inbound Rule у Windows Firewall

e. На панелі ліворуч виберіть параметр Протокол і порти (Protocol and Ports) та за допомогою спадного меню Тип протоколу виберіть ICMPv4, а потім натисніть кнопку Далі.

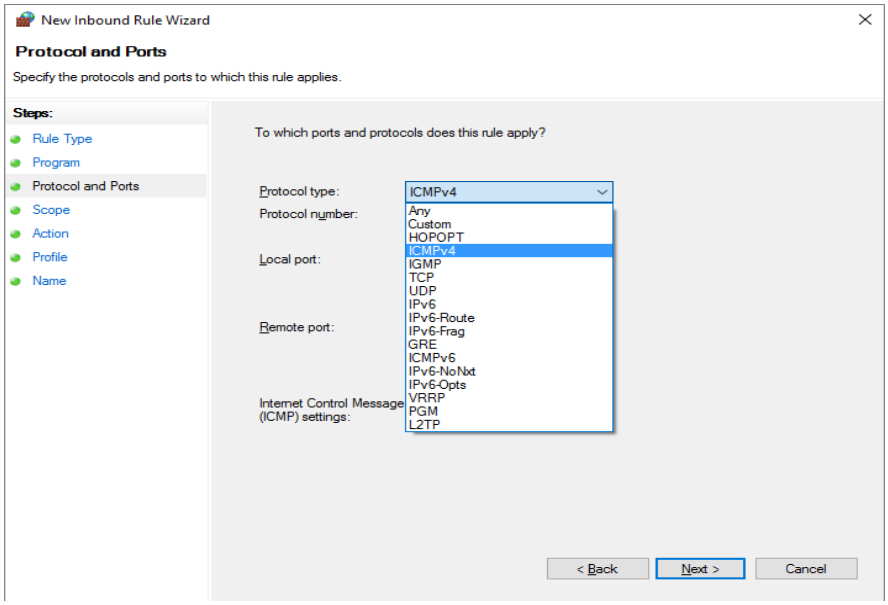


Рисунок 14. Налаштування протоколу та портів у майстрі створення правила Windows Firewall

Питання. *Перелічіть три протоколи, окрім ICMP, які можна відфільтравати за допомогою нового правила брандмауера для вхідних даних. (відповідь напишіть у звіті).*

f. На панелі ліворуч виберіть параметр «Ім'я» (Name) та в полі «Ім'я» введіть « Дозволити запити ICMP» (Allow ICMP Requests). Натисніть Готово .

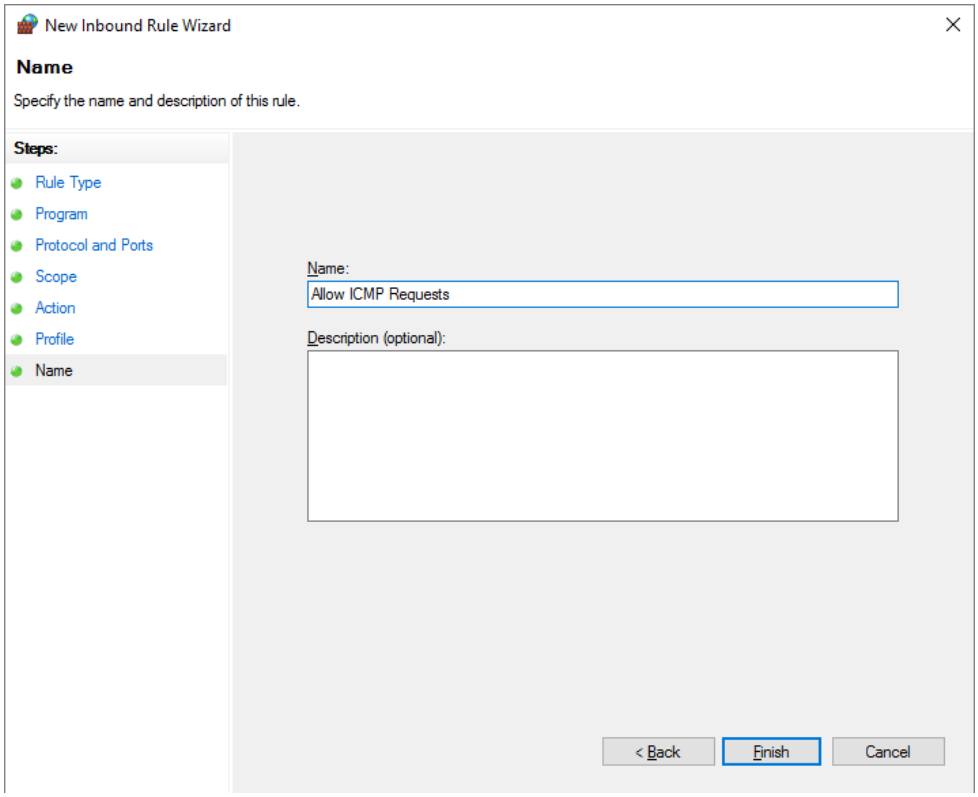


Рисунок 15. Завершення створення правила: введення назви нового

Inbound Rule

Це нове правило має дозволити членам вашої команди отримувати відповіді ping від PC-A. Повторіть команди кроку 2, щоб додати нове правило на PC-B.

g. Перевірте нове правило брандмауера, повторивши команди ping, використані на кроці 1. Цей запит має бути успішним. Якщо ні, перегляньте налаштування брандмауера, щоб переконатися, що нове правило налаштоване правильно.

Крок 3: Вимкнення або видалення нового правила ICMP

Після завершення лабораторної роботи ви можете вимкнути або навіть видалити нове правило, створене на кроці 2. Використання параметра **Вимкнути** правило (Disable Rule) дає змогу знову ввімкнути правило пізніше. Видалення правила назавжди видаляє його зі списку вхідних правил.

a. У вікні «Розширений захист» (Advanced Security) на лівій панелі клацніть Inbound Rules, а потім знайдіть правило, яке ви створили на кроці 1.

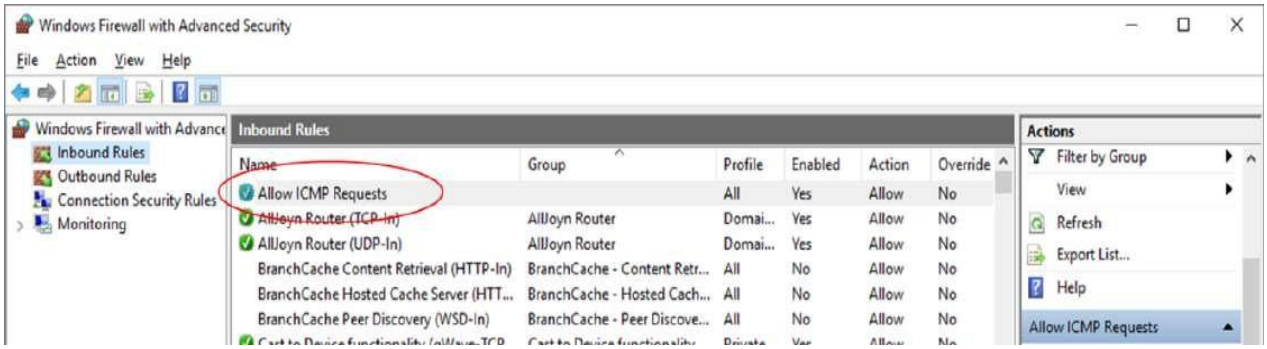


Рисунок 16. Створене правило Allow ICMP Requests у списку Inbound Rules

b. Щоб вимкнути правило, натисніть опцію Вимкнути правило (Disable Rule). Коли ви виберете цей параметр, ви побачите, що цей параметр змінюється на Увімкнути правило (Enable Rule). Ви можете перемикатися між «Вимкнути правило» та «Увімкнути правило»; статус правила також відображається в стовпці Enabled у списку правил для вхідних запитів.

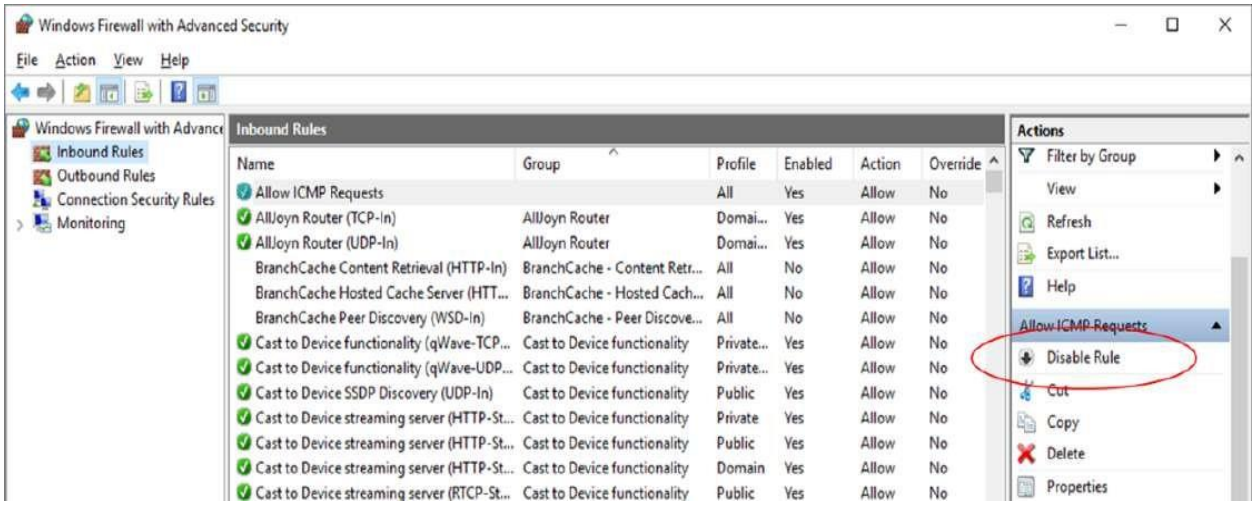


Рисунок 17. Вимкнення правила Allow ICMP Requests у Windows Firewall

c. Щоб остаточно видалити правило ICMP, натисніть Видалити (**Delete**). Якщо ви виберете цей параметр, вам доведеться знову створити правило, щоб дозволити відповіді ICMP.

d. Виконайте команди ping, виконані на кроці 1, щоб переконатися, що брандмауер знову блокує запити ping.

Частина 2. Для виконання цієї частини скачайте з ВНС файл configure-a-zpf.pka і відкрийте його у програмі Packet Tracer.

Networking Academy

Packet Tracer - Configure a ZPF

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Рисунок 18. Адресна таблиця для конфігурації ZPF у Cisco Packet Tracer

Цілі:

— Перевірте підключення між пристроями перед налаштуванням брандмауера.

— Налаштуйте брандмауер зонної політики (ZPF) на R3.

— Перевірте роботу брандмауера ZPF за допомогою ping, SSH і веббраузера.

Передумови/Сценарій:

Брандмауери зонної політики (ZPF) є останньою розробкою в еволюції технологій брандмауерів Cisco. У цій вправі ви налаштуєте базовий ZPF на межовому маршрутизаторі R3, який надає внутрішнім хостам доступ до зовнішніх ресурсів і блокує зовнішнім хостам доступ до внутрішніх ресурсів. Потім ви перевірите роботу брандмауера на внутрішніх і зовнішніх хостах.

Маршрутизатори були попередньо налаштовані за такими параметрами:

— Пароль консолі: ciscoconpa55

— Пароль для рядків vty: ciscovtypa55

— Увімкнути пароль: ciscoenpa55

— Імена хостів та IP-адреси

— Локальний логін і пароль: Admin / Adminpa55

— Статична маршрутизація

Хід виконання:

Частина 1: Перевірка базового підключення до мережі

Перевірте підключення до мережі перед налаштуванням брандмауера зонної політики.

Крок 1. У командному рядку PC-A виконайте пінг PC-C за адресою 192.168.3.3.

Крок 2. Отримайте доступ до R2 за допомогою SSH.

a. З командного рядка PC-C перейдіть по SSH до інтерфейсу S0/0/1 на R2 у 10.2.2.2. Для входу використовуйте ім’я користувача **Admin** і пароль **Adminpa55**.

C:\> ssh -l Admin 10.2.2.2

b. Вийдіть із сесії SSH.

Крок 3. **З PC-C відкрийте веббраузер на сервері PC-A.**

a. Клацніть вкладку «Робочий стіл»/Desktop, а потім виберіть програму «Веббраузер». Введіть на PC-A IP-адресу 192.168.1.3 як URL-адресу. Має відобразитися сторінка привітання Packet Tracer з вебсервера.

b. Закрийте браузер на PC-C.

Частина 2: Створіть зони брандмауера на R3

Примітка. Для всіх завдань конфігурації обов'язково використовуйте точні імена, як зазначено.

Крок 1: Створіть внутрішню зону (internal zone).

Скористайтеся командою zone security, щоб створити зону під назвою IN-ZONE. R3(config)# zone security IN-ZONE

R3(config-sec-zone) exit

Крок 2: Створіть зовнішню зону (external zone).

Скористайтеся командою zone security, щоб створити зону під назвою OUT-ZONE.

R3(config-sec-zone)# zone security OUT-ZONE

R3(**config-sec-zone)# exit**

Частина 3: Ідентифікація трафіка за допомогою Class-Map

Крок 1. Створіть ACL, який визначає внутрішній трафік.

Використовуйте команду access-list, щоб створити розширений ACL 101, щоб дозволити всі IP- протоколи з вихідної мережі 192.168.3.0/24 до будь-якого призначення.

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any

Крок 2: Створіть карту класів із посиланням на ACL внутрішнього трафіка.

Використовуйте команду class-map type inspect з опцією match-all, щоб створити карту класів під назвою IN-NET-CLASS-MAP. Використовуйте команду match access-group, щоб зіставити ACL 101.

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP

R3(config-cmap)# match access-group 101

R3(config-cmap)# exit

Частина 4: Вкажіть політики брандмауера

Крок 1. Створіть карту політики, щоб визначити, що робити з відповідним трафіком.

Використовуйте команду policy-map type inspect і створіть карту політики під назвою IN-2-OUT-PMAP

R3(config)# policy-map type inspect IN-2-OUT-PMAP

Крок 2: Вкажіть тип класу перевірки та посилання на карту класів IN-NET-CLASS-MAP.

R3(config-pmap)# class type inspect IN-NET-CLASS-MAP

Крок 3: Уточніть дію перевірки для цієї карти політики.

Використання команди inspect викликає контекстне керування доступом (інші параметри включають передачу та скидання).

R3(config-pmap-c)# inspect

У класі IN-NET-CLASS-MAP не уточнено конкретний протокол для перевірки. Усі протоколи будуть перевірені.

Напишіть команду exit двічі, щоб вийти з режиму config-pmap-c і повернутися до режиму конфігурації (config).

R3(config-pmap-c)# exit R3(config-pmap)# exit

Частина 5: Застосування політик брандмауера

Крок 1: Створіть пару зон.

Використовуючи команду безпеки zone-pair, створіть пару зон під назвою IN-2-OUT-ZPAIR. Вкажіть зони джерела та призначення, які були створені раніше.

R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE

Крок 2: Вкажіть карту політики для обробки трафіка між двома зонами.

Приєднайте карту політики та пов’язані з нею дії до пари зон за допомогою команди service-policy type inspect та посилайтеся на раніше створену карту політики IN-2-OUT-PMAP.

R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

R3(config-sec-zone-pair)# exit R3(config)#

Крок 3: Призначте інтерфейси відповідним зонам безпеки.

Використовуйте команду zone-member security в режимі конфігурації інтерфейсу, щоб призначити G0/1 для IN-ZONE і S0/0/1 для OUT-ZONE.

R3(config)# interface g0/1

R3(config-if)# zone-member security IN-ZONE

R3(config-if)# exit R3(config)# interface s0/0/1

R3(config-if)# zone-member security OUT-ZONE

R3(config-if)# exit

Крок 4: Скопіюйте запущену конфігурацію до початкової конфігурації.

Частина 6: Перевірте функціональність брандмауера від IN-ZONE до OUT-ZONE.

Переконайтеся, що внутрішні хости можуть отримати доступ до зовнішніх ресурсів після налаштування ZPF.

Крок 1: із внутрішнього PC-C виконайте пінг зовнішнього сервера PC-A.

У командному рядку PC-C виконайте пінг PC-A за адресою 192.168.1.3. Пінг має бути успішним.

Крок 2: від внутрішнього PC-C, SSH до інтерфейсу R2 S0/0/1.

a. З командного рядка PC-C перейдіть по SSH до R2 у 10.2.2.2. Використовуйте ім’я користувача Admin і пароль Adminpa55 для доступу до R2. Сеанс SSH має бути успішним.

b. Коли сеанс SSH активний, виконайте команду show policy-map type inspect zone-pair sessions на R3, щоб переглянути встановлені сеанси.

Питання: відповіді подати у звіті.

1. Яка IP-адреса джерела та номер порту?

2. Яка IP-адреса призначення та номер порту?

Крок 3. З PC-C вийдіть із сеансу SSH на R2 і закрийте вікно командного рядка.

Крок 4. З внутрішнього PC-C відкрийте веббраузер на вебсторінку сервера PC-A.

У веббраузері на PC-C перейдіть до 192.168.1.3. Сеанс HTTP має бути успішним. Поки HTTP-сеанс активний, виконайте команду show policy-map type inspect zone-pair sessions на R3, щоб переглянути встановлені сеанси.

Примітка. Якщо сеанс HTTP минув перед виконанням команди на R3, вам доведеться натиснути кнопку Go на PC-C, щоб створити сеанс між PC-C і PC-A.

Питання: відповіді подати у звіті.

1. Яка IP-адреса джерела та номер порту?
2. Яка IP-адреса призначення та номер порту?

Крок 5. Закрийте браузер на PC-C.

Частина 7: Перевірте функціональність брандмауера від OUT-ZONE до IN-ZONE.

Переконайтеся, що зовнішні хости НЕ МОЖУТЬ отримати доступ до внутрішніх ресурсів після налаштування ZPF.

Крок 1. У командному рядку сервера PC-A виконайте ping PC-C.

У командному рядку PC-A виконайте пінг PC-C за адресою 192.168.3.3. Пінг не має проходити.

Крок 2: з R2 виконайте пінг PC-C.

З R2 виконайте пінг PC-C за адресою 192.168.3.3. Пінг не має проходити.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	G0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
	G0/0/1.3	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	G0/0/1.33	192.168.33.1	255.255.255.0	N/A	S3 F0/5
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18
PC-C	NIC	192.168.33.3	255.255.255.0	192.168.33.1	S3 F0/23

Рисунок 19. Адресна таблиця мережевих пристроїв

Частина 3. Налаштування ZPF

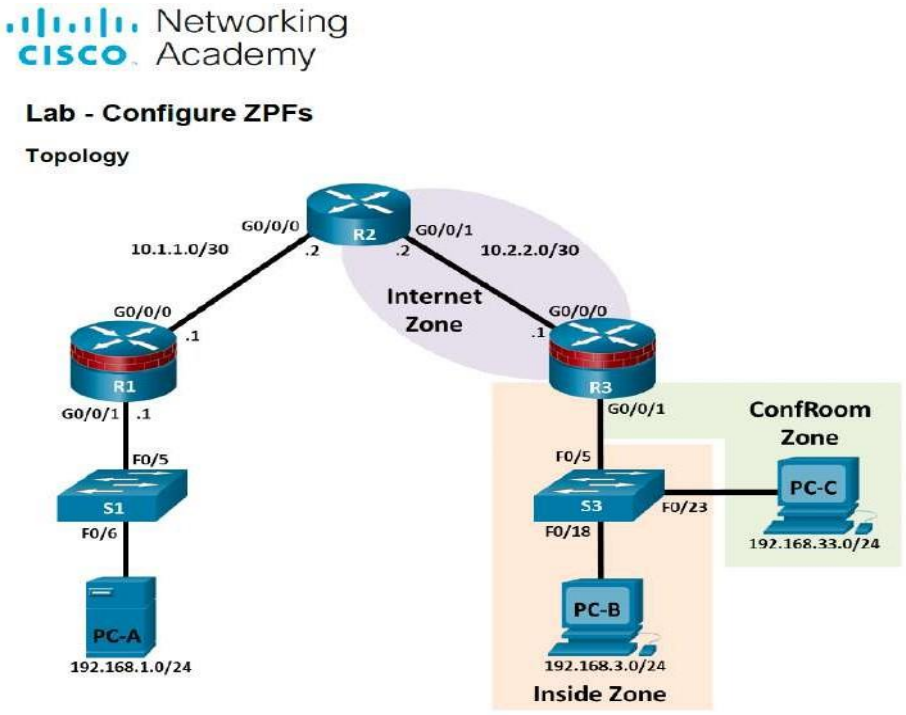


Рисунок 20. Топологія мережі для налаштування Zone-Based Policy Firewall (ZPF)

Мета:

Частина 1: Основна конфігурація пристрою

— Налаштуй’те імена хостів, IP-адреси інтерфейсу та паролі доступу на маршрутизаторах.

— Налаштуйте статичні маршрути, щоб увімкнути наскрізне підключення на маршрутизаторах.

— Налаштуйте порти доступу та магістралі на комутаторі.

Частина 2: Налаштування брандмауера політики на основі зони (ZPF)

— Використовуйте CLI, щоб налаштувати брандмауер політики на основі зони.

— Використовуйте CLI, щоб перевірити конфігурацію. Частина 3: Перевірка функціональності брандмауера ZPF

Хід виконання роботи

Частина 1: Основна конфігурація пристрою

У цій частині цієї лабораторної роботи ви налаштовуєте топологію мережі та налаштовуєте основні параметри, такі як IP-адреса інтерфейсу адреси, статична маршрутизація, доступ до пристрою та паролі. Усі завдання слід виконувати на маршрутизаторах R1, R2 і R3. Процедури показані лише для одного з маршрутизатора.

Крок 1. Підключіть мережу, як показано в топології.

Підключіть пристрої, як показано на схемі топології, і кабель, якщо необхідно.

Крок 2. Вимкніть пошук DNS.

Щоб запобігти спробам маршрутизатора перекласти неправильно введені команди, вимкніть пошук DNS

Крок 3. Налаштуйте основні параметри для кожного маршрутизатора.

а. Налаштуйте імена хостів, як показано в топології.

б. Налаштуйте IP-адреси інтерфейсу, як показано в таблиці IP-адрес. Конфігурація IP-адреси для маршрутизатора R3 наведено нижче.

```
R3(config)# interface GigabitEthernet0/0/0
R3(config-if)# ip address 10.2.2.1 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet0/0/1
R3(config-if)# no shutdown
R3(config-if)# interface GigabitEthernet0/0/1.3
R3(config-if)# encapsulation dot1Q 3
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)#interface GigabitEthernet0/0/1.33
R3(config-if)# encapsulation dot1Q 33
R3(config-if)# ip address 192.168.33.1 255.255.255.0
```

Рисунок 21. Приклад налаштування підінтерфейсів та адресації на маршрутизаторі R3

Крок 4. Налаштуйте статичні маршрути на R1, R2 і R3.

a. Щоб досягти наскрізної доступності IP, на R1, R2 і R3 повинні бути налаштовані належні статичні маршрути. R1 і R3 є заглушеними маршрутизаторами, і тому потрібен лише маршрут за усталеним налаштуванням, що вказує на R2. R2, поводиться як провайдер, повинен знати, як отримати доступ до внутрішніх мереж R1 і R3 до досягнення наскрізної IP-досяжності. Нижче, це статична конфігурація маршруту для R1, R2 і R3. На R1 скористайтеся такою командою:

R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

b. На R2 використовуйте такі команди.

R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1

R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1

R2(config)# ip route 192.168.33.0 255.255.255.0 10.2.2.1

c. На R3 скористайтеся такою командою

R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2

Крок 5. Налаштуйте S3.

a. Налаштувати магістральну лінію (транк):

S3(config)# interface f0/5

S3(config-if)# switchport mode trunk

b. Налаштуйте порти доступу:

S3(config)# interface f0/18

S3(config-if)# switchport mode access S3(config-if)# switchport access vlan 3 S3(config-if)# interface f0/23 S3(config-if)# switchport mode access

S3(config-if)# switchport access vlan 33

Крок 6. Налаштуйте IP-адреси хоста ПК.

Налаштуйте статичну IP-адресу, маску підмережі та шлюз за усталеним налаштуванням для PC-A, PC-B і PC-C, як показано на таблиці IP-адресації.

Крок 7. Перевірте основне підключення до мережі.

a. Пінг від R1 до R3. Якщо ping не вдається, перш ніж продовжити, усуньте неполадки в основних конфігураціях пристрою.

b. Проведіть ping з PC-A в локальній мережі R1 на PC-B і PC-C у

локальних мережах R3. Якщо ping не вдається, перш ніж продовжити, усуньте неполадки в основних конфігураціях пристрою.

Примітка. Якщо ви можете виконати ping з PC-A на PC-C, ви продемонстрували, що наскрізну IP-доступність було досягнуто. Якщо ви не можете виконати ping, але інтерфейси пристрою UP, а IP-адреси правильні, скористайтеся команди show interface, show ip interface та show ip route, щоб допомогти визначити проблеми.

Крок 8: Налаштуйте обліковий запис користувача, зашифровані паролі та криптоключі для SSH. Для паролів у цьому завданні встановлено мінімум 10 символів, але вони відносно прості. У виробничій мережі рекомендуються більш складні паролі.

a. Налаштуйте мінімальну довжину пароля за допомогою команди Security passwords, щоб встановити мінімальний пароль довжиною 10 символів.

R1(config)# security passwords min-length 10

b. Налаштуйте доменне ім’я.

R1(config)# ip domain-name netsec.com

c. Налаштуйте криптоключі для SSH

R1(config)# crypto key generate rsa general-keys modulus 1024

d. Налаштуйте обліковий запис користувача admin01 за допомогою algorithm-type scrypt для шифрування та пароля cisco12345.

R1(config)# username admin01 algorithm-type scrypt secret cisco12345

e. Налаштуйте рядкову консоль 0, щоб використовувати локальну базу даних користувачів для входу в систему. Для додаткової безпеки команда exec-timeout змушує рядок вийти з системи через 5 хвилин бездіяльності. Команда logging synchronous запобігає перериванню введення команди повідомленнями консолі. З метою уникнення повторної автентифікації під час виконання лабораторної роботи, команду exec-timeout можна встановити на 0 0, що запобігає його закінченню; однак така практика не вважається безпечною.

R1(config)# line console 0 R1(config-line)# login local R1(config-line)# exec-timeout 5 0

R1(config-line)# logging synchronous

f. Налаштуйте рядок aux 0, щоб використовувати локальну базу даних користувачів для входу в систему.

R1(config)# line aux 0 R1(config-line)# login local

R1(config-line)# exec-timeout 5 0

g. Налаштуйте рядок vty 0 4, щоб використовувати локальну базу даних користувачів для входу та обмежити доступ лише до з'єднань SSH.

R1(config)# line vty 0 4 R1(config-line)# login local

R1(config-line)# transport input ssh R1(config-line)# exec-timeout 5 0

h. Налаштуйте пароль увімкнення з надійним шифруванням.

R1(config)# enable algorithm-type scrypt secret class12345

Крок 9. Збережіть базову робочу конфігурацію для всіх трьох маршрутизаторів.

Збережіть поточну конфігурацію до конфігурації запуску з привілейованого підказки EXEC

R1# copy running-config startup-config

Частина 2: Налаштування брандмауера політики на основі зони (ZPF)

У цій частині ви створите брандмауер на основі політики зони на R3 за допомогою інтерфейсу командного рядка (CLI), він діє не тільки як маршрутизатор, а й як брандмауер. R3 наразі відповідає за маршрутизацію пакетів для трьох мереж, підключених до нього. Ролі інтерфейсу R3 налаштовуються таким чином:

— G0/0/0 підключено до Інтернету. Оскільки це загальнодоступна мережа, вона вважається ненадійною мережею і повинен мати найнижчий рівень безпеки.

— G0/0/1.3 підключено до внутрішньої мережі. Тільки авторизовані користувачі мають доступ до цієї мережі. На додачу, ресурси життєво важливих установ також знаходяться в цій мережі. Внутрішню мережу слід вважати надійною мережею і вона повинна мати найвищий рівень безпеки.

— G0/0/1.33 підключено до конференц-залу. Конференц-зал використовується для проведення зустрічей з людьми, які не є частиною організації.

Політика безпеки, яка повинна застосовуватися R3, коли він діє як брандмауер, диктує, що:

— Не можна допускати трафік, ініційований з Інтернету, у внутрішні мережі або мережі конференц- залів.

— Повернення інтернет-трафіка (повернення пакетів, що надходять з Інтернету на сайт R3, у відповідь на запити, що надходять з будь-якої з мереж R3), має бути дозволено.

— Комп'ютери у внутрішній мережі R3 вважаються довіреними і мають право ініціювати будь-який тип трафіка (трафік на основі TCP, UDP або ICMP).

— Комп'ютери в мережі конференц-залу R3 вважаються ненадійними і мають право ініціювати лише веб-трафік (HTTP або HTTPS) до Інтернету.

— Заборонений трафік між внутрішньою мережею та мережею конференц-залу. Немає жодних гарантій щодо стану гостьових комп'ютерів у мережі конференц-залів. Такий комп'ютери можуть бути заражені зловмисним програмним забезпеченням і намагатися розсилати спам або інший шкідливий трафік.

Крок 1. Перевірте мережеве підключення.

На цьому кроці ви перевірите наскрізне мережеве підключення перед впровадженням ZPF. Відкрийте вікно конфігурації

а. Проведіть ping з R1 на R3, використовуючи обидві IP-адреси інтерфейсу G0/0/1 R3 (192.168.3.1 і 192.168.33.1). Якщо ping не вдається, перш ніж продовжити, усуньте неполадки в основних конфігураціях пристрою.

б. Проведіть ping з PC-A в локальній мережі R1 на PC-C у локальній мережі конференц-залу R3. Якщо ping не вдається, перш ніж продовжити, усуньте неполадки в основних конфігураціях пристрою.

с. Проведіть ping з PC-A у локальній мережі R1 на PC-B у внутрішній локальній мережі R3. Якщо ping не вдається, перш ніж продовжити, усуньте неполадки в основних конфігураціях пристрою.

Крок 2. Відобразіть поточні конфігурації R3.

На цьому кроці перевірите запущені конфігурації R3 перед впровадженням

ZPF.

a. Виконайте команду show ip interface brief на R3, щоб переконатися, що правильно призначено IP- адреси. Використовуйте таблицю адрес, щоб перевірити адреси.

б. Видайте команду show ip route на R3, щоб переконатися, що він має статичний маршрут за усталеним налаштуванням, що вказує на інтерфейс G0/0/1 R2.

c. Виконайте команду show run, щоб переглянути поточну базову конфігурацію на R3.

Крок 3: Створення зон безпеки.

Зона безпеки – це група інтерфейсів зі схожими властивостями та вимогами безпеки. Наприклад, якщо маршрутизатор має три інтерфейси, які підключені до внутрішніх мереж, усі три інтерфейси можна помістити в одну зону під назвою «внутрішня». Оскільки всі властивості безпеки налаштовані на зону, а не на індивідуальний інтерфейс маршрутизатора, дизайн брандмауера набагато більш масштабований.

R3 має три інтерфейси: один підключений до внутрішньої надійної мережі, один підключений до мережі конференц-залу, а інший підключений до Інтернету. Оскільки всі три мережі мають різні вимоги та властивості безпеки, ми створимо три різні зони безпеки.

Зони безпеки створюються в режимі глобальної конфігурації, і команда дозволяє визначити назву зони. У R3 створіть три зони з іменами INSIDE, CONFROOM та INTERNET:

R3(config)# zone security INSIDE R3(config)# zone security CONFROOM R3(config)# zone security INTERNET

Крок 4: Створення політики безпеки

Перш ніж ZPF зможе вирішити, чи слід дозволити чи заборонити певний специфічний трафік, йому має бути повідомлено, який трафік має бути розглянуто. Cisco IOS використовує карти класів для вибору трафіка.

Цікавий трафік (Interesting traffic) – це загальне позначення трафіка, який вибрано за допомогою карти класів. У той час як карти класів вибирають трафік,

не їхня робота вирішувати, що станеться з вибраним трафіком; Карти політики вирішують долю вибраного трафіка.

Політики трафіка ZPF визначаються як карти політик і використовують карти класів для вибору трафіка. Іншими словами, карти класів визначають, який трафік потрібно контролювати, тоді як карти політики визначають дію, яку потрібно виконати з вибраним трафіком.

Карти політики можуть скидати, пропускати або перевіряти рух. Оскільки ми хочемо, щоб брандмауер спостерігав за трафіком, який рухається в напрямку пар зон, ми створимо карти політики перевірки. Перевірте карти політики, які дозволяють динамічно обробляти зворотний трафік.

Спочатку створіть карти класів. Після створення карт класів створіть карти політики та прикріпіть файли карти класів до карт політики.

а. Створіть карту класів, щоб узгодити трафік, який буде дозволено із зони INSIDE в зону INTERNET. Оскільки ми довіряємо зоні INSIDE, ми дозволяємо всі основні протоколи.

У наведених нижче командах перший рядок створює карту класів для перевірки. Ключове слово **match-any** повідомляє маршрутизатору, що будь-який з операторів протоколу відповідності буде кваліфіковано як успішний збіг, що призведе до застосування політики. Результатом є збіг для пакетів TCP, UDP або ICMP. Команда відповідності **match** стосується певних протоколів, які підтримує Cisco NBAR. Для отримання додаткової інформації виконайте пошук в Інтернеті для Cisco NBAR.

R3(config)# class-map type inspect match-any INSIDE_PROTOCOLS R3(config-cmap)# match protocol tcp

R3(config-cmap)# match protocol udp R3(config-cmap)# match protocol icmp

б. Аналогічно створіть карту класів, щоб відповідати трафіка, який буде дозволено із зони CONFROOM до зони ІНТЕРНЕТ. Оскільки ми не повністю довіряємо зоні CONFROOM, ми повинні обмежити те, що сервер може надсилати в Інтернет:

R3(config)# class-map type inspect match-any CONFROOM_PROTOCOLS R3(config-cmap)# match protocol http

R3(config-cmap)# match protocol https R3(config-cmap)# match protocol dns

c. Тепер, коли карти класів створені, ви можете створити карти політик.

У наведених нижче командах перший рядок створює карту політики перевірки під назвою INSIDE_TO_INTERNET. Другий рядок прив'язує раніше створену карту класів INSIDE_PROTOCOLS до карти політики.

Усі пакети, які відповідають карті класів INSIDE_PROTOCOLS, будуть піддані діям, здійсненим картою політики INSIDE_TO_INTERNET. Нарешті, третій рядок визначає фактичну дію, яку ця карта політик застосовуватиме до відповідних пакетів. У цьому випадку будуть перевірені відповідні пакети.

Наступні три рядки створюють подібну карту політики під назвою CONFROOM_TO_INTERNET і долучають карту класів CONFROOM_PROTOCOLS.

Команди такі:

R3(config)# policy-map type inspect INSIDE_TO_INTERNET R3(config-pmap)# class type inspect INSIDE_PROTOCOLS R3(config-pmap-c)# inspect

R3(config)# policy-map type inspect CONFROOM_TO_INTERNET R3(config-pmap)# class type inspect CONFROOM_PROTOCOLS R3(config-pmap-c)# inspect

Крок 5. Створіть пари зон

Пара зон дозволяє вказати політику односпрямованого брандмауера між двома зонами безпеки. Наприклад, загальноприйнята політика безпеки диктує, що внутрішня мережа може ініціювати будь-який трафік до Інтернету, але не можна дозволяти трафіка, що походить з Інтернету, досягати внутрішньої мережі. Для цієї політики трафіка потрібна лише одна пара зон, INTERNAL to INTERNET Оскільки пари зон визначають односпрямований потік трафіка, потрібно створити іншу пару зон, якщо Інтернет-ініційований трафік має надходити в напрямку INTERNET to INTERNAL.

Зверніть увагу, що Cisco ZPF можна налаштувати для перевірки трафіка, який рухається в напрямку, визначеному парою зон. У цій ситуації брандмауер спостерігає за трафіком і динамічно створює правила, що дозволяють зворотному або пов’язаному з ним трафіка протікати назад через маршрутизатор.

Щоб визначити пару зон, скористайтеся командою zone-pair security. Напрямок руху визначається зонами джерела та призначення.

Для цієї лабораторної роботи ви створите дві пари зон:

INSIDE_TO_INTERNET: Дозволяє трафік виходити з внутрішньої мережі в Інтернет. CONFROOM_TO_INTERNET: Дозволяє доступ до Інтернету з мережі ConfRoom.

a. Створіть пари зон:

R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET R3(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination INTERNET

б. Переконайтеся, що пари зон було створено правильно, виконавши команду show zone-pair security. Зверніть увагу, що з парами зон поки що не пов’язано жодної політики. На наступному кроці до пар зон будуть застосовані політики безпеки.

R3# show zone-pair security

Zone-pair name INSIDE_TO_INTERNET

Source-Zone INSIDE Destination-Zone INTERNET service-policy not configured

Zone-pair name CONFROOM_TO_INTERNET

Source-Zone CONFROOM Destination-Zone INTERNET service-policy not configured

Крок 6: Застосування політики безпеки

a. Як останній крок налаштування, застосуйте карти політики до пар зон: R3(config)# zone-pair security INSIDE_TO_INTERNET

R3(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET R3(config)# zone-pair security CONFROOM_TO_INTERNET

R3(config-sec-zone-pair)# service-policy type inspect CONFROOM_TO_INTERNET

б. Видайте команду show zone-pair security ще раз, щоб перевірити конфігурацію зони-пари. Зверніть увагу що тепер відображаються служби-

політики:

R3# show zone-pair security

Zone-pair name INSIDE_TO_INTERNET

Source-Zone INSIDE Destination-Zone INTERNET service-policy INSIDE_TO_INTERNET

Zone-pair name CONFROOM_TO_INTERNET

Source-Zone CONFROOM Destination-Zone INTERNET service-policy CONFROOM_TO_INTERNET

c. Щоб отримати більше інформації про пари зон, їх карти політик, карти класів і лічильники збігів, скористайтеся командою show policy-map type inspect zone-pair:

R3# show policy-map type inspect zone-pair

```
 Class-map: CONFROOM_PROTOCOLS (match-any)
   Match: protocol http
   Match: protocol https
   Match: protocol dns
   Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     Last half-open session total 0

 Class-map: class-default (match-any)
   Match: any
   Drop (default action)
     0 packets, 0 bytes
Zone-pair: INSIDE_TO_INTERNET
Service-policy inspect : INSIDE_TO_INTERNET
```

Рисунок 22. Приклад налаштування class-map і service-policy у Zone-Based Policy Firewall

Zone-pair: CONFROOM_TO_INTERNET Service-policy inspect : CONFROOM_TO_INTERNET

```
Class-map: INSIDE_PROTOCOLS (match-any)
  Match: protocol tcp
  Match: protocol udp
  Match: protocol icmp
  Inspect
    Session creations since subsystem startup or last reset 0
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:0:0]
    Last session created never
    Last statistic reset never
    Last session creation rate 0
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    0 packets, 0 bytes <output omitted>
```

Рисунок 23. Конфігурація class-map для протоколів у внутрішній зоні (INSIDE_PROTOCOLS)

Крок 7. Призначте інтерфейси відповідним зонам безпеки

Інтерфейси (фізичні та логічні) призначаються зонам безпеки за допомогою команди zone-member security.

a. Призначте G0/0 R3 до зони безпеки CONFROOM:

R3(config)# interface g0/0/1.33

R3(config-if)# zone-member security CONFROOM б. Призначте G0/1 R3 до зони безпеки INSIDE:

R3(config)# interface g0/0/1.3

R3(config-if)# zone-member security INSIDE

c. Призначте R3 S0/0/1 зоні безпеки INTERNET:

R3(config)# interface g0/0/0

R3(config-if)# zone-member security INTERNET

Крок 8. Перевірте призначення зони

a. Видайте команду **show zone security**, щоб переконатися, що зони створено належним чином, а інтерфейси правильно призначені:

```
R3# show zone security
zone self
  Description: System defined zone

zone service
  Description: System defined zone

zone INSIDE
  Member Interfaces:
    GigabitEthernet0/0/1.3

zone CONFROOM
  Member Interfaces:
    GigabitEthernet0/0/1.33

zone INTERNET
  Member Interfaces:
    GigabitEthernet0/0/0
```

Рисунок 24. Результат виконання команди show zone security на маршрутизаторі R3

б. Незважаючи на те, що жодних команд для створення «власної» зони не було, у наведених вище результатах вона все одно відображається.

Питання: Чому R3 відображає зону під назвою «self»? Яке значення має ця зона? (відповідь подати у звіті).

Частина 3: Перевірка функціональності брандмауера ZPF

Крок 1: Трафік, що надходить з Інтернету

а. Щоб перевірити ефективність брандмауера, відправте ping PC-B з PC-A. У PC-A відкрийте командний рядок і введіть ping до 192.168.3.3. PC-A:\> ping 192.168.3.3

Питання: Пінг був успішним? Поясніть.

б. Відправте ping PC-C з PC-A. У PC-A відкрийте командне вікно та відправте ping 192.168.33.3. PC-A:\> ping 192.168.1.3

Питання: Пінг був успішним? Поясніть

в. Відправте ping PC-A з PC-B. У PC-B відкрийте командне вікно та введіть ping на 192.168.1.3 PC-B:\> ping 192.168.1.3

Питання: Пінг був успішним? Поясніть.

d. Відправте ping PC-A з PC-C. У PC-C відкрийте командне вікно та

відправте ping на 192.168.1.3 PC-C:\> ping 192.168.1.3

Питання: Пінг був успішним? Поясніть.

Крок 2: Самоперевірка зони

а. З інтерфейсу G0/0/1.3 PC-A ping R3:

Питання: PC-A:\> ping 192.168.3.1 Пінг був успішним? Чи коректна (правильна) поведінка? Поясніть.

б. З інтерфейсу G0/0/1.3 PC-C ping R3: PC-C:\> ping 192.168.3.1 Питання: Пінг був успішним? Чи коректна (правильна) поведінка? Поясніть.

в. Створіть належну пару зон, карти класів і політики та налаштуйте R3, щоб запобігти Інтернет трафіка від досягнення самої ж зони (Create the proper zone-pair, class-maps, and policy-maps and configure R3 to prevent Internet originating traffic from reaching the Self Zone).

Кілька інтерфейсів в одній зоні

Однією з переваг брандмауерів ZPF є те, що вони добре масштабуються в порівнянні з класичним брандмауером. Якщо новий інтерфейс брандмауера буде додано ті самі вимоги безпеки, адміністратор може просто додати новий інтерфейс як член існуючої зони безпеки.

Однак деякі версії IOS не дозволяють пристроям, підключеним до різних інтерфейсів однієї зони, зв'язуватися за усталеним налаштуванням. У цих випадках слід створити пару зон, використовуючи ту саму зону, що й джерело та місце призначення. Трафік між однаково зонованими інтерфейсами завжди буде двонаправленим через те, що вихідні та цільові зони пари зон однакові. Через це немає необхідності перевіряти трафік, щоб забезпечити автоматичну обробку зворотного трафіка; зворотний трафік завжди буде дозволений, оскільки він завжди відповідатиме визначенню пари зон. У цьому випадку карта політики повинна мати дію пропуску замість перевірки. Через дію пропуску маршрутизатор не буде перевіряти пакети, які відповідають карті політики, він просто перенаправить їх до місця призначення.

У контексті цієї лабораторної роботи, якби R3 мав інтерфейс G0/0/1.2, також призначений для зони INSIDE, а версія IOS маршрутизатора не підтримувала дозвіл трафіка між інтерфейсами, налаштованими на ту саму зону,

додаткова конфігурація виглядала б так:

Нова пара зон: **Inside to Inside** дозволяє маршрутизувати трафік між внутрішніми довіреними інтерфейсами.

