Лабораторна робота 8

Тема: Міжмережеве екранування.

Мета: Вивчити призначення, налаштування та використання міжмережевого екранування.

1. Теоретичні відомості

Міжмережевий екран можна визначити як певний засіб захисту інформації. Спеціальне поєднання в ньому апаратного та програмного забезпечення дозволяє здійснювати аналіз та фільтрацію мережевих пакетів, що проходять через нього. Залежно від встановлених правил, міжмережевий екран пропускає або знищує пакети і таким чином дозволяє або забороняє мережеві з'єднання. Встановлюють міжмережевий екран на межі між внутрішньою (захищеною) та зовнішньою (потенційно небезпечною) мережами. Це класичний засіб захисту периметра комп'ютерної мережі, який контролює з'єднання між вузлами цих мереж. Синонімами за визначенням міжмережевого екрану є фаєрвол (від англ. терміну firewall) та брандмауер (німецький термін brandmauer).

Фільтрація пакетів проводиться на підставі правил. Найбільш безпечним для формування правил міжмережевого екрану вважається підхід «заборонено все, що явно не дозволено». У цьому випадку мережевий пакет перевіряється на відповідність дозвільним правилам, а якщо таких не знайдеться, то пакет буде відкинуто. Але в деяких випадках застосовується і зворотний принцип: "дозволено все, що явно не заборонено". Тоді перевірка проводиться на відповідність забороннним правилам, і якщо таких не буде знайдено, пакет буде пропущено.

Фільтрацію можна проводити на різних рівнях еталонної моделі мережевої взаємодії OSI. За цією ознакою міжмережеві екрани можна поділити на три класи:

- брандмауер екранного маршрутизатора;
- екранувальний транспорт (шлюз сеансового рівня);
- екранувальний шлюз (шлюз прикладного рівня).

Брандмауер екранного маршрутизатора також відомий як брандмауер мережевого рівня або брандмауер з фільтруванням пакетів. Пакетна фільтрація є однією із давно відомих та розповсюджених технологій управління доступом до мережі, тому, зазвичай, брандмауери мають таку функцію. Брандмауер з фільтрацією пакетів це або маршрутизатор, або виконувана на сервері програма, які відповідно до своєї конфігурації фільтрують вхідні та вихідні пакети. Брандмауер пропускає або відкидає пакети у відповідності до інформації, яка є у IP-заголовках пакетів. Наприклад, пакети можуть пропускатись або відхилятись на основі інформації, що дозволяє асоціювати цей пакет із конкретними відправником та отримувачем (повна асоціація), яка складається із наступних елементів:

– адреса відправника;
– адреса отримувача;

– інформація про додаток або протокол;

– номер порту джерела;

– номер порту отримувача.

Усі маршрутизатори (навіть ті, які не налаштовані для фільтрації пакетів), зазвичай перевіряють повну асоціацію пакета, щоб визначити, куди його потрібно направити. Брандмауер із фільтрацією пакетів перед відправленням пакета одержувачу порівнює його повну асоціацію з таблицею правил, відповідно до яких він повинен пропустити або відбракувати цей пакет. Якщо брандмауер отримав пакет, який не відповідає жодному табличному правилу, він застосовує правило, задане за замовчуванням, яке також має бути чітко визначене в таблиці брандмауера. З міркувань безпеки це правило зазвичай вказує на необхідність відбракування всіх пакетів, що не задовольняють жодному з інших правил.

Можна задати правила фільтрації пакетів, які «вказуватимуть» брандмауеру, які пакети повинні бути пропущені, а які відбраковані. Наприклад, можна визначити правила таким чином, щоб брандмауер відбраковував пакети, що надходять від зовнішніх серверів, IP-адреси яких вказані в таблиці. Можна також задати правило, відповідно до якого буде дозволено пропускати лише вхідні повідомлення електронної пошти, адресовані поштовому серверу, або правило блокування всіх поштових повідомлень, що надходять від зовнішнього хоста, яке розсилало спам.

Також можна налаштувати брандмауер для фільтрації пакетів на основі номерів портів, що задаються в заголовках пакетів TCP та UDP (User Datagram Protocol). У цьому випадку можна буде пропускати окремі види пакетів (наприклад, Telnet або FTP), лише якщо вони надсилаються до певних серверів (відповідно до Telnet або FTP). Однак успішне виконання подібного правила залежить від того, які угоди прийняті в мережі, що функціонує на основі TCP/IP: для роботи додатків TCP/IP сервери та клієнти зазвичай використовують конкретні порти (які часто називають відомими, тобто наперед визначеними), однак це не є обов'язковою умовою.

Наприклад, програма Telnet на серверах мережі з TCP/IP зазвичай працює через порт 23. Щоб дозволити сеанси Telnet тільки з певним сервером, необхідно задати правила, одне з яких "змусить" брандмауер пропускати всі пакети, що запитують порт 23 за адресою 123.45.6.7 (приклад IP-адреси сервера Telnet), а інше – відбраковувати вхідні пакети, які вимагають цей порт за іншими адресами. Зазвичай, реальні правила є складнішими і передбачають виконання декількох умов одночасно.

Переваги брандмауерів з фільтруванням пакетів:

– відносна невисока вартість;

– невелика затримка під час проходження пакетів.