Створення карти політики:

R3(config)# policy-map type inspect inside R3(config-pmap)# class class-default R3(config-pmap-c)# pass

```
R3(config)# zone-pair security INSIDE source INSIDE destination INSIDE
R3(config-sec-zone-pair)# service-policy type inspect inside
```

To verify the existence of the new pair, use **show zone-pair security:**

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET
Zone-pair name INSIDE
    Source-Zone INSIDE Destination-Zone INSIDE
    service-policy inside
```

Рисунок 25. Результат виконання команди show zone-pair security на маршрутизаторі R3

Створення пари зон і призначення їй нової карти політики. Зверніть увагу, що зона INSIDE є одночасно джерелом і призначенням пари зон: Зведена таблиця інтерфейсу маршрутизатора:

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Примітка. Щоб дізнатися, як налаштовано маршрутизатор, подивіться на інтерфейси, щоб визначити тип маршрутизатора та кількість інтерфейсів у маршрутизатора. Немає способу ефективно перерахувати всі комбінації конфігурацій для кожного класу маршрутизатора. Ця таблиця містить ідентифікатори для можливих комбінацій Ethernet і послідовного інтерфейсу в пристрої. Таблиця не містить іншого типу інтерфейсу, навіть якщо певний

маршрутизатор може містити його. Прикладом цього може бути інтерфейс ISDN BRI. Рядок у дужках – це юридична абревіатура, яка може використовуватися в командах Cisco IOS для представлення інтерфейсу.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (AAA, автентифікація/авторизація, e-mail, FTP – 1–2 сторінки).
4. Практичну частину, що включає:

— опис налаштування AAA-сервера (створені користувачі, скріншоти/схематичні рисунки);

— опис налаштування бездротового доступу на HQ-Laptop-1, HQ-Laptop-2 та отриманих IP-адрес;

— опис налаштування поштового сервера та клієнтів, приклад надісланого й отриманого листа;

— опис налаштування FTP-сервера, створених облікових записів та результатів виконання команд get/put/delete/rename для різних користувачів.

5. Висновки:

— узагальнення щодо ролі AAA та контролю доступу у захисті мережевих служб;

— отримані практичні навички;

— рекомендації щодо побудови безпечної архітектури доступу до Wi-Fi, e-mail та FTP.

6. Список використаних джерел згідно з вимогами до оформлення бібліографічних посилань.

4. Підбиття підсумків заняття

— обговорення результатів налаштування AAA, поштових та FTP-служб;

— аналіз правильності реалізації прав доступу користувачів;

— оцінювання повноти та якості звітів, уміння пояснювати вплив налаштувань на безпеку;

— формулювання узагальнених висновків щодо значення комплексного підходу до контролю доступу в мережі.

6. Список рекомендованої літератури

Основна:

1. Cisco IOS Zone-Based Policy Firewall Configuration Guide [Electronic resource]. – 2023. – Access mode: https://www.cisco.com.

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022. – 45 p. – ISO.

3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. – Geneva : ISO, 2022. – 118 p. – ISO.

4. NIST SP 800-41 Rev.1. Guidelines on Firewalls and Firewall Policy [Electronic resource]. – Gaithersburg : NIST, 2024. – Access mode: https://csrc.nist.gov

5. Next-Generation Firewalls – Security Practices and Use Cases [Electronic resource]. – Heraklion : ENISA, 2023. – Access mode: https://www.enisa.europa.eu

Додаткова:

1. Cheswick W., Bellovin S., Rubin A. Firewalls and Internet Security: Repelling the Wily Hacker. – 2nd ed. – Boston : Addison-Wesley, 2023. – 720 p.

2. Scarfone K., Hoffman P. Guidelines for Network Security Testing : NIST SP 800-115. – Gaithersburg : NIST, 2023. – 85 p.

3. Northcutt S. Network Intrusion Detection: An Analyst's Handbook. – 4th ed. – Indianapolis : New Riders, 2022. – 612 p.

4. Behl A., Belapure N. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford : Oxford University Press, 2023. – 296 p.

Інформаційні ресурси

1. Cisco Networking Academy [Electronic resource]. – Access mode: https://www.netacad.com

2. NIST Cybersecurity Framework [Electronic resource]. – Access mode: https://www.nist.gov/cyberframework

3. Віртуальний університет ЛДУБЖД [Електронний ресурс]. URL: https://virt.ldubgd.edu.ua

ЛАБОРАТОРНА РОБОТА № 4

Тема: налаштування безпеки бездротових мереж WLAN.

Мета: навчитися будувати локальну мережу з використанням бездротових технологій, здійснювати налаштування параметрів безпеки WLAN, підключати дротові та бездротові клієнти, конфігурувати точку доступу та змінювати базові мережеві параметри маршрутизатора..

Місце проведення: згідно з розкладом.

Час: 8 годин.

Основні поняття: *Бездротова локальна мережа (WLAN)* – це мережа, в якій передавання даних здійснюється за допомогою радіохвиль у стандарті IEEE 802.11.

SSID (Service Set Identifier) – ідентифікатор бездротової мережі, який використовується для її ідентифікації клієнтськими пристроями.

WPA2 (Wi-Fi Protected Access 2) – стандарт захисту WLAN, що використовує стійке шифрування AES та механізм автентифікації користувачів.

Точка доступу (Access Point, AP) – пристрій, який забезпечує підключення бездротових клієнтів до дротової мережі.

DHCP (Dynamic Host Configuration Protocol) – протокол, що автоматично призначає IP-адреси мережевим пристроям.

Pre-Shared Key (PSK) – попередньо заданий спільний ключ для автентифікації користувачів у бездротовій мережі.

Обладнання та програмне забезпечення: персональні комп’ютери / ноутбуки з доступом до мережі; операційна система: Windows / Linux (на розсуд викладача); симулятор мережі Cisco Packet Tracer (актуальна версія); веббраузер для роботи з електронним курсом та мережевими сервісами (Chrome / Firefox / Edge або аналог); текстовий редактор (MS Word / LibreOffice Writer / Google Docs або аналог); електронний навчальний курс у віртуальному університеті ЛДУБЖД.

План

1. Організаційні заходи

- повідомлення теми та мети лабораторного заняття;

- мотивація навчальної діяльності: значення захисту бездротових мереж Wi-Fi для забезпечення конфіденційності, цілісності та доступності інформації;
- ознайомлення з місцем розташування матеріалів лабораторної роботи в електронному навчальному середовищі «Віртуальний університет»;
- інструктаж з техніки безпеки під час роботи з комп'ютерною технікою та програмним забезпеченням;
- пояснення порядку оформлення, подання та захисту звіту, критеріїв оцінювання.

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: знання базових понять локальних комп'ютерних мереж (LAN, IP-адресація, DHCP, шлюз за усталеним налаштуванням); уявлення про принципи роботи бездротових мереж стандарту IEEE 802.11; розуміння основних механізмів захисту WLAN (SSID, фільтрація за MAC-адресами, WPA2-PSK, шифрування AES); уявлення про роботу бездротового маршрутизатора, точки доступу, клієнтських пристроїв.

Перелік дидактичних одиниць для перевірки: поняття WLAN, SSID, точка доступу (AP), бездротовий маршрутизатор; стандарти 802.11b/g/n/ac, діапазони частот 2,4 ГГц та 5 ГГц; режими захисту: WEP, WPA, WPA2, WPA3 (оглядово); DHCP у локальній мережі, роль маршрутизатора як DHCP-сервера; призначення попередньо спільного ключа (Pre-Shared Key, PSK) у режимі WPA2-Personal.

Питання для усного опитування / самоконтролю:

1. Що таке SSID і для чого він використовується в бездротових мережах?
2. У чому принципова відмінність між дротовою LAN та бездротовою WLAN?
3. Які основні вразливості беззахисної (відкритої) Wi-Fi мережі?
4. Чим відрізняються режими безпеки WEP, WPA та WPA2?
5. Що таке WPA2-PSK і чому важливо використовувати складну парольну фразу?
6. Яку роль відіграє DHCP у роботі бездротового маршрутизатора?
7. Для чого використовують окрему точку доступу (AP), якщо вже є бездротовий маршрутизатор?

3. Формування професійних умінь та навичок

У ході виконання лабораторної роботи здобувачі мають:

— навчитися під’єднувати адміністраторський ПК до бездротового маршрутизатора та отримувати IP-адресу через DHCP;

— опанувати навички входу до вебінтерфейсу маршрутизатора та зміни базових параметрів (LAN-адреса, DHCP-пул, DNS, пароль доступу);

— налаштувати параметри бездротової мережі (SSID, канал, режим безпеки WPA2-PSK, парольну фразу);

— під’єднати бездротових клієнтів до WLAN, перевірити доступ до зовнішнього ресурсу (www.cisco.pka);

— налаштувати точку доступу для розширення покриття бездротової мережі;

— змінити внутрішню адресу маршрутизатора та діапазон DHCP, оновити IP-адреси клієнтів та перевірити працездатність мережі після зміни параметрів.

3.1. Практична частина

У цьому завданні ви налаштуєте бездротовий маршрутизатор і точку доступу для обслуговування бездротових клієнтів і забезпечення маршрутизації IP-пакетів. Крім того, ви також оновите деякі з налаштувань маршрутизатора за усталеним налаштуванням.

Частина 1: Під'єднання до бездротового маршрутизатора

Крок 1: Під'єднайте комп'ютер Admin до бездротового маршрутизатора WR.

a. Під’єднайте Admin до WR, використовуючи прямий кабель Ethernet, через порти Ethernet. У нижньому лівому куті екрана середовища Packet Tracer виберіть піктограму блискавки – пункт Connections (З'єднання). Виберіть кабель Copper Straight-Through (Мідний прямий), зображений у вигляді суцільної чорної лінії.

b. Коли курсор перейде в режим приєднання, натисніть на Admin і виберіть FastEthernet0. Натисніть на WR і виберіть доступний порт Ethernet, щоб під'єднати інший кінець кабеля. WR працюватиме як комутатор для пристроїв, під'єднаних до локальної мережі, і як маршрутизатор для з'єднання з Інтернетом.

Комп'ютер Admin тепер під'єднаний до мережі LAN (GigabitEthernet 1). Коли у вікні Packet Tracer з'являться зелені трикутники з обох сторін з'єднання між Admin та WR, переходьте до наступного кроку.

Примітка: Якщо зелених трикутників немає, переконайтесь, що вибрано Show Link Lights (Показувати індикатори з'єднання) в меню Options (Сервіс) > Preferences (Параметри). Можна також натиснути на Fast Forward Time (Прискорити) прямо над вікном Connections (З'єднання) на жовтій панелі.

Крок 2: Налаштуйте комп'ютер Admin для використання протоколу DHCP.

Щоб потрапити на сторінку керування WR, комп'ютер Admin повинен бути під'єднаний до мережі. Бездротовий маршрутизатор зазвичай виконує функції DHCP-сервера, який за усталеним налаштуванням увімкнений у мережі LAN. Admin отримає інформацію про IP-адресу від DHCP-сервера на маршрутизаторі WR.

a. Натисніть на Admin і виберіть вкладку Desktop (Робочий стіл).

b. Натисніть на IP Configuration (Налаштування IP-адреси) і виберіть DHCP.

Запитання :

1. Яка IP-адреса у цього комп’ютера?
2. Напишіть тут свою відповідь.
3. Яка маска підмережі у цього комп'ютера?

Напишіть тут свою відповідь.

4. Яка адреса шлюзу за усталеним налаштуванням (default gateway) у цього комп'ютера? Напишіть тут свою відповідь.

c. Закрийте вікно IP Configuration (Налаштування IP-адреси).

Примітка: Значення можуть змінюватися у межах діапазону адрес мережі при нормальній роботі DHCP.

Крок 3: Під'єднайтесь до вебінтерфейсу WR.

a. На вкладці Desktop (Робочий стіл) на комп'ютері Admin виберіть Web Browser.

b. В поле URL-адреси введіть 192.168.0.1, щоб відкрити вебсторінку

налаштування бездротового маршрутизатора.

c. Введіть admin як ім’я користувача та пароль.

d. Під заголовком Network Setup (Налаштування мережі) на сторінці Basic Setup (Базове налаштування) перегляньте діапазон IP-адрес DHCP-сервера.

Питання: Чи знаходиться IP-адреса комп'ютера Admin в цьому діапазоні? Чи повинна знаходитись? Поясніть свою відповідь.

Крок 4: Налаштуйте Інтернет-порт маршрутизатора WR.

Цей крок передбачає налаштування маршрутизації на маршрутизаторі WR для надсилання пакетів від бездротових клієнтів до Інтернету. Для цього необхідно налаштувати порт Internet на маршрутизаторі WR.

a. На вкладці Internet Setup (Налаштування Інтернет-з'єднання)у верхній частині сторінки Basic Setup (Базове налаштування) змініть спосіб налаштування IP-адреси Internet з Automatic Configuration – DHCP (Автоматичне налаштування - DHCP) на Static IP (Статична IP-адреса).

b. Введіть IP-адресу, щоб призначити її Інтернет-інтерфейсу:

Internet IP Address (IP-адреса Internet): 209.165.200.225

Subnet Mask (Маска підмережі): 255.255.255.252

Default Gateway (Шлюз за усталеним налаштуванням): 209.165.200.226

DNS Server (DNS-сервер): 209.165.201.1

c. Прокрутіть донизу сторінки та натисніть Save Settings (Зберегти параметри).

Примітка: При отриманні повідомлення Request Timeout закрийте вікно Admin і дочекайтеся, коли помаранчеві індикатори перетворяться на зелені трикутники. Щоб прискорити процес, натисніть на кнопку перемотування вперед. Потім знову під'єднайтеся до маршрутизатора WR з веббраузера Admin, виконавши процедуру, описану в Кроці 3.

d. Щоб перевірити з'єднання, відкрийте новий веббраузер і перейдіть на сервер www.cisco.pka.

Примітка. Під'єднання до мережі може тривати кілька секунд. Для прискорення процесу натисніть Fast Forward Time (Прискорення) або Alt+D.

Частина 2: Налаштування параметрів бездротового з'єднання

У цьому завданні ви налаштуєте параметри бездротового з'єднання суто для частоти 2,4 ГГц.

Крок 1: Налаштуйте ідентифікатор SSID маршрутизатора WR.

a. Перейдіть у графічний інтерфейс WR на 192.168.0.1 у веббраузері комп'ютера Admin.

b. Перейдіть до Wireless (Бездротове з'єднання) > Basic Wireless Settings (Основні параметри бездротової мережі).

c. Змініть Network Name (SSID) на aCompany тільки для частоти 2,4 ГГц. Зверніть увагу, що ідентифікатор SSID чутливий до регістру.

d. Змініть Standard Channel на 6 – 2.437 GHz.

e. У цьому завданні вимкніть обидві частоти 5 ГГц. Інші параметри залишіть без змін.

f. Прокрутіть донизу вікна і натисніть Save Settings (Зберегти параметри).

Крок 2: Налаштуйте параметри безпеки бездротового зв'язку.

У цьому завданні ви налаштуєте параметри безпеки бездротової мережі, використовуючи режим безпеки WPA2 з шифруванням і парольною фразою.

a. Перейдіть до Wireless (Бездротове з'єднання)> Wireless Security (Безпека бездротової мережі).

b. Під заголовком 2.4 GHz виберіть для режиму безпеки Security Mode налаштування WPA2 Personal.

c. У полі Encryption (Шифрування) залишіть налаштування за усталеним налаштуванням AES.

d. У полі Passphrase введіть парольну фразу Cisco123!.

e. Натисніть Save Settings (Зберегти параметри).

f. Перевірте, чи налаштування на сторінках базових параметрів бездротового доступу Basic Wireless Settings і безпеки бездротового доступу Wireless Security правильні та збережені.

Крок 3: Під'єднайте бездротових клієнтів.

a. Відкрийте Laptop1. Виберіть вкладку Desktop. Натисніть на PC Wireless.

b. Виберіть вкладку Connect. За необхідності натисніть Refresh. Виберіть ім'я бездротової мережі aCompany.

c. Введіть пароль або парольну фразу, налаштовану на попередньому кроці. Введіть Cisco123! у полі PSK (Наперед визначений спільний ключ, Pre-Shared Key) і натисніть Connect. Закрийте вікно PC Wireless.

d. Відкрийте веббраузер і переконайтесь, що ви можете перейти на сервер www.cisco.pka.

e. Повторіть наведені вище кроки для під'єднання ноутбука Laptop2 до бездротової мережі.

Частина 3: Під'єднання бездротових клієнтів до точки доступу.

Точка доступу (Access Point, AP) – це пристрій, що дозволяє розширити покриття локальної бездротової мережі. Точка доступу під'єднується до дротового маршрутизатора за допомогою кабелю Ethernet, щоб передавати сигнал у потрібне місце.

Крок 1: Налаштуйте точку доступу.

a. З'єднайте Port 0 точки доступу AP з доступним портом Ethernet бездротового маршрутизатора WR за допомогою прямого кабелю Ethernet.

b. Натисніть на AP. Виберіть вкладку Config.

c. Під заголовком INTERFACE виберіть Port 1.

d. У поле SSID введіть aCompany.

e. Виберіть WPA2-PSK. Введіть парольну фразу Cisco123! у полі Pass Phrase.

f. Залишіть AES як метод шифрування Encryption Type за усталеним налаштуванням.

Крок 2: Під'єднайте бездротових клієнтів.

a. Відкрийте Laptop3. Виберіть вкладку Desktop. Натисніть PC Wireless.

b. Виберіть вкладку Connect. За необхідності натисніть Refresh. Виберіть ім'я бездротової мережі Wireless Network Name aCompany з найсильнішим сигналом (Channel 1) і натисніть Connect.

c. Відкрийте веббраузер і перевірте, чи можете ви перейти на сервер www.cisco.pka.

Частина 4: Інші завдання адміністрування

Крок 1: Змініть пароль доступу до WR.

a. Перейдіть у графічний інтерфейс WR на 192.168.0.1.

b. Перейдіть до Administration > Management і змініть поточний пароль маршрутизатора Router Password на cisco.

c. Прокрутіть донизу вікна і натисніть Save Settings.

d. Для входу на бездротовий маршрутизатор використовуйте ім'я користувача admin і новий пароль cisco. Натисніть OK, щоб продовжити.

e. Натисніть Continue і перейдіть до наступного кроку.

Крок 2: Змініть діапазон DHCP-адрес на маршрутизаторі WR.

У цьому завданні ви зміните внутрішню мережну адресу з 192.168.0.0/24 на 192.168.50.0/24. Під час зміни мережної адреси LAN необхідно оновити IP-адреси пристроїв у мережах LAN і WLAN, щоб нові IP-адреси були отримані до закінчення терміну оренди.

a. Перейдіть у Setup > Basic Setup.

b. Прокрутіть вниз сторінки до параметрів налаштування мережі Network Setup.

c. Маршрутизатору Router IP призначено IP-адресу 192.168.0.1. Змініть її на 192.168.50.1. Перевірте, чи IP-адреси починаються з .100, а в пулі DHCP є 50 IP-адрес.

d. Додайте до налаштувань DHCP адресу DNS-сервера 209.165.201.1.

e. Прокрутіть донизу вікна і натисніть Save Settings.

f. Зверніть увагу, що діапазон адрес DHCP був автоматично оновлений відповідно до зміни IP-адреси. Невдовзі у веббраузері з'явиться повідомлення про закінчення часу очікування запиту Request Timeout.

Питання: Чому?

Напишіть тут свою відповідь.

g. Закрийте веббраузер на Admin.

h. У вкладці Admin Desktop, натисніть Command Prompt.

i. Введіть ipconfig /renew, щоб Admin знов отримав інформацію про IP-адресу через DHCP.

Зазначте нову IP-адресу комп'ютера Admin.

Напишіть тут свою відповідь.

j. Відкрийте веббраузер і перевірте, чи можете ви перейти на сервер www.cisco.pka.

k. Оновіть IP-адреси на інших ноутбуках і перевірте, чи можете ви перейти на сервер www.cisco.pka.

l. Зверніть увагу, що ноутбук Laptop1 під'єднаний до точки доступу AP, а не до бездротового маршрутизатора WR.

Питання: Чому?

4.Вимоги до результатів роботи та оформлення звіту

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (WLAN, SSID, WPA2, DHCP, точка доступу, маршрутизатор, IP-адресація – 1–2 сторінки).
4. Практичну частину, що включає:

— схему побудованої бездротової мережі;

— опис налаштування маршрутизатора WR (Internet-порт, DHCP, зміна IP-адреси);

— опис налаштування бездротової мережі (SSID, канал, WPA2, пароль);

— опис підключення ноутбуків Laptop1, Laptop2, Laptop3;

— опис налаштування точки доступу AP;

— результати команд ipconfig /renew;

— підтвердження доступу до ресурсу www.cisco.pka.

5. Висновки, що повинні містити:

— роль безпечних налаштувань WLAN у захисті мережі;

— отримані практичні навички;

— значення використання WPA2 та зміни стандартних параметрів маршрутизатора.

6. Список використаних джерел відповідно до вимог ДСТУ 8302:2015.

5. Підбиття підсумків заняття

Під час підбиття підсумків здійснюється:

— обговорення результатів налаштування бездротового маршрутизатора та точки доступу;

— аналіз коректності роботи DHCP та отримання IP-адрес клієнтами;

— перевірка правильності реалізації безпеки WLAN (WPA2, пароль, шифрування);

— контроль доступу до зовнішнього ресурсу;

— оцінювання повноти та якості звітів;

— оцінка вміння здобувачів пояснювати принципи роботи бездротових мереж та їх захисту;

— формулювання узагальнених висновків щодо значення безпечної конфігурації WLAN у корпоративних мережах.

6. Список рекомендованої літератури

Основна:

1. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах : навч. посіб. Київ, 2013. 435 с.

2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 213 с.

3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : ХНЕУ, 2013. 476 с.

4. Полотай О., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи // Захист інформації в інформаційно-комунікаційних системах : зб. тез III Всеукр. наук.-практ. конф. (Львів, 28 листоп. 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.

Додаткова:

1. Кавун С. В., Смірнов О. А., Столбов В. Ф. Основи інформаційної безпеки : навч. посіб. Кіровоград : КНТУ, 2012. 414 с.

2. Гарасимчук О. І., Дудикевич В. Б., Ромака В. А. Комплексні системи санкціонованого доступу : навч. посіб. Львів : Вид-во Львів. політехніки, 2010. 212 с.

3. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

Нормативні документи та стандарти:

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022.

2. NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs). – Gaithersburg : NIST, 2012.

3. IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – IEEE Standards Association.

Інформаційні ресурси:

1. Cisco Networking Academy. Офіційний сайт мережевої академії Cisco [Електронний ресурс]. URL: https://www.netacad.com

2. Електронний навчальний курс дисципліни у віртуальному університеті ЛДУБЖД.

ЛАБОРАТОРНА РОБОТА № 5

Тема: налаштування протоколу IPsec в операційній системі Windows.

Мета: вивчити принципи захисту мережевого трафіка за допомогою протоколу IPsec; навчитися створювати, редагувати та активувати політики безпеки IPsec у Windows; навчитися налаштовувати фільтри та дії фільтра для контролю мережевого трафіка; уміти перевіряти факт шифрування/захисту даних та оцінювати вплив IPsec на продуктивність системи; сформувати практичні навички використання IPsec як механізму VPN та простого міжмережевого екрана.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *Internet Protocol Security (IPsec)* – набір протоколів і механізмів, що забезпечують шифрування, цілісність та автентифікацію IP-трафіка на мережевому рівні (L3). Використовується для побудови VPN, захисту трафіка між хостами та фільтрації пакетів.

Політика безпеки IPsec (IP Security Policy) – сукупність правил, які визначають, який трафік і яким чином має бути захищений. Містить правила, списки фільтрів та дії фільтрів.

Правило IPsec (Rule) – елемент політики безпеки, який пов’язує: список фільтрів IP (до якого трафіка застосовується правило); дію фільтра (що робити з цим трафіком – дозволити, блокувати, узгоджувати безпеку); параметри автентифікації, тип з’єднання, режим роботи (тунельний / транспортний).

Список фільтрів IP (IP Filter List) – набір фільтрів, що описують трафік, до якого застосовуються правила IPsec. Може включати: IP-адресу джерела / призначення або підмережу; протокол (TCP, UDP, ICMP, Any); номер порту (HTTP – 80, HTTPS – 443, DNS – 53 тощо).

Фільтр IP (IP Filter) – конкретна умова відбору трафіка: «з такої IP-адреси на таку IP-адресу, протокол TCP, порт 80» тощо.

Дія фільтра (Filter Action) – визначає, що робити з трафіком, який відповідає фільтра: Permit – дозволити трафік без застосування IPsec; Block – заблокувати

трафік; Negotiate security – узгодити параметри захисту та застосувати IPsec (AH/ESP).

SA (Security Association) – «угода безпеки», логічний зв'язок між двома вузлами, у межах якого визначаються: алгоритми шифрування та цілісності, ключі, час життя з'єднання, режим роботи тощо. SA є однонаправленою (окремо для кожного напрямку).

Протокол AH (Authentication Header) – протокол IPsec, що забезпечує автентифікацію джерела та цілісність IP-пакета (але не забезпечує конфіденційність, тобто не шифрує дані).

Протокол ESP (Encapsulating Security Payload) – протокол IPsec, що забезпечує конфіденційність (шифрування) даних, а також, за потреби, автентифікацію та цілісність. Найчастіше використовується в сучасних конфігураціях IPsec.

Транспортний режим (Transport Mode) – режим IPsec, у якому захищається тільки корисне навантаження (payload) транспортного протоколу, а заголовок IP зберігається незмінним. Використовується для захисту трафіка «кінець-кінець» між хостами.

Тунельний режим (Tunnel Mode) – режим IPsec, у якому шифрується весь вихідний IP-пакет, який інкапсулюється у новий IP-пакет. Використовується для побудови VPN-тунелів між шлюзами (gateway–gateway, gateway-host).

IKE (Internet Key Exchange) – протокол, що використовується для автоматичного узгодження параметрів безпеки (SA) та безпечного обміну криптографічними ключами між вузлами IPsec.

Методи автентифікації в IPsec (у Windows): Kerberos – стандартний протокол автентифікації в домені Windows; Сертифікат – автентифікація на основі інфраструктури відкритих ключів (PKI); Попередньо узгоджений ключ (Preshared key) – текстовий секрет, який задається вручну на обох вузлах.

Міжмережевий екран (Firewall) – засіб захисту, що контролює та фільтрає мережеві пакети відповідно до заданих правил. Політики IPsec у Windows можуть частково виконувати функції простого міжмережевого екрана (фільтрація за IP-адресами, протоколами, портами, дією фільтра).

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до локальної мережі; операційна система: Windows 10 / Windows 11 (на розсуд викладача); права локального адміністратора на робочій станції; вбудовані засоби ОС Windows: оснастка Local Security Policy (secpol.msc); оснастка MMC – IP Security Policies on Local Computer; за потреби – друга робоча станція / віртуальна машина для тестування «клієнт–сервер»; командний рядок Windows (PowerShell або Command Prompt); текстовий редактор (MS Word / Google Docs або аналог); електронний навчальний курс дисципліни у «Віртуальному університеті» (опис завдання, скріншоти, додаткові матеріали).

План:

1. **Організаційні заходи**

— повідомлення теми, мети та очікуваних результатів лабораторної роботи;

— мотивація навчальної діяльності: роль IPsec у побудові захищених корпоративних мереж, VPN-тунелів та фільтрації трафіка;

— ознайомлення з місцем розміщення матеріалів лабораторної роботи в електронному курсі «Віртуальний університет»;

— інструктаж з техніки безпеки під час роботи з комп'ютерною технікою та налаштуваннями безпеки ОС.

2. **Контроль опорного рівня знань**

Вимоги до теоретичної готовності здобувачів: розуміння моделі OSI та ролі мережевого (3-го) рівня; знання базових понять криптографії (шифрування, цілісність, автентичність); уявлення про VPN-з'єднання, тунелювання, міжмережеві екрани; розуміння принципів роботи TCP/UDP, портів, клієнт–серверної моделі.

Перелік дидактичних одиниць для перевірки: поняття IPsec, SA (Security Association), політика безпеки, правило, фільтр, дія фільтра; протоколи AH та ESP, їх призначення; режими роботи IPsec: транспортний та тунельний; типи автентифікації в IPsec (Kerberos, сертифікати, попередній спільний ключ); призначення протоколів ICMP, HTTP/HTTPS, DNS, SQL-серверів (TCP/UDP порти).

Питання для усного опитування / самоконтролю:

1. Що таке IPsec? На якому рівні моделі OSI він працює?
2. У чому різниця між AH та ESP?
3. Чим відрізняються транспортний та тунельний режими IPsec?
4. Які типи даних можна фільтравати за допомогою політик IPsec у Windows?
5. Які ризики дозволяє зменшити використання IPsec в корпоративній мережі?

3. Формування професійних вмінь та навичок

3.1. Теоретичні відомості

Internet Protocol Security (IPsec) – це набір протоколів і механізмів захисту, що забезпечують шифрування, автентифікацію та цілісність IP-трафіка. IPsec працює на мережевому рівні (3-й рівень моделі OSI) і дозволяє захистити будь-який транспорт (TCP, UDP, ICMP тощо), незалежно від прикладного протоколу (HTTP, FTP, Telnet, RDP тощо).

Основні властивості IPsec:

— конфіденційність – забезпечується шифруванням даних;

— цілісність – забезпечується хеш-функціями та кодами автентифікації повідомлень;

— автентифікація – перевірка справжності вузлів, що обмінюються даними;

— контроль доступу – через політики та фільтри IP-трафіка.

3.1.1. Архітектура IPsec

До складу IPsec входять такі ключові компоненти:

— SA (Security Association) – однонаправлена «угода безпеки», яка визначає параметри захисту (алгоритми, ключі, тайм-аут тощо) для конкретного напрямку трафіка;

— AH (Authentication Header) – протокол, що забезпечує автентифікацію та цілісність пакета (але не конфіденційність);

— ESP (Encapsulating Security Payload) – протокол, що забезпечує конфіденційність (шифрування) та, за потреби, автентифікацію й цілісність;

— IKE (Internet Key Exchange) – протокол узгодження параметрів безпеки та обміну ключами.

— 3.1.2. Режими роботи IPsec

— Транспортний режим – шифруються (і/або хешуються) тільки корисні дані (payload) транспортного протоколу; заголовок IP зберігається. Використовується для захисту трафіка «кінець-кінець» (host-host).

— Тунельний режим – шифрується весь IP-пакет, який інкапсулюється у новий IP-пакет. Використовується для побудови VPN-тунелів між шлюзами (gateway-gateway або gateway-host).

3.1.3. Політики, правила, фільтри та дії фільтра

У Windows набір налаштувань IPsec оформлюється у вигляді політики безпеки IP (IP Security Policy), яка складається з:

— правил (Rules) – логічних блоків, що описують обробку певного трафіка;

— списків фільтрів IP (IP Filter Lists) – визначають, до якого трафіка застосовується правило (джерело, призначення, протокол, порт);

— дій фільтра (Filter Actions) – визначають, що зробити з трафіком:

- Permit (дозволити);
- Block (заблокувати);
- Negotiate security (узгоджувати безпеку – використовувати IPsec з певними параметрами AH/ESP).

Параметри фільтра можуть включати:

— IP-адресу джерела / призначення, підмережі, DNS-ім’я;

— тип протоколу (TCP, UDP, ICMP, «Any»);

— номери портів TCP/UDP (80, 443, 53, 1433, 1434 тощо).

3.1.4. Вплив IPsec на продуктивність

Застосування IPsec потребує додаткових обчислень (шифрування, хешування, обмін ключами), що:

— збільшує завантаження процесора;

— може зменшувати швидкість передачі даних;

— особливо помітно при використанні «важких» алгоритмів (3DES, деякі варіанти AES) і великих обсягів трафіка.

Тому на практиці завжди треба балансувати між:

— рівнем захисту (комбінація AH/ESP, довжина ключів, алгоритми шифрування) та допустимими втратами продуктивності.

3.2. Практична частина

Примітка: усі кроки виконуються на локальному комп'ютері під обліковим записом з правами адміністратора. За можливості використовується пара «клієнт-сервер» для перевірки трафіка.

1. Етапи налаштування та встановлення з'єднання IPSec

Етапи налаштування та встановлення з'єднання IPSec:

1. Створення політики безпеки IPSEC.

2. Додавання правила безпеки у створену політику.

3. Додавання фільтра для трафіка, який шифруватиметься.

4. Визначення дій фільтра (Filter Action).

5. Завершальне налаштування IPSEC.

6. Запуск та перевірка роботи IPSEC з'єднання.

Загальний набір параметрів безпеки IPSec називається політикою IPSec. Політика складається з набору правил, які визначають обробку мережного трафіка. Кожне правило містить набір фільтрів і дії, що відносяться до нього, які дане правило буде виробляти з пакетом, відповідним умовам фільтра. Як параметри фільтрів можуть бути задані IP-адреси, адреси мережі або повне доменне ім'я відправника та одержувача пакета, тип IP-протоколу (ICMP, TCP, UDP тощо), номери TCP та UDP портів відправника та одержувача.

У ОС Windows 10 налаштування IPsec можна виконати за допомогою функції «Локальні параметри безпеки» / «Local Security Policy». Запуск може бути здійснено з меню «Адміністрування» «Панелі управління» або за допомогою команди «Виконати» «secpol.msc». При роботі з IPSec є можливість використання створених за умовчанням політик або створення нової.

1. Створення нової політики безпеки

Для створення нової політики безпеки IP необхідно вибрати зі списку пункт «Політики безпеки IP» та в меню при натисканні правої кнопки миші вибрати дію «Створити політику безпеки IP» або в меню «Дія» вибрати «Створити політику безпеки IP» (рис. 1).

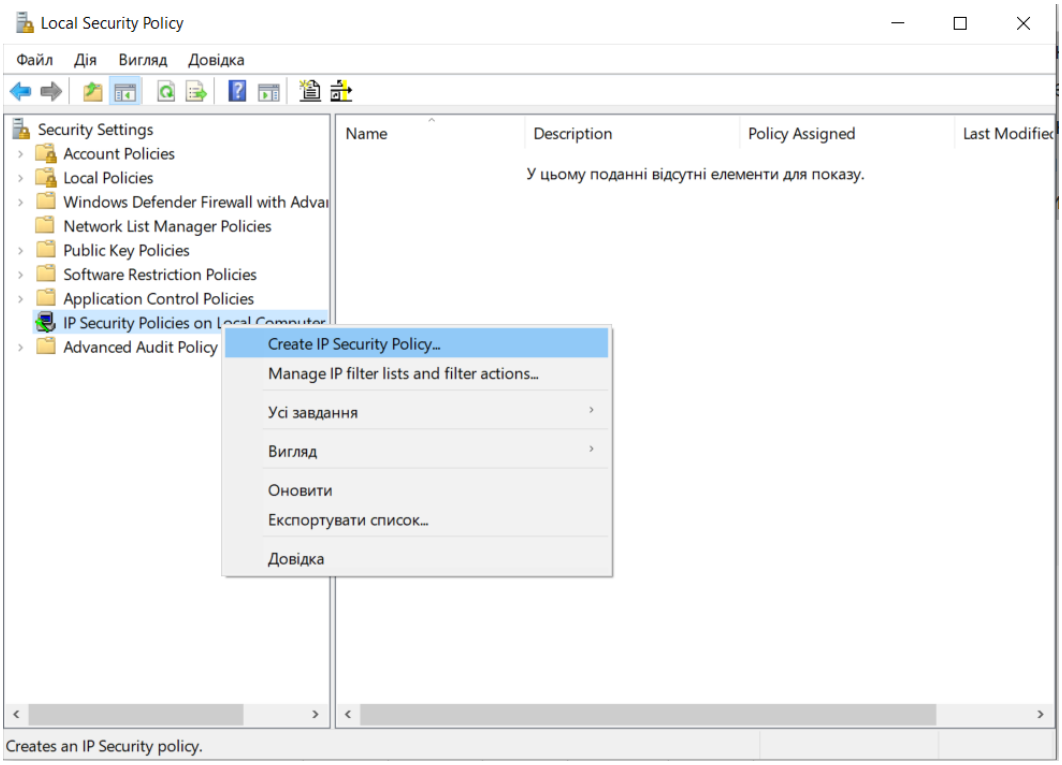


Рисунок 1. Локальні параметри безпеки

Після цього відкриється «IP Security Policy Wizard». Для продовження потрібно натиснути на кнопку «Далі». В результаті чого відкриється вікно, де потрібно ввести ім’я нової політики і натиснути кнопку «Далі» (рис. 2).

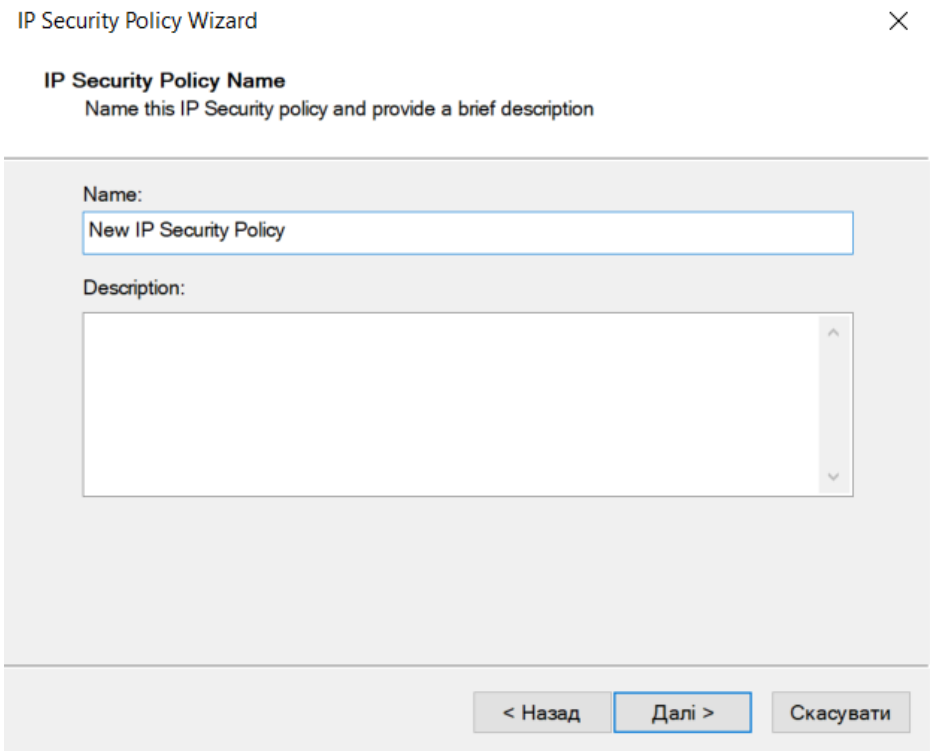


Рисунок 2. Створення нової політики

У наступному вікні «IP Security Policy Wizard» запропонує ухвалити рішення про використання правила за усталеним налаштуванням. Використання правила за усталеним налаштуванням можна скасувати після створення політики, якщо виникне така потреба (рис. 3).

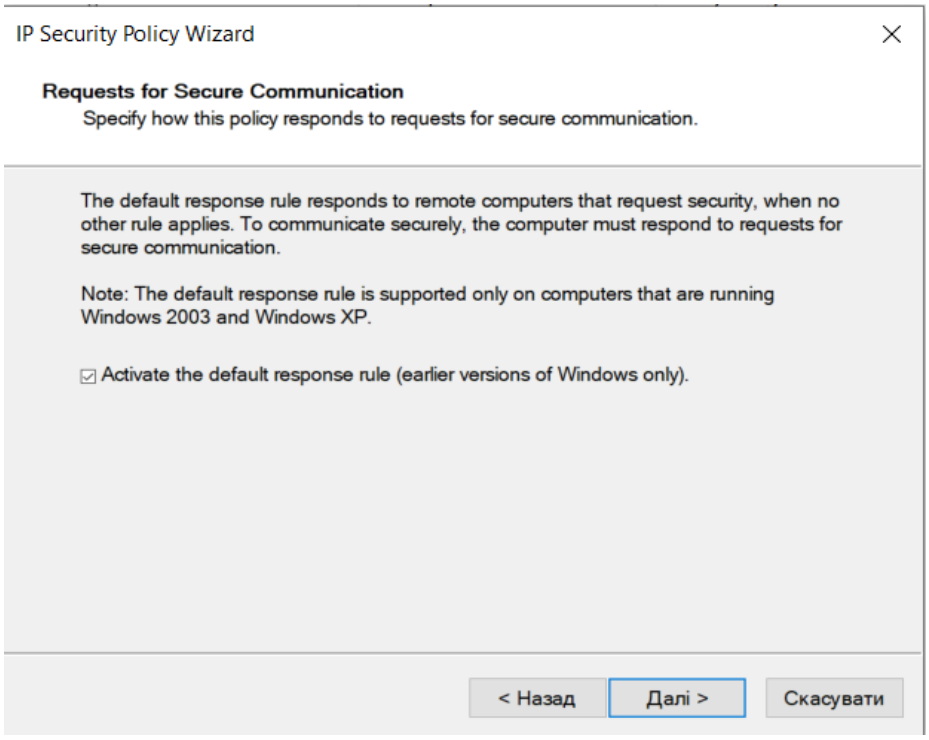


Рисунок 3. Створення нової політики

Далі «IP Security Policy Wizard» пропонує кілька способів автентифікації користувача, які підтримує IPsec: за допомогою протоколу Kerberos (стандартний протокол автентифікації в доменах Windows), за допомогою сертифіката користувача, або на підставі рядка захисту (попереднього ключа). Якщо в мережі немає контролерів домену, і користувачі мережі не мають дійсних сертифікатів, слід вибрати автентифікацію за допомогою попереднього ключа (рис. 4).

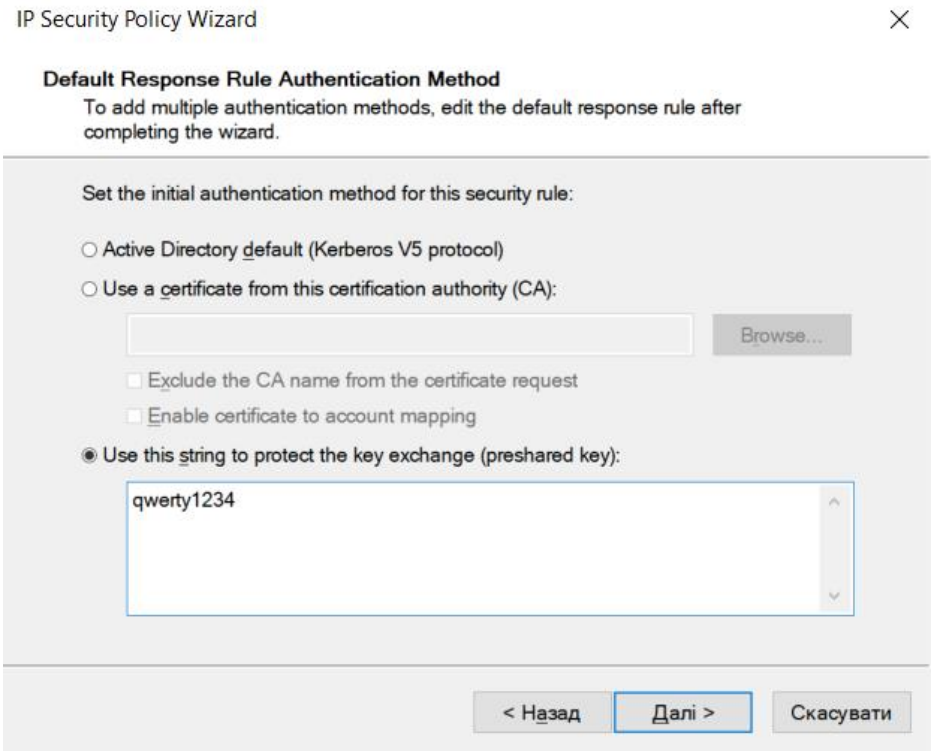


Рисунок 4. Налаштування автентифікації користувача

Отже, створення політики практично завершене (рис. 5). Змінити властивості можна після завершення роботи майстра (вікно властивостей відкриється автоматично), або, виділивши потрібну політику і вибравши з контекстного меню пункт «Властивості».



Рисунок 5. Завершення початкового налаштування

Далі необхідно змінити властивості політики таким чином, щоб вони відповідали вимогам, а отже необхідно створити правила безпеки IP, фільтр та визначити дію фільтра.

2. Додавання правила безпеки для створеної політики Для створення правила безпеки слід відкрити властивості створеної політики безпеки IP та на вкладці «Властивості» натиснути кнопку «Додати/Add», попередньо знявши прапорець «Використовувати майстер/Use Add Wizard» (рис. 6).

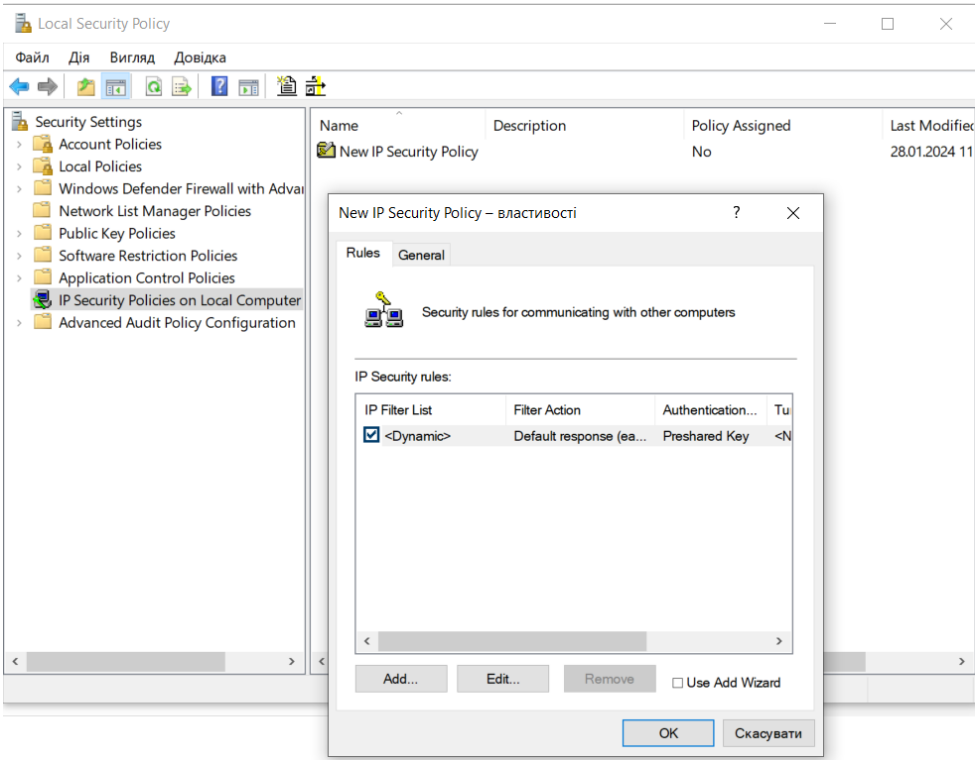


Рисунок 6. Властивості політики

Оскільки з'єднання IPSec налаштовується для транспортного режиму, на закладці «Параметри тунелю/Tunnel Settings» немає необхідності змінювати щось. На закладці «Тип підключення/Connections Type» можна вибрати мережні підключення, для яких застосовуватиметься створюване правило – всі підключення, лише локальні підключення, лише віддалені підключення. Таким чином, надається можливість створення різних правил для мережних підключень з різною швидкістю передачі даних, що дозволяє для більш повільних і, як правило, менш захищених віддалених підключень встановити інші параметри автентифікації, перевірки цілісності та шифрування (рис. 7).

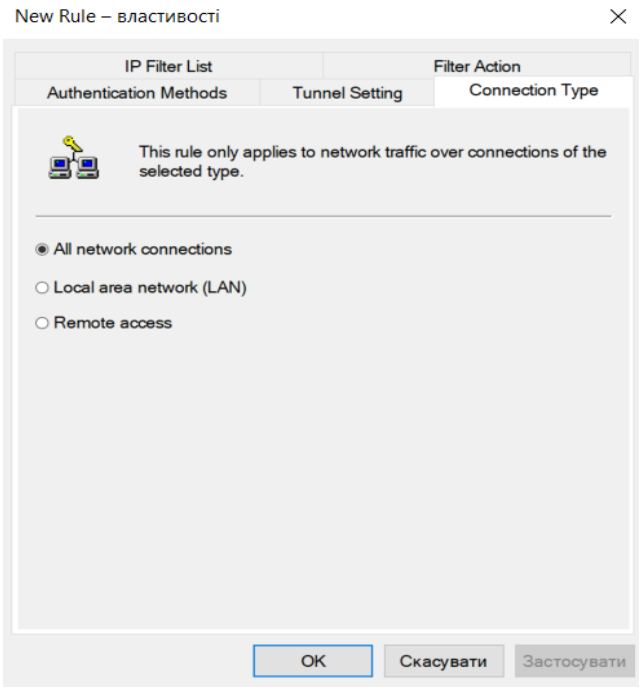


Рисунок 7. Тип підключення

На закладці «Методи автентифікації/ Authentication Methods» є можливість додати кілька методів перевірки та змінити порядок їх переваги, що дозволяє гнучкіше налаштувати правило для зв'язку з різними вузлами, що підтримують різні способи автентифікації (рис. 8).

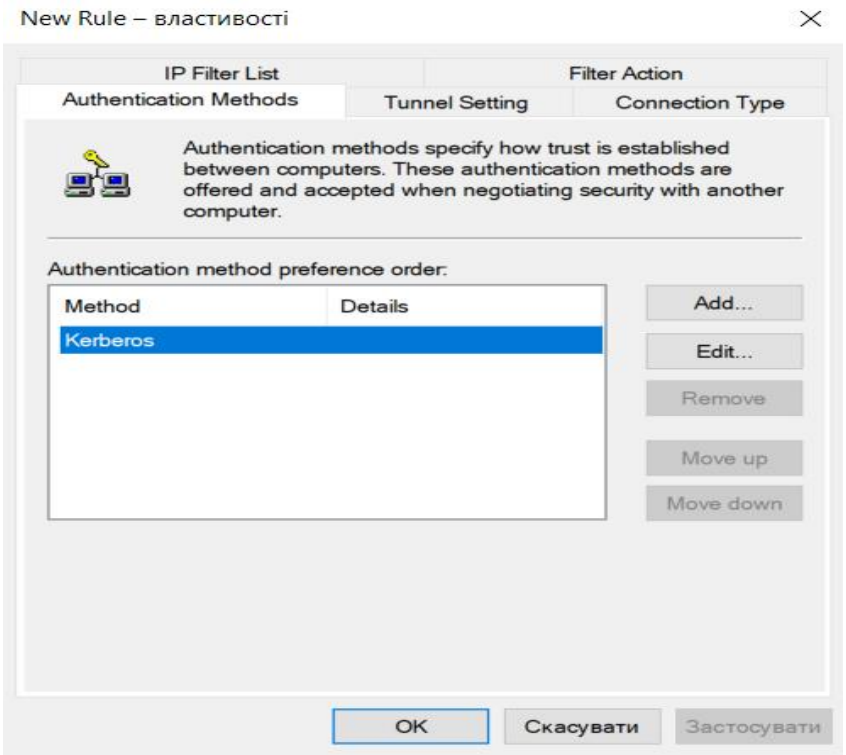


Рисунок 8. Методи автентифікації

3. Додавання фільтра

Далі на закладці «Список фільтрів IP» необхідно вибрати фільтр IP та дію фільтра, або створити новий. Фільтри, створені за усталеним налаштуванням:

— Повний IP-трафік, який застосовується до всього IP-трафіка, незалежно від протоколу вищого рівня;

— Повний ICMP-трафік, який застосовується до всього ICMP-трафіка.

Для створення нового фільтра необхідно натиснути кнопку «Додати», внаслідок чого відкриється вікно «Список фільтрів IP», де необхідно зняти галочку «Використовувати майстер / Use Add Wizard» та після введення імені списку фільтрів натиснути кнопку «Додати» (рис. 9).

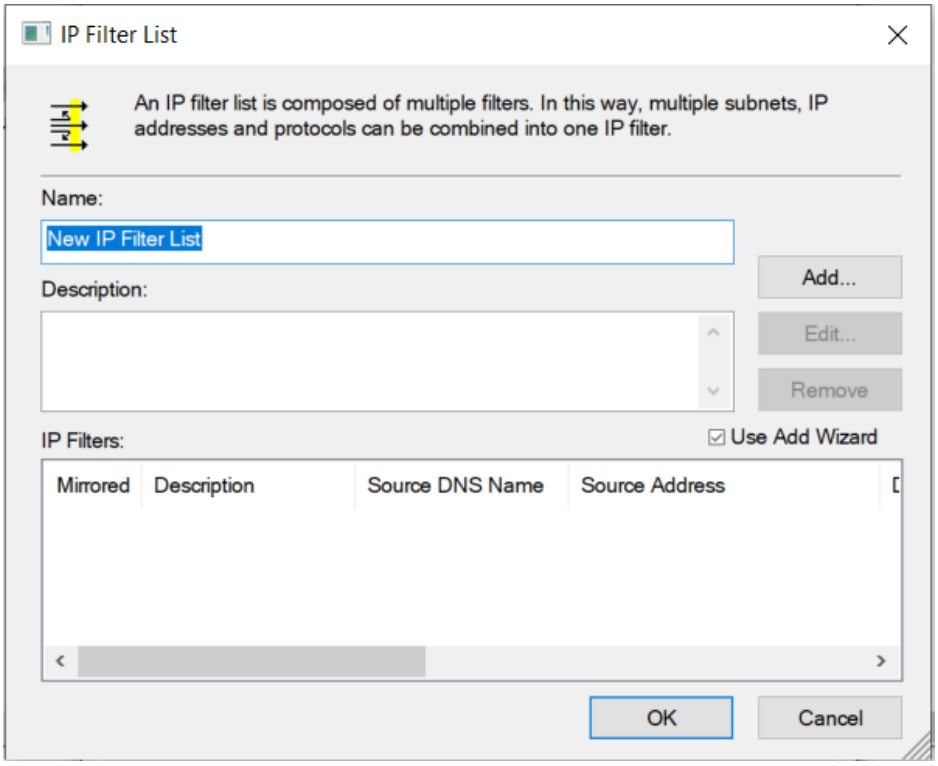


Рисунок 9. Додавання нового фільтра

Далі відкриється вікно «IP Фільтр – Властивості», де необхідно вказати адреси джерела та одержувача пакетів, до яких застосовуватиметься фільтр, а також, за необхідності, протокол та порти джерела та одержувача (рис. 10).

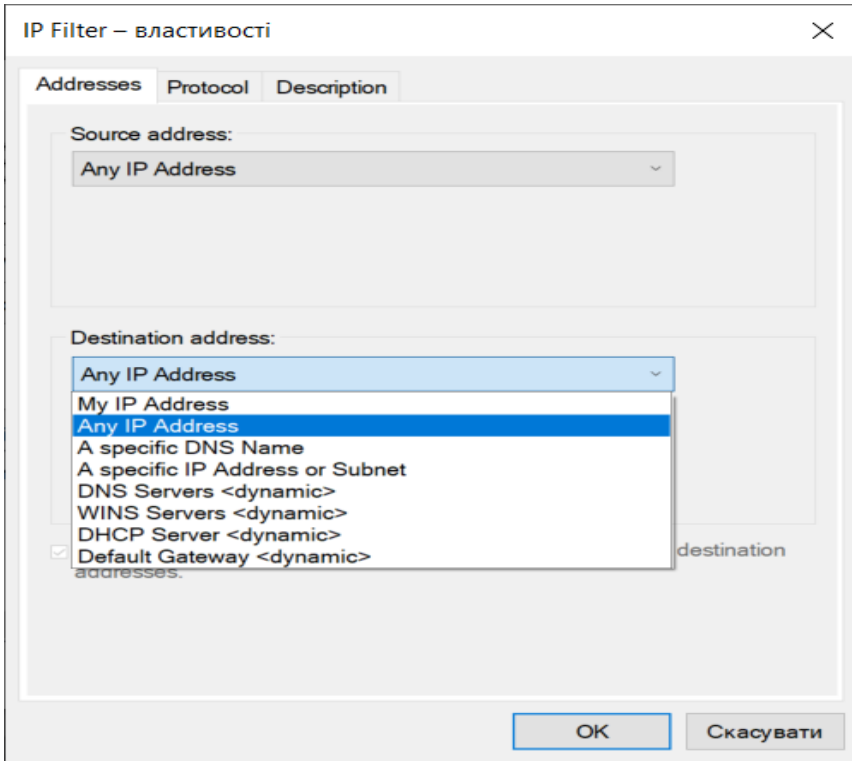


Рисунок 10. Додавання нового фільтра

4. Визначення дії фільтра

Далі необхідно визначити дію фільтра. На закладці «Дія фільтра / Filter Action» можна вибрати стандартні дії або створити нову. Нову дію можна створити, знявши прапорець «Використовувати майстер» та натиснувши кнопку «Додати / Add». На вкладці «Методи безпеки / Security Methods» вікна «Властивості: створення дії фільтра / New filter action – властивості», що відкриється, необхідно вибрати: чи потрібно дозволити проходження даних, заблокувати їх, або узгодити безпеку.

При виборі пункту «Узгодити безпеку / Negotiate Security,» можна додати методи безпеки та змінити порядок їх переваги. При додаванні методів безпеки слід вибрати, чи використовуватиметься AH, ESP, або налаштувати безпеку вручну, вибравши пункт «Безпека, що налаштовується / Custom» (рис. 11).

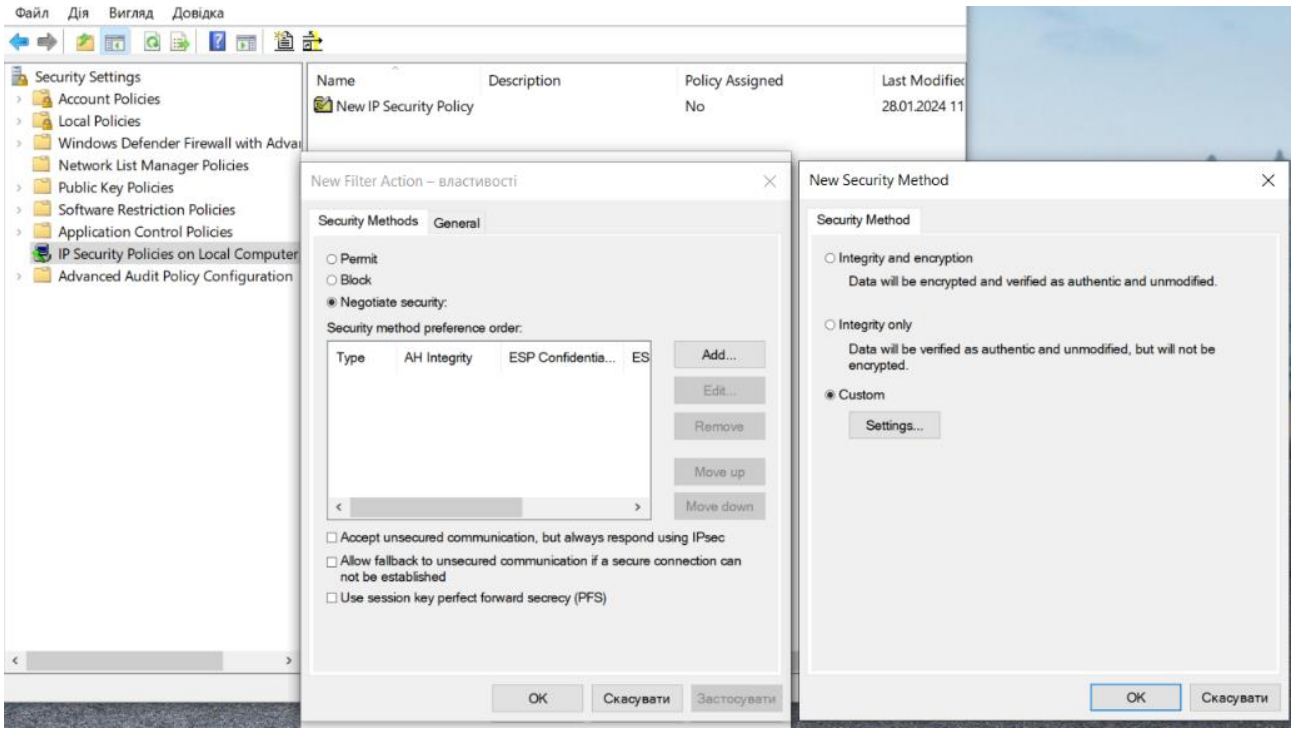


Рисунок 11. Додавання нового фільтра

У параметрах безпеки, що настроюється, встановлюються необхідні протоколи (AH і ESP), а також надано можливість вручну вибрати алгоритми перевірки цілісності та шифрування, параметри зміни ключів сеансу (рис. 12). За усталеним налаштуванням ключі змінюються щогодини або через кожні 100 Мб переданої інформації.

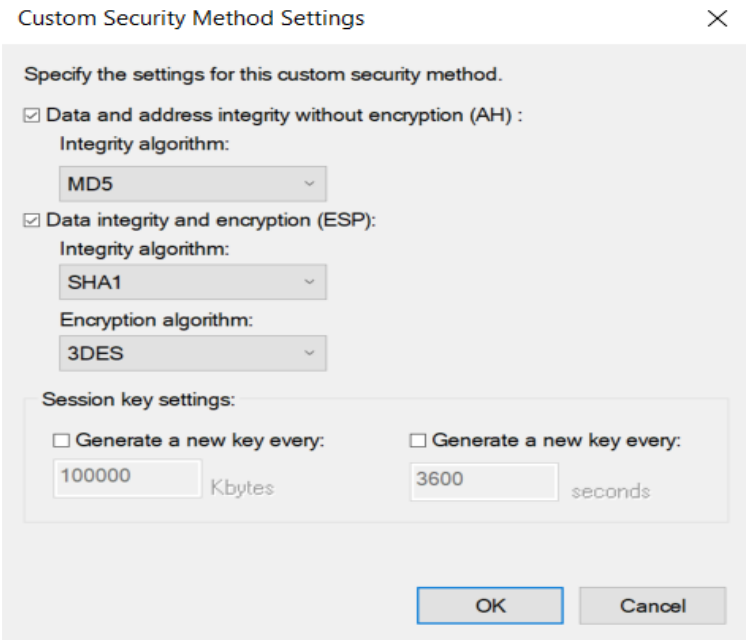


Рисунок 12. Налаштування параметрів безпеки

5. Завершальне налаштування IPSec

Після вибору дій фільтрів налаштування політики безпеки IP можна вважати завершеним. За допомогою натискання кнопок «ОК» та «Застосувати» необхідно завершити роботу з «Майстром налаштування».

Далі необхідно призначити створену безпекову політику натиснувши «Assign» (рис. 13).

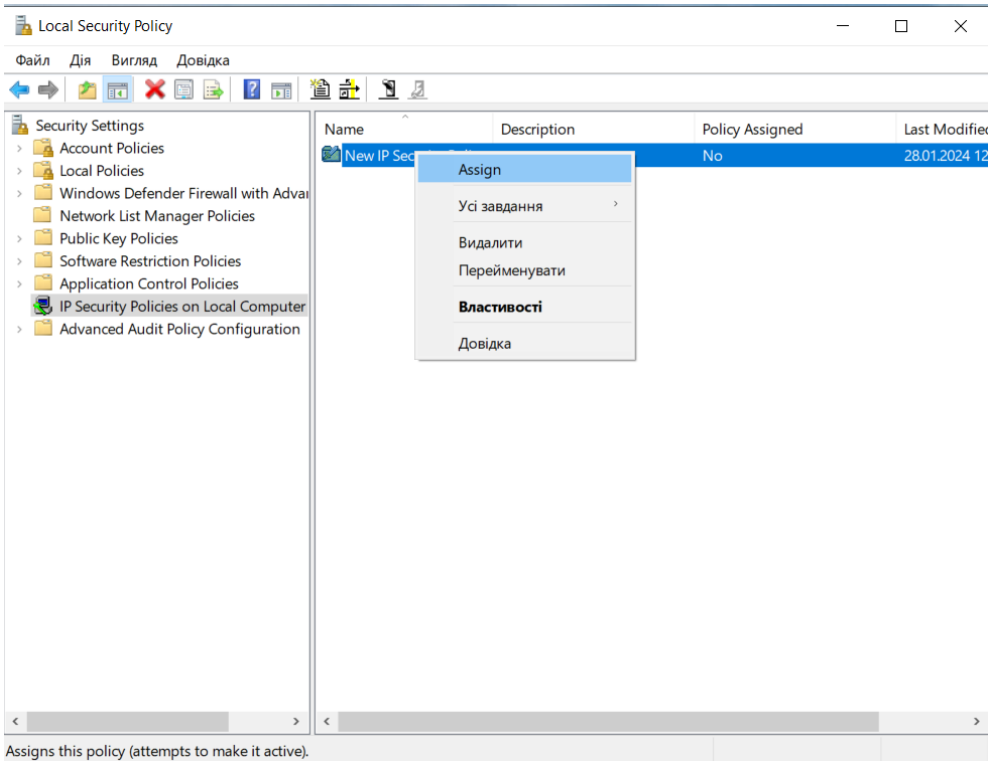


Рисунок 13. Призначення створеної політики безпеки

Якщо налаштування здійснювалось у Windows 10, для транспортного режиму IPsec, то таку ж операцію слід зробити на кожному комп'ютері. Засоби автоматизації Windows Server дозволяють централізовано розгорнути політику IP на всіх робочих станціях домену.

6. Запуск та перевірка IPSec з'єднання

Перевірити, чи з'єднання IPSec встановилося, можна за допомогою утиліти ping у командному рядку. Рядки «Узгодження рівня безпеки IP, що використовується» означають, що системи вибирають загальні типи шифрування.

2. Тестування продуктивності протоколу IPSec

Під час виконання бакалаврської кваліфікаційної роботи було проведено тестування продуктивності протоколу IPsec для того, щоб виявити рівень

навантаження на центральний процесор під час передачі даних по мережі з використанням різних криптографічних алгоритмів. Тестування проводилося на комп'ютері, який має такі технічні характеристики (таблиця 1).

Таблиця 1

Характеристики комп’ютера, який тестувався

	Комп’ютер 1
Процесор	11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz 1.80 GHz
Материнська плата	Dell latitude 5520
Пам’ять	16,0 ГБ
Вінчестер	Samsung 512 ГБ ssd
Мережевий адаптер	Intel(R) Ethernet Connection (13) I219-LM

Файл, об'єм якого становив 105 Мб, передавався по мережі між двома комп'ютерами з різними налаштуваннями IPsec у транспортному режимі (Transport Mode), а також без використання протоколу, що розглядається.

Необхідно пам'ятати, що у транспортному режимі протоколи AH і ESP шифрують і хешують лише корисні дані, а не весь пакет, як відбувається при інкапсуляції в тунельному режимі.

У вимірюваннях можлива деяка похибка, оскільки вимірювання завантаженості процесора та часу передачі файлу проводилися за допомогою годинника та диспетчера завдань Windows.

1. Передача файлу через мережу без використання IPsec. Час передачі файлу склало 9 с, а середня швидкість передачі даних досягла 11,67 Ггц. При цьому завантаженість процесорів становила 23% (рис. 14).

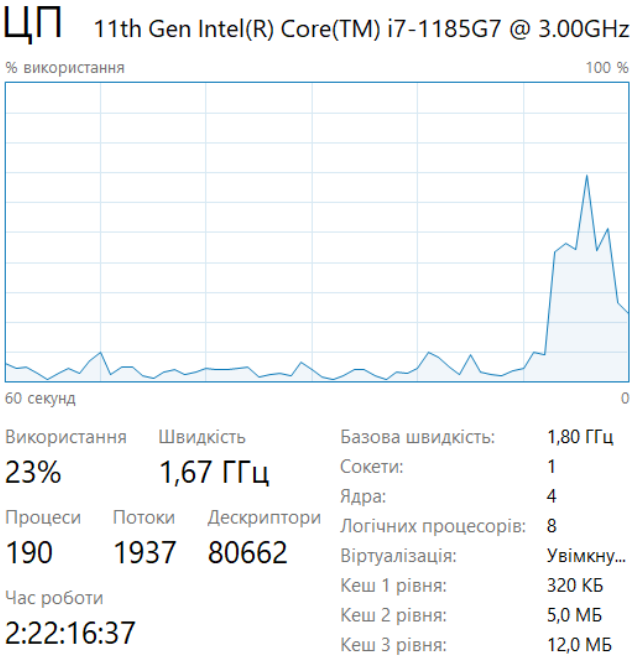


Рисунок 14. Завантаження процесора на комп'ютері

2. Передача файлу по мережі з настроєною політикою IPsec, з використанням фільтра для забезпечення цілісності даних, що передаються (протокол AH з використанням SHA-1). При цьому час передачі збільшився незначно, до 12 с, а швидкість трохи змінилася, до 3 Ггц. При цьому також трохи зросло завантаження процесора до 42%, як показано на рис. 15.

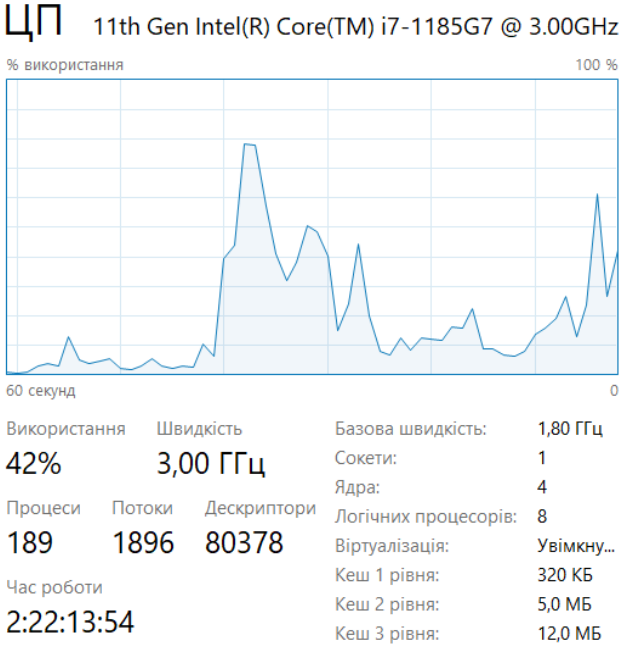


Рисунок 15. Завантаження процесора на комп'ютері

3. Передача файлу по мережі з настроєною політикою IPsec, із застосуванням фільтра ESP без використання AH, із шифруванням за допомогою

алгоритму DES та хешуванням MD5. Значних змін у продуктивності цієї конфігурації порівняно з попередніми не сталося. Час передачі файлу зріс до 15 с, а швидкість передачі досягла 3,2 Ггц. Завантаження процесора становить 48%, що показано на рис. 16.

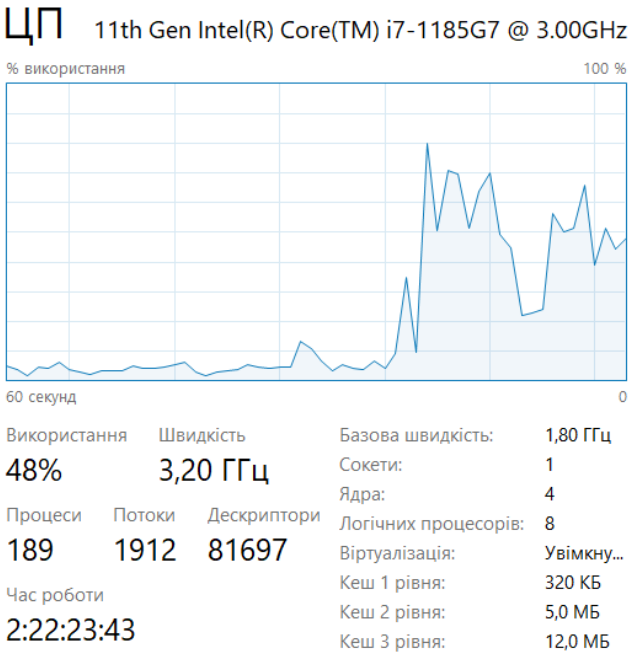


Рисунок 16. Завантаження процесора на комп'ютері

DES є застарілим алгоритмом і не рекомендується до використання там, де дані, що захищаються, мають велику цінність, але стійкість цього алгоритму може бути значно покращена завдяки більш частій зміні ключа.

4. Передача файлу по мережі з настроєною політикою безпеки IPsec, із застосуванням фільтра ESP, що використовує шифрування за допомогою алгоритму 3DES, замість алгоритму DES, та хешування MD5. При цьому час передачі файлу значно зріс і дорівнює 19 с, а швидкість передачі файлу відповідно – 3,77 Ггц. Рівень завантаження процесора при цьому становив 76%, що показано на рис. 17.

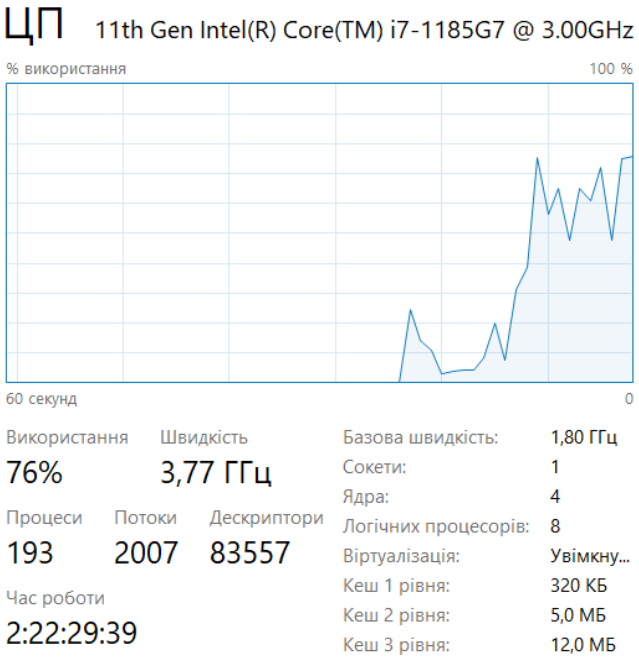


Рисунок 17. Завантаження процесора на комп'ютері

5. Передача файлу через мережу з налаштованою політикою безпеки IPsec, із застосуванням фільтра ESP з 3DES та SHA1. При цьому час передачі файлу дорівнює 20 с, а швидкість передачі файлу – 1,87 Ггц. Рівень завантаження процесорів у системі становив 46 %, що проілюстровано на рис. 18.

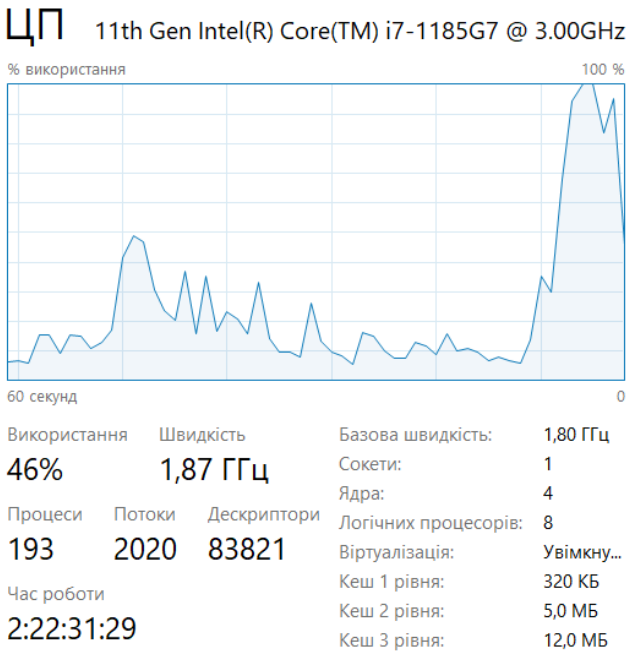


Рисунок 18. Завантаження процесора на комп'ютері

6. Передача файлу через мережу з налаштованою політикою безпеки IPsec, з використанням протоколу ESP разом із протоколом AH. При цій найбільш

безпечній, а отже, найбільш ресурсомісткій конфігурації, доступній у Windows 10, отримані такі результати: час передачі збільшився до 25 с, швидкість впала до 1,68 Мбіт/с. Завантаження процесора склало 82 %, і показано на рис. 19.

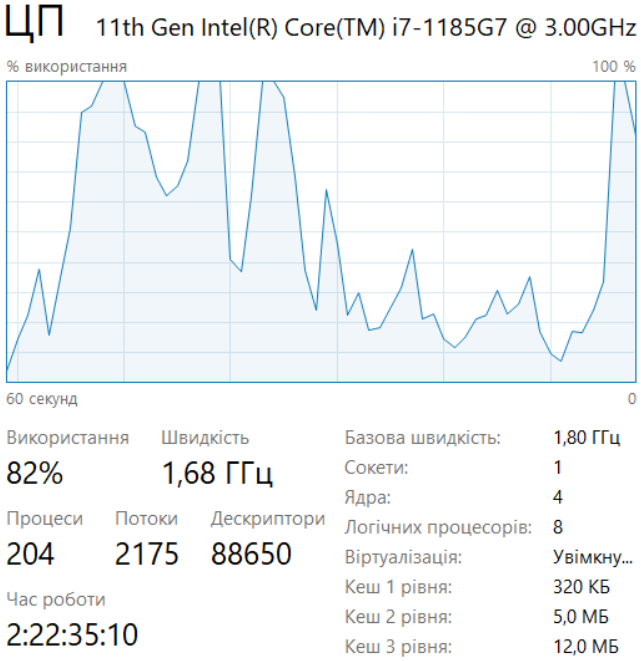


Рисунок 19. Завантаження процесора на комп'ютері

У ході тестування можна було спостерігати, як змінюються час та швидкість передачі від класу процесорів. Результати тестування показують, що ресурсомісткість IPsec невисока лише за використання протоколу AH і за допомогою протоколу ESP з алгоритмом шифрування DES. При використанні протоколу ESP з більш сильним алгоритмом шифрування 3DES продуктивність значно знижується, але при низьких швидкостях передачі даних продуктивності навіть застарілих процесорів буде достатньо. У випадках, де потрібна висока швидкість обміну даними, може виявитися достатнім використання алгоритму DES із частою зміною ключа.

Таким чином, IPsec може бути рекомендований для використання в багатьох мережах для підвищення безпеки.

3. Налаштування політики безпеки IPSec для роботи як міжмережевий екран

Протокол IPsec використовується в основному для організації VPN-тунелів. У цьому випадку протоколи ESP та AH працюють у режимі тунелювання. Крім того, налаштування політики безпеки певним чином протокол можна використовувати для створення міжмережевого екрана.

Основним призначенням міжмережевого екрана є здійснення контролю та фільтрація мережевих пакетів, що проходять через нього, на різних рівнях моделі OSI відповідно до заданих правил. У загальному випадку, встановлюється набір правил (формується фільтр), використовуючи які, екран переглядає всі пакети, що передаються і прийняті системою. З пакетами, які підпадають під критерії відбору, задані у фільтрі, екран робить необхідні дії.

Існує можливість використання IPSec, що дозволяє реалізувати подібність міжмережевого екрана. Використання IPSec не є повноцінною заміною брандмауера, проте дозволяє реалізувати безліч подібних завдань з використанням штатних засобів ОС Windows.

Розглянемо приклад, у якому IPSec використовується у тому, щоб заборонити весь Інтернет-трафік на локальній машині.

Щоб заборонити весь обмін Інтернет-трафіком на комп'ютері, необхідно налаштувати політику IPSec, яка забороняє весь обмін даними за протоколами HTTP та HTTPS. Зображення діалогових вікон та послідовність дій будуть показані нижче на прикладі використання Windows 10.

Створити нову політику IPSec також можна, використовуючи консоль MMC (Пуск - Виконати - mmc). У меню вікна консолі необхідно вибрати команду Консоль, потім пункт Додати або видалити оснастку (рис. 20).

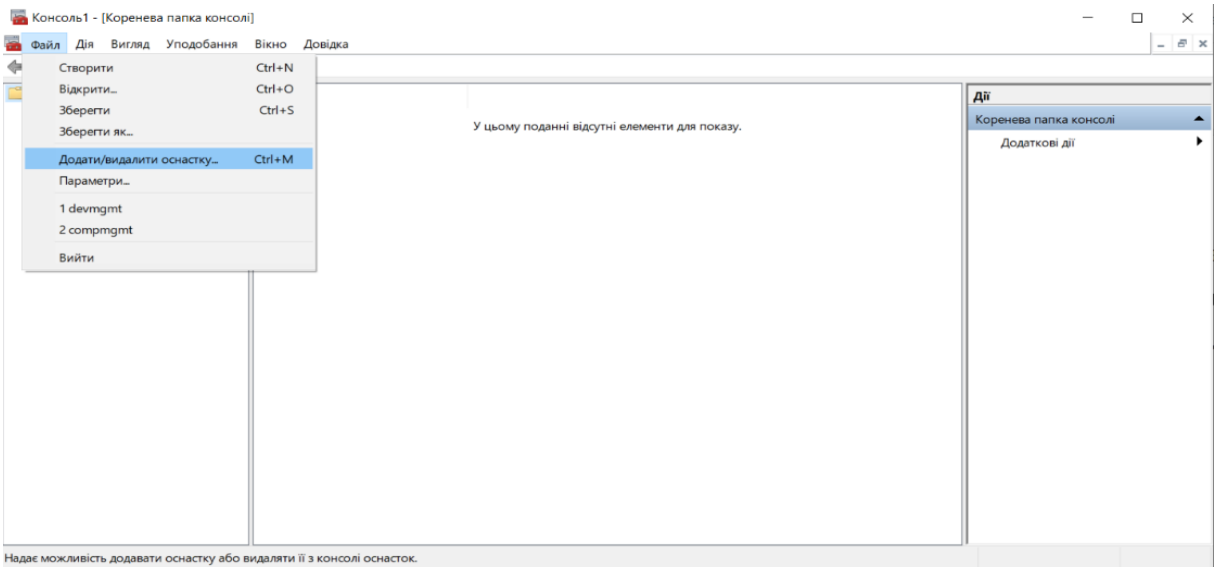


Рисунок 20. Створення нової політики IPSec

Для керування IPSEC з'єднаннями у Windows 10 необхідно додати оснащення «Керування політикою безпеки IP» (рис. 21).

Після натискання кнопки «Додати» потрібно вказати, що політика безпеки застосовується на локальному комп'ютері (рис. 22).

Далі необхідно послідовно закрити вікна, натискаючи кнопку Готово, Закрити, ОК. Після чого на вузлі Політики безпеки IP на «Локальний комп'ютер» в лівій панелі консолі необхідно зробити клацання правою кнопкою миші і вибрати команду Управління списками IP-фільтра (рис. 23).

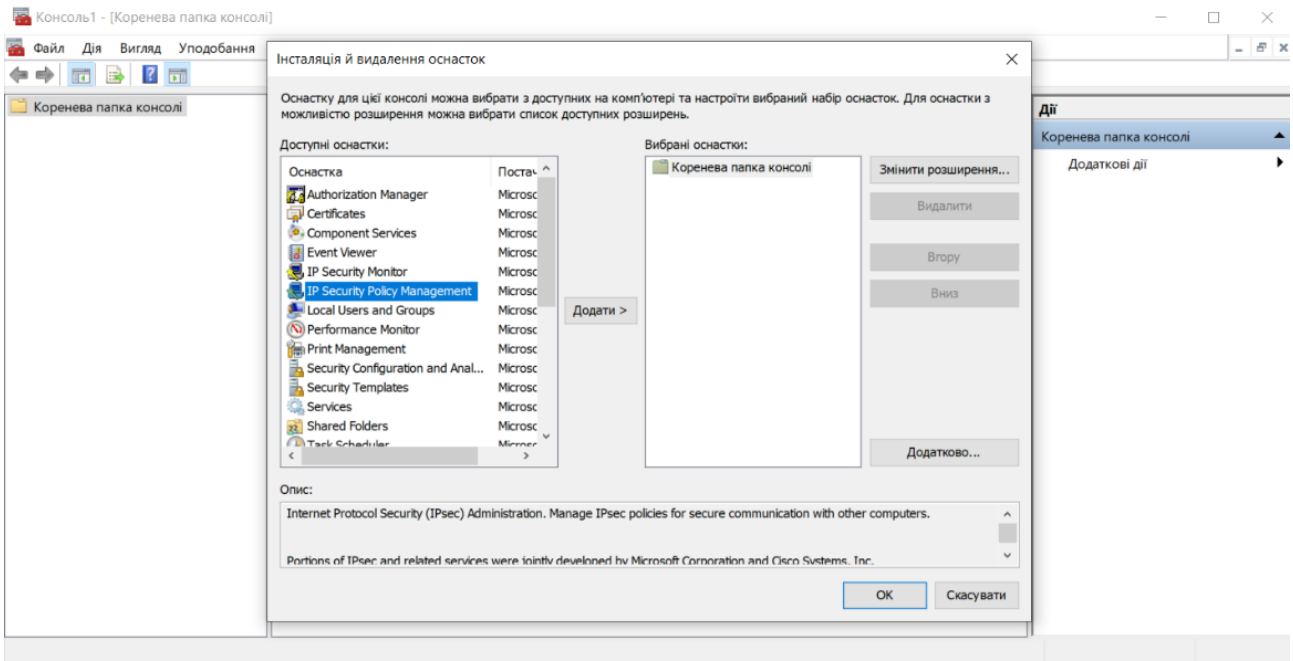


Рисунок 21. Створення нової політики IPSec

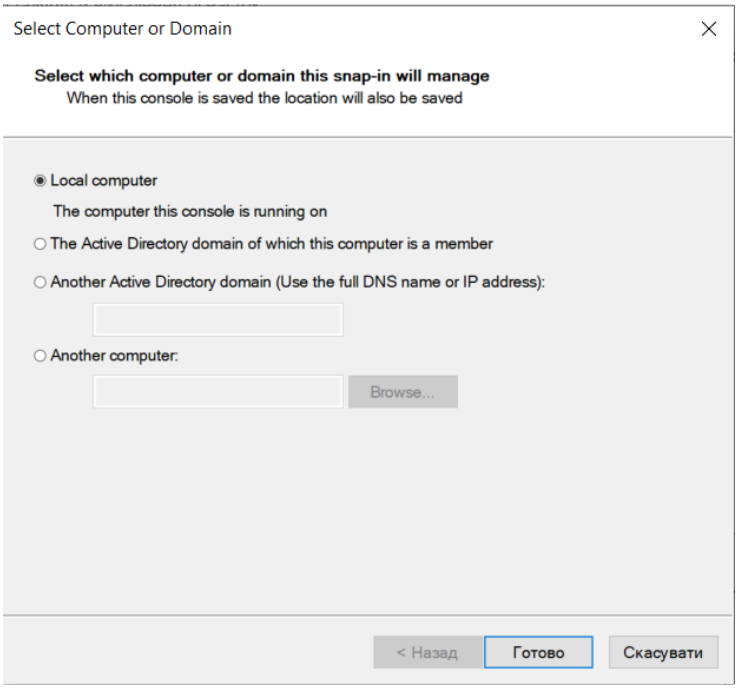


Рисунок 22. Створення нової політики IPSec

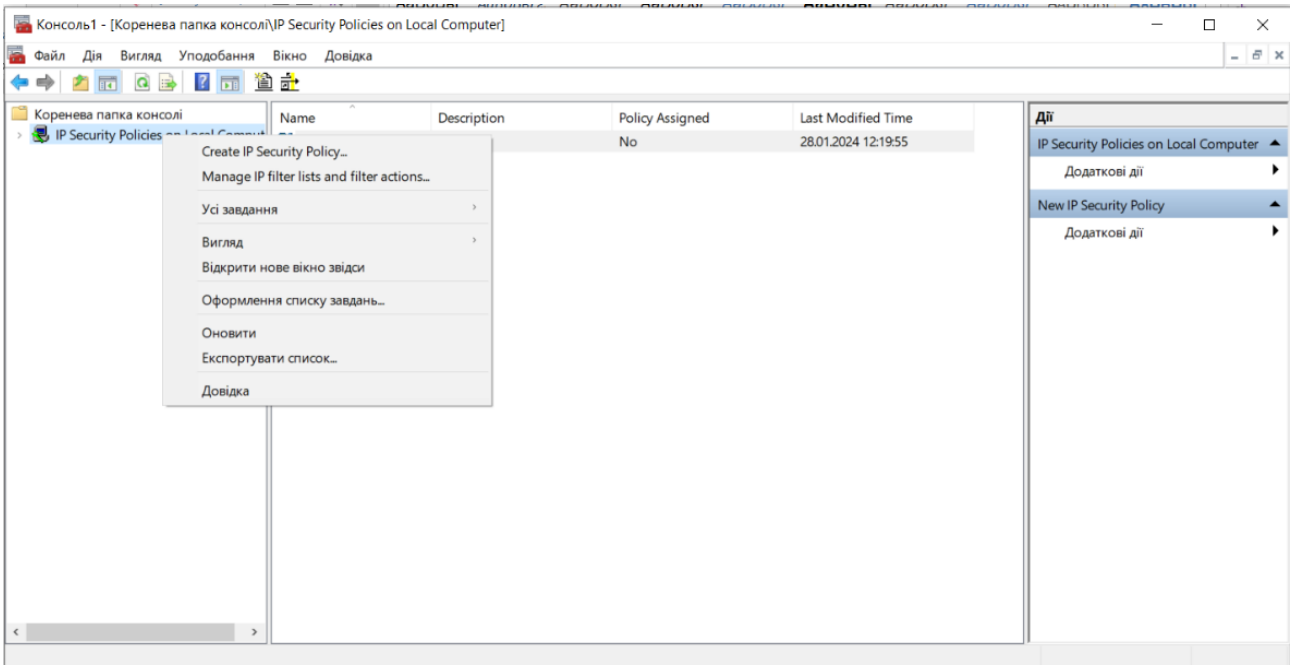


Рисунок 23. Створення нової політики IPSec

У діалозі при натисканні кнопки «Додати» відкриється вікно Список фільтрів. Необхідно задати назву нового фільтра, наприклад, HTTP, HTTPS, і розпочати створення фільтра, натиснувши кнопку Додати/Add (рис. 24).

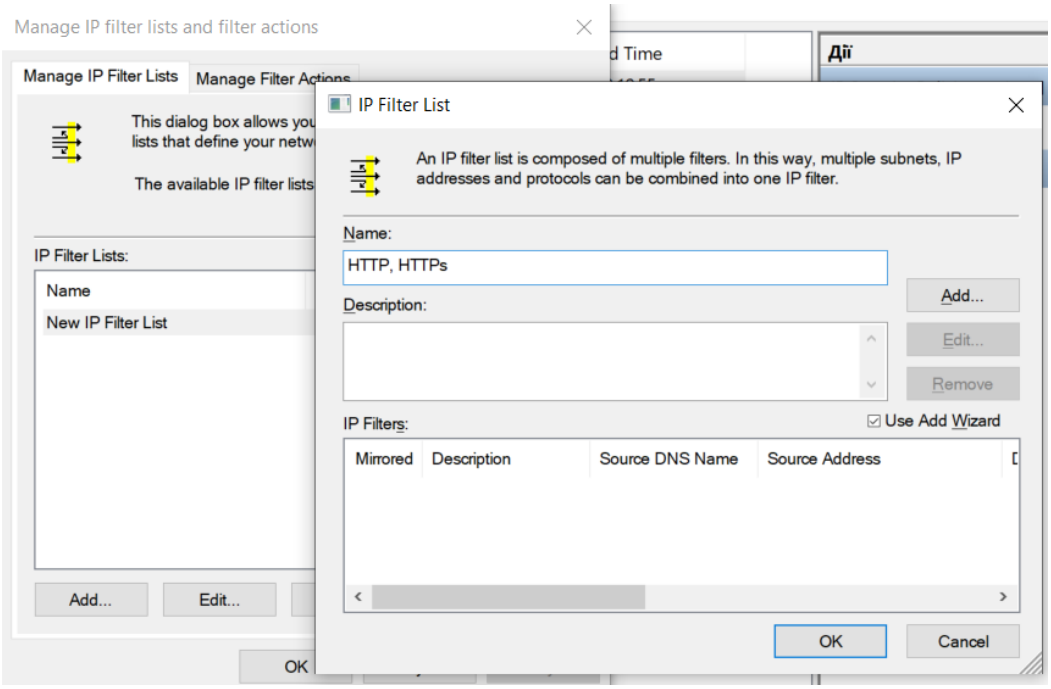


Рисунок 24. Створення нової політики IPSec

Далі потрібно вказати адресу джерела IP-пакетів, у цьому прикладі необхідно вказати Мій IP-адрес, задати адресу призначення, вибравши Будь-яку IP-адресу та натиснути кнопку ОК (рис. 25).

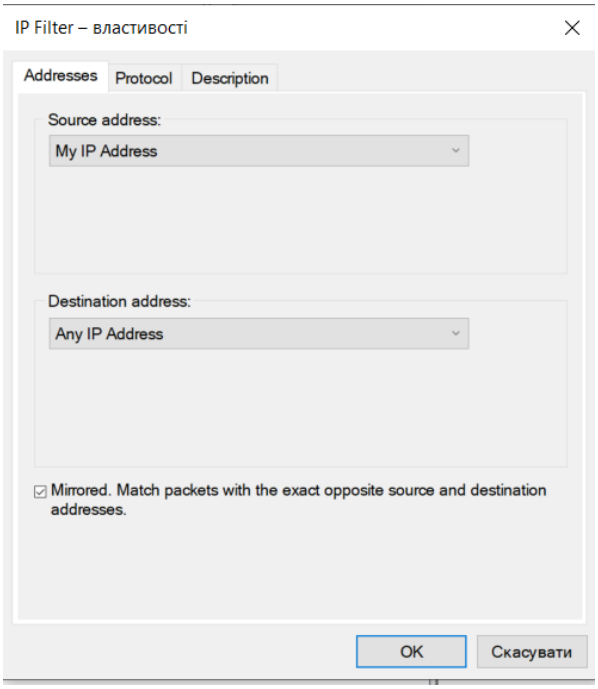


Рисунок 25. Створення нової політики IPSec

Далі слід зазначити тип протоколу. Для цього завдання необхідно вибрати протокол TCP (рис. 26)

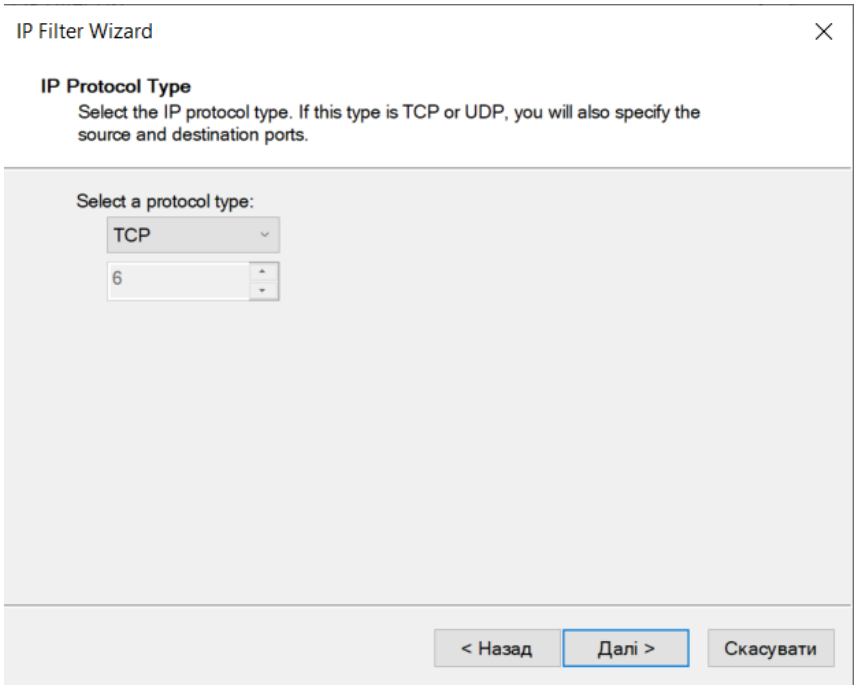


Рисунок 26. Створення нової політики IPSec

Верхній перемикач слід залишити в положенні Пакети з будь-якого порту, а нижній переключити в положення Пакети на цей порт і ввести значення HTTP-порту – 80 (рис. 27).

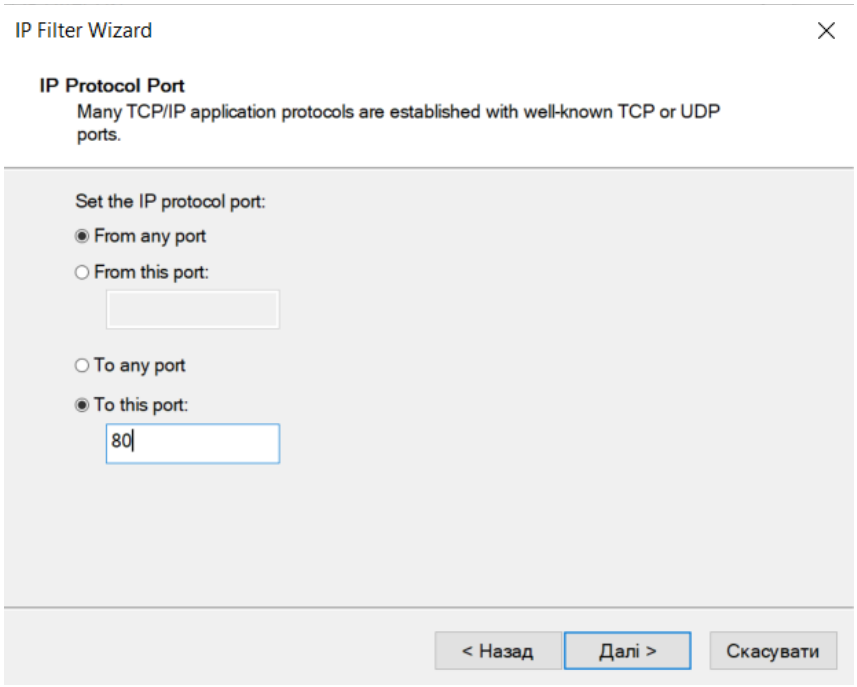


Рисунок 27. Створення нової політики IPSec

Після натискання кнопки Готово у нижньому вікні списку з'явиться створений фільтр.

Далі, натиснувши кнопку Додати, слід зробити всі попередні операції ще раз, але вже вказавши значення порту 443 (для HTTPS). У списку нижнього вікна повинні бути обидва створені правила фільтрації пакетів.

Тепер необхідно визначити дії, які робитиме створений фільтр. Для цього необхідно перейти на закладку Керування діями фільтра та натиснути кнопку Додати. Після цього слід вказати назву дії, наприклад, Block, та натиснути кнопку Далі. Як дія потрібно вибрати перемикач Блокувати, натиснути Далі та ОК (рис. 28).

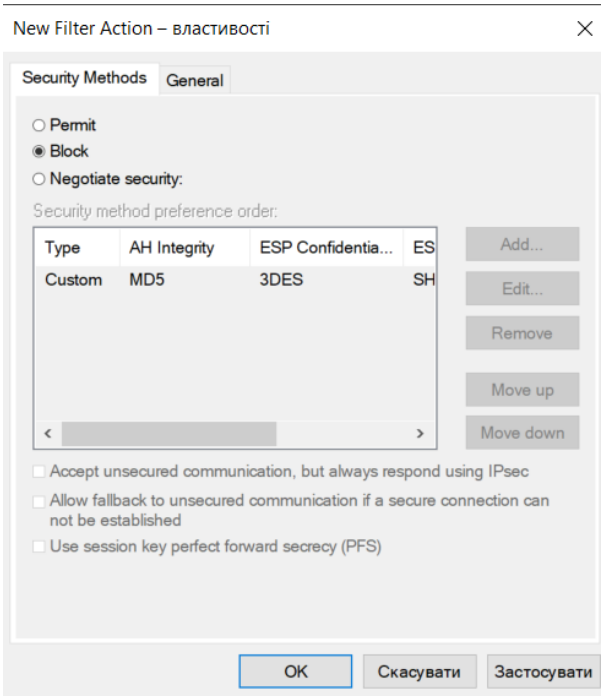


Рисунок 28. Створення нової політики IPSec

Таким чином, фільтр створено, дія для нього визначена, залишилося створити політику та призначити її. У вікні консолі MMC, натиснути правою кнопкою миші на вузол Політики безпеки IP та вибрати команду Створити політику безпеки IP (рис. 29).

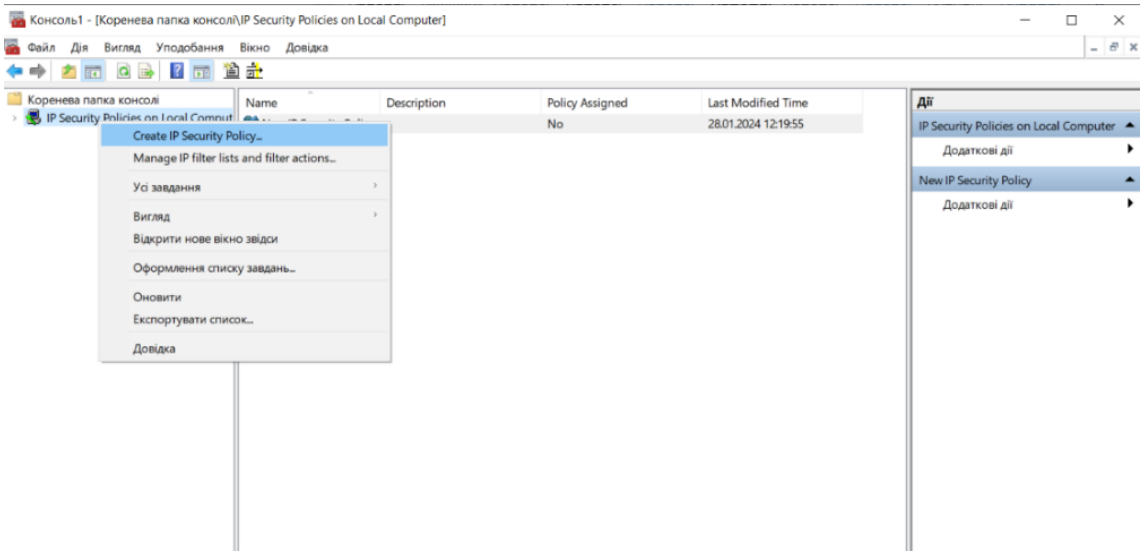


Рисунок 29. Створення нової політики IPSec

У вікні майстра потрібно вказати політики, наприклад, Block Web і натиснути Далі (рис. 30).

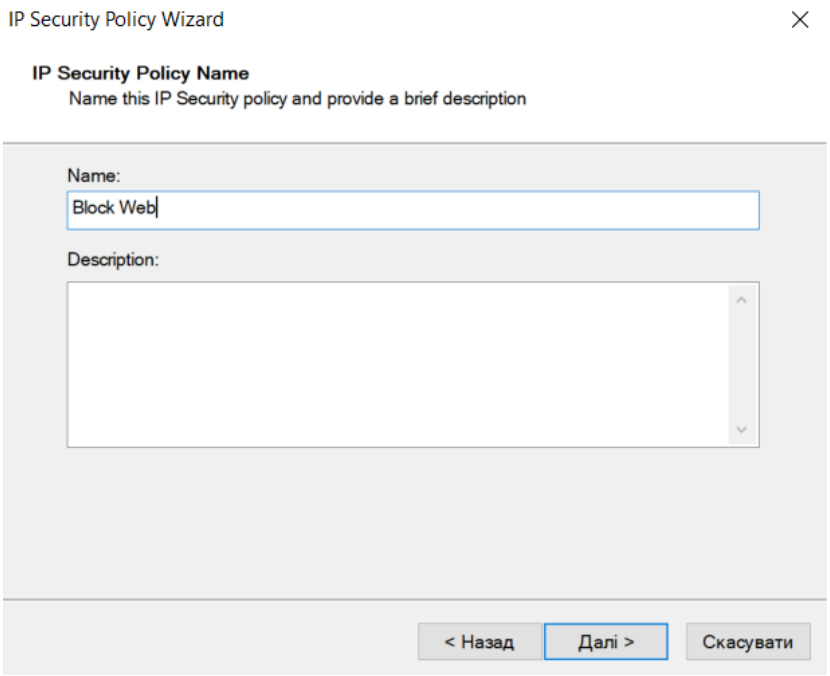


Рисунок 30. Створення нової політики IPSec

У вікні властивостей політики необхідно натиснути кнопку Додати (рис. 31).

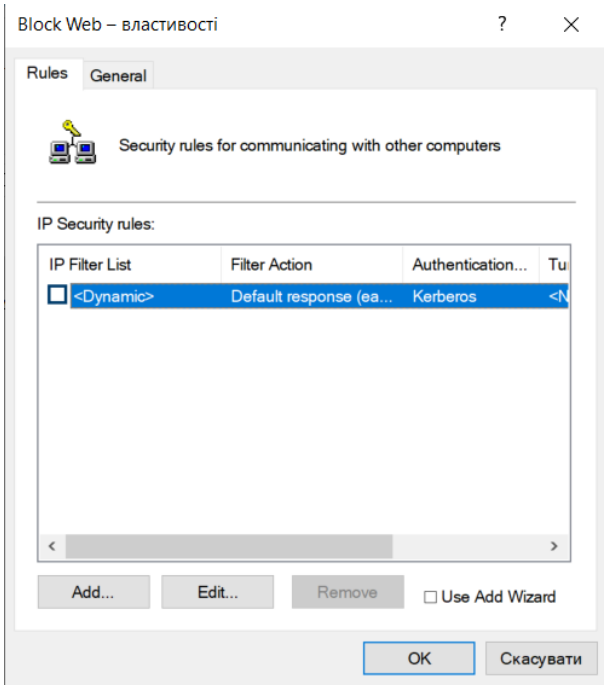


Рисунок 31. Створення нової політики IPSec

Після цього слід натиснути Далі, залишивши перемикач у положенні. Це правило не визначає тунель. Тип мережі – слід вказати Усі підключення до мережі, натиснути Далі. Тепер потрібно вибрати створений фільтр зі списку (рис. 32).

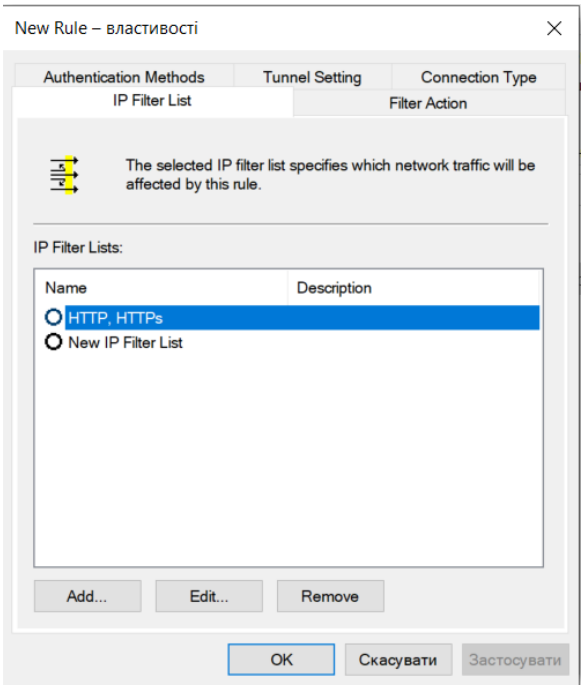


Рисунок 32. Створення нової політики IPSec

Так само слід вибрати створену дію для фільтра –BLOCK WEB, натиснути Далі та Готово.

Тепер у правій панелі консолі MMC з'явиться створена політика під назвою BLOCK WEB. Все, що лишилося зробити – призначити її. Для цього правою кнопкою миші потрібно викликати меню та вибрати команду Призначити.

Для перевірки роботи створеної політики IPSec слід запустити браузер. Якщо політика працює правильно, то сторінка браузера має виглядати так (рис. 33)

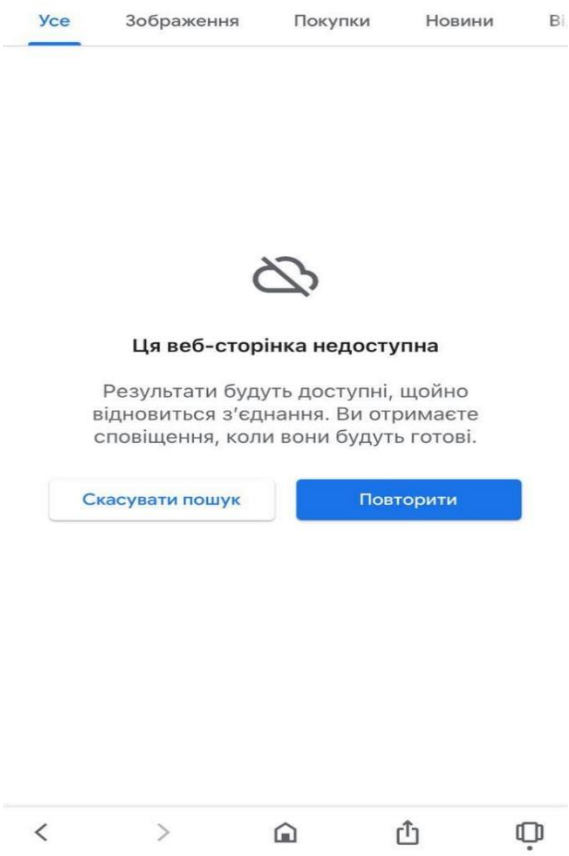


Рисунок 33. Перевірка

Також можна додати фільтр, який дозволятиме підключення лише до певних вузлів Інтернету. Для цього в консолі MMC необхідно двічі клацнути назву політики BLOCK WEB. У вікні властивостей натиснути кнопку Додати, потім подвійним клацанням вибрати фільтр HTTP, HTTPS. На вкладці Список фільтрів додати новий фільтр, вказавши для нього ім'я, натиснути Додати, Далі, як джерело пакетів вибрати варіант Мій IP-адресу, а в якості адреси призначення вибрати рядок Визначене DNS-ім'я, а в полі Ім'я вузла вказати ім'я певного вузла, до якого буде дозволено підключення.

Тепер фільтр міститиме два фільтри, один з яких забороняє весь http-трафік, а інший дозволяє з'єднання з певною IP-адресою. Тепер, при переході на

дозволений вузол браузер повинен відобразити зміст цього вузла, ресурси, розташовані на іншому хості (наприклад, рекламні банери), не відображатимуться – вони також фільтраватимуться застосованою політикою IPSec.

Завдання до лабораторної роботи

1. Запустіть консоль керування *IPSec* на вашому комп'ютері. Виберіть одну з політик *IPSec, використовувану за усталеним налаштуванням*, для цього відкрийте меню «*Локальна політика безпеки*» (*Local Security Policy*) у директорії «*Адміністрування*» (*Administrative Tools*) і виберіть розділ «*Політики безпеки IP на локальному комп'ютері*» (*IP Security Policies on Local Computer*). Ознайомтесь з принципами даної політики безпеки.

2. Створіть свій список фільтрів, зазначений, залежно від варіанта. Для цього виберіть у вікні «*Локальні настроювання безпеки*» *(Local Security Settings*) і виберіть у контекстному меню «*Дія*» пункт «*Керування списками IP-Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*). На закладці «*Керування списками фільтрів IP*» (*Manage IP Filter Lists*) натисніть кнопку «*Додати*» (*Add*). Введіть у поле ім'я назву списку. У стартовому вікні майстра *фільтрів* IP натисніть кнопку «Додати», а потім кнопку «Далі» (Next). Виберіть один із пропонованих варіантів в якості джерела призначення і протокол, що задовольняє вимогам вашого завдання. Виберіть пункт «*Пакети на цей порт*» (*To this port*) і введіть у поле значення, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готове*» (*Finish*).

Як джерело ви можете вибрати:

– «*Моя IP-Адреса*» (*My IP Address*);
– «*Люба IP-Адреса*» (*Any IP Address*);
– «*Певне DNS-Ім'я*» (*DNS name*);
– «*Певна IP-Адреса*» (*IP Address*);
– «*Певна* підмережа *IP*» (*IP network*).

Як призначення ви можете вибрати:

– «*Моя IP-Адреса*» (*My IP Address*);

– «*Люба IP-Адреса*» (*Any IP Address*);

– «*Певне DNS-Ім'я*» (*DNS name*)4

– «*Певна IP-Адреса*» (*IP Address*);

– «*Певна* підмережа *IP*» (*IP network*).

Як протокол ви можете вибрати:

– *EGP;*

– *HMP;*

– *ICMP;*

– *RAW;*

– *RDP;*

– *RVD;*

– *TCP;*

– *UDP;*

– *XNS-IDP;*

– *інші, із вказівкою номера порту;*

– *кожний*.

3. Створіть власну дію фільтра, зазначену, залежно від варіанта. Для цього в діалоговому вікні «*Керування списками IP-Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*) перейдіть на закладку «*Керування діями фільтра*» (*Manage Filter Actions*) і натисніть кнопку «*Додати*». У стартовому вікні майстра настроювання дій *фільтрів* IPSec натисніть кнопку «Далі». У вікні настроювання загальних параметрів дії фільтра виберіть один із пропонованих варіантів, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готово*». Для завершення настроювання списку і дій фільтрів, натисніть кнопку «*Закрити*» (*Close*).

У вікні настроювання загальних параметрів дії фільтра ви можете вибрати одну з наступних дій:

– «*погодити*» (*Negotiate*);

– «б*локувати*» (*Block*);

– «*дозволити*» (*Permit*).

4. Створіть свою політику *IPSec*. Для цього у вікні «*Локальні настроювання безпеки*» виберіть із контекстного меню пункт «*Створити політику безпеки IP*» (*Create IP Security Policy*) і у вікні майстра *політики IP*-безпеки натисніть кнопку «Далі». Уведіть у поле ім'я, назву вашої політики. Відмовтеся від використання пункту «*Використовувати правило за усталеним налаштуванням*» (*Activate the default response rule*) і натисніть «*Далі*». Залишіть пункт «*Змінити властивості*» (*Edit properties*) і натисніть кнопку «*Готово*» для завершення роботи майстра.

5. Додайте до створеної вами політики правило за зазначеними критеріями, залежно від варіанта. Для цього в діалоговому вікні властивостей політики натисніть кнопку «*Додати*», потім кнопку «*Далі*». З переліку списків фільтрів виберіть назву вашої політики. Зі списку дій фільтрів виберіть одну з дій. Для завершення роботи майстра натисніть кнопку «*Готове*».

6. Призначте обрану політику, для цього виберіть пункт «*Призначити*» (*Assign*) політики «*Назва вашої політики»*.

Варіанти завдань для виконання лабораторної роботи (Настроювання параметрів фільтра й політики *IPSec*):

1. Установлюючи політики на сервері вашої організації, створіть для комп'ютерів, які повинні використовувати безпечні з'єднання, політику, яка допускає небезпечні з'єднання з комп'ютерами не підтримуючими *IPSec*. Передбачте, щоб комп'ютер приймав незахищений трафік, але завжди виконував спробу захистити додаткові зв'язки, посилаючи відправникові запит безпеки. Включіть в політику правило запиту безпеки для всього *IP-трафіка,* метод перевірки дійсності *Kerberos*, без параметрів тунелюваня, для типу підключення – всіх мережних підключень.

2. Установлюючи політики на сервері вашої організації, створіть для комп'ютерів політику, яка дозволяє пересилати весь *ICMP-трафік*, не перевіряючи дійсність, без параметрів тунелюваня, для типу підключення – всіх мережних підключень.

3. Установлюючи політики на сервері вашої організації, створіть для

комп'ютерів політики відгуку за усталеним налаштуванням для відповіді на запити безпеки від інших комп'ютерів. Включіть в політику динамічний список фільтрів, для дії фільтра – відгук за усталеним налаштуванням, з методом перевірки *Kerberos*, без тунелювання, для типу підключення – всіх мережних підключень.

4. Сервер вашої організації передає секретні дані. Установіть політики на сервері, для комп'ютерів таким чином, щоб вони завжди вимагали захист усього вихідного трафіка, допускаючи відсутність захисту тільки для початкового вхідного запиту на з'єднання. Для цього включіть правило запиту безпеки для всього *IP-трафіка*, не перевіряючи дійсність, без тунелювання, для типу підключення – всіх мережних підключень.

5. Установіть політики на сервері вашої організації, для комп'ютерів, таким чином, щоб дозволити пересилати весь *ICMP-трафік*, перевіряючи дійсність методом *Kerberos*, без тунелювання, для типу підключення – всіх мережних підключень

6. Установіть політики на сервері вашої організації, для комп'ютерів, забезпечивши правило відгуку за усталеним налаштуванням для відповіді на запити безпеки від інших комп'ютерів. Для цього включіть в правило динамічний список фільтрів *IP*, з дією фільтра за усталеним налаштуванням, методом перевірки дійсності *Kerberos*, без тунелювання, для типу підключення – всіх мережних підключень.

7. Створіть політики для комп'ютерів, які захищають дані за запитом, для рішення задачі, коли клієнти інтрамережі можуть не вимагати використання *IPSec*, крім випадків, коли запит виходить із іншого комп'ютера, щоб забезпечити комп'ютеру, на якому активізована політика, відповідати на запити безпечного зв'язку. Включіть в політику правило відгуку за усталеним налаштуванням, що створює динамічні фільтри *IP* для вхідного і вихідного трафіка на основі методу перевірки дійсності *Kerberos*, без тунелювання, для типу підключення – всіх мережних підключень.

8. Дозвольте дію, задавши, у фільтрі *IP*, політику для взаємодії з *DNS* сервером таким чином, щоб дані передавалися з адреси вашого комп'ютера, на

будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, за 53 порт *tcp* і *udp* протоколів. Включіть в політику правило зв'язку списку з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.

9. Дозвольте дію, задавши, у фільтрі *IP*, політики для взаємодії з *SQL* сервером таким чином, щоб дані передавалися з адреси вашого комп'ютера на будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, за порт *1433* порту *tcp* і *udp* протоколами. Включіть в політику правило зв'язку списку з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності кожної з них, без тунелюваня, для типу підключення – всіх мережних підключень.

10. Дозвольте дію, задавши, у фільтрі *IP*, політики для Web-*Сервера* таким чином, щоб з будь-якої адреси й будь-якого порту передавалися дані на адресу вашого комп'ютера, за *80*/*tcp* портом й з будь-якої адреси, будь-якого порту, передавалися дані на адресу вашого комп'ютера за портом *443*/*tcp*.

11. Створіть політики для комп'ютерів, створивши правило для фільтрації вихідного трафіка, тобто від адреси комп'ютера, на будь-яку адресу, за портом *1434*/*udp*. За допомогою даного правила заблокуйте будь-який вихідний трафік через порти *UDP 1434* інших комп'ютерів мережі.

12. Налаштуйте політики ізолювання доменів використовуючи наступні правила. Використовуйте налаштування для всього трафіка *IP*, дія фільтра: тільки *Encapsulating Security Payload* (*ESP*), нульове шифрування (null encryption), перевірка цілісності *SHA-1* (*SHA-1 integrity*), обов'язковий захист (*require security*), заборона взаємодії між комп'ютерами без використання протоколу *IPSec*. При цьому дозволивши дії фільтрів, що містять адреси або діапазон адрес контролерів домена.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (1-2 сторінки):

— призначення IPsec, основні компоненти (AH, ESP, SA, політика, фільтр, дія фільтра);

— режими роботи IPsec (транспортний / тунельний);

— приклади використання IPsec у корпоративних мережах.

4. Практичну частину, що включає:

— опис створення політики IPsec (назва політики, метод автентифікації, тип з'єднання);

— опис створених списків фільтрів (джерело, призначення, протокол, порти);

— опис створених дій фільтра (Block / Permit / Negotiate, параметри ESP/AH);

— скріншоти ключових вікон налаштування (Local Security Policy, властивості політики, списки фільтрів, дії фільтра);

— результати перевірки роботи політики (ping, доступ/відсутність доступу до веб-ресурсів тощо);

— за можливості – таблицю результатів тестування продуктивності (час передачі, швидкість, завантаженість процесора для різних конфігурацій IPsec).

5. Відповіді на контрольні питання / аналіз виконаного варіанта індивідуального завдання.

6. Висновки, де здобувач вищої освіти:

— узагальнює роль IPsec у захисті мережевого трафіка;

— описує отримані практичні навички;

— оцінює вплив увімкнення IPsec на продуктивність системи;

— формулює рекомендації щодо використання IPsec та політик фільтрації в реальних мережах.

7. Список використаних джерел – згідно з вимогами до оформлення бібліографічних посилань (ДСТУ 8302:2015).

4. Підбиття підсумків заняття

— обговорення результатів налаштування політик IPsec у студентів;

— аналіз правильності реалізації фільтрів та дій фільтра, відповідності індивідуальним варіантам;

— аналіз впливу різних конфігурацій IPsec на продуктивність і зручність використання;

— оцінювання повноти та якості звітів, уміння аргументувати вибір параметрів безпеки;

— формулювання узагальнених висновків щодо значення IPsec у комплексній системі захисту мережі.

5. Список рекомендованої літератури

Основна:

1. Комп’ютерні мережі : навч. посіб. / А. Саченко, Ю. Кулаков, В. Кочан [та ін.]. Тернопіль : ВПЦ «Економічна думка ТНЕУ», 2016. 476 с.
2. Буров Є. В. Комп’ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.
3. Валецька Т. М. Комп’ютерні мережі : апаратні засоби : навч. посіб. Київ : Ельга, 2004.
4. Лозінова Г. М. Комп’ютерні мережі : навч. посіб. Київ : Кондор, 2003.

Додаткова:

1. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.
2. Кулаков Ю. О. Комп’ютерні мережі : навч. посіб. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 247 с. URL: https://ela.kpi.ua/handle/123456789/51465.

Інформаційні ресурси:

1. Віртуальний університет ЛДУБЖД : електронне навчальне середовище. URL: https://virt.ldubgd.edu.ua
2. Cisco Networking Academy [Електронний ресурс]. URL: http://www.netacad.com

ЛАБОРАТОРНА РОБОТА № 6

Тема: налаштування віртуальних локальних мереж VLAN та маршрутизації між ними.

Мета: сформувати розуміння принципів логічної сегментації мережі за допомогою VLAN; набути практичних навичок створення та налаштування VLAN на комутаторах рівня 2 і 3; навчитися конфігурувати порти доступу та транкові порти, у тому числі з використанням native VLAN та voice VLAN; відпрацювати налаштування маршрутизації між VLAN (Router-on-a-Stick, багаторівневий комутатор); сформувати навички діагностики та усунення несправностей, пов'язаних з VLAN та інтер-VLAN маршрутизацією.

Місце проведення: згідно з розкладом.

Час: 8 годин.

Основні поняття: *VLAN (Virtual Local Area Network)* – віртуальна локальна мережа, логічна група вузлів в межах одного або кількох комутаторів. Вузли однієї VLAN належать до одного широкомовного домена, незалежно від фізичного розміщення портів.

Порт доступу (Access port) – порт комутатора, який передає трафік лише однієї VLAN. Приєднані до нього кінцеві пристрої (PC, принтери, IP-телефони) бачать звичайні кадри Ethernet без тегу VLAN.

Транковий порт (Trunk port) – порт, який одночасно передає трафік кількох VLAN. Для розділення трафіка використовується інкапсуляція IEEE 802.1Q (додається тег VLAN у заголовок кадру). Застосовується для з'єднання комутаторів між собою або з маршрутизатором / L3-комутатором.

Native VLAN – VLAN за усталеним налаштуванням для транкового порту. Трафік цієї VLAN передається без тегу 802.1Q. Невідповідність native VLAN на різних кінцях транку може призвести до помилок маршрутизації та потенційних вразливостей безпеки.

Data VLAN – VLAN, яка використовується для передавання звичайного користувацького трафіка (робочі станції, сервіси).

Voice VLAN – VLAN, виділена для IP-телефонії. Дозволяє відокремити голосовий трафік, налаштувати QoS (quality of service) та забезпечити прийнятну якість голосового зв'язку.

Management VLAN – VLAN, що використовується для віддаленого адміністрування комутаторів та інших мережевих пристроїв (Telnet/SSH, SNMP, HTTP(S)-доступ).

QoS (Quality of Service) – механізми забезпечення якості обслуговування: пріоритизація трафіка, резервування пропускної здатності, управління чергами.

CoS (Class of Service) – поле у тегу 802.1Q, яке дозволяє маркувати кадри Ethernet пріоритетами для подальшої обробки QoS.

Router-on-a-Stick – спосіб маршрутизації між VLAN, коли один фізичний інтерфейс маршрутизатора працює в магістральному режимі (trunk), а для кожної VLAN створюються підінтерфейси з власними IP-адресами (шлюзами за усталеним налаштуванням для відповідних VLAN).

SVI (Switched Virtual Interface) – логічний інтерфейс VLAN на багаторівневому комутаторі. SVI має IP-адресу і виконує роль шлюзу для вузлів VLAN, а комутатор рівня 3 здійснює маршрутизацію між цими SVI.

Багаторівневий комутатор (Layer 3 switch) – комутатор, здатний виконувати операції L2 (комутація) та L3 (маршрутизація). Забезпечує високошвидкісну маршрутизацію між VLAN без необхідності окремого маршрутизатора.

Маршрутизація між VLAN (Inter-VLAN routing) – процес передавання трафіка між різними VLAN за допомогою маршрутизатора або багаторівневого комутатора. Кожна VLAN є окремою IP-підмережею, і для її зв'язку з іншими потрібен L3-пристрій.

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до локальної мережі та Інтернету; операційна система: Windows / Linux (на розсуд викладача); симулятор мережі Cisco Packet Tracer (актуальна версія); веббраузер для роботи з електронним курсом та мережевими сервісами; текстовий редактор (MS Word / LibreOffice Writer / Google Docs або аналог) для оформлення звіту; електронний навчальний курс дисципліни у ВНС «Віртуальний університет»; віртуальні мережеві пристрої в Packet Tracer: – комутатори L2 (S1, S2, S3); – багаторівневий комутатор L3; – маршрутизатор (R1); – кінцеві пристрої (PC, IP Phone); попередньо підготовлені файли-сценарії Packet Tracer (topology файли для Завдань 1-5 – за потреби).

План:

1. Організаційні заходи

— повідомлення теми, мети та завдань лабораторної роботи;

— мотивація: роль VLAN та маршрутизації між VLAN у безпеці, масштабованості й керованості корпоративних мереж;

— ознайомлення з матеріалами лабораторної роботи в електронному курсі («Віртуальний університет»);

— інструктаж з техніки безпеки при роботі з комп'ютерною технікою та програмним забезпеченням;

— пояснення вимог до оформлення звіту та критеріїв оцінювання.

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: базові поняття комп'ютерних мереж (LAN, MAC-адреса, кадр Ethernet, комутатор, маршрутизатор); розуміння різниці між фізичною (L1) та канальною (L2) топологією; уявлення про VLAN, порти доступу (access) та транкові порти (trunk); базове розуміння маршрутизації між підмережами (default gateway, інтерфейс маршрутизатора); знайомство з базовими командами Cisco IOS (enable, configure terminal, interface, show vlan brief, show interface trunk тощо).

Перелік дидактичних одиниць для перевірки: поняття VLAN, типи VLAN (data VLAN, voice VLAN, management VLAN, native VLAN); призначення портів access і trunk; інкапсуляція 802.1Q; агальний принцип Router-on-a-Stick; роль

багаторівневого комутатора (Layer 3 switch, SVI); принцип роботи шлюзу за усталеним налаштуванням для вузлів у VLAN.

Приблизні питання для усного опитування / самоконтролю:

1. Що таке VLAN і для чого її використовують?
2. У чому різниця між портом access і trunk?
3. Що таке native VLAN і чому її неправильно налаштовані значення можуть бути загрозою безпеці?
4. Що таке voice VLAN і навіщо її виділяють окремо?
5. Як реалізується маршрутизація між VLAN методом Router-on-a-Stick?
6. У чому відмінність між інтер-VLAN маршрутизацією на маршрутизаторі (Router-on-a-Stick) та на багаторівневому комутаторі (SVI)?
7. Чому вузли в різних VLAN не можуть обмінюватися трафіком без маршрутизації?

3. Формування професійних умінь та навичок

Завдання 1 – Налаштування VLAN

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	10
PC2	NIC	172.17.20.22	255.255.255.0	20
PC3	NIC	172.17.30.23	255.255.255.0	30
PC4	NIC	172.17.10.24	255.255.255.0	10
PC5	NIC	172.17.20.25	255.255.255.0	20
PC6	NIC	172.17.30.26	255.255.255.0	30

Цілі та задачі:

Частина 1. Перегляд налаштувань VLAN за усталеним налаштуванням.

Частина 2. Налаштування VLAN.

Частина 3. Встановлення належності портів до VLAN.

ДОВІДКОВА ІНФОРМАЦІЯ

VLAN корисні при адмініструванні логічних груп користувачів, дозволяючи їх легко переміщувати, змінювати або додавати. Це завдання

фокусується на створенні VLAN, призначенні їм назв та встановленні належності портів доступу до певних VLAN.

Частина 1. Перегляд налаштувань VLAN за усталеним налаштуванням

Крок 1. Відображення наявних VLAN

На комутаторі S1 виконаємо команду, яка відображає всі налаштовані VLAN. За усталеним налаштуванням всі інтерфейси комутатора належать до VLAN 1.

Крок 2. Перевірка зв'язку між комп'ютерами однієї мережі

Зверніть увагу, що кожен комп'ютер може перевірити зв'язок за допомогою команди ping з іншим комп'ютером, який належить ті й же підмережі.

— Комп'ютер PC1 може перевірити зв'язок за допомогою команди ping з комп'ютером PC4

— Комп'ютер PC2 може перевірити зв'язок за допомогою команди ping з комп'ютером PC5

— Комп'ютер PC3 може перевірити зв'язок за допомогою команди ping з комп'ютером PC6 Перевірити зв'язок за допомогою команди ping з вузлами з інших мереж не вдається.

Які переваги використання VLAN у комп'ютерній мережі?

Частина 2. Налаштування VLAN

Крок 1. Створення та іменування VLAN на комутаторі S1

a. Створіть такі VLAN. Назви VLAN чутливі до регістру і повинні точно відповідати вимогам:

VLAN 10: Faculty/Staff

S1# (config)# vlan 10

S1# (config-vlan)# name Faculty/Staff

b. Створіть решту VLAN.

VLAN 20: Students

VLAN 30: Guest(Default)

VLAN 99: Management&Native

VLAN 150: VOICE

Крок 2. Перевірка налаштувань VLAN

Яка команда відобразить лише ім'я VLAN, її стан та перелік включених до неї портів ?

Крок 3. Створення VLAN на комутаторах S2 та S3

Використовуйте команди з кроку 1, щоб створити і іменувати відповідні VLAN на комутаторах S2 та S3.

Крок 4. Перевірка налаштувань VLAN.

Частина 3. Встановлення належності портів до VLAN

Крок 1. Встановлення належності активних портів до VLAN на комутаторі S2

a. Налаштуйте інтерфейси комутатора як порти доступу і встановіть їх належність до VLAN:

VLAN 10: FastEthernet 0/11

S2(config)# interface f0/11

S2(config-if)# switchport mode acces

S2(config-if)# switchport access vlan 10

b. Встановіть належність решти портів до відповідних VLAN.

VLAN 20: FastEthernet 0/18

VLAN 30: FastEthernet 0/6

Крок 2. Встановлення належності активних портів до VLAN на комутаторі S3

На комутаторі S3 використовуються такі ж налаштування портів доступу VLAN, що і на комутаторі S2. Налаштуйте інтерфейси комутатора як порти доступу і встановіть їх належність до VLAN:

VLAN 10: FastEthernet 0/11

VLAN 20: FastEthernet 0/18

VLAN 30: FastEthernet 0/6

Крок 3. Встановлення належності порту FastEthernet 0/11 до VOICE VLAN на комутаторі S3

На рисунку показано, що до інтерфейсу FastEthernet 0/11 комутатора S3

підключені IP-телефон Cisco IP Phone0 і комп'ютер PC4. IP-телефон містить вбудований трипортовий комутатор 10/100 Мбіт/с. Один порт телефона має позначення Switch і саме через нього телефон підключений до порту комутатора F0/11. Ще один порт телефона має позначення PC і саме до нього підключається комп'ютер PC4. IP-телефон також має вбудований порт, через який забезпечується доступ до його функцій.

Інтерфейс F0/11 комутатора S3 повинен бути налаштований таким чином, щоб забезпечити передачу трафіка користувача комп'ютера PC4 (VLAN 10) і голосового трафіка IP-телефона (VLAN 150). Також на цьому інтерфейсі необхідно активувати функцію QoS та використання значень класу обслуговування (CoS), призначених IP-телефоном. Підтримка прийнятної якості голосового зв'язку для голосового IP-трафіка вимагає виділення мінімальної пропускної здатності. Наведена нижче команда дозволяє забезпечити мінімальну пропускну здатність на порті комутатора.

```
S3(config)# interface f0/11
S3(config-if)# mls qos trust cos
S3(config-if)# switchport access vlan 150
```

Крок 4. Перевірка втрати зв'язку

Раніше комп'ютери, що мали спільний доступ до однієї мережі, могли успішно перевіряти зв'язок один з одним за допомогою команди ping.

Проаналізуйте результати виведення команди, що виконана на комутаторів S2 та, використовуючи Ваші знання щодо VLAN, дайте відповіді на питання. Зверніть увагу на налаштування порту Gig0/1.

```
S2# show vlan brief
VLAN Name Status Ports
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/12,
Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17,
Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2
10 Faculty/Staff active Fa0/11
```

20 Students active Fa0/18

30 Guest(Default) active Fa0/6

99 Management&Native active

150 VOICE active

Спробуйте перевірити зв'язок між комп'ютерами PC1 і PC4 за допомогою команди ping.

Хоча для портів доступу було виконано налаштування належності до певних VLAN, чи була перевірка зв'язку успішною? Поясніть.

Що можна зробити для вирішення цієї проблеми?

Завдання 2 – Налаштування транкового каналу

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Порт комутатора	VLAN
PC1	NIC	172.17.10.21	255.255.255.0	S2 F0/11	10
PC2	NIC	172.17.20.22	255.255.255.0	S2 F0/18	20
PC3	NIC	172.17.30.23	255.255.255.0	S2 F0/6	30
PC4	NIC	172.17.10.24	255.255.255.0	S3 F0/11	10
PC5	NIC	172.17.20.25	255.255.255.0	S3 F0/18	20
PC6	NIC	172.17.30.26	255.255.255.0	S3 F0/6	30

Цілі та задачі:

Частина 1. Перевірка VLAN.

Частина 2. Налаштування транкових каналів зв'язку.

ДОВІДКОВА ІНФОРМАЦІЯ

Транкові канали необхідні для передавання інформації певних VLAN між комутаторами. Порт комутатора може бути або портом доступу, або транковим портом. Порти доступу передають трафік тієї VLAN, до якої він належить. За усталеним налаштуванням транковий порт є членом всіх VLAN. Тому він передає трафік всіх VLAN. Це завдання фокусується на створенні транкових портів і налаштуванні для них Native VLAN, відмінної від прийнятої за усталеним налаштуванням.

Інструкції

Частина 1. Перевірка налаштувань VLAN

Крок 1. Відображення наявних VLAN

a. На комутаторі S1 виконайте команду, яка відобразить всі налаштовані на ньому VLAN. Всього має бути десять VLAN. Зверніть увагу на те, що всі 26 портів доступу комутатора належать до VLAN 1.

b. На комутаторах S2 та S3 виведіть перелік VLAN та переконайтеся, що всі VLAN налаштовані коректно, також переконайтеся, що порти комутатора належать до відповідних VLAN. Для перевірки скористайтеся даними таблиці адресації.

Крок 2. Перевірка втрати зв'язку між комп'ютерами однієї і тієї ж мережі

За допомогою команди ping перевірте зв'язок між вузлами, що належать до однієї VLAN, але підключені до різних комутаторів. Хоча комп'ютери PC1 та PC4 належать до однієї мережі, вони не можуть взаємодіяти один з одним. Це пояснюється тим, що для портів, які з'єднують комутатори, за усталеним налаштуванням налаштовано належність до VLAN 1. Для того, щоб забезпечити передавання даних між комп'ютерами однієї мережі та VLAN, необхідно налаштувати транкові канали зв'язку.

Частина 2. Налаштування транкового каналу

Крок 1. Налаштування транкового каналу на комутаторі S1 та налаштування використання VLAN 99 як Native VLAN

a. Налаштуйте інтерфейси G0/1 і G0/2 комутатора S1 для транкування.

S1(config)# interface range g0/1 - 2

S1(config-if)# switchport mode trunk

b. Налаштування VLAN 99 як Native VLAN для інтерфейсів G0/1 і G0/2 комутатора S1.

S1(config-if)# switchport trunk native vlan 99

Транковому портові необхідний певний час для того, щоб стати активним. Ця затримка викликана необхідністю виконання процедур протоколу Spanning Tree Protocol. Для прискорення процесу натисніть кнопку Fast Forward Time.

Після того, як порти стануть активними, Ви періодично отримуватимете такі syslog-повідомлення:

- %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (99), with S3 GigabitEthernet0/2 (1).
- %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (99), with S2 GigabitEthernet0/1 (1).

Ви налаштували VLAN 99 як Native VLAN на комутаторі S1. Однак комутатори S2 і S3 ще використовують VLAN 1 як Native VLAN за замовчування, про що зазначено у syslog-повідомленні.

Хоча ви маєте невідповідність Native VLAN, перевірка зв'язку за допомогою команди ping між комп'ютерами однієї і тієї ж VLAN вже є успішною. Поясніть.

Крок 2. Перевірка, чи активовано транкування на комутаторах S2 та S3

Виконайте команду show interface trunk на комутаторах S1 та S2 для того, щоб пересвідчитися, що протокол DTP успішно узгодив параметри транкових каналів між комутатором S1 та комутаторами S2 та S3. Виведені результати також відображають інформацію про транкові інтерфейси комутаторів S2 і S3. Ви дізнаєтеся більше про протокол DTP при подальшому розгляді курсу.

Яким активним VLAN дозволено передавати свої дані через транковий канал?

Крок 3. Виправлення невідповідності Native VLAN на комутаторах S2 і S3

a. Налаштуйте VLAN 99 як Native VLAN для відповідних інтерфейсів на комутаторах S2 і S3.

b. Виконайте команду show interface trunk для того, що перевірити правильність налаштування Native VLAN.

Крок 4. Перевірка налаштувань на комутаторах S2 та S3

a. Виконайте команду show interface switchport для того, щоб переконатися, що Native VLAN має номер 99.

b. Використайте команду show vlan для відображення інформації щодо налаштованих VLAN. Чому порт G0/1 комутатора S2 більше не належить до VLAN 1?

Завдання 3 - Налаштування маршрутизації між VLAN методом Router-on-a-Stick

Таблиця адресації

Пристрій	Інтерфейс	Адреса IPv4	Маска підмережі	Шлюз за усталеним налаштуванням
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.30	172.17.30.1	255.255.255.0	
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1
PC2	NIC	172.17.30.10	255.255.255.0	172.17.30.1

Цілі та задачі

Частина 1: Додавання VLAN на комутаторі

Частина 2: Налаштування підінтерфейсів маршрутизатора

Частина 3: Перевірка з'єднання та маршрутизації між VLAN

Сценарій. У цьому завданні ви налаштуєте VLAN і маршрутизацію між VLAN. А також налаштуєте магістральні інтерфейси і перевірите зв'язок між мережами VLAN.

Інструкції

Частина 1: Додавання VLAN на комутаторі

Крок 1: Створіть VLAN на комутаторі S1

Створіть VLAN 10 і VLAN 30 на S1.

Крок 2: Налаштуйте належність портів до VLAN

a. Налаштуйте інтерфейси F0/6 і F0/11 в якості портів доступу і призначте їм VLAN.

- Призначте порт, підключений до PC1 для VLAN 10.
- Призначте порт, підключений до PC3 для VLAN 30.

b. Виконайте команду show vlan brief, щоб перевірити конфігурацію VLAN.

S1# show vlan brief

VLAN Name Status Ports

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/12, Fa0/13, Fa0/14 Fa0/15,

Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20,

Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gig0/1, Gig0/2

10 VLAN0010 active Fa0/11

30 VLAN0030 active Fa0/6

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

Крок 3: Перевірте з'єднання між PC1 і PC3

Відправте запит ping з PC1 на PC3.

Чи був ping вдалим? Чому ви отримали такий результат?

Частина 2: Налаштування підінтерфейсів

Крок 1: Налаштуйте підінтерфейси на R1 за допомогою інкапсуляції 802.1Q

a. Створіть підінтерфейс G0/0.10.

- Встановіть тип інкапсуляції 802.1Q і призначте VLAN 10 для підінтерфейсу.
- Зверніться до Таблиці адресації і призначте підінтерфейсу правильну IP-адресу.

R1(config)# int g0/0.10

R1(config-subif)# encapsulation dot1Q 10

R1(config-subif)# ip address 172.17.10.1 255.255.255.0

b. Повторіть це для підінтерфейсу G0/0.30.

Крок 2: Перевірте конфігурацію

a. Команда show ip interface brief застосовується для перевірки конфігурації підінтерфейсу. Обидва підінтерфейси відключені. Підінтерфейси - це віртуальні інтерфейси, пов'язані з фізичним інтерфейсом. Тому для того, щоб включити підінтерфейси, необхідно включити фізичний інтерфейс, з яким вони пов'язані.

b. Увімкніть інтерфейс G0/0. Переконайтеся, що підінтерфейси тепер активні.

Частина 3: Перевірка з'єднання та маршрутизації між VLAN

Крок 1: Відправите запит ping з PC1 до PC3

Відправте запит ping з PC1 на PC3. Запит ping повинен завершитися помилкою. Поясніть.

Крок 2: Увімкніть магістральний канал

a. На S1 вводимо команду show vlan.

Яку VLAN призначено для G0/1?

b. Оскільки маршрутизатор був налаштований з декількома підінтерфейсами, призначеними для різних VLAN, порт комутатора, що підключається до маршрутизатора, повинен бути налаштований як магістральний канал. Увімкніть магістральний канал на інтерфейсі G0/1.

Як можна визначити за допомогою команди show vlan, що інтерфейс є магістральним каналом?

c. Виконайте команду show interface trunk, щоб переконатися, що інтерфейс налаштований як магістральний канал.

Крок 3: Перевірка з'єднання

Якщо конфігурації правильні, PC1 і PC3 повинні мати можливість відправляти запити ping на свої шлюзи за усталеним налаштуванням і один до одного.

Які адреси використовують PC1 і PC3 як адреси шлюзу за усталеним налаштуванням?

Завдання 4 - Налаштування комутації рівня 3 та маршрутизації між VLAN

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс
Багаторівневий комутатор	VLAN 10	192.168.10.254 /24
		2001:db8:acad:10::1/64
	VLAN 20	192.168.20.254 /24

		2001:db8:acad:20::1/64
	VLAN 30	192.168.30.254/24
		2001:db8:acad:30::1/64
	VLAN 99	192.168.99.254/24
	G0/2	209.165.200.225
		2001:db8:acad:a::1/64
PC0	NIC	192.168.10.1
PC1	NIC	192.168.20.1
PC2	NIC	192.168.30.1
PC3	NIC	192.168.10.2/24
		2001:db8:acad:10::2/64
PC4	NIC	192.168.20.2/24
		2001:db8:acad:20::2/64
PC5	NIC	192.168.30.2
		2001:db8:acad:10::2/64
S1	VLAN 99	192.168.99.1
S2	VLAN 99	192.168.99.2
S3	VLAN 99	192.168.99.3

Цілі та задачі

Частина 1: Налаштування комутації рівня 3

Частина 2: Налаштування маршрутизації між VLAN

Частина 3: Налаштування IPv6 маршрутизації між VLAN

Сценарій. Багаторівневий комутатор, такий як Cisco Catalyst 3650, здатний виконувати як комутацію рівня 2, так і маршрутизацію рівня 3. Однією з переваг використання багаторівневого комутатора є подвійний функціонал. Вигода для компанії малого і середнього розміру буде в тому, щоб придбати один багаторівневий комутатор замість окремих комутатора і маршрутизатора. Функціонал багаторівневого комутатора включає можливість маршрутизації трафіка з однієї VLAN в іншу за допомогою декількох комутованих віртуальних

інтерфейсів (SVI), а також можливість перетворення комутаційного порту рівня 2 в інтерфейс рівня 3.

Інструкції

Частина 1: Налаштування комутації рівня 3

У частині 1 ви налаштуєте порт GigabitEthernet 0/2 на багаторівневому комутаторі як маршрутизований порт і переконаєтеся, що ви можете отримувати відповіді команди ping з іншої адреси рівня 3.

a. На багаторівневому комутаторі налаштуйте G0/2 як маршрутизований порт і призначте IP-адресу відповідно до таблиці адресації.

MLS(config)# interface g0/2

MLS(config-if)# no switchport

MLS(config-if)# ip address 209.165.200.225 255.255.255.252

b. Перевірте підключення до хмари Cloud, надіславши запит ping на адресу 209.165.200.226.

MLS# ping 209.165.200.226

Type escape sequence to abort.

Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Частина 2: Налаштування маршрутизації між VLAN

Крок 1: Додайте мережі VLAN

Додайте VLAN в багаторівневий комутатор відповідно до наведеної нижче таблиці. Підрахунок балів у Packet Tracer чутливий до регістру, тому введіть імена точно так, як показано.

Номер VLAN	Назва VLAN
10	Staff
20	Student
30	Faculty

Крок 2: Налаштуйте SVI на багаторівневому комутаторі

Налаштуйте та активуйте інтерфейс VLAN 1 на комутаторі відповідно до

таблиці адресації. Конфігурація для VLAN 10 показана нижче як приклад.

MLS(config)# interface vlan 10

MLS(config-if)# ip address 192.168.10.254 255.255.255.0

Крок 3: Налаштуйте магістральний канал на багаторівневому комутаторі

Налаштування магістрального каналу трохи відрізняється на комутаторі рівня 3. На комутаторі рівня 3 інтерфейс магістрального каналу потрібно інкапсулювати протоколом dot1q, однак номери VLAN вказувати не обов'язково так, як це робиться з маршрутизатором і під-інтерфейсами.

a. На багаторівневому комутаторі MLS налаштуйте інтерфейс g0/1.

b. Переведіть інтерфейс в статичний магістральний порт.

MLS(config-if)# switchport mode trunk

c. Вкажіть native VLAN як 99.

MLS(config-if)# switchport trunk native vlan 99

d. Інкапсулюйте з'єднання за протоколом dot1q.

MLS(config-if)# switchport trunk encapsulation dot1q

Примітка: Packet Tracer може не оцінити інкапсуляцію магістрального каналу.

Крок 4: Налаштуйте магістральний канал на S1

a. Налаштуйте інтерфейс g0/1 S1 як магістральний канал.

b. Налаштуйте native VLAN на магістральному каналі.

Крок 5: Активуйте маршрутизацію

a. Використовуйте команду show ip route . Чи є активні маршрути?

b. Щоб увімкнути маршрутизацію, введіть команду ip routing в режимі глобальної конфігурації.

MLS(config)# ip routing

c. Використовуйте команду show ip route , щоб перевірити, що маршрутизація увімкнена.

MLS# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, Vlan10 C 192.168.20.0/24 is directly connected, Vlan20 C 192.168.30.0/24 is directly connected, Vlan30 C 192.168.99.0/24 is directly connected, Vlan99

209.165.200.0/30 is subnetted, 1 subnets

C 209.165.200.224 is directly connected, GigabitEthernet0/2

Крок 6: Перевірте наскрізне з'єднання

Відправте запит ping з PC0 на PC3 або на MLS для перевірки підключення в межах VLAN 10.

a. Відправте запит ping з PC1 на PC4 або на MLS для перевірки підключення в межах VLAN 20.

b. Відправте запит ping з PC2 на PC5 або на MLS для перевірки підключення в межах VLAN 30.

c. Відправте запит ping з S1 на S2 та S3 або на MLS для перевірки підключення в межах VLAN 99.

d. Щоб перевірити маршрутизацію між VLAN, відправте запит ping на пристрої поза VLAN відправника.

e. З будь-якого пристрою відправте запит ping на адресу 209.165.200.226 всередині хмари Cloud.

Комутатор рівня 3 тепер маршрутизує трафік між VLAN і забезпечує маршрутизацію підключення до хмари.

Частина 3: Налаштування IPv6 маршрутизації між VLAN

Комутатори рівня 3 також можуть виконувати маршрутизацію між мережами IPv6.

Крок 1: Увімкніть маршрутизацію IPv6

Введіть команду ipv6 unicast-routing, щоб увімкнути маршрутизацію IPv6

в режимі глобальної конфігурації.

MLS(config)# ipv6 unicast-routing

Крок 2: Налаштуйте SVI для IPv6 на багаторівневому комутаторі

Налаштуйте адресацію IPv6 на SVI для VLAN 10, 20 і 30 згідно з таблицею адресації. Конфігурація для

VLAN 10 представлена нижче.

MLS(config)# interface vlan 10

MLS(config-if)# ipv6 address 2001:db8:acad:10::1/64

Крок 3: Налаштуйте G0/2 для IPv6 на MLS

a. Налаштуйте адресацію IPv6 на G0/2.

MLS(config)# interface G0/2

MLS(config-if)# ipv6 address 2001:db8:acad:a::1/64

b. Використовуйте команду show ipv6 route для перевірки підключених мереж IPv6.

MLS# show ipv6 route

IPv6 Routing Table - 10 entries

Codes: C – Connected, L – Local, S – Static, R – RIP, B – BGP U – Per-user Static route, M – MIPv6

I1 – ISIS L1, I2 – ISIS L2, IA – ISIS interarea, IS – ISIS summary O – OSPF intra, OI – OSPF inter, OE1 – OSPF ext 1, OE2 – OSPF ext 2 ON1 – OSPF NSSA ext 1, ON2 – OSPF NSSA ext 2

D – EIGRP, EX – EIGRP external S ::/0 [1/0]

via 2001:DB8:ACAD:A::2, GigabitEthernet0/2 C 2001:DB8:ACAD:A::/64 [0/0]

via ::, GigabitEthernet0/2 L 2001:DB8:ACAD:A::1/128 [0/0]

via ::, GigabitEthernet0/2 C 2001:DB8:ACAD:10::/64 [0/0]

via ::, Vlan10

L 2001:DB8:ACAD:10::1/128 [0/0]

via ::, Vlan10

C 2001:DB8:АКАД:20 /64 [0/0]

via ::, Vlan20

L 2001:DB8:ACAD:20::1/128 [0/0]

via ::, Vlan20

C 2001:DB8:ACAD:30::/64 [0/0]

via ::, Vlan30

L 2001:DB8:ACAD:30::1/128 [0/0]

via ::, Vlan30 L FF00::/8 [0/0]

via ::, Null0

Крок 4: Перевірте з'єднання IPv6

Пристрої PC3, PC4 і PC5 були налаштовані з адресами IPv6. Перевірте маршрутизацію IPv6 між VLAN та підключення до хмари Cloud.

a. Відправте запит ping з PC3 на MLS для перевірки підключення в межах VLAN 10.

b. Відправте запит ping з PC4 на MLS для перевірки підключення в межах VLAN 20.

c. Відправте запит ping з PC5 на MLS для перевірки підключення в межах VLAN 30.

d. Щоб перевірити міжмережеву маршрутизацію, відправте запит ping між пристроями PC3, PC4 та PC5.

e. Відправте запит ping з PC3 на адресу 2001:db8:acad:a::2 всередині хмари Cloud.

Завдання 5 – Усунення несправностей маршрутизації між мережами VLAN

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за усталеним налаштуванням	VLAN
R1	G0/1.10	172.17.10.1	255.255.255.0	N/A	VLAN 10
	G0/1.30	172.17.30.1	255.255.255.0	N/A	VLAN 30
PC1	NIC	172.17.10.10	255.255.255.0	172.17.10.1	VLAN 10
PC3	NIC	172.17.30.10	255.255.255.0	172.17.30.1	VLAN 30

Цілі та задачі

Частина 1: Пошук несправностей мережі

Частина 2: Реалізація способів вирішення

Частина 3: Перевірка мережного з'єднання

Сценарій. У цьому завданні ви будете виправляти неполадки підключення, викликані неправильними конфігураціями, пов'язаними з VLAN і маршрутизацією між VLAN.

Інструкції

Частина 1: Пошук несправностей мережі

Перевірте мережу і знайдіть джерело будь-яких проблем із підключенням.

Команди, які вам можуть бути корисними:

R1# show ip interface brief R1# show interface g0/1.10 R1# show interface g0/1.30 S1# show interfaces trunk

- Перевірте підключення та використовуйте необхідні команди show для перевірки конфігурацій.
- Переконайтеся, що всі налаштовані параметри відповідають вимогам, зазначеним у таблиці адресації.

Перерахуйте всі проблеми та можливі рішення в таблиці документації.

Таблиця документації

Проблеми	**Рішення**

Частина 2: Реалізація способів вирішення

Реалізуйте рекомендовані рішення.

Частина 3: Перевірка мережного з'єднання

Переконайтеся, що ПК можуть відповідати на запити ping один від одного та R1. Якщо ж ні, продовжуйте виправлення неполадок до тих пір, поки ping не будуть успішними.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи № 6 повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (1-2 сторінки):

— сутність VLAN, типи VLAN (data, voice, management, native);

— порти access та trunk, інкапсуляція 802.1Q;

— принципи маршрутизації між VLAN (Router-on-a-Stick, SVI на L3-комутаторі).

4. Практичну частину, що включає, для кожного завдання:

— опис початкової топології та таблицю адресації;

— перелік використаних команд налаштування (для комутаторів і маршрутизатора);

— результати перевірки налаштувань (вивід команд show vlan brief, show interface trunk, show ip interface brief, show ip route, ping тощо);

— скріншоти з Packet Tracer або текстові логи перевірки зв'язку (успішний/неуспішний ping) з коротким аналізом;

— для Завдання 5 – заповнену таблицю «Проблеми – Рішення» з описом знайдених помилок та застосованих дій.

5. Висновки, де необхідно:

— узагальнити роль VLAN, транків та маршрутизації між VLAN у побудові керованої й безпечної мережі;

— перелічити отримані практичні навички (створення VLAN, налаштування доступних і транкових портів, Router-on-a-Stick, SVI, L3-комутатор, пошук несправностей);

— відзначити типові помилки, з якими зіткнувся(лась) студент(ка), та способи їх усунення.

6. Список використаних джерел (відповідно до вимог щодо оформлення бібліографічних посилань).

4. Підбиття підсумків заняття

— обговорення результатів виконання Завдань 1-5 (коректність налаштування VLAN, транків, inter-VLAN маршрутизації);

— аналіз типових помилок (невірні VLAN на портах, відсутність транку, неправильна native VLAN, помилки у масках, шлюзах, підінтерфейсах тощо);

— оцінювання якості оформлення звітів та вміння студентів пояснювати вплив налаштувань VLAN на доступність та безпеку мережі;

— формулювання узагальнених висновків щодо значення логічної сегментації та маршрутизації між VLAN у сучасних комп'ютерних мережах.

5. Список рекомендованої літератури

Основна:

1. Комп'ютерні мережі : навч. посіб. / А. Саченко, Ю. Кулаков, В. Кочан [та ін.]. Тернопіль : ВПЦ «Економічна думка ТНЕУ», 2016. 476 с.

2. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

3. Валецька Т. М. Комп'ютерні мережі : апаратні засоби : навч. посіб. Київ : Ельга, 2004. 304 с.

4. Жуков О. М. Комп'ютерні мережі : навч. посіб. Київ : НАУ-друк, 2009. 392 с.

5. Лозінова Г. М. Комп'ютерні мережі : навч. посіб. Київ : Кондор, 2003. 280 с.

Додаткова:

1. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі. Ч. 1 : навч. посіб. для студ. спец. 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології» [Електронний ресурс]. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с. URL: https://ela.kpi.ua/handle/123456789/38118

2. Кулаков Ю. О. Комп'ютерні мережі : навч. посіб. для здобувачів ступеня магістра за освітньою програмою «Комп'ютерні системи та мережі» спец. 123 «Комп'ютерна інженерія» [Електронний ресурс]. Київ : КПІ ім. Ігоря Сікорського, 2022. 247 с. URL: https://ela.kpi.ua/handle/123456789/51465

Інформаційні ресурси

1. Електронний курс дисципліни «Комп'ютерні мережі» у віртуальному університеті ЛДУБЖД [Електронний ресурс]. URL: https://virt.ldubgd.edu.ua

2. Cisco Networking Academy. Офіційний сайт мережевої академії Cisco [Електронний ресурс]. URL: https://www.netacad.com

3. Cisco Packet Tracer. Довідкові матеріали та приклади лабораторних робіт [Електронний ресурс]. URL: https://skillsforall.com та https://www.netacad.com

ЛАБОРАТОРНА РОБОТА № 7

Тема: налаштування списків контролю доступу ACL.

Мета: навчитися виконувати налаштування IP ACL для дозволу або заборони певного трафіка, обмеження несанкціонованого доступу та зменшення кількості мережевих атак.

Місце проведення: згідно з розкладом.

Час: 8 годин.

Основні поняття: *ACL (Access Control List, список контролю доступу)* – набір правил фільтрації трафіка, що визначає, які пакети (за IP-адресою джерела/призначення, протоколом, портами тощо) дозволено або заборонено пропускати через інтерфейс маршрутизатора чи комутатора.

IP ACL – списки контролю доступу, що застосовуються до IP-трафіка; використовуються для пакетної фільтрації, обмеження доступу, сегментації мережі та базового функціоналу брандмауера.

Стандартний ACL (Standard ACL) – список контролю доступу, який виконує фільтрацію лише за IP-адресою джерела (source); не враховує адресу призначення та порти. Нумерація: 1-99, 1300-1999. Рекомендовано розміщувати якомога ближче до одержувача.

Розширений ACL (Extended ACL) – список контролю доступу, який може фільтравати трафік за IP-адресою джерела і призначення, типом протоколу (IP, TCP, UDP, ICMP тощо), номерами портів, флагами TCP тощо. Нумерація: 100-199, 2000-2699. Рекомендовано розміщувати якомога ближче до джерела трафіка.

Іменований ACL (Named ACL) – список контролю доступу, що замість номера використовує символьне ім’я; спрощує адміністрування, читання та модифікацію правил. Може бути стандартним або розширеним.

Wildcard-маска (маска підстановки) – «зворотна» маска підмережі, яка визначає, які біти IP-адреси повинні збігатися, а які можна ігнорувати при фільтрації. Обчислюється як різниця: 255.255.255.255 – маска підмережі (наприклад, для 255.255.255.0 → 0.0.0.255).

Пакетна фільтрація (packet filtering) – механізм, за якого маршрутизатор/комутатор перевіряє кожен пакет відповідно до правил ACL та вирішує, чи дозволити його подальшу передачу, чи відкинути.

Вхідний (inbound) та вихідний (outbound) напрямок ACL – спосіб прив'язки ACL до інтерфейсу: in – ACL застосовується до трафіка, що заходить на інтерфейс; out – ACL застосовується до трафіка, що виходить з інтерфейсу.

Implicit deny (неявне «deny any») – приховане правило в кінці кожного ACL, яке автоматично забороняє весь трафік, що не підпадає під жодну з попередніх умов permit/deny.

VTY-лінії (Virtual Teletype Lines) – віртуальні лінії доступу до пристрою (Telnet/SSH), до яких можна застосовувати ACL (команда access-class) для обмеження віддаленого керування маршрутизатором чи комутатором.

SSH (Secure Shell) – захищений протокол віддаленого керування мережевими пристроями, що забезпечує шифрування автентифікації та переданих даних. На відміну від Telnet, не передає логін/пароль у відкритому вигляді.

Фільтрація за портами (port-based filtering) – використання в ACL операторів eq, gt, lt, range та номерів портів (або їх імен, напр. ftp, http, https, ssh) для дозволу/заборони доступу до певних сервісів (DNS, SMTP, FTP, HTTPS тощо).

ACL для ліній VTY / доступу до маршрутизатора – списки доступу, які не фільтрають транзитний трафік, а обмежують можливість підключення до самого пристрою (наприклад, дозволити SSH тільки з однієї керуючої станції).

Обладнання та програмне забезпечення. Персональні комп'ютери / ноутбуки з доступом до мережі Інтернет; операційна система: Windows / Linux (за наявності – декілька ОС для порівняння); веббраузер для роботи з електронним курсом та пошуку інформації; текстовий редактор (MS Word / Google Docs або аналог) для оформлення звіту; програмне забезпечення Cisco Packet Tracer (або інше середовище для моделювання мереж Cisco); (за наявності) мережеве обладнання Cisco (маршрутизатори, комутатори) для відпрацювання налаштувань ACL у реальному середовищі; доступ до електронного навчального курсу у віртуальному університеті та матеріалів мережевої академії Cisco (розділи, що стосуються ACL, фільтрації трафіка, брандмауерів та SSH).

План

1. Організаційні заходи

— Повідомлення теми та мети лабораторного заняття.

— Мотивація навчальної діяльності: значення списків контролю доступу (ACL) для захисту мережевого трафіка, обмеження несанкціонованого доступу та зменшення мережевих атак.

— Ознайомлення з місцем розташування матеріалів лабораторної роботи в електронному навчальному середовищі «Віртуальний університет» (інструкції, топології, Packet Tracer-файли, скрипти налаштувань).

— Короткий огляд інтерфейсу Cisco Packet Tracer (або іншого ПЗ), пояснення, де вводяться команди, як переглядати конфігурацію, як перевіряти з'єднання (ping, traceroute).

— Інструктаж з техніки безпеки при роботі з комп'ютерною технікою та мережевим обладнанням (при роботі в аудиторії з «живими» маршрутизаторами/комутаторами).

— Пояснення порядку оформлення, подання та захисту звіту, критеріїв оцінювання (наявність скріншотів, коректність команд ACL, обґрунтованість відповідей на контрольні питання).

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: розуміння базових понять комп'ютерних мереж (моделі OSI та TCP/IP, призначення маршрутизатора і комутатора); знання принципів маршрутизації та роботи IP-протоколу; загальні уявлення про мережеву безпеку, фільтрацію трафіка, брандмауери; базове розуміння призначення SSH / Telnet, відмінностей між ними.

Перелік дидактичних одиниць для перевірки: поняття ACL (Access Control List), призначення списків контролю доступу; класифікація ACL: стандартні, розширені, іменовані; поняття inbound / outbound трафіка, прив'язка ACL до інтерфейсів маршрутизатора; принцип implicit deny (неявне deny any); призначення wildcard-маски та її відмінність від маски підмережі; загальні принципи налаштування SSH на маршрутизаторі та обмеження доступу до VTY-ліній за допомогою ACL.

Питання для усного опитування / самоконтролю:

1. Що таке ACL у комп’ютерних мережах і для чого вони використовуються?
2. Чим відрізняються стандартні та розширені списки контролю доступу?
3. Що таке wildcard-маска і як вона обчислюється на основі маски підмережі?
4. У чому різниця між застосуванням ACL у напрямках in та out?
5. Чому в кінці кожного ACL існує неявне правило deny any?
6. Яке призначення SSH і чому його рекомендують замість Telnet?
7. Як за допомогою ACL обмежити віддалений доступ до маршрутизатора лише з однієї керуючої станції?

3. Формування професійних умінь та навичок

3.1. Теоретичні відомості

ACL (англ. Access Control List – список контролю доступу) визначає, хто або що може отримувати доступ до конкретного об'єкта, і які саме операції дозволено або заборонено виконувати над об'єктом. У мережах ACL подають список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрою третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволений доступ до сервісу. Мережеві ACLможуть бути налаштовані як на звичайному сервері, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком, в якості брандмауера.

Списки ACL визначають дозволений і небажаний мережевий трафік. Перед тим, як почати дозволяти або забороняти певний тип мережевого трафіка, необхідно визначитисяз відповідними критеріями. При розробці критеріїв дозволу або відхилення трафіка мережі слід встановити порядок важливості для цих критеріїв. Залежно від встановлених критеріїв, у кінці процесу відбору відмова або дозвіл на доступ до мережі можуть отримати один або декілька вузлів.

ACL застосовується:

— на інтерфейсі: пакетна фільтрація;

— на лінії Telnet: обмеження доступу до маршрутизатора;

— VPN: який трафік потрібно шифрувати;

— QoS: який трафік обробляти приоритетніше;

— NAT: які адреси необхідно транслювати.

ACL розміщуються на інтерфейсах, самі вони створюються незалежно, а вже потім вони налаштовуються до інтерфейсу. Як тільки ви його налаштували до інтерфейсу, маршрутизатор починає переглядати трафік. Маршрутизатор розглядає трафік як вхідний і вихідний. Трафік, який входить в маршрутизатор називається вхідним, той який з нього виходить – вихідним. Відповідно ACL розміщуються на вхідному або на вихідному напрямі.

Наприклад, з приватної мережі приходить пакет на інтерфейс маршрутизатора fa0/1, маршрутизатор перевіряє, чи є ACL на інтерфейсі чи ні, якщо він є, то далі обробка ведеться за правилами списку доступу строго в тому порядку, в якому записані вирази, якщо список доступу дозволяє проходити пакета, то в даному випадку маршрутизатор відправляє пакет провайдеру через інтерфейс fa0/0, якщо список доступу не дозволяє проходити пакета, пакет знищується. Якщо списку доступу немає – пакет пролітає без всяких обмежень. Перед тим, як відправити пакет провайдеру, маршрутизатор ще перевіряє інтерфейс fa0/0 на наявність вихідного ACL. Наприклад у нас є ACL з правилом заборонити всім вузлам в Інтернеті посилати в нашу мережу пакети. На який інтерфейс прикріпити даний ACL? Якщо ми прикріпимо ACL на інтерфейс fa0/1 як вихідний, це буде не зовсім правильно, хоча і ACL працювати буде. На маршрутизатор приходить ехо-запит для якогось вузла в приватній мережі, він перевіряє на інтерфейсі fa0/0 чи є ACL, його немає, далі перевіряє інтерфейс fa0/1, на даному інтерфейсі є ACL, він налаштований як вихідний, тоді пакет не проникає в мережу, а знищується маршрутизатором. Але якщо ми прикріпимо ACL за інтерфейсом fa0/0 як вхідний, то пакет знищиться відразу, як прийде на маршрутизатор. Останнє рішення є правильним, оскільки маршрутизатор менше навантажує свої обчислювальні ресурси. Розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача. Це потрібно для того, щоб не ганяти пакети по всій мережі даремно.

ACL являє собою набір текстових виразів, в яких написано permit

(дозволити) або deny (заборонити), і обробка ведеться строго в тому порядку в якому задані вирази. Відповідно, коли пакет потрапляє на інтерфейс, він перевіряється на першу умову, якщо перша умова збігається з пакетом, подальша його обробка припиняється. Пакет або перейде далі, або знищиться. Якщо пакет збігся з умовою, далі він не обробляється. Якщо перша умова не збіглася, йде обробка другої умови, якщо вона збіглася, обробка припиняється, якщо немає, йде обробка третьої умови і так далі поки не перевіряться всі умови, якщо жодна з умов не збігається, пакет знищується. У кожному кінці списку стоїть неявний deny any (заборонити весь трафік).

ACL поділяються на два типи:

— стандартні (Standard): можуть перевіряти тільки адреси джерел;

— розширені (Extended): можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти.

Стандартні ACL нумеруються в діапазоні (1-99) та (1300-1999), розширені (100-199)та (2000-2699). Позначаються списки доступу або номерами, або символьними іменами. ACL також використовуються для різних мережевих протоколів. Символьні ACL поділяються теж на стандартні і розширені. Розширені ACL можуть перевіряти набагато більше, ніж стандартні, а й працюють вони повільніше, оскільки доведеться заглядати всередину пакета, на відміну від стандартних, де ми дивимося тільки поле Source Address (Адреса відправника).

При створенні ACL кожен запис списку доступу позначається порядковим номером, за усталеним налаштуванням в рамках десяти (10, 20, 30 і т.д). Не можна розмістити більше ніж один список доступу на одному інтерфейсі для одного протоколу в одному напрямі.

Якщо у нас є маршрутизатор і у нього є інтерфейс, ми можемо на вхідний напрямок для IP-протоколу розмістити тільки один список доступу, наприклад під номером 10. Ще одне правило, яке стосується самих маршрутизаторів, ACL не діє на трафік, згенерований самим маршрутизатором.

Для фільтрації адрес в ACL використовується WildCard-маска. Це зворотна маска.

Беремо шаблонний вираз: 255.255.255.255 і віднімаємо від шаблону звичайну маску:255.255.255.255- 255.255.255.0, у нас виходить WildCard маска 0.0.0.255.

Налаштування ACL:

Самі ACL створюються окремо, тобто це просто список, який створюється в режимі глобальної конфігурації, потім він присвоюється до інтерфейсу і тільки тоді він і починає працювати. Необхідно пам'ятати деякі моменти, для того, щоб правильно налаштувати списки доступу:

— обробка ведеться строго в тому порядку, в якому записані умови;

— якщо пакет збігся з умовою, далі він не обробляється;

— у кінці кожного списку доступу варто неявний deny any (заборонити все);

— розширені ACL потрібно розміщувати якомога ближче до джерела, стандартні – якомога ближче до одержувача;

— не можна розмістити більше 1 списку доступу на інтерфейс, на протокол, на напрям;

— ACL не діє на трафік, згенерований самим маршрутизатором;

— для фільтрації адрес використовується WildCard маска.

Стандартний список доступу:

Router (config) # access-list <номер списку> {permit | deny | remark} {address | any |host} [source-wildcard] [log],

permit: дозволити;

deny: заборонити;

remark: коментар про список доступу; address: забороняємо або дозволяємо мережу; any: дозволяємо або забороняємо все;

host: дозволяємо або забороняємо хосту;

source-wildcard: WildCard маска мережі;

log: вмикає реєстрацію пакетів, які проходять через відповідний запис ACL.

Правило deny ip any any часто дописують в кінці правил, щоб явно бачити по спрацьовуванню лічильників, що трафік заблокував ACL.

Розширений список доступу:

Router (config) # access-list <номер списку> {permit | deny | remark} protocol source[source-wildcard] [operator operand] [port <порт або назва протоколу> [established], protocol source: який протокол будемо дозволяти або ні (ICMP, TCP, UDP, OSPFтощо);

deny: заборонити;

operator:

A.B.C.D – адреса одержувача;

any – будь-який кінцевий хост;

eq – тільки пакети на цьому порті;

gt – тільки пакети з великим номером порту;

host – єдиний кінцевий хост;

lt – тільки пакети з нижчим номером порту; neq – тільки пакети не на даному номері порту; range – діапазон портів;

port: номер порту (TCP або UDP), можна вказати ім'я;

established: дозволяємо проходження TCP-сегментів, які є частиною створеної TCP-сесії.

Прикріплення ACL до інтерфейсу

Router (config-if) #ip access-group <номер списку або ім'я ACL> {in | out}in: вхідний напрямок;

out: вихідний напрямок.

Іменовані списки доступу

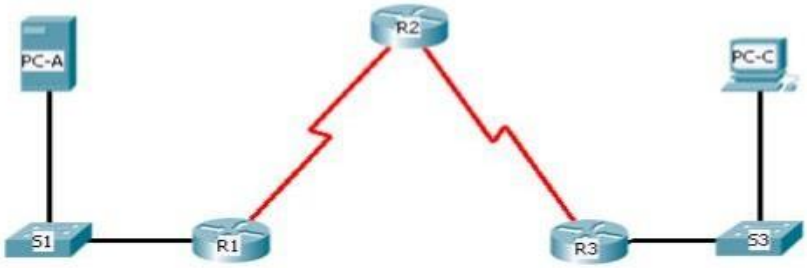
Router (config) #ip access-list {standard | extended} {<номер ACL> | <Ім'я ACL>}Router (config- ext-nacl) # {default | deny | exit | no | permit | remark}

standard: стандартний ACL;

extended: розширений ACL;

default: встановити команду в значення за усталеним налаштуванням.

Приклади: Нехай у нас є мережа заданої топології та таблиця адресації пристроїв даної мережі.



Таблиця адресації

Пристрій	Інтерфейс	IP - адреса	Маска підмережі	Шлюз за усталеним налаштуванням
R N (R1)	Fa0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R N+1 (R2)	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	LoO	192.168.2.1	255.255.255.0	N/A
R N+2 (R3)	Fa0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Необхідно, щоб виконувались такі умови:

Доступ до маршрутизаторів R1, R2 і R3 повинен бути дозволений лише від вузла PC-C. PC-C також використовується для перевірки підключень до PC-A, сервер надає DNS,

SMTP, FTP, і HTTPS послуги. Стандартний режим роботи повинен використовувати ACL на граничних маршрутизаторах, для зменшення спільної загрози до атак, заснованих на IP-адресі джерела та/або адресі призначення.

Необхідно створити ACL на граничних маршрутизаторах R1 і R3 та перевірити роботу ACL від внутрішніх і зовнішніх вузлів.

Виконання роботи:

1) Перевірити зв'язки мережі

Перевірити підключення до мережі перед налаштуванням IP ACL:

Від PC-C в командному рядку, зробити ping до PC-A сервера.

Від PC-C в командному рядку, підключитися через SSH до маршрутизатора R2 на Lo0інтерфейс.

Вийти з сеансу SSH.

Від PC-C, відкрити web браузер і підключитися на PC-A сервер, щоб відобразити webсторінку.

Закрити браузер на PC-C.

Від PC-A сервера в командному рядку, зробити ping PC-C.

2) Безпечний доступ до маршрутизатора

Налаштувати ACL 10, щоб заблокувати весь віддалений доступ до маршрутизаторів окрім як від PC-C. Використати команду access-list щоб створити нумерований IP ACL наR1, R2, і R3.

R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0

R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0

R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0

Застосувати ACL 10 до вхідного трафіка на VTY лінії. Використати команду access-class щоб застосувати нумерований список доступу (access-list) до вхідного трафіка на VTY лінії.

R1(config-line)# access-class 10 inR2(config-line)# access-class 10 inR3(config-line)# access-class 10 in

Перевірити монопольний доступ від станції управління PC-C.SSH до 192.168.2.1 від PC-C (повинен бути вдалим).

SSH до 192.168.2.1 від PC-A (повинен бути невдалим).

3) Створити нумерований IP ACL 100. На R3, блокувати всі пакети, що містять IP- адресу джерела з наступних адрес: 127.0.0.0 / 8, будь-яких RFC 1918 приватних адрес, а також будь-які широкомовні IP адреси.

Налаштувати ACL 100 для блокування певного трафіка із зовнішньої мережі. Також блокувати трафік, отриманий від внутрішнього адресного простору, якщо це не адреса RFC 1918 (у цьому випадку, внутрішнє адресний простір - частина приватного адресного простору, визначеного в RFC 1918).

Використати команду access-list щоб створити нумерований IP ACL.

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any R3(config)# access-list 100 permit ip any any

Застосувати ACL до інтерфейсу Serial 0/0/1. Використати команду ip access-group, щоб застосувати список доступу до вхідного трафіка на інтерфейсі Serial 0/0/1.

R3(config)# interface s0/0/1 R3(config-if)# ip access-group 100 in

Переконатися, що вказаний трафік приходить на інтерфейс Serial 0/0/1 заблокованим. З командного рядка PC-C пропінгувати сервер PC-A. ICMP exo-відповіді блокуються ACL, оскільки вони отримані від адресного простору 192.168.0.0.

Прибрати ACL з Serial 0/0/1.

Видалити ACL. В іншому випадку, весь трафік від зовнішньої мережі (розглядаючи щодо приватних IP адрес джерела) буде закритий для інших. Команда no ip access-group видаляє список доступу з інтерфейсу Serial 0/0/1.

R3(config)# interface s0/0/1

R3(config-if)# no ip access-group 100 in

4) Створити нумерований IP ACL 110

Заборонити всі вихідні пакети з адреси джерела за межами діапазону внутрішніх IPадрес.

Налаштувати ACL 110 на дозвіл доступу трафіка тільки з внутрішньої мережі. Скористатися командою access-list для створення нумерованого списку IP ACL.

R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Застосувати ACL для інтерфейсу F0/1.

Використати команду ip access-group щоб застосувати список доступу до вхідного трафіка на інтерфейсі F0/1.

R3(config)# interface fa0/1 R3(config-if)# ip access-group 110 in

5) Створити нумерований IP ACL 120 Дозволити будь-який зовнішній вузол для DNS, SMTP, і FTP сервісів на сервері PC-A, заборонити будь-який зовнішній доступ до служби HTTPS на PC-A, і дозволити PC-C доступ до R1 через SSH.

Перевірити, що PC-C може отримати доступ до PC-A через HTTPS, використовуючи веббраузер переконатися, що відключили HTTP і включили HTTPS на PC-A сервері.

Налаштувати ACL 120, на дозвіл і заборону зазначеного трафіка. Використати команду access-list, щоб створити пронумерований IP ACL.

R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443 R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

Застосувати ACL до інтерфейсу S0/0/0. Використати команду ip access-group, щобзастосувати список доступу до вхідного трафіка на інтерфейсі S0/0/0.

R1(config)# interface s0/0/0 R1(config-if)# ip access-group 120 in

Перевірити, що PC-C не зможе отримати доступ до PC-A через HTTP, використовуючи веббраузер.

6) Зміна існуючого ACL/ Дозволити ICMP exo-відповіді та недосяжні адресату повідомлення із зовнішньої мережі (порівняно з R1); заборонити всі інші вхідні ICMP пакети.

Перевірити, що PC-A не може успішно виконати ping-запит loopback інтерфейс на R2. Змінити ACL 120, щоб дозволяти і забороняти вказаний трафік. Використати команду access-list щоб створити пронумерований IP ACL.

R1(config)# access-list 120 permit icmp any any echo-reply R1(config)# access-list 120 permit icmp any any unreachable R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any

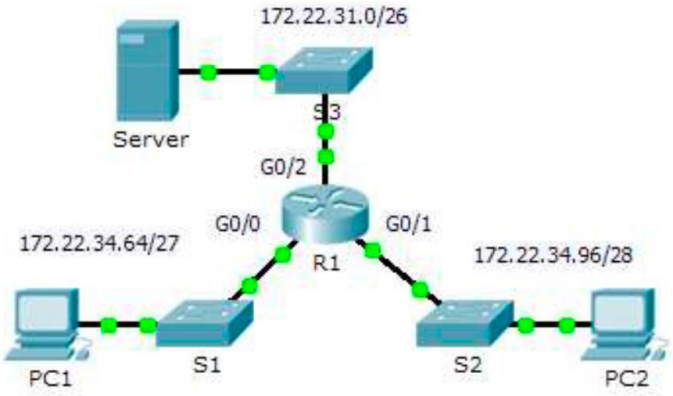
Перевірити, що PC-A може успішно виконати ping-запит на петлевий

(loopback) інтерфейс R2.

Хід виконання лабораторної роботи

Епізод 1:

Налаштування розширених списків керування доступом



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Передісторія / Сценарій. Двом співробітникам потрібен доступ до послуг, що надаються сервером. PC1 потребує лише доступу до FTP, тоді як PC2 потребує лише доступу до Інтернету. Обидва комп'ютери можуть пінгувати сервер, але не один одному.

Частина 1. Налаштування, застосування та перевірка розширеного нумерованого списку керування доступом

Крок 1. Налаштуйте ACL, щоб дозволити FTP і ICMP

a. У режимі глобальної конфігурації на R1 введіть таку команду, щоб визначити перший дійсний номер для розширеного списку доступу.

R1(config)# access-list ?

<1-99> IP standard access list

<100-199> IP extended access list

b. Додайте 100 до команди, а потім знак питання.

R1(config)# access-list 100 ? deny Specify packets to reject permit Specify packets to forward

remark Access list entry comment

Щоб дозволити FTP-трафік, введіть permit , а потім знак питання. R1(config)# access-list 100 permit ?

ahp Authentication Header Protocol eigrp Cisco's EIGRP routing protocol esp Encapsulation Security Payload gre Cisco's GRE tunneling

icmp Internet Control Message Protocol ip Any Internet Protocol

ospf OSPF routing protocol

tcp Transmission Control Protocol udp User Datagram Protocol

c. Цей ACL дозволяє FTP і ICMP. ICMP вказано вище, але FTP ні, оскільки FTP використовує TCP. Отже, ви вводите TCP. Введіть tcp , щоб додатково уточнити довідку ACL.

R1(config)# access-list 100 permit tcp ?

A.B.C.D Source address any Any source host host A single source host

d. Зауважте, що ми можемо відфільтравати лише для ПК1 за допомогою ключового слова host або дозволити будь-який хост. У цьому випадку дозволено використовувати будь-який пристрій, який має адресу, що належить до мережі 172.22.34.64/27. Введіть мережеву адресу, а потім знак питання. R1(config)# access-list 100 permit tcp 172.22.34.64 ?

A.B.C.D Source wildcard bits

e. Обчисліть маску підстановки, яка визначає двійкову протилежність маски підмережі. 11111111,11111111,11111111,11100000 = 255,255,255,224

00000000,00000000,00000000,00011111 = 0,0,0,31

f. Введіть маску підстановки, а потім знак питання.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?

A.B.C.D Destination address any Any destination host

eq Match only packets on a given port number

gt Match only packets with a greater port number host A single destination host

lt Match only packets with a lower port number neq Match only packets not on a given port number

range Match only packets in the range of port numbers

g. Налаштуйте адресу призначення. У цьому сценарії ми фільтраємо трафік для одного місця призначення — сервера. Введіть ключове слово хоста, а потім IP-адресу сервера.

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ? dscp Match packets with given dscp value

eq Match only packets on a given port number established established

gt Match only packets with a greater port number lt Match only packets with a lower port number

neq Match only packets not on a given port number precedence Match packets with given precedence value range Match only packets in the range of port numbers

<cr>

Зверніть увагу, що одним із варіантів є <cr> (повернення каретки). Іншими словами, ви можете натиснути Enter, і оператор дозволить весь трафік TCP. Однак ми дозволяємо лише FTP-трафік; тому введіть ключове слово eq , а потім знак питання, щоб відобразити доступні параметри. Потім введіть ftp і натисніть Enter .

R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?

<0-65535> Port number

ftp File Transfer Protocol (21) pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25) telnet Telnet (23)

www World Wide Web (HTTP, 80)

R1(config)# access-list 100 permit

h. Створіть другий оператор списку доступу, щоб дозволити трафік ICMP (ping тощо) від ПК1 до сервера . Зауважте, що номер списку доступу залишається незмінним, а конкретний тип трафіка ICMP вказувати не потрібно.

R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

i. Увесь інший трафік за усталеним налаштуванням заборонено.

Крок 2. Застосуйте ACL до правильного інтерфейсу, щоб фільтравати трафік

З точки зору R1, трафік, до якого застосовується ACL 100, входить із мережі, підключеної до інтерфейсу Gigabit Ethernet 0/0. Увійдіть в режим конфігурації інтерфейсу та застосуйте ACL.

R1(config)# interface gigabitEthernet 0/0 R1(config-if)# ip access-group 100 in

Крок 3: Перевірте реалізацію ACL

a. Відправити ping з ПК1 на сервер . Якщо пінги не вдалися, перевірте IP-адреси, перш ніж продовжити.

b. FTP з ПК1 на сервер . Ім'я користувача та пароль є cisco.

PC> ftp 172.22.34.62

c. Вийдіть із служби FTP Сервера.

ftp> quit

d. Відправити ping з ПК1 на ПК2. Хост призначення повинен бути недоступним, оскільки трафік не був явно дозволений.

Частина 2: Налаштування, застосування та перевірка розширеного іменованого списку керування доступом

Крок 1. Налаштуйте ACL, щоб дозволити доступ HTTP та ICMP

a. Іменовані списки керування доступом починаються з ключового слова ip . У режимі глобальної конфігурації R1 введіть таку команду, а потім знак питання.

R1(config)# ip access-list ? extended Extended Access List standard Standard Access List

b. Ви можете налаштувати іменовані стандартні та розширені списки керування доступом. Цей список доступу фільтрає як вихідні, так і цільові IP-адреси; тому його необхідно продовжити. Введіть HTTP_ONLY як назву. (Для оцінки Packet Tracer ім'я чутливе до регістру.)

R1(config)# ip access-list extended HTTP_ONLY

Підказка змінюється. Тепер ви перебуваєте в режимі конфігурації розширеного іменованого ACL. Усі пристрої в локальній мережі PC2 потребують доступу TCP. Введіть мережеву адресу, а потім знак питання.

R1(config-ext-nacl)# permit tcp 172.22.34.96 ?

A.B.C.D Source wildcard bits

c. Альтернативний спосіб обчислення символу підстановки — відняти маску підмережі з 255.255.255.255.

255.255.255.255

- 255.255.255.240

= 0. 0. 0. 15

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?

d. Завершіть операцію, вказавши адресу сервера, як ви зробили в частині 1, і відфільтрававши трафік www .

R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

e. Створіть другий оператор списку доступу, щоб дозволити трафік ICMP (ping тощо) від ПК2 до сервера. Примітка. Підказка залишається незмінною, а конкретний тип трафіка ICMP вказувати не потрібно.

R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

f. Увесь інший трафік за усталеним налаштуванням заборонено. Вийти з режиму конфігурації розширеного іменованого списку керування доступом.

Крок 2. Застосуйте ACL до правильного інтерфейсу, щоб фільтравати трафік

З точки зору R1, трафік, до якого застосовується список доступу HTTP_ONLY, входить із мережі, підключеної до інтерфейсу Gigabit Ethernet 0/1. Увійдіть у режим конфігурації інтерфейсу та застосуйте ACL.

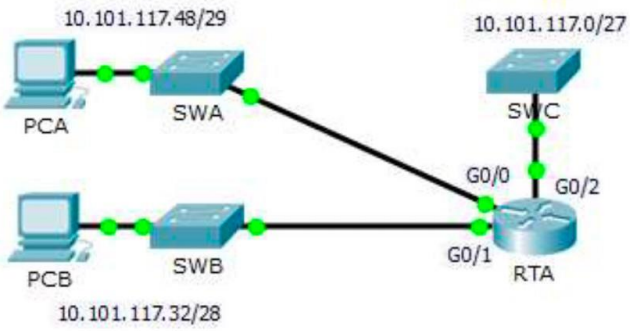
R1(config)# interface gigabitEthernet 0/1 R1(config-if)# ip access

Крок 3: Перевірте реалізацію ACL

a. Відправити ping з ПК2 на сервер. Якщо пінг не вдався, перевірте IP-адреси, перш ніж продовжити. б. FTP з ПК2 на сервер. З’єднання має зірватися.

b. Відкрийте веббраузер на ПК2 і введіть IP-адресу сервера як URL-адресу.

З'єднання має бути успішним.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.101.117.49	255.255.255.248	N/A
	G0/1	10.101.117.33	255.255.255.240	N/A
	G0/2	10.101.117.1	255.255.255.224	N/A
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWA	VLAN 1	10.101.117.50	255.255.255.248	10.101.117.49
SWB	VLAN 1	10.101.117.34	255.255.255.240	10.101.117.33
SWC	VLAN 1	10.101.117.2	255.255.255.224	10.101.117.1

Епізод 2:

Передісторія / Сценарій. У цьому сценарії пристроям в одній локальній мережі дозволено віддалено отримувати доступ до пристроїв в іншій локальній мережі за допомогою протоколу Telnet. Крім ICMP, заборонено весь трафік з інших мереж.

Частина 1. Налаштування, застосування та перевірка розширеного нумерованого списку керування доступом

Налаштуйте, застосуйте та перевірте ACL, щоб відповідати такій політиці:

Трафік Telnet від пристроїв у мережі 10.101.117.32/28 дозволений до пристроїв у мережах 10.101.117.0/27.

Трафік ICMP дозволений з будь-якого джерела до будь-якого місця призначення Весь інший трафік до 10.101.117.0/27 заблоковано.

Крок 1. Налаштуйте розширений ACL

а. У відповідному режимі конфігурації на RTA використовуйте останній дійсний номер розширеного списку доступу, щоб налаштувати ACL. Виконайте наступні кроки, щоб створити перший оператор ACL:

1) Останній номер розширеного списку – 199.

2) Протокол TCP.

3) Вихідна мережа 10.101.117.32.

4) Підстановку можна визначити шляхом віднімання 255.255.255.240 від 255.255.255.255.

5) Мережа призначення – 10.101.117.0.

6) Підстановку можна визначити шляхом віднімання 255.255.255.224 від 255.255.255.255.

7) Протокол Telnet.

Який перший оператор ACL?

access-list 199 permit tcp 10.101.117.32 0.0.0.15 10.101.117.0 0.0.0.31 eq telnet.

b. ICMP дозволено, і потрібен другий оператор ACL. Використовуйте той самий номер списку доступу, щоб дозволити весь трафік ICMP, незалежно від адреси джерела або адреси призначення. Що таке другий оператор ACL? (Порада: використовуйте будь-які ключові слова)

access-list 199 permit icmp any any

c. Весь інший IP-трафік за усталеним налаштуванням заборонений.

Крок 2. Застосуйте розширений ACL

Загальне правило – розташовувати розширені списки доступу до джерела близько до джерела. Однак, оскільки список доступу 199 впливає на трафік, що надходить з обох мереж 10.101.117.48/29 і 10.101.117.32/28, найкраще розташування для цього списку доступу може бути на інтерфейсі Gigabit Ethernet 0/2 у вихідному напрямку. Яка команда застосувати ACL 199 до інтерфейсу Gigabit Ethernet 0/2?

ip access-group 199 out

Крок 3. Перевірте реалізацію розширеного списку керування доступом

а. Проведіть ping з PCB на всі інші IP-адреси в мережі. Якщо пінги не вдалися, перевірте IP-адреси, перш ніж продовжити.

б. Telnet від PCB до SWC . Пароль cisco.

c. Вийдіть із служби Telnet SWC .

d. Проведіть ping від PCA до всіх інших IP-адрес у мережі. Якщо пінги не

вдалися, перевірте IP- адреси, перш ніж продовжити.

e. Telnet від PCA до SWC. Список доступу змушує маршрутизатор відхиляти з'єднання.

f. Telnet від PCA до SWB . Список доступу розміщено на G0/2 і не впливає на це підключення.

g. Після входу в SWB не виходьте з системи. Telnet до SWC .

Епізод 3: Налаштування IP ACLs для пом'якшення атак

Мета:

— Перевірити підключення між пристроями перед налаштуванням брандмауера.

— Використайте списки ACL, щоб забезпечити віддалений доступ до маршрутизаторів лише зі станції керування PC-C.

— Налаштуйте списки керування доступом на R1 та R3, щоб пом'якшити атаки.

— Перевірте функціональність ACL.

Передісторія / сценарій. Доступ до маршрутизаторів R1, R2 і R3 повинен бути дозволений лише з PC-C, станції керування. PC-C також використовується для тестування підключення до PC-A, який є сервером, що надає послуги DNS, SMTP, FTP і HTTPS.

Стандартна операційна процедура полягає в застосуванні ACL на граничних маршрутизаторах, щоб пом'якшити поширені загрози на основі IP-адрес джерела та призначення. У цій роботі ви створите списки керування доступом на граничних маршрутизаторах R1 і R3 для досягнення цієї мети. Потім ви перевірите функціональність ACL з внутрішніх і зовнішніх хостів.

Маршрутизатори були попередньо налаштовані таким чином:

— Увімкнути пароль: ciscoenpa55

— Пароль для консолі: ciscoconpa55

— Ім'я користувача та пароль для входу в SSH: SSHadmin/ciscosshpa55

— IP-адреса

— Статична маршрутизація

Частина 1: Перевірка базового підключення до мережі

Перевірте підключення до мережі, перш ніж налаштовувати списки доступу до IP-адресів.

Крок 1. З PC-A перевірте підключення до PC-C і R2

а. З командного рядка виконайте ping PC-C (192.168.3.3).

б. З командного рядка встановіть сеанс SSH до інтерфейсу R2 Lo0 (192.168.2.1), використовуючи ім’я користувача SSHadmin і пароль ciscosshpa55 . Після завершення вийдіть із сеансу SSH.

SERVER> ssh -l SSHadmin 192.168.2.1

Крок 2. З PC-C перевірте підключення до PC-A і R2

а. З командного рядка виконайте ping PC-A (192.168.1.3).

б. З командного рядка встановіть сеанс SSH до інтерфейсу R2 Lo0 (192.168.2.1), використовуючи ім’я користувача SSHadmin і пароль ciscosshpa55 . Закрийте сеанс SSH, коли закінчите.

PC> ssh -l SSHadmin 192.168.2.1

с. Відкрийте веббраузер на сервері PC-A (192.168.1.3), щоб відобразити вебсторінку. Закрийте браузер, коли закінчите.

Частина 2: Безпечний доступ до маршрутизаторів

Крок 1. Налаштуйте ACL 10, щоб блокувати весь віддалений доступ до маршрутизаторів, крім PC-C

Використовуйте команду access-list , щоб створити нумерований IP ACL на R1, R2 і R3 .

R1(config)# access-list 10 permit host 192.168.3.3

R2(config)# access-list 10 permit host 192.168.3.3

R3(config)# access-list 10 permit host 192.168.3.3

Крок 2. Застосуйте ACL 10 до вхідного трафіка на лініях VTY

Використовуйте команду access-class , щоб застосувати список доступу до вхідного трафіка на лініях VTY.

R1(config-line)# access-class 10 in R2(config-line)# access-class 10 in R3(config-line)# access-class 10 in

Крок 3: Перевірте ексклюзивний доступ зі станції керування PC-C

а. Встановіть сеанс SSH до 192.168.2.1 з PC-C (повинен бути успішним).

PC> ssh –l SSHadmin 192.168.2.1

б. Встановіть сеанс SSH до 192.168.2.1 з PC-A (повинен бути невдалим).

Частина 3: Створіть нумерований IP ACL 120 на R1

Створіть IP ACL з номером 120 з такими правилами:

— Дозволити будь-якому зовнішньому хосту отримати доступ до служб DNS, SMTP і FTP на сервері PC-A .

— Заборонити будь-який сторонній хост доступ до служб HTTPS на PC-A .

— Дозволити PC-C отримати доступ до R1 через SSH.

Примітка. Результати перевірки не відображатимуть правильну конфігурацію для ACL 120, доки ви не зміните її в частині 4.

Крок 1. Переконайтеся, що PC-C може отримати доступ до PC-A через HTTPS за допомогою веббраузера

Обов’язково вимкніть HTTP і ввімкніть HTTPS на сервері PC-A.

Крок 2. Налаштуйте ACL 120 для спеціального дозволу та заборони вказаного трафіка

Використовуйте команду access-list , щоб створити нумерований IP ACL. R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443

R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22

Крок 3: Застосуйте ACL до інтерфейсу S0/0/0.

Використовуйте команду ip access-group, щоб застосувати список доступу до вхідного трафіка на інтерфейсі S0/0/0.

R1(config)# interface s0/0/0 R1(config-if)# ip access-group 120 in

Крок 4. Переконайтеся, що PC-C не може отримати доступ до PC-A через HTTPS за допомогою веббраузера

Частина 4: Змінення існуючого списку керування доступом на R1

Дозволити ICMP echo-відповіді та призначення недоступних

повідомлень із зовнішньої мережі (відносно R1). Заборонити всі інші вхідні пакети ICMP.

Крок 1. Переконайтеся, що ПК-А не може успішно пінгувати інтерфейс зворотного зв'язку на R2

Крок 2. Внесіть необхідні зміни в ACL 120, щоб дозволити та заборонити вказаний трафік

Використовуйте команду access-list , щоб створити нумерований IP ACL.

R1(config)# access-list 120 permit icmp any any echo-reply R1(config)# access-list 120 permit icmp any any unreachable R1(config)# access-list 120 deny icmp any any

R1(config)# access-list 120 permit ip any any

Крок 3. Переконайтеся, що PC-A може успішно відправити ping інтерфейсу зворотного зв'язку на R2

Частина 5: Створіть нумерований IP ACL 110 на R3

Заборонити всі вихідні пакети з адресою джерела за межами діапазону внутрішніх IP-адрес на R3.

Крок 1. Налаштуйте ACL 110, щоб дозволити лише трафік із внутрішньої мережі.

Використовуйте команду access-list , щоб створити нумерований IP ACL. R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any

Крок 2: Застосуйте ACL до інтерфейсу G0/1

Використовуйте команду ip access-group , щоб застосувати список доступу до вхідного трафіка на інтерфейсі G0/1.

R3(config)# interface g0/1

R3(config-if)# ip access-group 110 in

Частина 6: Створіть нумерований IP ACL 100 на R3

На R3 заблокуйте всі пакети, що містять вихідну IP-адресу з наступного пулу адрес: будь-які приватні адреси RFC 1918, 127.0.0.0/8 та будь-яка адреса багатоадресної IP-адреси. Оскільки PC-C використовується для віддаленого адміністрування, дозвольте SSH-трафіка з мережі 10.0.0.0/8 повертатися на хост PC-C .

Крок 1. Налаштуйте ACL 100 для блокування всього вказаного трафіка із зовнішньої мережі

Ви також повинні заблокувати трафік, отриманий з вашого внутрішнього адресного простору, якщо це не адреса RFC 1918. У цій дії ваш внутрішній адресний простір є частиною приватного адресного простору, зазначеного в RFC 1918.

Використовуйте команду access-list , щоб створити нумерований IP ACL. R3(config)# access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host

192.168.3.3

R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any

R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any

R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any

R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any R3(config)# access-list 100 permit ip any any

Крок 2: Застосуйте ACL до інтерфейсу Serial 0/0/1

Використовуйте команду ip access-group, щоб застосувати список доступу до вхідного трафіка на інтерфейсі Serial 0/0/1.

R3(config)# interface s0/0/1 R3(config-if)# ip access-group 100 in

Крок 3: Переконайтеся, що вказаний трафік, який надходить у інтерфейс Serial 0/0/1, обробляється правильно

а. З командного рядка PC-C виконайте ping сервер PC-A. Відповіді на exo ICMP блокуються ACL, оскільки вони надходять з адресного простору 192.168.0.0/16.

б. Встановіть сеанс SSH до 192.168.2.1 з PC-C (повинен бути успішним).

Крок 4: Перевірте результати

Ваш відсоток виконання має становити 100%. Натисніть Перевірити результати , щоб переглянути відгуки та перевірити, які необхідні компоненти виконано.

Скрипти для R1

access-list 10 permit host 192.168.3.3

line vty 0 4

access-class 10 in

access-list 120 permit udp any host 192.168.1.3 eq domain access-list 120 permit tcp any host 192.168.1.3 eq smtp access-list 120 permit tcp any host 192.168.1.3 eq ftp access-list 120 deny tcp any host 192.168.1.3 eq 443

access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22 interface s0/0/0

ip access-group 120 in

access-list 120 permit icmp any any echo-reply access-list 120 permit icmp any any unreachable access-list 120 deny icmp any any

access-list 120 permit ip any

Скрипти для R2

access-list 10 permit host 192.168.3.3

line vty 0 4

access-class 10 in

Скрипти для R3

access-list 10 permit host 192.168.3.3

line vty 0 4

access-class 10 in

access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3

access-list 100 deny ip 10.0.0.0 0.255.255.255 any

access-list 100 deny ip 172.16.0.0 0.15.255.255 any

access-list 100 deny ip 192.168.0.0 0.0.255.255 any

access-list 100 deny ip 127.0.0.0 0.255.255.255 any

access-list 100 deny ip 224.0.0.0 15.255.255.255 any access-list 100 permit ip any any

interface s0/0/1

ip access-group 100 in

access-list 110 permit ip 192.168.3.0 0.0.0.255 any interface g0/1

ip access-group 110 in

3.2. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (поняття ACL, стандартні та розширені ACL, wildcard-маска, принцип неявного deny any, напрямки застосування in/out, призначення SSH).
4. Практичну частину, що включає:

— скріншот створеної топології мережі в Cisco Packet Tracer;

— опис налаштування стандартних ACL (10) для доступу до маршрутизаторів;

— опис налаштування розширених ACL (100, 110, 120, 199);

— скріншоти або копії введених команд налаштування ACL;

— результати виконання команд ping, ssh, ftp, web-доступу;

— пояснення результатів блокування та дозволу трафіка.

5. Висновки:

— узагальнення щодо ролі списків контролю доступу у забезпеченні мережевої безпеки;

— опис отриманих практичних навичок;

— оцінка ефективності використання ACL для захисту мережі.

6. Список використаних джерел

4. Підбиття підсумків заняття

— обговорення результатів налаштування списків контролю доступу;

— аналіз правильності застосування ACL на інтерфейсах маршрутизаторів;

— оцінювання якості виконаних налаштувань та результатів тестування доступу;

— формування узагальнених висновків щодо значення ACL у побудові захищеної мережевої інфраструктури**;**

— оцінювання повноти та якості звітів, уміння пояснювати вплив ACL на мережеву безпеку.

5. Питання до лабораторної роботи

1. Яке призначення ACL? Які є типи ACL?
2. Які є правила налаштування ACL?
3. Яке призначення простих і розширених ACL?
4. Які ви знаєте команди ACL?
5. Яке призначення SSH?
6. Які правила налаштування SSH? Як налаштувати маршрутизатор лише на SSH з'єднання?
7. Як заборонити/дозволити вхідний/вихідний трафік на/з маршрутизатора?
8. Як заборонити первинний тип трафіка на деякий вузол мережі?

6. Список рекомендованої літератури

Основна:

1. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах : навч. посіб. Київ, 2013. 435 с.
2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 213 с.
3. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : ХНЕУ, 2013. 476 с.

Додаткова:

1. Кавун С. В., Смірнов О. А., Столбов В. Ф. Основи інформаційної безпеки. Кропивницький : КНТУ, 2012. 414 с.
2. Гарасимчук О. І., Дудикевич В. Б., Ромака В. А. Комплексні системи санкціонованого доступу : навч. посіб. Львів : Львівська політехніка, 2010. 212 с.

Інформаційні ресурси:

1. Cisco Networking Academy. Introduction to Networks, Switching, Routing and Wireless Essentials. URL: https://www.netacad.com
2. RFC 791 – Internet Protocol. URL: https://www.rfc-editor.org

3. RFC 1918 – Address Allocation for Private Internets. URL: https://www.rfc-editor.org

4. Віртуальний університет ЛДУБЖД : електронне навчальне середовище. URL: https://virt.ldubgd.edu.ua

ЛАБОРАТОРНА РОБОТА № 8

Тема: організація безпеки за допомогою утиліт, що виявляють уразливості локальної мережі. Використання Wireshark для перегляду та аналізу мережного трафіка.

Мета: навчитися виявляти та аналізувати уразливості локальної мережі шляхом захоплення, фільтрації та інтерпретації мережного трафіка з використанням програмного забезпечення Wireshark.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *Локальна комп'ютерна мережа (LAN)* – сукупність взаємопов'язаних комп'ютерів та мережевих пристроїв, об'єднаних у межах обмеженої території для спільного використання ресурсів та обміну даними.

Мережний трафік – сукупність усіх даних, що передаються між вузлами комп'ютерної мережі за певний проміжок часу.

Кадр Ethernet – базова одиниця передавання даних на канальному рівні моделі OSI, яка містить MAC-адреси відправника й отримувача, службову інформацію та корисне навантаження.

IP-пакет – структурований блок даних, що передається на мережевому рівні моделі OSI та містить IP-адреси джерела і призначення, службову інформацію та дані користувача.

Протокол TCP (Transmission Control Protocol) – транспортний протокол, що забезпечує надійне, впорядковане та контрольоване передавання даних між вузлами мережі з підтвердженням доставки.

Протокол UDP (User Datagram Protocol) – транспортний протокол без встановлення з'єднання, що забезпечує швидку передачу даних без гарантії доставки та порядку надходження пакетів.

Порти TCP/UDP – логічні ідентифікатори прикладних процесів у мережі, які використовуються для встановлення з'єднання між клієнтськими та серверними програмами.

DNS (Domain Name System) – розподілена система доменних імен, призначена для перетворення доменних імен у відповідні IP-адреси комп'ютерів у мережі.

Тристороннє квитування TCP (Three-Way Handshake) – процедура встановлення TCP-з'єднання між двома вузлами шляхом обміну трьома службовими пакетами SYN, SYN-ACK та ACK.

Мережний аналізатор (sniffer) – програмний або апаратний засіб для перехоплення, перегляду та аналізу мережного трафіка з метою діагностики, дослідження або виявлення загроз.

Фільтри Wireshark – спеціальні правила відбору пакетів, які дозволяють відображати лише ті кадри, що відповідають заданим умовам (IP, порти, протоколи тощо).

Уразливість мережі – слабке місце в архітектурі, програмному або апаратному забезпеченні мережі, яке може бути використане зловмисником для здійснення атаки.

Мережна атака – цілеспрямований вплив на комп'ютерну мережу з метою порушення її працездатності, конфіденційності, цілісності або доступності інформації.

Перехоплення трафіка – несанкціоноване або дослідницьке отримання доступу до мережних пакетів з метою аналізу передаваних даних.

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до мережі Інтернет; операційна система Windows / Linux; веббраузер для роботи з електронним курсом та пошуку інформації; текстовий редактор (MS Word / Google Docs або аналог); встановлене програмне забезпечення Wireshark; (за наявності) антивірусне ПЗ та/або демоверсії засобів захисту; доступ до електронного навчального курсу у віртуальному університеті та матеріалів мережевої академії Cisco.

План:

1. **Організаційні заходи**

— Повідомлення теми та мети лабораторного заняття.

— Мотивація навчальної діяльності: значення аналізу мережного трафіка для виявлення уразливостей, контролю безпеки передачі даних та своєчасного виявлення мережевих атак.

— Ознайомлення з місцем розташування матеріалів лабораторної роботи в електронному навчальному середовищі «Віртуальний університет».

— Інструктаж з техніки безпеки під час роботи з комп'ютерною технікою, мережею Інтернет та програмним забезпеченням Wireshark.

— Пояснення порядку оформлення, подання та захисту звіту, критеріїв оцінювання результатів лабораторної роботи.

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: розуміння базових принципів роботи комп'ютерних мереж; знання рівневої моделі OSI і TCP/IP; уявлення про мережні протоколи TCP, UDP, DNS, IP; розуміння призначення портів, кадру Ethernet та мережного трафіка.

Перелік дидактичних одиниць для перевірки: поняття локальної комп'ютерної мережі; мережний трафік; кадр Ethernet; IP-пакет; протоколи TCP та UDP; система доменних імен DNS; тристороннє квитування TCP; мережний аналізатор Wireshark; фільтрація трафіка; основи перехоплення мережних пакетів.

Питання для усного опитування / самоконтролю:

1. Що таке мережний трафік і з яких елементів він складається?
2. Яке призначення протоколів TCP та UDP?
3. У чому полягає суть тристороннього квитування TCP?
4. Що таке DNS та яку функцію він виконує в комп'ютерній мережі?
5. Що таке мережний аналізатор та для чого використовується Wireshark?
6. Яку інформацію містить IP-пакет і кадр Ethernet?
7. Яке призначення портів TCP/UDP?

3. Формування професійних вмінь та навичок

3.1. Теоретичні відомості

Ознайомлення з принципами аналізу мережного трафіка за допомогою програми Wireshark; вивчення структури кадру Ethernet, IP-пакета, TCP- та UDP-сегментів; дослідження процесу тристороннього квитування TCP; аналіз DNS-

запитів та відповідей; використання фільтрів для відбору мережних пакетів; визначення уразливостей локальної мережі на основі результатів аналізу трафіка.

Завдання 1. Спостереження за процесом тристороннього квитування протоколу TCP за допомогою програми Wireshark

Частина 1. Підготовка програми Wireshark до захоплення пакетів

Частина 2. Захоплення, пошук і вивчення пакетів

Загальні відомості / сценарій. У даній лабораторній роботі вам належить скористатися програмою Wireshark для захоплення і вивчення пакетів, якими обмінюються браузер ПК, який використовує HTTP-протокол, і вебсервер, наприклад www.google.com. При першому запуску на хості додатки, наприклад HTTP або FTP, протокол TCP встановлює між двома вузлами надійний TCP-сеанс за допомогою тристороннього квитування. Наприклад, при перегляді на ПК сторінок Інтернету через вебоглядач ініціюється тристоронню квитування і встановлюється сеанс зв'язку між хост-комп'ютером і вебсервером. Одночасно на ПК можуть мати місце відразу кілька активних TCP-сеансів з різними вебсайтами.

Частина 1. Підготовка програми Wireshark до захоплення пакетів

Необхідні ресурси

Один ПК (під управлінням Windows 7, 8 або 10 з доступом до командного рядка, доступом до Інтернету і встановленою програмою Wireshark)

У частині 1 вам необхідно запустити програму Wireshark і вибрати відповідні інтерфейси для початку захоплення пакетів.

Крок 1: Дізнайтеся адреси інтерфейсів ПК

У даній лабораторній роботі вам необхідно дізнатися IP-адрес комп'ютера і фізичний адрес мережевої інтерфейсної плати, також званий MAC-адресом.

a. Відкрийте вікно командного рядка, введіть команду ipconfig /all і натисніть клавішу Enter.

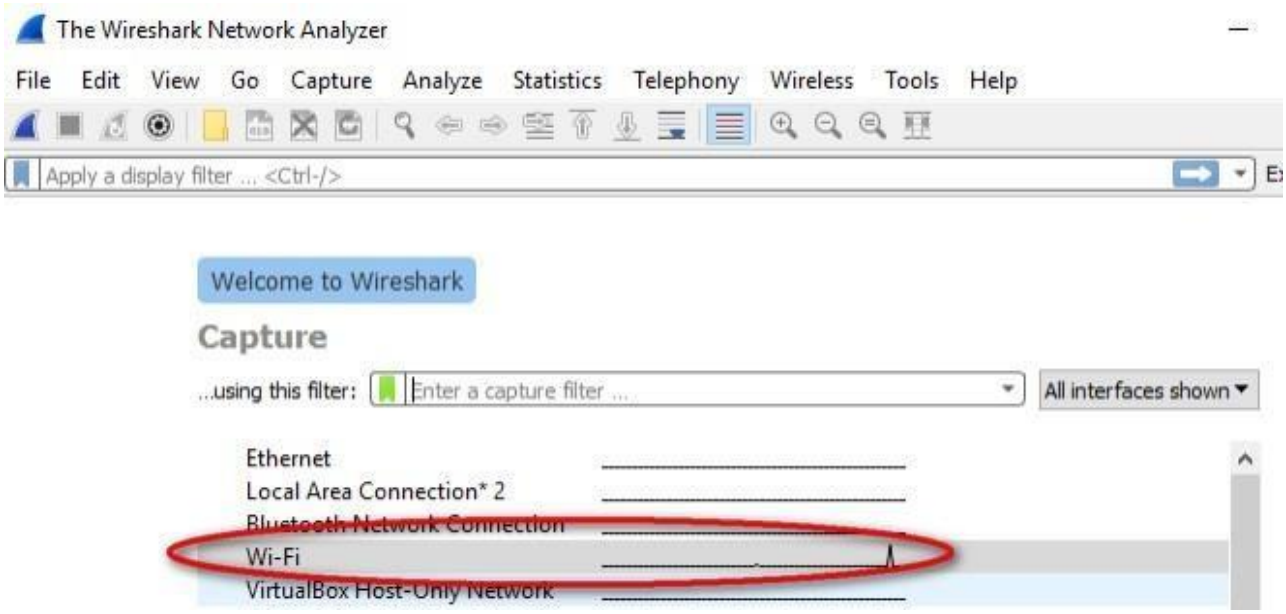
```
Physical Address. . . . . : 00-24-D7-1C-50-44
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80dd:5657:ad20:f4b3%16(Preferred)
IPv4 Address. . . . . : 192.168.1.146(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

b. Запишіть отримані IP-адреси і MAC-адреси, пов'язані з обраним адаптером Ethernet. Це адреса джерела, який потрібно знайти при вивченні захоплених пакетів. IP-адреса вузла ПК:

Крок 2: Запустіть програму Wireshark і виберіть відповідний інтерфейс

a. Натисніть кнопку Start (Пуск) в системі Windows. У спливаючому меню двічі клацніть Wireshark.

b. Після запуску програми Wireshark виберіть активний інтерфейс для захоплення даних. В активному інтерфейсі будуть відображатися відомості про трафік.



Частина 2: Захоплення, пошук і вивчення пакетів

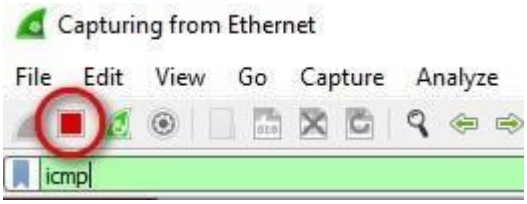
Крок 1: Виконайте захоплення даних.

a. Натисніть кнопку Start (Почати), щоб почати захоплення даних.

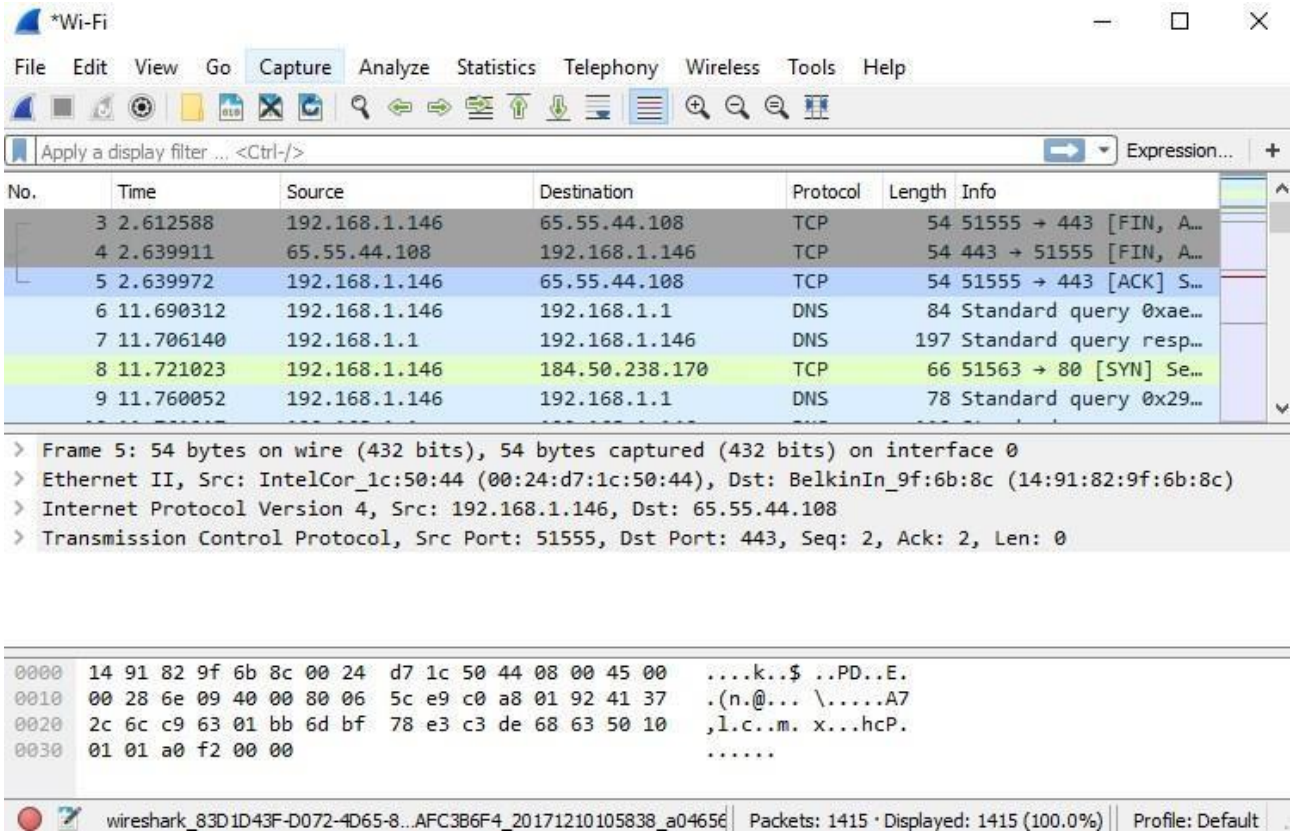


Відкрийте веббраузер і перейдіть на сторінку www.google.com.

b. Згорніть вікно браузера і поверніться в Wireshark. Зупиніть процес захоплення даних.



Тепер вікно захоплення даних активне. Знайдіть стовпці Source (Джерело), Destination (Призначення) і Protocol (Протокол).



Крок 2: Знайдіть відповідні пакети для вебсеансу

Якщо комп'ютер увімкнено недавно і ще не використовувався для доступу в Інтернет, в захоплених даних ви зможете побачити весь процес, включаючи протокол дозволу адрес (ARP), систему доменних імен (DNS) і тристороннє квитування TCP. Якщо на ПК вже був запис ARP для шлюзу, це означає, що був створений DNS-запит для перетворення адреси www.google.com.

a. У кадрі 6 показаний DNS-запит від ПК до DNS-сервера, який намагається перетворити доменне ім'я www.google.com в IP-адреса вебсервера. Перш ніж відправити перший пакет на вебсервер, ПК повинен дізнатися IP-адрес.

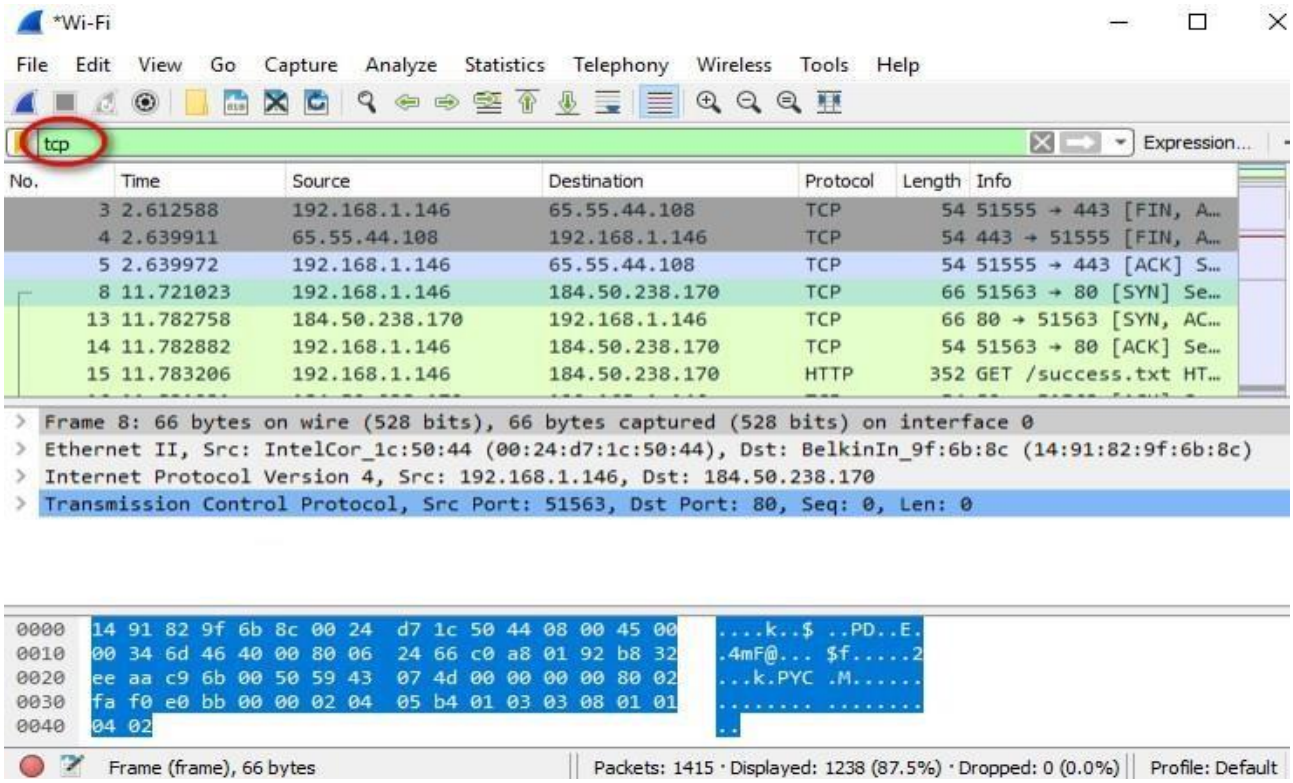
Назвіть IP-адрес DNS-сервера, запитаного комп'ютером.

b. Кадр 7 являє собою відповідь DNS-сервера. Він містить IP-адрес сайту

www.google.com.

c. Знайдіть відповідний пакет, щоб запустити процедуру тристороннього квитування.

В даному прикладі кадр 8 є початком тристороннього квитування TCP. Назвіть IP-адрес вебсервера Google.



Якщо ви отримали багато пакетів, не пов'язаних з TCP-з'єднанням, можливо, доцільно скористатися засобами фільтрації програми Wireshark. В поле значення фільтра програми Wireshark введіть TCP і натисніть Enter (Введення).

Крок 3: Вивчіть дані, які містяться в пакетах, включаючи IP-адреси, номера портів TCP і прапори управління TCP

a. У наведеному прикладі кадр 8 відповідає початку процесу тристороннього квитування між ПК та вебсервером Google. На панелі списку пакетів (верхній розділ основного вікна) виберіть кадр.

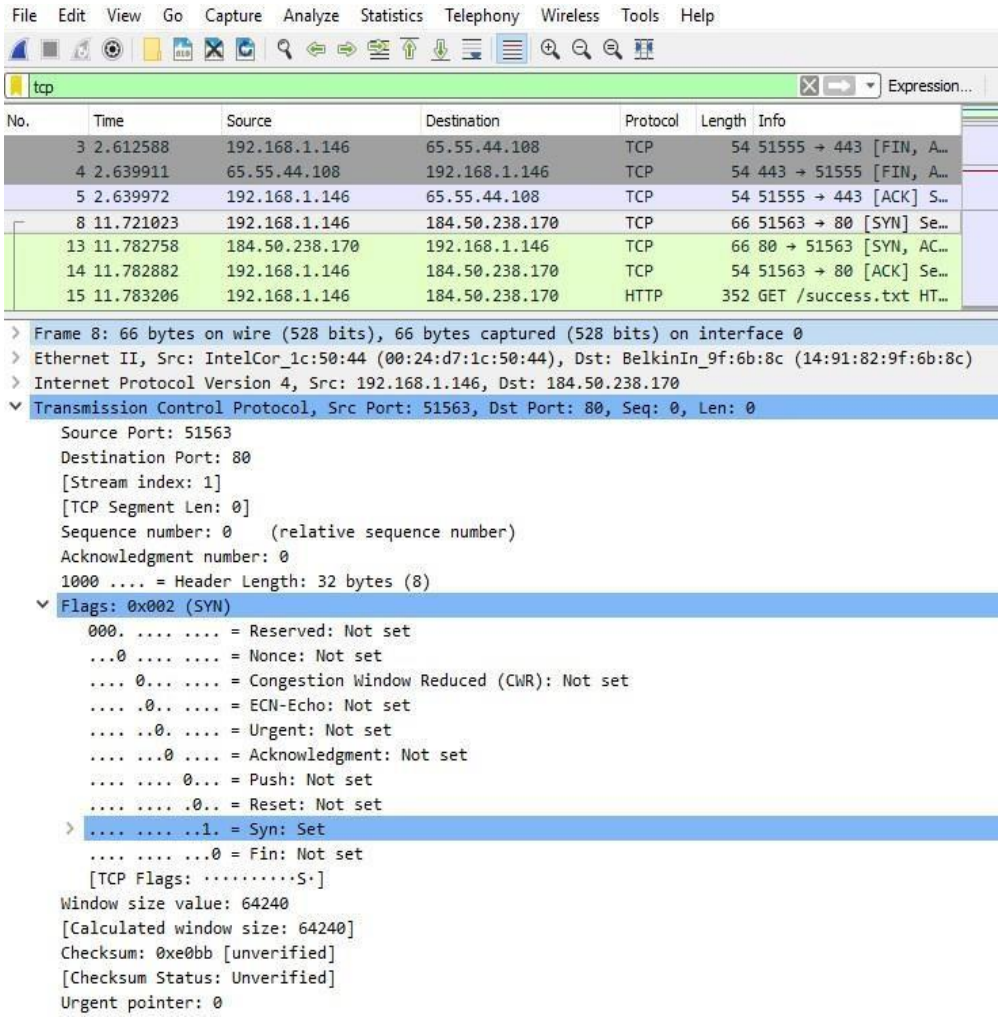
Після цього буде виділена рядок і відображена декодована інформація з цього пакета в двох нижніх панелях. Вивчіть дані TCP в панелі відомостей про пакети (середній розділ основного вікна).

b. На панелі відомостей про пакети натисніть на значок + зліва від рядка

Transmission Control Protocol (Протокол управління передачею даних), щоб побачити детальну інформацію про TCP.

c. Натисніть на значок + зліва від рядка Flags (Прапори). Зверніть увагу на порти джерела і місця призначення, а також на встановлені прапори.

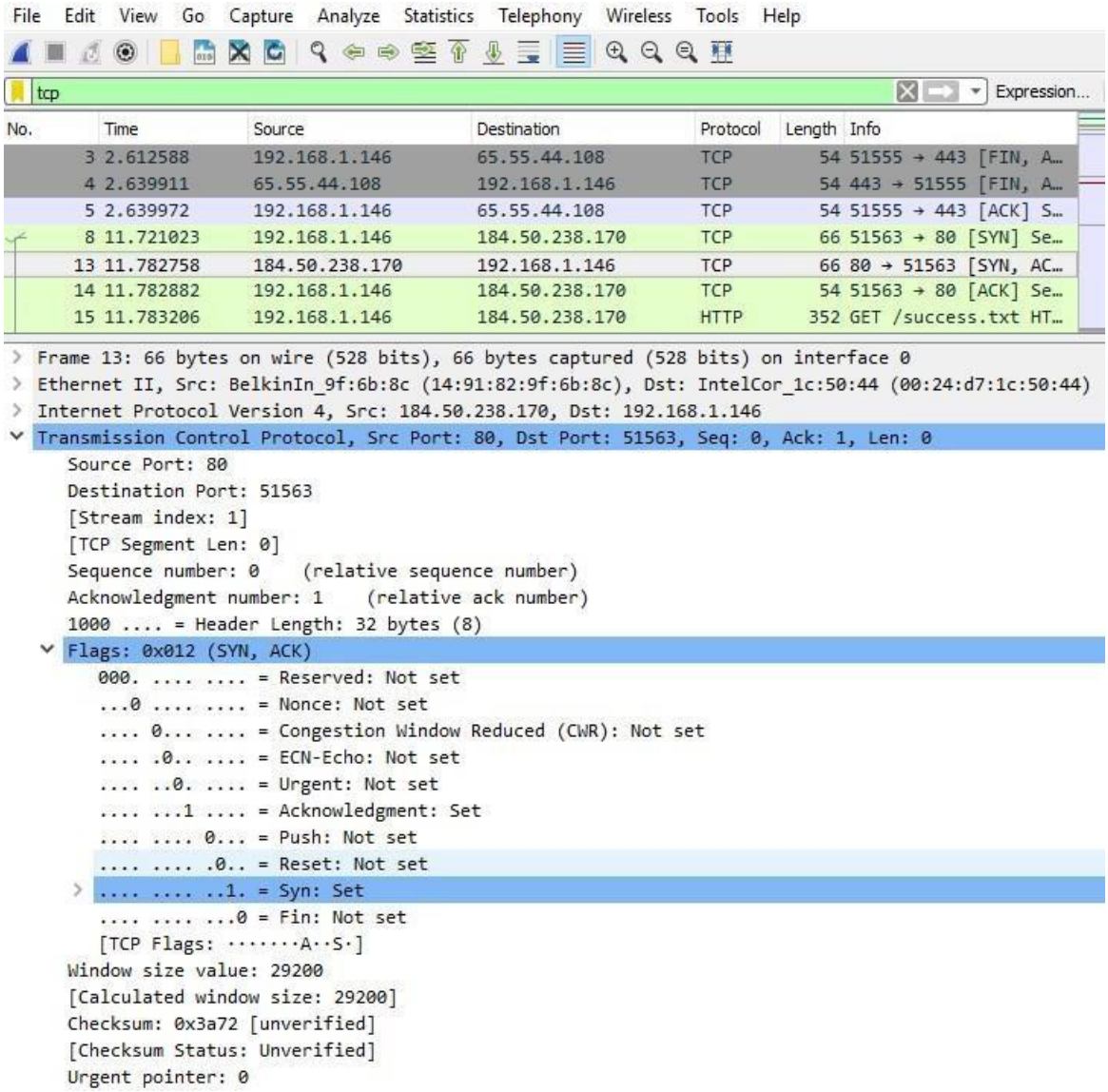
Примітка. Щоб відобразити всі необхідні дані, може знадобитися скорегувати розміри верхнього і середнього вікон програми Wireshark.



- Назвіть номер порту джерела TCP.
- Як би ви класифікували порт джерела?
- Назвіть номер порту призначення TCP.
- Як би ви класифікували порт призначення?
- Які встановлені прапори?
- Яке значення задано для відносного порядкового номера?

d. Для того щоб вибрати наступний кадр в тристоронньому квитуванні, в меню програми Wireshark виберіть пункт Go (Перейти), а потім Next Packet in Conversation (Наступний пакет в діалозі). В даному прикладі це кадр 13. Це

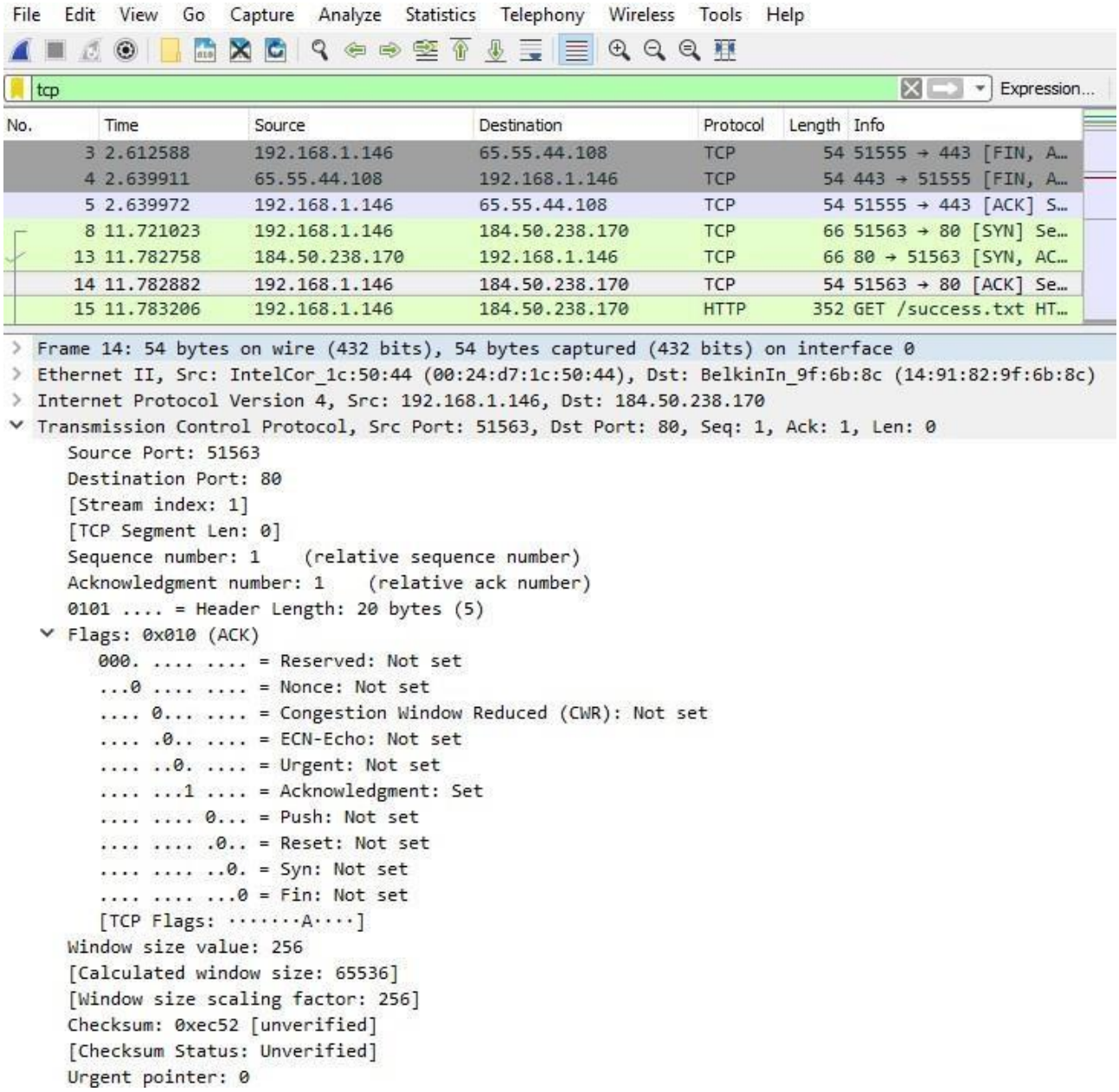
відповідь вебсервера Google на вихідний запит для початку сеансу.



Назвіть значення портів джерела і призначення.

- Які встановлені прапори?
- Які значення задані для відносного порядкового номера і відносного номера підтвердження?

е. І нарешті, вивчіть третій пакет тристороннього квитування в даному прикладі. натиснувши на кадрі 14 в верхньому вікні, ви побачите наступну інформацію в даному прикладі.



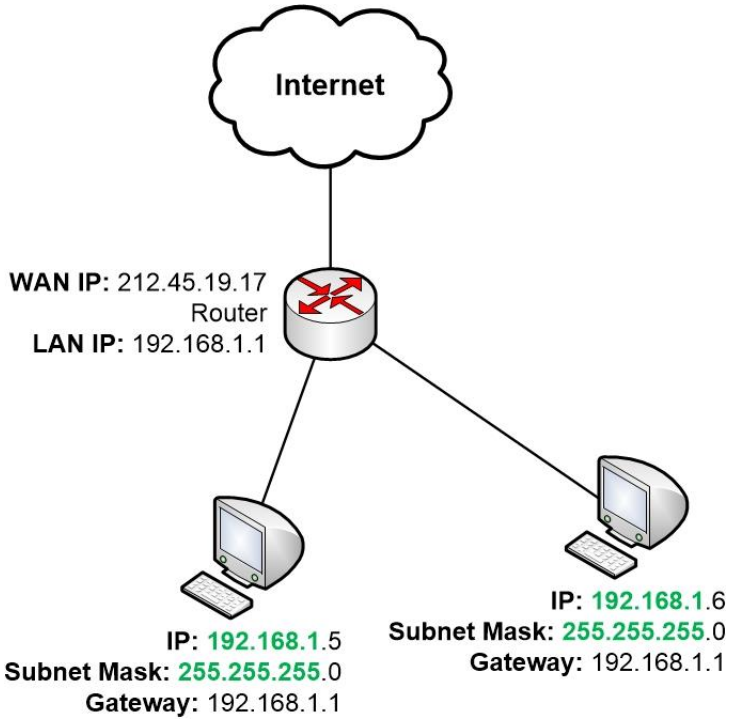
Вивчіть третій і останній пакет квитування.

Які встановлені прапори?

Для відносного порядкового номера і відносного номера підтвердження в якості вихідного значення вибрано значення 1. TCP-зв'язок і тепер може бути розпочато передача даних між ПК-джерелом і вебсервером.

f. Закрийте програму Wireshark.

Завдання 2. Вивчення захоплених пакетів DNS і UDP за допомогою програми Wireshark



Частина 1. Запис даних про конфігурацію IP на ПК

Частина 2. Захоплення запитів і відповідей DNS за допомогою програми Wireshark

Частина 3. Аналіз захоплених пакетів DNS або UDP

Загальні відомості / сценарій. Якщо ви хоча б один раз виходили в Інтернет, то користувалися системою доменних імен (DNS). DNS – це розподілена мережа серверів, яка перетворює зрозумілі людині імена доменів, наприклад www.google.com, в IP-адреси. При введенні в браузері URL-адреси будь-якого веб-сайту комп'ютер відправляє DNS-запит на IP-адрес DNS-сервера. При запиті комп'ютером DNS-сервера і відповіді DNS-сервера в якості протоколу транспортного рівня використовується протокол призначених для користувача датаграм (UDP). На відміну від TCP, UDP є протоколом без встановлення з'єднання і не вимагає встановлення сеансу. Запити та відповіді DNS мають надзвичайно малий обсяг і не потребують використання службової інформації TCP. В ході лабораторної роботи ви будете обмінюватися даними з DNS-сервером, відправляючи DNS-запити за допомогою транспортного

протоколу UDP. Для аналізу обміну даними з сервером доменних імен буде використовуватися програма Wireshark.

Частина 1: Запис даних IP-конфігурації ПК

У частині 1 за допомогою команди ipconfig /all на локальному ПК вам потрібно буде знайти і записати MAC адрес і IP-адрес мережевої інтерфейсної плати свого ПК, IP-адрес зазначеного шлюзу і IP-адрес DNS-сервера, вказаного для ПК. Запишіть ці дані в наведену нижче таблицю. Вони будуть потрібні вам для аналізу пакетів в наступних частинах лабораторної роботи.

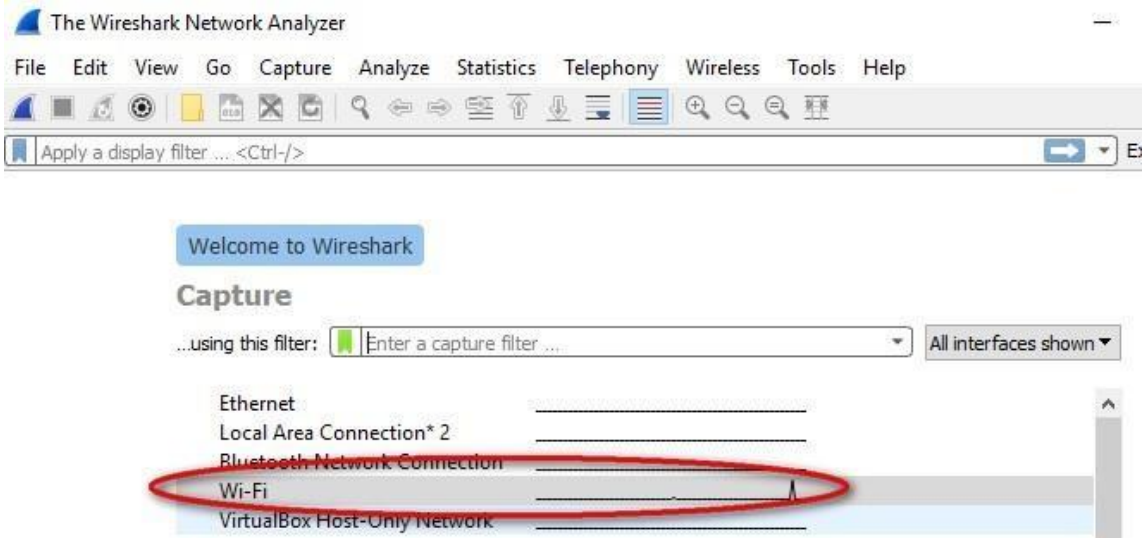
IP-адрес	
MAC-адрес	
IP-адрес шлюзу по замовчуванню	
IP-адрес DNS-сервера	

Частина 2: Захоплення запитів і відповідей DNS за допомогою програми Wireshark

У частині 2 вам потрібно буде налаштувати програму Wireshark для захоплення пакетів запитів і відповідей DNS, щоб продемонструвати використання транспортного протоколу UDP при обміні даними з DNS-сервером.

a. Натисніть кнопку Пуск і відкрийте програму Wireshark.

b. Виберіть інтерфейс для захоплення пакетів з допомогою Wireshark. Виберіть (виділіть) активний інтерфейс захоплення.



c. Вибравши потрібний інтерфейс, натисніть Start (Пуск), щоб почати

захоплення пакетів.

d. Відкрийте веббраузер і введіть адрес www.google.com. Для продовження натисніть клавішу Enter.

e. Як тільки відкриється головна сторінка Google, натисніть кнопку Stop (Зупинити), щоб зупинити захоплення даних програмою Wireshark.

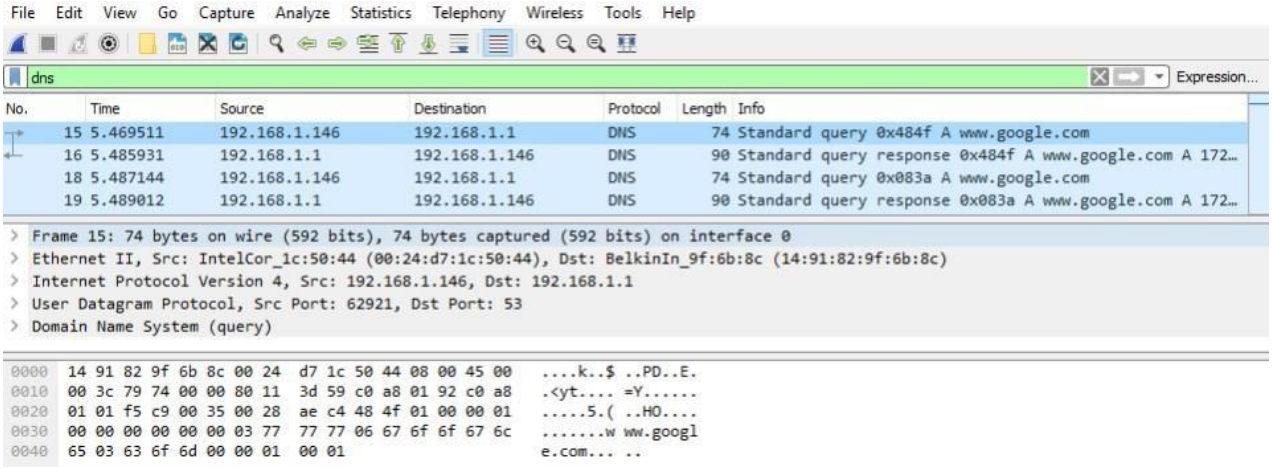
Частина 3: Аналіз захоплених пакетів DNS або UDP

У частині 3 вам необхідно буде вивчити пакети UDP, створені при обміні даними з DNS-сервером для IP-адрес www.google.com.

Крок 1: Фільтравати DNS-пакети

a. У головному вікні програми Wireshark введіть dns в поле Filter (Фільтр) інструментальної панелі і натисніть Enter (Введення).

Примітка. Якщо після застосування фільтра DNS ви не бачите ніяких результатів, закрийте браузер. У вікні командного рядка введіть ipconfig /flushdns для видалення всіх попередніх результатів DNS. Перезапустіть захоплення даних програмою Wireshark і повторіть кроки 2Б - 2Д. Якщо таким чином вирішити проблему не вдалося, то замість використання браузера введіть у вікні командного рядка команду nslookup www.google.com.

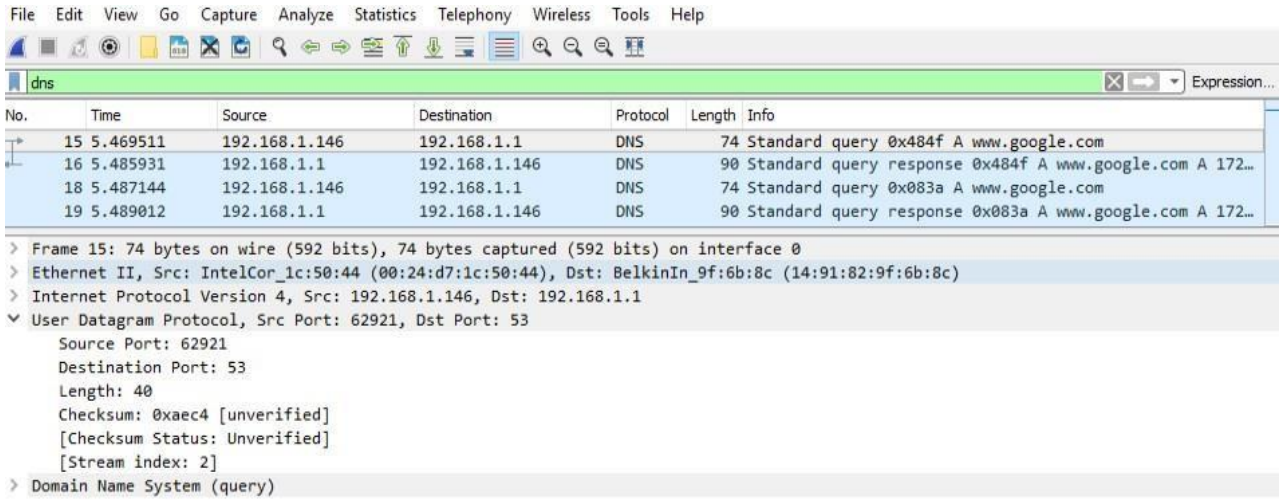


b. На панелі списку пакетів (верхній розділ) в головному вікні програми знайдіть пакет з інформацією Standard query (Стандартний запит) і A www.google.com (Запит сайту google.com). Як приклад можна взяти кадр 15.

Крок 2: Вивчіть сегмент UDP за допомогою DNS-запиту

Вивчіть дані UDP, використовуючи DNS-запит для адреси www.google.com, захоплений програмою Wireshark. В даному прикладі для

аналізу обраний захоплений програмою Wireshark кадр 15 на панелі списку пакетів. Протоколи в цьому запиті відображаються на панелі відомостей про пакети (Середній розділ) в головному вікні. Відомості про протокол виділені сірим кольором.



a. Як показано в першому рядку на панелі відомостей про пакетах, кадр 15 містив 74 байта даних у час передачі. Цю кількість байтів потрібно відправити в якості DNS-запиту на сервер, який запитує IP-адреси сайту www.google.com.

b. Рядок Ethernet II містить MAC-адреси джерела і місця призначення. MAC-адрес джерела належить вашому локальному ПК як джерела DNS-запиту. MAC-адрес призначення – це шлюз, оскільки це остання зупинка перед виходом запиту з локальної мережі. Чи збігається MAC-адрес джерела з адресом, записаним в частині 1 для локального ПК?

c. У рядку Internet Protocol Version 4 захоплені дані IP-пакета показують, що IP-адрес джерела даного DNS-запиту - 192.168.1.146, а IP-адрес призначення - 192.168.1.1. В даному прикладі адрес призначення – це шлюз. В даній мережі шлюзом за усталеним налаштуванням є маршрутизатор. Чи можете ви вказати IP-адрес та MAC-адрес для пристроїв джерела і призначення?

Пристрій	IP-адрес	MAC-адрес
Локальний ПК		
Шлюз по замовчування		

IP-пакет і заголовок інкапсулюють сегмент UDP. Сегмент UDP містить DNS-запит у вигляді даних.

d. Заголовок UDP має тільки чотири поля: порт джерела, порт призначення, довжина і контрольна сума. Як показано нижче, довжина кожного поля в заголовку UDP становить всього 16 біт.

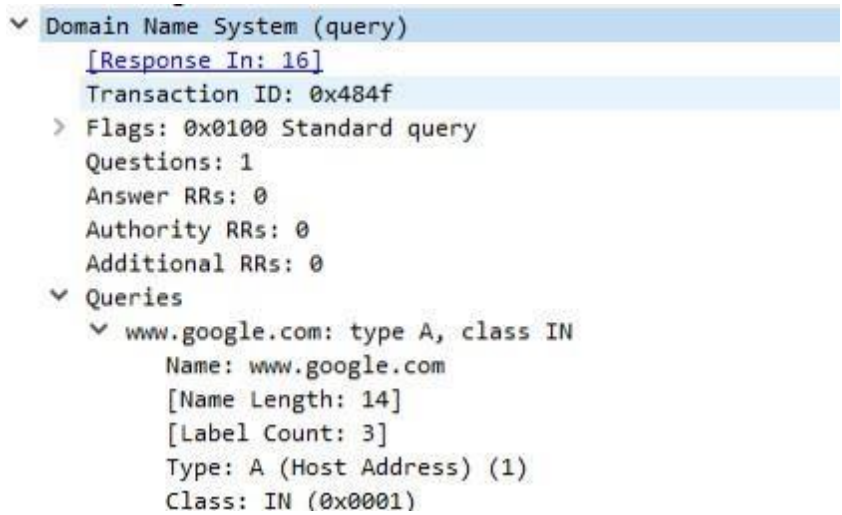
Біти	Поле заголовка UDP	Опис
0-15	Порт джерела UDP (Source Port)	Номер порту відправника; використовується для зворотної доставки сегмента.
16-31	Порт призначення UDP (Destination Port)	Номер порту одержувача; визначає цільовий застосунок.
32-47	Довжина повідомлення UDP (Length)	Загальна довжина UDP-сегмента (заголовок + дані), мінімум 8 байтів.
48-63	Контрольна сума UDP (Checksum)	Використовується для виявлення помилок у заголовку та даних.
64-…	Дані (Data)	Корисне навантаження, що передається протоколом UDP.

Розгорніть вузол User Datagram Protocol на панелі відомостей про пакет, натиснувши на значок «плюс» (+). Зверніть увагу на те, що відображаються лише чотири поля. Номер порту джерела в даному прикладі - 60868. Порт джерела був випадково згенерований локальним ПК з використанням не зарезервованих номерів портів. Порт призначення - 53. Порт 53 – це «добре відомий порт», зарезервований для використання з DNS. DNS-сервери прослуховують порт 53 для отримання DNS-запитів від клієнтів.



В даному прикладі довжина сегмента UDP становить 40 байт. 8 з 40 байт використовуються в якості заголовка. Решта 32 байта використовуються даними DNS-запиту. На наступному рисунку виділені 32 байта даних DNS-запиту на панелі відображення байтів пакета (нижній розділ головного вікна Wireshark).

Контрольна сума використовується для визначення цілісності пакета після його передачі через Інтернет.



Заголовок UDP несе мало службової інформації, оскільки протокол UDP не має полів, пов'язаних з тристороннім квитуванням в протоколі TCP. Будь-які проблеми з надійністю передачі даних повинні вирішуватися на прикладному рівні. Запишіть результати захоплення даних програмою Wireshark в наведену нижче таблицю.

Розмір кадру	
MAC-адрес джерела	
MAC-адрес призначення	
IP-адрес джерела	
IP-адрес призначення	
Порт джерела	
Порт призначення	

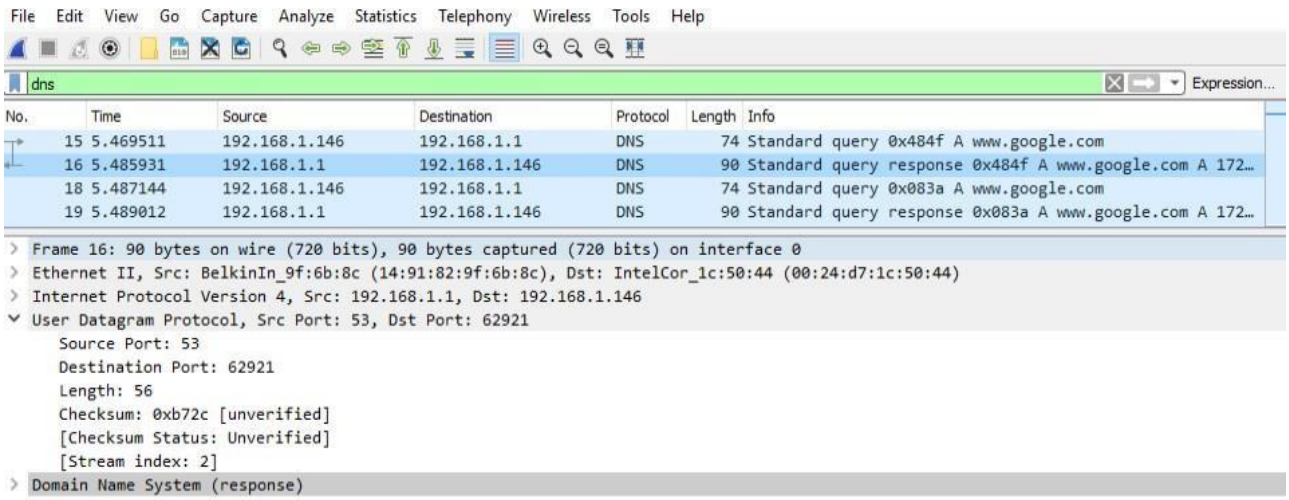
Чи збігається IP-адрес джерела з IP-адресом локального ПК, записаним в частині 1?

Чи збігається IP-адрес призначення зі шлюзом за усталеним налаштуванням, записаним в частині 1?

Крок 3: Вивчіть сегмент UDP за допомогою DNS-відповіді

У цьому кроці вам потрібно вивчити пакет DNS-відповіді і переконатися в тому, що він також використовує протокол UDP.

a. В даному прикладі відповідним пакетом DNS-відповіді є кадр 16. Зверніть увагу на те, що кількість байтів під час передачі становить 90. Цей пакет перевищує за обсягом пакет DNS-запиту.



b. Якщо судити по кадру Ethernet II для DNS-відповіді, якому пристрою відповідає MAC-адрес джерела і який пристрій відповідає MAC-адресу призначення?

c. Зверніть увагу на IP-адреси джерела і призначення в IP-пакеті. Назвіть IP-адрес призначення. Назвіть IP-адрес джерела.

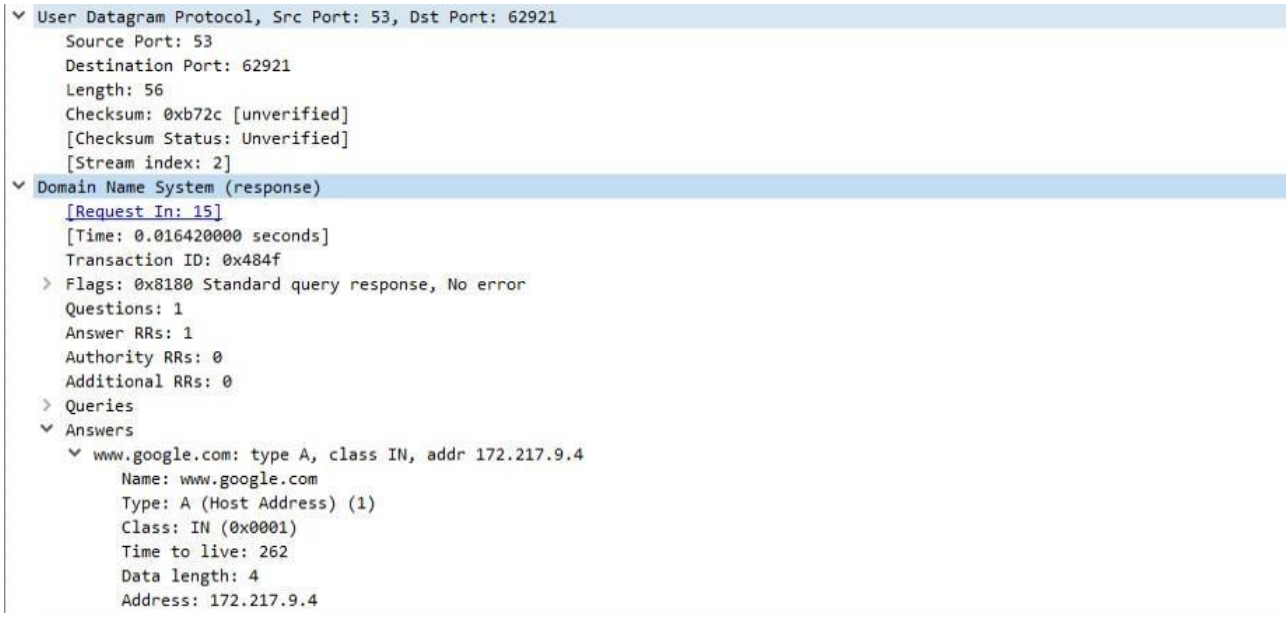
IP-адрес призначення:

IP-адрес джерела:

Що сталося з ролями джерела і призначення локального вузла та стандартного шлюзу?

d. У сегменті UDP ролі номерів портів також змінилися на протилежні. номер порту призначення – 62921. Номер порту 62921 – це той же номер порту, який був згенерований локальним ПК при відправці DNS-запиту на DNS-сервер. Ваш локальний ПК прослуховує цей порт для отримання DNS-відповіді. Номер порту джерела – 53. DNS-сервер прослуховує порт 53 для отримання DNS-запиту, а потім відправляє DNS-відповідь з номером порту джерела 53 назад ініціатору DNS-запиту.

Після того як буде розгорнутий рядок DNS-запиту, зверніть увагу на перетворені IP-адреси сайту www.google



3.2. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш (за встановленим зразком кафедри).
2. Тему, мету та завдання лабораторної роботи.
3. Короткі теоретичні відомості (TCP, UDP, DNS, тристороннє квитування, мережний аналізатор Wireshark – 1–2 сторінки).
4. Практичну частину, що включає:

— скріншоти захопленого трафіка;

— фрагменти TCP-сеансу з відображенням SYN, SYN-ACK, ACK;

— приклади DNS-запиту та DNS-відповіді;

— таблицю з IP- та MAC-адресами, портами джерела і призначення;

— результати фільтрації трафіка в Wireshark.

5. Висновки, які повинні містити:

— узагальнення щодо можливостей аналізу мережного трафіка;

— оцінку ефективності використання Wireshark для виявлення мережевих уразливостей;

— отримані практичні навички;

— рекомендації щодо використання мережного аналізу для підвищення рівня безпеки локальної мережі.

6. Список використаних джерел, оформлений відповідно до вимог ДСТУ 8302:2015.

4. Підбиття підсумків заняття

— обговорення результатів аналізу TCP-, UDP- та DNS-трафіка;

— аналіз правильності визначення IP- та MAC-адрес, портів, прапорів TCP;

— узагальнення результатів дослідження тристороннього квитування;

— оцінювання повноти та якості виконаного звіту;

— формулювання висновків щодо значення аналізу мережного трафіка для забезпечення інформаційної безпеки.

5. Список рекомендованої літератури

Основна:

1. Таненбаум Е., Веселінг Д. Комп'ютерні мережі : підручник. 5-те вид. – Київ : Діалектика, 2016. 960 с.

2. Лозінова Г. М. Комп'ютерні мережі : навч. посібник. Київ : Кондор, 2003. 352 с.

3. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

4. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

Додаткова:

1. Кулаков Ю. О. Комп'ютерні мережі : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2022. 247 с.

2. Столінгс В. Мережна безпека. Принципи та практика. Київ : Вільямс, 2018. 864 с.

Інформаційні ресурси:

1. Електронний навчальний курс дисципліни у середовищі «Віртуальний університет».
2. Офіційний сайт Wireshark – https://www.wireshark.org
3. Офіційний сайт мережевої академії Cisco – https://www.netacad.com

ЛАБОРАТОРНА РОБОТА № 9

Тема: мережевий захист ресурсів операційної системи за допомогою IPSec.

Мета: формування у здобувачів вищої освіти знань про механізми захисту мережевого трафіка на основі IPSec, його протоколи та режими роботи; набуття практичних навичок створення політик безпеки, фільтрів, правил й методів перевірки дійсності, а також застосування IPSec для забезпечення конфіденційності, цілісності та автентичності даних в інформаційно-телекомунікаційних системах.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *IPSec (Internet Protocol Security)* – набір мережевих протоколів, що забезпечують конфіденційність, цілісність та автентичність IP-трафіка за допомогою шифрування, контролю доступу та перевірки дійсності комунікації.

IP-фільтр – правило, яке визначає характеристики мережевого трафіка (IP-адреси джерела й призначення, протокол, порти), що підлягає аналізу або обробці в рамках політики IPSec.

Політика IPSec – сукупність правил, фільтрів, дій фільтрів та методів автентифікації, що регулюють порядок обробки, шифрування або блокування IP-трафіка в операційній системі.

Фільтр-лист (Filter List) – логічно згрупований набір IP-фільтрів, що визначає, до якого саме трафіка застосовуватиметься дія політики IPSec.

Фільтр-екшн (Filter Action) – набір параметрів, що визначає дію над трафіком, який відповідає фільтра (дозволити, блокувати, узгодити параметри захищеного з'єднання).

ESP (Encapsulating Security Payload) – протокол IPSec, який забезпечує шифрування даних, контроль їх цілісності та автентичність, а також захист від повторних атак.

AH (Authentication Header) – протокол IPSec, що забезпечує автентичність та цілісність IP-пакетів без виконання їх шифрування.

Транспортний режим IPSec – режим, у якому захищається лише корисне навантаження пакета, тоді як початковий IP-заголовок залишається незмінним; використовується для зв'язку між кінцевими вузлами.

Тунельний режим IPSec – режим, у якому весь IP-пакет інкапсулюється в новий пакет і може бути повністю зашифрований; застосовується для створення VPN-тунелів та взаємодії між шлюзами.

Методи перевірки дійсності (Authentication Methods) – механізми встановлення довіри між учасниками IPSec-з'єднання (Kerberos, цифрові сертифікати, попередньо узгоджені ключі).

Kerberos – централізований протокол автентифікації, що використовує систему квитків для підтвердження особи клієнта та сервера без передавання паролів мережею.

Безпечне з'єднання (Secure Connection) – з'єднання, у якому трафік захищений за допомогою механізмів IPSec, що забезпечують конфіденційність, автентичність та контроль цілісності даних.

Шифрування трафіка – процес перетворення даних у недоступний для стороннього спостерігача вигляд із використанням криптографічних алгоритмів з метою захисту під час передачі мережею.

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до мережі Інтернет; операційна система Windows / Linux; веббраузер для роботи з електронним курсом та пошуку інформації; текстовий редактор (MS Word / Google Docs або аналог); консоль Local Security Policy; засоби адміністративного керування Windows; доступ до електронного курсу у «Віртуальному університеті»; (за необхідності) віртуальні машини VMware / VirtualBox для моделювання мережних взаємодій.

План

1. Організаційні заходи

- повідомлення теми, мети та завдань лабораторної роботи;
- мотивація навчальної діяльності: роль IPSec у захисті мережевих систем, серверів, критичної інфраструктури та державних реєстрів;
- ознайомлення зі структурою матеріалів у «Віртуальному університеті»;

- інструктаж з правил безпеки під час роботи з ОС Windows та мережевими службами;
- пояснення вимог до оформлення та порядку подання звіту.

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: базові знання TCP/IP; поняття контролю доступу та фільтрації трафіка; розуміння принципів шифрування та автентифікації; загальні уявлення про роботу мережевих сервісів.

Перелік дидактичних одиниць для перевірки: призначення протоколів IPSec; транспортний і тунельний режими; протоколи ESP і AH; поняття політики безпеки, фільтрів і дій фільтрів; механізми перевірки дійсності (Kerberos, сертифікати, ключі).

Питання для усного опитування / самоконтролю:

1. У чому полягає принцип роботи IPSec?
2. Які відмінності між ESP і AH?
3. Чим різняться транспортний і тунельний режими?
4. Які функції виконує політика IPSec?
5. Які параметри включає IP-фільтр?
6. Які методи автентифікації підтримує IPSec?
7. Які види трафіка доцільно шифрувати в корпоративних мережах?

3. Формування професійних умінь та навичок

3.1. Теоретичні відомості

IPSec є одним із ключових механізмів забезпечення безпечного обміну даними в мережах. Він працює на мережевому рівні та дає можливість прозорого захисту будь-яких протоколів верхніх рівнів.

У Windows IPSec реалізується у вигляді політик безпеки, що містять:

- списки фільтрів (визначають, який трафік захищається);
- дії фільтрів (визначають, дозволити/блокувати/захищати трафік);
- правила політики (поєднання фільтрів і дій);
- методи перевірки дійсності (Kerberos, сертифікати, ключі).

IPSec може забезпечувати захист служб, у яких використовується незашифрований трафік (FTP, Telnet, SMB), а також дозволяє створювати захищені канали між серверами, комп'ютерами та шлюзами.

3.2. Зміст лабораторної роботи

1. Запустіть консоль керування *IPSec* на вашому комп'ютері. Виберіть одну з політик *IPSec, використовувану за усталеним налаштуванням*, для цього відкрийте меню «*Локальна політика безпеки*» (*Local Security Policy*) у директорії «*Адміністрування*» (*Administrative Tools*) і виберіть розділ «*Політики безпеки IP на локальному комп'ютері*» (*IP Security Policies on Local Computer*). Ознайомтесь з принципами даної політики безпеки.

2. Створіть свій список фільтрів, зазначений, залежно від варіанта. Для цього виберіть у вікні «*Локальні настроювання безпеки*» *(Local Security Settings*) і виберіть у контекстному меню «*Дія*» пункт «*Керування списками IP- Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*). На закладці «*Керування списками фільтрів IP*» (*Manage IP Filter Lists*) натисніть кнопку «*Додати*» (*Add*). Введіть у поле ім'я назву списку. У стартовому вікні майстра *фільтрів* IP натисніть кнопку «Додати», а потім кнопку «Далі» (Next). Виберіть один із пропонованих варіантів в якості джерела призначення і протокол, що задовольняє вимогам вашого завдання. Виберіть пункт «*Пакети на цей порт*» (*To this port*) і введіть у поле значення, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готове*» (*Finish*).

Як джерело ви можете вибрати:

– «*Моя IP-Адреса*» (*My IP Address*);
– «*Люба IP-Адреса*» (*Any IP Address*);
– «*Певне DNS-Ім'я*» (*DNS name*);
– «*Певна IP-Адреса*» (*IP Address*);
– «*Певна* підмережа *IP*» (*IP network*). Як призначення ви можете вибрати:
– «*Моя IP-Адреса*» (*My IP Address*);
– «*Люба IP-Адреса*» (*Any IP Address*);
– «*Певне DNS-Ім'я*» (*DNS name*)4
– «*Певна IP-Адреса*» (*IP Address*);

– «*Певна* підмережа *IP*» (*IP network*). Як протокол ви можете вибрати:
– *EGP;*
– *HMP;*
– *ICMP;*
– *RAW;*
– *RDP;*
– *RVD;*
– *TCP;*
– *UDP;*
– *XNS-IDP;*
– *інші, із вказівкою номера порту;*
– *кожний*.

3. Створіть власну дію фільтра, зазначену, залежно від варіанта. Для цього в діалоговому вікні «*Керування списками IP-Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*) перейдіть на закладку «*Керування діями фільтра*» (*Manage Filter Actions*) і натисніть кнопку «*Додати*». У стартовому вікні майстра настроювання дій *фільтрів* IPSec натисніть кнопку «Далі». У вікні настроювання загальних параметрів дії фільтра виберіть один із пропонованих варіантів, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готово*». Для завершення настроювання списку і дій фільтрів, натисніть кнопку «*Закрити*» (*Close*).

У вікні настроювання загальних параметрів дії фільтра ви можете вибрати одну з наступних дій:

– «*погодити*» (*Negotiate*);
– «б*локувати*» (*Block*);
– «д*озволити*» (*Permit*).

4. Створіть свою політику *IPSec*. Для цього у вікні «*Локальні настроювання безпеки*» виберіть із контекстного меню пункт «*Створити політику безпеки IP*» (*Create IP Security Policy*) і у вікні майстра *політики IP*-безпеки натисніть кнопку «Далі». Уведіть у поле ім'я, назву вашої політики. Відмовтеся від використання пункту «*Використовувати правило за усталеним*

налаштуванням» (*Activate the default response rule*) і натисніть «*Далі*». Залишіть пункт «*Змінити властивості*» (*Edit properties*) і натисніть кнопку «*Готово*» для завершення роботи майстра.

5. Додайте до створеної вами політики правило за зазначеними критеріями, залежно від варіанта. Для цього в діалоговому вікні властивостей політики натисніть кнопку «*Додати*», потім кнопку «*Далі*». З переліку списків фільтрів виберіть назву вашої політики. Зі списку дій фільтрів виберіть одну з дій. Для завершення роботи майстра натисніть кнопку «*Готове*».

6. Призначте обрану політику, для цього виберіть пункт «*Призначити*» (*Assign*) політики «*Назва вашої політики»*.

Варіанти завдань для виконання лабораторної роботи (Настроювання параметрів фільтра й політики IPSec):

1. Установлюючи політики на сервері вашої організації, створіть для комп'ютерів, які повинні використовувати безпечні з'єднання, політику, яка допускає небезпечні з'єднання з комп'ютерами не підтримуючими *IPSec*. Передбачте, щоб комп'ютер приймав незахищений трафік, але завжди виконував спробу захистити додаткові зв'язки, посилаючи відправникові запит безпеки. Включіть в політику правило запиту безпеки для всього *IP-трафіка*, метод перевірки дійсності *Kerberos*, без параметрів тунелюваня, для типу підключення – всіх мережних підключень.

2. Установлюючи політики на сервері вашої організації, створіть для комп'ютерів політику, яка дозволяє пересилати весь *ICMP-трафік*, не перевіряючи дійсність, без параметрів тунелюваня, для типу підключення – всіх мережних підключень.

3. Установлюючи політики на сервері вашої організації, створіть для комп'ютерів політики відгуку за усталеним налаштуванням для відповіді на запити безпеки від інших комп'ютерів. Включіть в політику динамічний список фільтрів, для дії фільтра – відгук за усталеним налаштуванням, з методом перевірки *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.

4. Сервер вашої організації передає секретні дані. Установіть політики на

сервері, для комп'ютерів таким чином, щоб вони завжди вимагали захист усього вихідного трафіка, допускаючи відсутність захисту тільки для початкового вхідного запиту на з'єднання. Для цього включіть правило запиту безпеки для всього *IP-трафіка*, не перевіряючи дійсність, без тунелюваня, для типу підключення – всіх мережних підключень.

5. Установіть політики на сервері вашої організації, для комп'ютерів, таким чином, щоб дозволити пересилати весь *ICMP-трафік*, перевіряючи дійсність методом *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень

6. Установіть політики на сервері вашої організації, для комп'ютерів, забезпечивши правило відгуку за усталеним налаштуванням для відповіді на запити безпеки від інших комп'ютерів. Для цього включіть в правило динамічний список фільтрів *IP*, з дією фільтра за усталеним налаштуванням, методом перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.

7. Створіть політики для комп'ютерів, які захищають дані за запитом, для рішення задачі, коли клієнти інтрамережі можуть не потребувати використання *IPSec*, крім випадків, коли запит виходить з іншого комп'ютера, щоб забезпечити комп'ютеру, на якому активізована політика, відповідати на запити безпечного зв'язку. Включіть в політику правило відгуку за усталеним налаштуванням, що створює динамічні фільтри *IP* для вхідного і вихідного трафіка на основі методу перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.

8. Дозвольте дію, задавши, у фільтрі *IP*, політику для взаємодії з *DNS* сервером таким чином, щоб дані передавалися з адреси вашого комп'ютера, на будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, за 53 порт *tcp* і *udp* протоколів. Включіть в політику правило зв'язку списку з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.

9. Дозвольте дію, задавши, у фільтрі *IP*, політики для взаємодії з *SQL* сервером таким чином, щоб дані передавалися з адреси вашого комп'ютера на

будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, за порт *1433* порту *tcp* і *udp* протоколами. Включіть в політику правило зв'язку списку з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності кожної з них, без тунелюваня, для типу підключення – всіх мережних підключень.

10. Дозвольте дію, задавши, у фільтрі *IP*, політики для Web-*Сервера* таким чином, щоб з будь-якої адреси й будь-якого порту передавалися дані на адресу вашого комп'ютера, за *80*/*tcp* портом й з будь-якої адреси, будь-якого порту, передавалися дані на адресу вашого комп'ютера за портом *443*/*tcp*.

11. Створіть політики для комп'ютерів, створивши правило для фільтрації вихідного трафіка, тобто від адреси комп'ютера, на будь-яку адресу, за портом *1434*/*udp*. За допомогою цього правила заблокуйте будь-який вихідний трафік через порти *UDP 1434* інших комп'ютерів мережі.

12. Налаштуйте політики ізолювання доменів використовуючи наступні правила. Використовуйте налаштування для всього трафіка *IP*, дія фільтра: тільки *Encapsulating Security Payload* (*ESP*), нульове шифрування (null encryption), перевірка цілісності *SHA-1* (*SHA-1 integrity*), обов'язковий захист (*require security*), заборона взаємодії між комп'ютерами без використання протоколу *IPSec*. При цьому дозволивши дії фільтрів, що містять адреси або діапазон адрес контролерів домена.

3.4. Вимоги до результатів роботи та оформлення звіту

Звіт повинен містити:

— титульний аркуш;

— тему, мету та завдання роботи;

— короткі теоретичні відомості (1–2 стор.);

— опис створених фільтрів, дій і політик (зі скріншотами);

— таблицю параметрів політики (адреси, протокол, порти, дії);

— результати перевірки (який трафік дозволено / заблоковано / захищено);

— висновки щодо ефективності IPSec у мережевому захисті;

— список використаних джерел.

4. Підбиття підсумків заняття

— обговорення коректності створених політик та правил;

— аналіз типових помилок;

— оцінювання повноти звітів та правильності виконання завдань;

— формування висновків щодо застосування IPSec у практиці кіберзахисту.

5. Список рекомендованої літератури

Основна:

1. Саченко А. А., Кулаков Ю. О., Кочан В. В. Комп’ютерні мережі : навч. посіб. Тернопіль : Економічна думка ТНЕУ, 2016. 476 с.

2. Буров Є. В. Комп’ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

3. Валецька Т. М. Комп’ютерні мережі: апаратні засоби : навч. посіб. Київ : Ельга, 2004. 304 с.

4. Жуков В. І. Комп’ютерні мережі : навч. посіб. Київ : НАУ-друк, 2009. 392 с.

5. Лозінова Г. М. Комп’ютерні мережі : навч. посіб. Київ : Кондор, 2003. 272 с.

6. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Boston : Pearson, 2023. 784 p.

7. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. New Jersey : Pearson, 2022. 512 p.

8. Tanenbaum A. S., Wetherall D. J. Computer Networks. 6th ed. Boston : Pearson, 2021. 960 p.

9. Maufer T. IPsec: A Guide to Implementation and Usage. Upper Saddle River : Prentice Hall, 2001. 412 p.

10. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 2nd ed. New Jersey : Prentice Hall, 2016. 750 p.

Додаткова:

1. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

2. Кулаков Ю. О. Комп’ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 247 с.

3. Мельник А. Ф. Захист інформації в комп’ютерних системах і мережах : навч. посіб. Київ : КНУБА, 2018. 268 с.

4. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023.

5. ДСТУ ISO/IEC 27002:2022. Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою. Київ : ДП «УкрНДНЦ», 2022.

6. Boyle R., Panko R. Corporate Computer Security. 5th ed. London : Pearson, 2021. 720 p.

7. Sheldon T. Encyclopedia of Networking & Telecommunications. 2nd ed. New York : McGraw-Hill, 2019. 960 p.

8. Kent S., Seo K. Security Architecture for the Internet Protocol. RFC 4301. IETF, 2005.

9. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC 6071. IETF, 2011.

10. Harkins D. IPsec Tutorial. IEEE Communications Surveys, 2020, Vol. 22, No. 4. P. 1225-1250.

Інформаційні ресурси:

1. Cisco Networking Academy. Introduction to Networks. URL: https://www.netacad.com

2. Microsoft Learn. IPsec configuration and management. URL: https://learn.microsoft.com

3. NIST Computer Security Resource Center. Guidelines for Network Security. URL: https://csrc.nist.gov

4. Internet Engineering Task Force (IETF). IPsec Documentation Library. URL: https://www.ietf.org

5. Віртуальний університет ЛДУБЖД. URL: https://virt.ldubgd.edu.ua

ЛАБОРАТОРНА РОБОТА № 10

Тема: дослідження VPN-технологій (GRE та IPSec VPN).

Мета: опанувати теоретичні основи функціонування віртуальних приватних мереж (VPN); сформувати практичні навички налаштування site-to-site GRE VPN та site-to-site IPSec VPN на базі Cisco IOS у середовищі Cisco Packet Tracer; навчитися виконувати пошук та усунення несправностей у роботі VPN-тунелів.

Місце проведення: згідно з розкладом.

Час: 4 години.

Основні поняття: *VPN (Virtual Private Network, віртуальна приватна мережа)* – логічна мережа, побудована поверх публічної мережі (наприклад, Інтернет), яка забезпечує захищений обмін даними між віддаленими вузлами або підмережами завдяки тунелювання та криптографічних механізмів.

Site-to-site VPN (VPN між двома пунктами) – тип VPN, що забезпечує постійно діюче захищене з'єднання між двома стаціонарними мережами (сайтами), здебільшого між двома маршрутизаторами або між маршрутизатором та шлюзом провайдера.

Remote-access VPN (VPN віддаленого доступу) – тип VPN, що надає окремим користувачам (мобільним або надомним працівникам) захищений доступ до корпоративної мережі з будь-якого місця через публічну мережу.

GRE (Generic Routing Encapsulation) – протокол тунелювання, розроблений Cisco, який інкапсулює пакети мережевого рівня в IP-пакети, створюючи логічний point-to-point канал між маршрутизаторами; сам по собі не забезпечує шифрування й автентифікації.

MPLS (Multiprotocol Label Switching) – технологія комутації за мітками, що використовує додаткові мітки замість традиційної маршрутизації за IP-адресами, дає змогу будувати VPN з типом з'єднання «any-to-any».

IPSec (Internet Protocol Security) – набір відкритих стандартів і протоколів мережевого рівня, що забезпечують шифрування, автентифікацію, цілісність та контроль доступу для IP-трафіка, у тому числі при побудові VPN.

ISAKMP (Internet Security Association and Key Management Protocol) – каркасний протокол, який визначає процедури встановлення зв'язків безпеки (SA) та управління ключами в IPSec.

IKE (Internet Key Exchange) – протокол обміну ключами в IPSec, що працює у дві фази: IKE Phase I (створення й захист ISAKMP-тунелю) та IKE Phase II (створення власне IPSec-тунелів для користувацьких даних).

Transform-set (набір перетворень IPSec) – комбінація протоколів IPSec (ESP, AH) та криптографічних алгоритмів (шифрування, хешування), що визначає спосіб захисту трафіка в IPSec-тунелі.

Crypto map (криптографічна карта) – сукупність параметрів IPSec (peer, transform-set, ACL «цікавого» трафіка тощо), яку прив'язують до вихідного інтерфейсу маршрутизатора для активації IPSec-тунелю.

Access Control List (ACL, список контролю доступу) – набір правил фільтрації трафіка, що визначають, які IP-пакети (за адресами, протоколами, портами) вважаються «цікавими» для шифрування в IPSec VPN.

Site-to-site GRE VPN – VPN, у якому логічний тунель між маршрутизаторами побудований на основі GRE, а весь трафік між сайтами інкапсулюється в GRE-пакети (може додатково захищатися IPSec).

Site-to-site IPSec VPN – VPN між двома пунктами, у якому захист трафіка забезпечується безпосередньо механізмами IPSec (шифрування, автентифікація, цілісність та секретний обмін ключами).

Обладнання та програмне забезпечення: персональні комп'ютери / ноутбуки з доступом до мережі Інтернет; операційна система Windows / Linux; веббраузер для роботи з електронним курсом та пошуку інформації; текстовий редактор (MS Word / Google Docs або аналог); встановлений Cisco Packet Tracer (версія, рекомендована кафедрою); віртуальні маршрутизатори Cisco (моделі 2911 у Cisco Packet Tracer); засоби адміністративного керування Windows; доступ до електронного курсу у «Віртуальному університеті»; (за необхідності) віртуальні машини VMware / VirtualBox для моделювання мережних взаємодій.

План

1. Організаційні заходи

— оголошення теми, мети й завдань лабораторної роботи;

— мотивація: роль VPN у захисті корпоративних мереж, критичної інфраструктури та віддаленого доступу;

— ознайомлення зі структурою матеріалів у «Віртуальному університеті»;

— інструктаж з техніки безпеки при роботі з ПЗ та мережевими симуляторами;

— пояснення вимог до оформлення та подання звіту.

2. Контроль опорного рівня знань

Вимоги до теоретичної готовності здобувачів: базові поняття моделі ISO/OSI та TCP/IP; принципи маршрутизації в IP-мережах; основи криптографічного захисту інформації; загальні уявлення про VPN, тунелювання, GRE та IPSec; виконувати базове налаштування інтерфейсів маршрутизаторів; налаштовувати статичну маршрутизацію; працювати з ACL у Cisco IOS на базовому рівні.

Перелік дидактичних одиниць для перевірки: поняття VPN, типи VPN (site-to-site, remote-access); GRE-тунелювання; основи IPSec, фази IKE; ACL як механізм визначення «цікавого» трафіка; принцип роботи site-to-site VPN.

Питання для усного опитування / самоконтролю:

1. Що таке VPN та з якою метою він використовується?
2. Чим відрізняється site-to-site VPN від remote-access VPN?
3. Які функції виконує GRE у побудові VPN?
4. Які основні задачі вирішує IPSec?
5. У чому полягає різниця між IKE Phase I та IKE Phase II?
6. Яку роль відіграє ACL при налаштуванні IPSec VPN?
7. Які переваги застосування VPN у порівнянні з виділеними каналами?

3. Формування професійних умінь та навичок

3.1. Теоретичні відомості

VPN (Virtual Private Network) реалізує логічне з’єднання між двома або більше мережами через публічну інфраструктуру (Інтернет), забезпечуючи при

цьому захищений обмін даними. Найпростішим прикладом VPN є тунель між двома маршрутизаторами, у якому користувацький трафік інкапсулюється в інший протокол (GRE, IPSec, MPLS).

Перші реалізації VPN базувалися на простому IP-тунелюванні (як-от GRE) без шифрування та автентифікації. Згодом з'явилися технології, що поєднують тунелювання та криптографію (IPSec, SSL VPN тощо).

IPSec – не один протокол, а комплекс стандартів, що описують:

— шифрування та забезпечення конфіденційності;

— автентифікацію вузлів;

— цілісність даних (хеш-функції MD5, SHA);

— захищений **обмін ключами (алгоритм Діффі–Гелмана, IKE).**

IPSec працює на мережевому рівні й може захищати трафік будь-яких протоколів верхніх рівнів. Заголовок IP, як правило, доступний для маршрутизації, що забезпечує прозоре проходження пакетів через мережу.

Переваги використання VPN:

— Економічність – відсутність потреби у власних виділених каналах, можливість використовувати Інтернет як транспорт.

— Секретність – захист від несанкціонованого доступу шляхом шифрування та автентифікації.

— Масштабованість – можливість легко додавати нових користувачів та віддалені майданчики без суттєвої зміни інфраструктури.

— Сумісність із широкосмуговими технологіями – підтримка доступу через DSL, оптово**локно, мобільні мережі, Wi-Fi тощо.**

У цій лабораторній роботі розглядається побудова:

— site-to-site GRE VPN – для створення логічного тунелю між маршрутизаторами;

— site-to-site IPSec VPN – для захищеного шифрованого тунелювання

трафіка між тими ж сайтами.

3.2. Зміст лабораторної роботи

Варто зазначити, що IPsec – це не один протокол, а комплекс (конструкція), що містить набір відкритих стандартів, які описують правила побудови захищеної (секретної) комунікації. IPsec реалізує існуючі криптографічні алгоритми для забезпечення шифрування, автентифікації, конфіденційності та секретного обміну ключами.

IPsec працює на мережевому рівні моделі ISO/OSI, захищаючи та автентифікуючи IP-пакет між двома IPsec-пристроями. Заголовок IP-пакета при цьому, як правило, подається у відкритому вигляді, тому не виникає проблем із маршрутизацією. IPsec може функціонувати поверх усіх протоколів канального рівня, таких як Ethernet, SDLC (Synchronous Data Link Control), HDLC (High-Level Data Link Control), ATM, Frame Relay тощо.

IPsec забезпечує такі основні функції:

— Конфіденційність – завдяки застосуванню алгоритмів шифрування, що унеможливлюють прочитання даних третіми сторонами.

— Цілісність – IPsec гарантує, що дані надходять до пункту призначення без змін, завдяки використанню алгоритмів хешування (MD5, SHA тощо).

— Автентифікація – IPsec використовує протокол IKE з метою автентифікації користувачів та пристроїв, які встановлюють зв’язок. IKE підтримує кілька типів автентифікації, включаючи:

ім’я користувача та пароль;

одноразовий пароль (OTP);

біометричні дані;

наперед визначені спільні ключі (pre-shared keys);

цифрові сертифікати.

- Секретний обмін ключами – IPsec використовує алгоритми Діффі–Геллмана (DH) для безпечного обміну публічними ключами в незахищеному каналі.

Переваги використання VPN:

Застосування VPN має низку важливих переваг:

— Економічність (збереження коштів) – досягається шляхом уникнення необхідності використання дорогих виділених ліній та модемів. Завдяки появі відносно недорогих широкосмугових технологій, які забезпечують високу пропускну здатність, організація може використовувати VPN для зниження вартості зв’язку та підвищення пропускної спроможності.

— Секретність – забезпечується захистом від несанкціонованого доступу до даних завдяки використанню протоколів шифрування та автентифікації.

— Масштабованість – є високою, оскільки VPN дозволяють використовувати вже наявну інфраструктуру Інтернет. Це дає змогу легко додавати нових користувачів та віддалені майданчики, фактично без суттєвої зміни структури мережі.

— Сумісність із широкосмуговими технологіями – VPN дають змогу мобільним і надомним працівникам отримати широкосмуговий, високошвидкісний доступ до корпоративних мереж підприємств, забезпечуючи при цьому високу гнучкість та ефективність зв’язку.

У найпростішому прикладі VPN можна розглядати як логічне з’єднання двох точок через публічну мережу. Таке логічне з’єднання може працювати або на канальному (2-му), або на мережевому (3-му) рівні моделі ISO/OSI. Прикладами VPN, що використовують 3-й рівень, є GRE, IPsec (з’єднання типу point-to-point) та MPLS (з’єднання типу any-to-any).

Виділяють два базові типи VPN:

1. Між двома пунктами (Site-to-site) – статичні (стабільні) тунелі між двома фіксованими сайтами або філіями. Прикладами site-to-site VPN є MPLS, GRE, ATM, Frame Relay.

2. VPN дистанційного (віддаленого) доступу (Remote-access) – забезпечують можливість співробітнику встановити захищений зв’язок із корпоративною мережею з дому або іншого (наперед невідомого) місця, використовуючи публічну мережу.

У межах цієї лабораторної роботи в середовищі Cisco Packet Tracer буде практично реалізовано та досліджено:

- site-to-site GRE VPN;

- site-to-site IPsec VPN.

Приклад практичної реалізації VPN у Cisco Packet Tracer:

Нехай маємо комп'ютерну мережу, зображену на рис. 1. Моделі маршрутизаторів – Cisco 2911 (обрані для забезпечення можливості активації ліцензії пакета технологій безпеки – Security).

Необхідно виконати:

1. Налаштувати site-to-site GRE VPN. IP-адреси тунелю мають бути:

— для Rt0: 192.168.1.1/30,

— для Rt3: 192.168.1.2/30.

2. Налаштувати site-to-site IPsec VPN. Параметри фази I ISAKMP (IKE Phase I):

— метод розповсюдження ключів – ISAKMP;

— алгоритм шифрування – 3DES;

— алгоритм хешування – SHA;

— метод автентифікації – pre-share;

— обмін ключами – група DH2;

— час життя IKE SA – 43200 с;

— ключ ISAKMP – my_password1.

Параметри фази II ISAKMP (IKE Phase II / IPSec SA):

— назва набору перетворень – my_set1;

— назва криптографічної карти (crypto map) – my_cryptomap;

— спосіб встановлення SA – ipsec-isakmp.

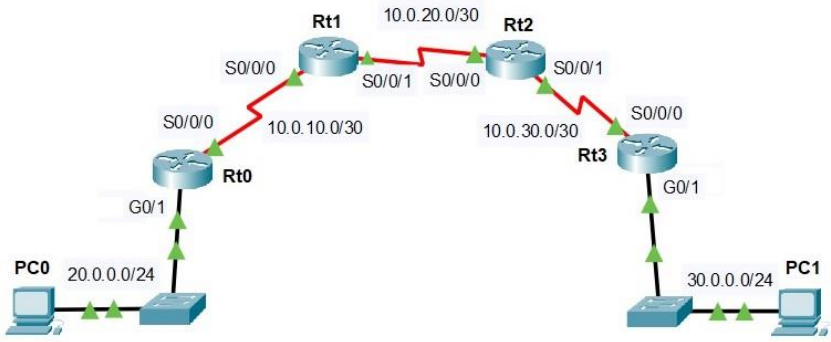


Рисунок 1 – Структура мережі для настроювання site-to-site VPN

Спочатку налаштуємо на маршрутизаторах Rt0 – Rt3 порти згідно з умовою.

```
Rt0(config)#interface Serial 0/0/0
Rt0(config-if)#ip address 10.0.10.1 255.255.255.252
Rt0(config-if)#no shutdown

Rt0(config-if)#interface GigabitEthernet 0/1
Rt0(config-if)#ip address 20.0.0.1 255.255.255.0
Rt0(config-if)#no shutdown

Rt1(config-if)#interface Serial 0/0/0
Rt1(config-if)#ip address 10.0.10.2 255.255.255.252
Rt1(config-if)#clock rate 64000
Rt1(config-if)#no shutdown

Rt1(config-if)#interface Serial 0/0/1
Rt1(config-if)#ip address 10.0.20.1 255.255.255.252
Rt1(config-if)#clock rate 64000
Rt1(config-if)#no shutdown

Rt2(config-if)#interface Serial 0/0/0
Rt2(config-if)#ip address 10.0.20.2 255.255.255.252
Rt2(config-if)#no shutdown

Rt2(config-if)#interface Serial 0/0/1
Rt2(config-if)#ip address 10.0.30.1 255.255.255.252
Rt2(config-if)#clock rate 64000
Rt2(config-if)#no shutdown

Rt3(config-if)#interface Serial 0/0/1
Rt3(config-if)#ip address 10.0.30.2 255.255.255.252
Rt3(config-if)#no shutdown
```

```
Rt3(config-if)#interface GigabitEthernet 0/1
Rt3(config-if)#ip address 30.0.0.1 255.255.255.0
Rt3(config-if)#no shutdown
```

Налаштуємо на маршрутизаторах Rt0 – Rt3 статичну маршрутизацію:

```
Rt0(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt0(config)#ip route 30.0.0.0 255.255.255.0
192.168.1.2

Rt1(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/1
Rt1(config)#ip route 20.0.0.0 255.255.255.0 10.0.10.1

Rt2(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt2(config)#ip route 30.0.0.0 255.255.255.0 10.0.30.2

Rt3(config)#ip route 0.0.0.0 0.0.0.0 Serial 0/0/0
Rt3(config)#ip route 20.0.0.0 255.255.255.0
192.168.1.1
```

Перевіримо зв’язок між кінцевими вузлами PC0 та PC1 шляхом здійснення трасування з PC0:

```
C:\>tracert 30.0.0.2

Tracing route to 30.0.0.2 over a maximum of 30 hops:
  1   0 ms   0 ms   0 ms   20.0.0.1
  2   *      0 ms   0 ms   10.0.10.2
  3   *      3 ms  11 ms   10.0.20.2
  4   *     12 ms  15 ms   10.0.30.2
  5   *     14 ms  12 ms   30.0.0.2
```

Налаштування site-to-site GRE VPN:

Налаштуємо тунель між маршрутизаторами Rt0 та Rt3. IP-адреса тунельного інтерфейсу на Rt0 має бути 192.168.1.1, а на Rt3 – 192.168.1.2.

```
Rt0(config)#interface tunnel 7
```

```
Rt0(config-if)#ip address 192.168.1.1 255.255.255.252
Rt0(config-if)#tunnel source Serial 0/0/0
Rt0(config-if)#tunnel destination 10.0.30.2
Rt0(config-if)#tunnel mode gre ip

Rt3(config)#interface tunnel 7
Rt3(config-if)#ip address 192.168.1.2 255.255.255.252
Rt3(config-if)#tunnel source Serial 0/0/0
Rt3(config-if)#tunnel destination 10.0.10.1
Rt3(config-if)#tunnel mode gre ip
```

Після налаштування тунелю результат аналогічного трасування проходитиме вже через GRE-тунель, минаючи маршрутизатори Rt1 та Rt2:

```
C:\>tracert 30.0.0.2

Tracing route to 30.0.0.2 over a maximum of 30 hops:
  1    0 ms    0 ms    0 ms   20.0.0.1
  2   12 ms   11 ms    0 ms   192.168.1.2
  3   12 ms   11 ms    0 ms   30.0.0.2
```

Отже, GRE-тунель функціонує так, як і передбачалося.

Налаштування site-to-site IPsec VPN

Процес створення IPSec-тунелю складається з двох фаз.

Фаза I – ISAKMP (Internet Security Association and Key Management Protocol)

На першому етапі два кінцевих маршрутизатори аутентифікують один одного та домовляються, які алгоритми шифрування будуть використовуватися для майбутнього IPSec-тунелю, а також генерують спільний секретний ключ. На цьому етапі, з метою запобігання перехопленню ключів, використовується алгоритм Діффі–Геллмана в рамках протоколу Internet Key Exchange (IKE), який дозволяє обмінюватися секретними ключами незахищеним каналом.

Коли секретний ключ сформовано, встановлюється захищений ISAKMP-тунель, і подальший обмін службовою інформацією відбувається вже в захищеному режимі.

Під час фази I пристрої мають домовитися щодо таких параметрів безпеки:

— алгоритм шифрування;

— метод автентифікації;

— спосіб обміну секретними ключами;

— термін життя сесії (Security Association, SA).

Цей набір параметрів визначає політику ISAKMP (у режим редагування якої можна перейти з глобального режиму конфігурації командою:

```
crypto isakmp policy <номер>
```

Можна налаштувати кілька політик ISAKMP, призначивши кожній свій пріоритет (номер). Чим менший номер, тим вищий пріоритет. Коли пристрої починають узгодження, вони послідовно перебирають політики, починаючи з найвищого пріоритету. Як тільки буде знайдено політику з однаковими параметрами на обох кінцях, узгодження завершується й створюється ISAKMP-тунель (перевірити наявність ISAKMP-тунелю можна командою `show crypto isakmp sa`).

Важливо підкреслити, що у фазі I ще не передаються користувацькі (корисні) дані, а лише службова інформація для побудови захищеного каналу.

Фаза II – встановлення IPSec-тунелю

На другій фазі учасники, які вже довіряють один одному (після успішного завершення фази I), домовляються, як будувати основний IPSec-тунель, через який передаватимуться користувацькі дані.

З метою безпеки маршрутизатори повторно узгоджують, які саме протоколи шифрування й алгоритми хешування будуть використовуватися між ними. Вони по черзі пропонують один одному варіанти, зазначені в команді:

```
crypto ipsec transform-set ...
```

Якщо обидві сторони знаходять сумісну комбінацію, встановлюється основний IPSec-тунель.

У підсумку формується два різні тунелі:

— ISAKMP-тунель (фаза I) – керує обміном службовою інформацією та оновленням параметрів безпеки;

— IPSec-тунель (фаза II) – переносить зашифровані користувацькі дані.

Кожен тунель має власний час життя (lifetime). Якщо потрібно продовжити сеанс зв'язку, ISAKMP-тунель оновить таймер та ключі безпеки. Тобто ISAKMP-тунель використовується для поновлення SA основного IPSec-тунелю. SA (Security Association) – це набір параметрів захищеного з'єднання (алгоритми, ключі, час життя тощо).

Після виконання зазначених процедур учасники отримують зашифрований тунель з узгодженими параметрами, через який надсилаються потоки даних, що підлягають шифруванню, тобто дані, які підпадають під список керування доступом, зазначений у crypto map.

Надалі, відповідно до значення `lifetime`, заданого в конфігурації, ключі шифрування для основного тунелю будуть періодично оновлюватися: учасники знову зв'язуються по ISAKMP-тунелю, проходять узгодження фази II та встановлюють новий набір параметрів для IPSec SA.

Загальні кроки конфігурування site-to-site IPsec VPN:

Щоб налаштувати site-to-site IPsec VPN, потрібно виконати такі кроки:

1. Визначити «цікавий» трафік на маршрутизаторах, які є кінцевими точками IPsec VPN-тунелю. Для цього на маршрутизаторах потрібно налаштувати ACL, що дозволяє трафік, який має шифруватися. Увесь інший трафік, що передається з цих локальних мереж, не шифрується.

2. Налаштувати параметри фази I ISAKMP на маршрутизаторах, що є кінцевими точками IPsec VPN. Необхідно вказати:

— метод розповсюдження ключів;

— алгоритми шифрування та хешування;

— метод автентифікації;

— метод обміну ключами;

— час життя IKE SA;

— ключ ISAKMP (pre-shared key).

3. Налаштувати параметри фази II ISAKMP (IPSec) на маршрутизаторі Rt0. Потрібно:

— створити набір перетворень (transform-set), де вказати комбінації протоколів захисту (ESP/AH) та криптоалгоритмів;

— створити криптографічну карту (crypto map), яка пов'язує всі параметри фази II;

— вказати IP-адресу peer (відповідного порта маршрутизатора на протилежному кінці тунелю);

— зв'язати створений на кроці 1 ACL із записом crypto map (щоб визначити «цікавий» трафік).

4. Налаштувати криптографічну карту для вихідного інтерфейсу. Потрібно прив'язати створену crypto map (наприклад, VPN-MAP / my_cryptomap) до вихідного інтерфейсу маршрутизатора, що виходить у тунель.

Зверніть увагу, що для виконання цього завдання має бути активована ліцензія пакета технологій безпеки (Security) на маршрутизаторах Rt0 та Rt3. Перевіримо це командою:

```
Rt0#show version

Technology      Technology-package      Current      Type
Technology-package Next reboot
ipbase          ipbasek9                None         Permanent
None
security        securityk9              None         Permanent
None
* * *
(подальше виведення не показано)
```

Як бачимо, ліцензію securityk9 не активовано. Активуємо її:

```
Rt0(config)#license boot module c2900 technology-
package securityk9
Rt0#reload
```

```
Rt0#show version

Technology    Technology-package    Current       Type
Technology-package Next reboot
security        securityk9                  Evaluation
securityk9
* * *
(подальше виведення не показано)
```

Аналогічно виконаємо активацію на маршрутизаторі Rt3:

```
Rt3(config)#license boot module c2900 technology-
package securityk9
Rt3#reload
```

Крок 1. Визначення «цікавого» трафіка

Визначимо «цікавий» трафік на маршрутизаторі Rt0. Для цього створимо ACL, який дозволяє трафік з локальної мережі за маршрутизатором Rt0 до локальної мережі за маршрутизатором Rt3. Саме цей трафік активуватиме VPN IPsec. Увесь інший трафік, що передається з цих локальних мереж, шифруватися не буде.

```
Rt0(config)#access-list  111  permit  ip  20.0.0.0
0.0.0.255 30.0.0.0 0.0.0.255
```

Крок 2. Налаштування параметрів фази I ISAKMP на Rt0

Налаштуємо параметри фази I ISAKMP на маршрутизаторі Rt0, враховуючи, що:

- метод розповсюдження ключів – ISAKMP;
- алгоритм шифрування – 3DES;
- алгоритм хешування – SHA;
- метод автентифікації – pre-share;
- група DH – 2;
- час життя IKE SA – 43200 с;
- ключ ISAKMP – my_password1.

```
Rt0(config)#crypto isakmp policy 22
```

Створюємо IKE-політику, у якій далі зазначимо бажані алгоритми та параметри для захищеного каналу, який буде запропонований партнеру. Цей канал захищає частину обмінів фази I та всі обміни фази II IKE. Номер політики (тут 22) має локальне значення й не пов'язаний із номерами політик на інших маршрутизаторах. На кожному маршрутизаторі можна створити кілька політик (номери від 0 до 10000). Чим менший номер – тим вищий пріоритет.

```
Rt0(config-isakmp)#authentication pre-share
```

Вказуємо, що автентифікація здійснюваним наперед визначеними ключами (pre-shared keys).

```
Rt0(config-isakmp)#encryption 3des
```

Обираємо алгоритм шифрування 3DES для забезпечення конфіденційності (також можливі AES, DES).

```
Rt0(config-isakmp)#group 2
```

Вибираємо групу DH2 для алгоритму обміну публічними ключами (альтернативи: DH1, DH5).

```
Rt0(config-isakmp)#hash sha
```

Визначаємо алгоритм хешування SHA для забезпечення цілісності (як альтернатива – MD5).

```
Rt0(config-isakmp)#lifetime 43200
Rt0(config-isakmp)#exit

Rt0(config)#crypto isakmp key my_password1 address
10.0.30.2
```

Оскільки для політики ISAKMP вказано `authentication pre-share`, потрібно налаштувати спільний ключ `my_password1`, який має бути однаковим на обох кінцях тунелю. Також задаємо IP-адресу peer – 10.0.30.2 (інтерфейс маршрутизатора Rt3).

Крок 3. Налаштування параметрів фази II ISAKMP (IPSec) на Rt0

Налаштуємо параметри фази II для IPsec, передбачаючи, що:

— назва набору перетворень – my_set1;

— назва криптографічної карти – my_cryptomap;

— установка SA – ipsec-isakmp.

```
Rt0(config)#crypto ipsec transform-set my_set1 esp-3des esp-sha-hmac
```

Формуємо набір перетворень, тобто комбінацію протоколів IPsec (ESP) і криптоалгоритмів (3DES, SHA-HMAC). Transform-set задає:

— які протоколи IPsec використовуються: ESP і/або AH;

— які алгоритми шифрування й хешування до них застосовуються.

Існує низка допустимих комбінацій перетворень, зокрема:

— AH Transform – ah-md5-hmac, ah-sha-hmac;

— ESP Authentication Transform – esp-md5-hmac, esp-sha-hmac;

— ESP Encryption Transform – esp-des, esp-3des, esp-aes-128, esp-aes-192, esp-aes-256 тощо.

Далі створюємо crypto map:

```
Rt0(config)#crypto map my_cryptomap 33 ipsec-isakmp
```

Створюємо криптографічну карту `my_cryptomap` з номером 33 та переходимо до її налаштування:

```
Rt0(config-crypto-map)#description IPSec VPN connection to Rt3
```

```
Rt0(config-crypto-map)#set peer 10.0.30.2
```

Вказуємо партнера (peer) на іншому кінці тунелю – маршрутизатор Rt3 з адресою 10.0.30.2.

```
Rt0(config-crypto-map)#set transform-set my_set1
```

Задаємо використання раніше створеного набору перетворень my_set1.

```
Rt0(config-crypto-map)#match address 111
```

Пов’язуємо crypto map з ACL № 111. Саме ACL визначатиме, який трафік є «цікавим» та повинен шифруватися й передаватися тунелем.

Крок 4. Прив’язка crypto map до інтерфейсу на Rt0

```
Rt0(config)#interface S0/0/0
Rt0(config-if)#crypto map my_cryptomap
```

Прив’язуємо криптографічну карту до вихідного інтерфейсу, через який трафік виходитиме в сторону peer.

Аналогічні (симетричні) налаштування виконаємо на маршрутизаторі Rt3.

Крок 1 (ACL на Rt3)

```
Rt3(config)#access-list 111 permit ip 30.0.0.0 0.0.0.255 20.0.0.0 0.0.0.255
```

Крок 2 (ISAKMP-політика)

```
Rt3(config)#crypto isakmp policy 44
Rt3(config-isakmp)#authentication pre-share
Rt3(config-isakmp)#encryption 3des
Rt3(config-isakmp)#group 2
Rt3(config-isakmp)#hash sha
Rt3(config-isakmp)#lifetime 43200
Rt3(config)#crypto isakmp key my_password1 address 10.0.10.1
```

Крок 3 (Transform-set і crypto map)

```
Rt3(config)#crypto ipsec transform-set my_set1 esp-3des esp-sha-hmac
Rt3(config)#crypto map my_cryptomap 55 ipsec-isakmp
Rt3(config-crypto-map)#description IPSec VPN connection to Rt0
Rt3(config-crypto-map)#set peer 10.0.10.1
Rt3(config-crypto-map)#set transform-set my_set1
Rt3(config-crypto-map)#match address 111
```

Крок 4 (прив’язка crypto map до інтерфейсу Rt3)

```
Rt3(config)#interface S0/0/0
Rt3(config-if)#crypto map my_cryptomap
```

Перевірка роботи IPSec VPN до появи «цікавого» трафіка

Переглянемо стан IPSec SA до того, як через тунель пройде «цікавий» трафік:

```
Rt0#show crypto ipsec sa
```

```
    interface: Serial0/0/0
    Crypto map tag: mycryptomap, local addr 10.0.10.1

       protected vrf: (none)
       local         ident         (addr/mask/prot/port):
(20.0.0.0/255.255.255.0/0/0)
       remote        ident         (addr/mask/prot/port):
(30.0.0.0/255.255.255.0/0/0)
       current_peer 10.0.30.2 port 500
         PERMIT, flags={origin_is_acl,}
       #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
       #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 0, #pkts compr. failed: 0
       #pkts not decompressed: 0, #pkts decompress failed:
0
       #send errors 0, #recv errors 0

       local  crypto  endpt.:  10.0.10.1,  remote  crypto
endpt.: 10.0.30.2
       path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
       current outbound spi: 0x0(0)
       * * *
       (подальше виведення не показано)
```

8-й та 9-й рядки виведення показують, що кількість інкапсульованих, зашифрованих, декапсульованих і дешифрованих пакетів дорівнює 0. Тобто тунель ще не використовувався.

Тепер надішлемо «цікавий» трафік: достатньо з комп'ютера PC0 пропінгувати PC1 (кілька разів). Після цього знову перевіримо роботу IPSec VPN:

```
    Rt0#show crypto ipsec sa
```

```
    interface: Serial0/0/0
    Crypto map tag: mycryptomap, local addr 10.0.10.1

       protected vrf: (none)
       local         ident         (addr/mask/prot/port):
(20.0.0.0/255.255.255.0/0/0)
       remote        ident         (addr/mask/prot/port):
(30.0.0.0/255.255.255.0/0/0)
       current_peer 10.0.30.2 port 500
         PERMIT, flags={origin_is_acl,}
       #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
       #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 0, #pkts compr. failed: 0
       #pkts not decompressed: 0, #pkts decompress failed:
0
       #send errors 1, #recv errors 0

       local  crypto  endpt.:  10.0.10.1,  remote  crypto
endpt.: 10.0.30.2
       path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
       current outbound spi: 0x894B87AF(2303428527)
       * * *
       (подальше виведення не показано)
```

Як бачимо, кількість інкапсульованих, зашифрованих, декапсульованих і дешифрованих пакетів збільшилася до 7. Отже, IPSec VPN-тунель було успішно використано.

Зверніть увагу, що у випадку проходження через тунель «нецікавого» трафіка (наприклад, якщо до порту G0/0 маршрутизатора Rt0 під'єднати ще один вузол PC2, який належатиме до іншої мережі, відмінної від 20.0.0.0/24, і з PC2 пропінгувати вузол PC1), кількість інкапсульованих, зашифрованих,

декапсульованих і дешифрованих пакетів не зміниться. Це свідчить про те, що для такого трафіка IPSec VPN-тунель не використовується, оскільки він не відповідає умовам ACL і не вважається «цікавим».

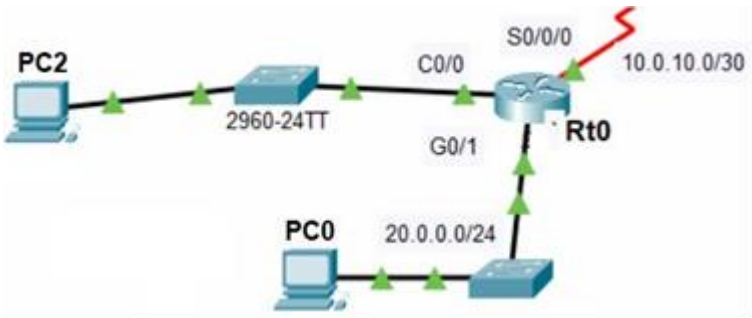


Рисунок 2 – Доповнення до мережі

3.2. Вимоги до результатів роботи та оформлення звіту

Звіт з лабораторної роботи повинен містити:

1. Титульний аркуш. Оформлений за встановленим зразком кафедри (назва ЗВО, кафедри, дисципліни, тема ЛР, ПІБ здобувача, група, ПІБ викладача, рік, місто).

2. Тему, мету та завдання лабораторної роботи

— повна назва теми;

— чітко сформульована мета (що саме здобувач має опанувати);

— за потреби – перелік конкретних завдань (налаштування GRE-тунелю, налаштування IPsec-тунелю, перевірка шифрування та цілісності трафіка тощо).

3. Короткі теоретичні відомості. Обсяг 1–2 сторінки, де стисло розглядаються:

— поняття та призначення VPN (Virtual Private Network);

— основні типи VPN (site-to-site, remote-access);

— GRE-тунелювання (призначення, особливості, обмеження);

— IPsec (базові поняття: SA, ESP, AH, IKE/ISAKMP, фаза I і фаза II);

— ACL для визначення «цікавого» трафіка;

— основні параметри безпеки (алгоритми шифрування, хешування, методи автентифікації, групи DH);

— поняття transform-set, crypto map, прив’язка до інтерфейсу.

4. Практичну частину, що включає:

— схему (рисунок) структури мережі для настроювання site-to-site GRE/IPsec VPN;

— результати налаштування GRE-тунелю (фрагменти конфігурацій маршрутизаторів Rt0-Rt3, налаштування tunnel interface, статична маршрутизація);

— результати трасування (tracert) та тестування зв'язку (ping) до і після налаштування GRE-тунелю, з короткими поясненнями;

— фрагменти конфігурацій, що стосуються IPsec (ACL «цікавого» трафіка, crypto isakmp policy, crypto isakmp key, crypto ipsec transform-set, crypto map, прив'язка до інтерфейсу);

— результати перевірки роботи IPsec VPN за допомогою команд:

– show crypto isakmp sa;

– show crypto ipsec sa (до передавання «цікавого» трафіка і після, з аналізом лічильників пакетів);

— (за наявності варіантів) – коротке формулювання індивідуального завдання (варіант топології, параметри тунелів, обрані алгоритми тощо).

5. Висновки, які повинні містити:

— узагальнення щодо можливостей VPN для захисту мережного трафіка;

— порівняльний аналіз GRE та IPsec (переваги, недоліки, сфери застосування);

— оцінку ефективності використання GRE+IPsec для побудови захищених каналів між віддаленими мережами;

— опис отриманих практичних навичок (налаштування тунелів, політик безпеки, аналіз SA, робота з ACL);

— рекомендації щодо використання VPN-технологій для підвищення рівня безпеки корпоративних і відомчих мереж.

6. Список використаних джерел, оформлений відповідно до вимог ДСТУ 8302:2015 (книги, навчальні посібники, стандарти, електронні ресурси).

4. Підбиття підсумків заняття

Обговорення результатів налаштування та тестування site-to-site GRE VPN і site-to-site IPsec VPN; аналіз правильності побудови тунелів (топологія, адресація, статична маршрутизація, ACL «цікавого» трафіка); аналіз коректності параметрів фази I та фази II IPsec (алгоритми шифрування, хешування, методи автентифікації, групи DH, час життя SA); розбір типових помилок під час налаштування VPN (розбіжність параметрів політик, неправильні ACL, відсутність призначення crypto map на інтерфейс тощо); узагальнення результатів дослідження процесу встановлення та функціонування IPsec-тунелю (інтерпретація виводу show crypto isakmp sa, show crypto ipsec sa); оцінювання повноти та якості виконаного звіту (наявність усіх обов'язкових розділів, скріншотів/фрагментів конфігурацій, коректність висновків); формулювання висновків щодо значення VPN-технологій для забезпечення конфіденційності, цілісності та доступності інформації в сучасних комп'ютерних мережах.

5. Список рекомендованої літератури

Основна:

1. Таненбаум Е., Веселінг Д. Комп'ютерні мережі : підручник / пер. з англ. 5-те вид. – Київ : Діалектика, 2016. 960 с.

2. Столінгс В. Мережна безпека. Принципи та практика : підручник / пер. з англ. Київ : Вільямс, 2018. 864 с.

3. Лозінова Г. М. Комп'ютерні мережі : навч. посібник. Київ : Кондор, 2003. 352 с.

4. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

5. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.

Додаткова:

1. Кулаков Ю. О. Комп'ютерні мережі : навч. посібник. Київ : КПІ ім. Ігоря Сікорського, 2022. 247 с.

2. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Boston : Pearson, 2017. – 752 p.

3. Odom W. CCNA Security Official Exam Certification Guide. – Indianapolis : Cisco Press, 2010. – 720 p.

4. Sarkar D. Cisco IPsec VPN Solutions. – Indianapolis : Cisco Press, 2005. – 512 p.

5. Wheeler D. IPSec VPN Design. – Indianapolis: Cisco Press, 2012. – 432 p.

Інформаційні ресурси:

1. Віртуальний університет ЛДУБЖД : електронне навчальне середовище. URL: https://virt.ldubgd.edu.ua

2. Cisco Networking Academy : офіційний освітній портал Cisco. URL: https://www.netacad.com

3. Cisco Systems : офіційна документація Cisco з налаштування VPN та IPsec. URL: https://www.cisco.com

4. RFC 4301. Security Architecture for the Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc4301

5. RFC 4302. IP Authentication Header (AH). URL: https://www.rfc-editor.org/rfc/rfc4302

6. RFC 4303. IP Encapsulating Security Payload (ESP). URL: https://www.rfc-editor.org/rfc/rfc4303

7. Wireshark Foundation. Офіційний сайт Wireshark. URL: https://www.wireshark.org

8. Cisco Packet Tracer. Інструменти та документація Cisco для симуляції мереж. URL: https://www.netacad.com/courses/packet-tracer

СПИСОК ЛІТЕРАТУРИ:

1. Буров Є. В. Комп’ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.
2. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах : навч. посіб. Київ, 2013. 435 с.
3. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
4. Жуков О. М. Комп’ютерні мережі : навч. посіб. Київ : НАУ-друк, 2009. 392 с.
5. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.
6. Лозінова Г. М. Комп’ютерні мережі : навч. посіб. Київ : Кондор, 2003. 352 с.
7. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. Харків : ХНЕУ, 2013. 476 с.
8. Полотай О., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи // Захист інформації в інформаційно-комунікаційних системах : зб. тез III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів (Львів, 28 листоп. 2019 р.). Львів : ЛДУБЖД, 2019. С. 76-78.
9. Саченко А. А., Кулаков Ю. О., Кочан В. В. Комп’ютерні мережі : навч. посіб. Тернопіль : ВПЦ «Економічна думка ТНЕУ», 2016. 476 с.
10. Столінгс В. Мережна безпека. Принципи та практика : підручник / пер. з англ. Київ : Вільямс, 2018. 864 с.
11. Таненбаум Е., Веселінг Д. Комп’ютерні мережі : підручник / пер. з англ. 5-те вид. – Київ : Діалектика, 2016. 960 с.

Додаткова:

1. Гарасимчук О. І., Дудикевич В. Б., Ромака В. А. Комплексні системи санкціонованого доступу : навч. посіб. Львів : Вид-во Львів. політехніки, 2010. 212 с.

2. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023.

3. ДСТУ ISO/IEC 27002:2022. Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою. Київ : ДП «УкрНДНЦ», 2022.

4. Кавун С. В., Смірнов О. А., Столбов В. Ф. Основи інформаційної безпеки : навч. посіб. Кіровоград : КНТУ, 2012. 414 с.

5. Кулаков Ю. О. Комп'ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 247 с.

6. Мельник А. Ф. Захист інформації в комп'ютерних системах і мережах : навч. посіб. Київ : КНУБА, 2018. 268 с.

7. Behl A., Belapure N. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford : Oxford University Press, 2023. – 296 p.

8. Boyle R., Panko R. Corporate Computer Security. – 5th ed. – London : Pearson, 2021. – 720 p.

9. Cheswick W., Bellovin S., Rubin A. Firewalls and Internet Security: Repelling the Wily Hacker. – 2nd ed. – Boston : Addison-Wesley, 2023. – 720 p.

10. ENISA. Next-Generation Firewalls – Security Practices and Use Cases. – Heraklion : ENISA, 2023.

11. Harkins D. IPsec Tutorial // IEEE Communications Surveys & Tutorials. – 2020. – Vol. 22, № 4. – P. 1225–1250.

12. IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. – New York : IEEE Standards Association, 2016.

13. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022. – 45 p.

14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. – Geneva : ISO, 2022. – 118 p.

15. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. – 2nd ed. – Upper Saddle River : Prentice Hall, 2016. – 750 p.

16. Maufer T. IPsec: A Guide to Implementation and Usage. – Upper Saddle River : Prentice Hall, 2001. – 412 p.

17. NIST SP 800-41 Rev.1. Guidelines on Firewalls and Firewall Policy. – Gaithersburg : NIST, 2024.

18. NIST SP 800-115. Technical Guide to Information Security Testing and Assessment. – Gaithersburg : NIST, 2023. – 85 p.

19. NIST SP 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs). – Gaithersburg : NIST, 2012.

20. Northcutt S. Network Intrusion Detection: An Analyst's Handbook. – 4th ed. – Indianapolis : New Riders, 2022. – 612 p.

21. Odom W. CCNA Security Official Exam Certification Guide. – Indianapolis : Cisco Press, 2010. – 720 p.

22. Sarkar D. Cisco IPsec VPN Solutions. – Indianapolis : Cisco Press, 2005. – 512 p.

23. Sheldon T. Encyclopedia of Networking & Telecommunications. – 2nd ed. – New York : McGraw-Hill, 2019. – 960 p.

24. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Boston : Pearson, 2017. – 752 p.

25. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Upper Saddle River : Pearson, 2022. – 512 p.

26. Tanenbaum A. S., Wetherall D. J. Computer Networks. – 6th ed. – Boston : Pearson, 2021. – 960 p.

Інформаційні ресурси:

1. Віртуальний університет ЛДУБЖД : електронне навчальне середовище [Електронний ресурс]. URL: https://virt.ldubgd.edu.ua

2. Cisco IOS Zone-Based Policy Firewall Configuration Guide [Електронний ресурс]. URL: https://www.cisco.com

3. Cisco Networking Academy. Офіційний сайт мережевої академії Cisco [Електронний ресурс]. URL: https://www.netacad.com

4. Cisco Packet Tracer. Довідкові матеріали та приклади лабораторних робіт [Електронний ресурс]. URL: https://skillsforall.com; https://www.netacad.com

5. Internet Engineering Task Force (IETF). IPsec Documentation Library [Електронний ресурс]. URL: https://www.ietf.org

6. Microsoft Learn. IPsec configuration and management [Електронний ресурс]. URL: https://learn.microsoft.com

7. NIST Computer Security Resource Center (CSRC) [Електронний ресурс]. URL: https://csrc.nist.gov

8. NIST Cybersecurity Framework [Електронний ресурс]. URL: https://www.nist.gov/cyberframework

9. RFC 791 – Internet Protocol [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc791

10. RFC 1918 – Address Allocation for Private Internets [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc1918

11. RFC 4301 – Security Architecture for the Internet Protocol [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc4301

12. RFC 4302 – IP Authentication Header (AH) [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc4302

13. RFC 4303 – IP Encapsulating Security Payload (ESP) [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc4303

14. RFC 6071 – IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap [Електронний ресурс]. URL: https://www.rfc-editor.org/rfc/rfc6071

15. Wireshark Foundation. Офіційний сайт Wireshark [Електронний ресурс]. URL: https://www.wireshark.org

НАВЧАЛЬНЕ ВИДАННЯ

Балацька Валерія Сергіївна
Полотай Орест Іванович
Федінець Наталія Іванівна
Ткаченко Артур Мар'янович

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Навчальний посібник

(Лабораторний практикум)

Літературний редактор **Галина Падик**

Технічний редактор
та ком'ютерна верстка **Маріанна Климус**
Валерія Балацька
Друк **Назарій Петролюк**

Підписано до друку 19.12.2025 р.
Формат 60x84/16. Гарнітура Times New Roman.
Друк цифровий. Папір офсетний.
Ум. друк. арк. 16,9

Друк ЛДУБЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
Тел. /факс: (032)233-24-79
E-mail: vnrd@ldubgd.edu.ua
Свідоцтво суб'єкта видавничої справи ДК №7249 від 09.02.2021 р.