Недоліки брандмауерів із фільтрацією пакетів:

– локальна мережа маршрутизується із Інтернет;

– правила фільтрації складні в описанні, тому потребують певні знання технологій TCP та UDP;

– відсутня автентифікація на рівні користувача;

– аутентифікацію з використанням IP-адреси можна обійти за допомогою IP-спуфінгу, коли атакуюча система видає себе за іншу через підміну IP-адреси.

Шлюз сеансового рівня стежить за підтвердженням зв'язку (квитування) між авторизованим клієнтом і зовнішнім хостом (і навпаки), визначаючи, чи сеанс зв'язку, що запитується, допустимим. При фільтрації пакетів шлюз сеансового рівня полягає в інформації, що у заголовках IP-пакетів сеансового рівня протоколу TCP, тобто. функціонує на два рівні вище, ніж брандмауер із фільтрацією пакетів.

Щоб визначити, чи є запит на сеанс зв'язку допустимим, шлюз сеансового рівня виконує приблизно таку процедуру. Коли авторизований клієнт запитує деяку послугу, шлюз приймає цей запит, перевіряючи, чи задовольняє клієнт базовим критеріям фільтрації (наприклад, чи DNS-сервер може визначити IP-адресу клієнта та асоційоване з ним ім'я). Потім, діючи від імені клієнта, шлюз встановлює з'єднання із зовнішнім хостом і слідкує за виконанням процедури квитування зв'язку протоколу TCP.

Ця процедура складається з обміну TCP-пакетами, які позначаються прапорами SYN (синхронізувати) та ACK (підтвердити). Перший пакет сеансу TCP, позначений прапором SYN і містить довільне число, наприклад 1000, є запитом клієнта на відкриття сеансу. Зовнішній хост, який одержав цей пакет, посилає у відповідь пакет, позначений прапором ACK і містить число, на одиницю більше, ніж у прийнятому пакеті (у нашому випадку 1001 – razgovorodele.ru), підтверджуючи таким чином прийом пакета SYN від клієнта. Після цього здійснюється зворотна процедура: хост посилає клієнту пакет SYN з вихідним числом (наприклад, 2000), а клієнт підтверджує отримання передачею пакета ACK, що містить число 2001.

У цьому процес квитування зв'язку завершується. Шлюз сеансового рівня "вважає" запитаний сеанс допустимим тільки в тому випадку, якщо при виконанні процедури квитування зв'язку прапори SYN і ACK, а також числа, що містяться в TCP-пакетах, логічно пов'язані між собою. Після того як шлюз «визначив», що довірений клієнт та зовнішній шлюз є авторизованими учасниками сеансу TCP, та перевірив допустимість цього сеансу, він встановлює з'єднання.

Починаючи з цього моменту, шлюз просто копіює і перенаправляє пакети туди і назад, не проводячи жодної фільтрації. Він підтримує таблицю встановлених з'єднань, пропускаючи дані, які стосуються одному з сеансів зв'язку, які зафіксовані у цій таблиці. Коли сеанс завершується, шлюз видаляє відповідний елемент з таблиці та розриває ланцюг, що використовується в даному сеансі. Для копіювання та перенаправлення пакетів у шлюзах сеансового рівня використовуються спеціальні програми, які іноді називають канальними посередниками (pipe proxies), оскільки вони встановлюють між двома мережами віртуальний ланцюг, або канал, а потім дозволяють пакетам (що генеруються додатками TCP/IP) проходити по цьому каналу.

Шлюз сеансового рівня виконує ще одну важливу функцію захисту: він використовується як сервер-посередник (proxy server). І хоча цей термін

передбачає наявність сервера, на якому працюють програми-посередники (що справедливо для шлюзу сеансового рівня), у цьому випадку він означає дещо інше. Сервером-посередником може бути брандмауер, який використовує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP-адрес в одну «надійну» IP-адресу. Ця адреса асоціюється з брандмауером, з якого передаються всі вихідні пакети.

В результаті в мережі зі шлюзом сеансового рівня всі вихідні пакети виявляються відправленими з цього шлюзу, що виключає прямий контакт між внутрішньою (авторизованою) мережею і потенційно небезпечною зовнішньою мережею (у нашому випадку мережа Інтернет – razgovorodele.ru). IP-адреса шлюзу сеансового рівня стає єдиною активною IP-адресою, яка потрапляє до зовнішньої мережі. Таким чином, шлюз сеансового рівня та інші сервери-посередники захищають внутрішні мережі від нападів типу spoofing (імітація адрес або підміна адрес).

Шлюзи сеансового рівня немає «вроджених» вразливих місць, проте після встановлення зв'язку такі шлюзи фільтрують пакети лише з сеансовому рівні, тобто. не можуть перевіряти вміст пакетів, що передаються між внутрішньою та зовнішньою мережею на рівні прикладних програм, тобто ця передача здійснюється «наосліп». Таким чином, хакер, що знаходиться в зовнішній мережі, може "протягнути" свої "шкідливі" пакети через шлюз і звернеться безпосередньо до внутрішнього Web-серверу, який сам по собі може не забезпечувати функції брандмауера. Іншими словами, якщо процедура квитування зв'язку успішно завершена, шлюз сеансового рівня встановить з'єднання і буде тупо копіювати і перенаправляти всі наступні пакети незалежно від їх вмісту.

Щоб фільтрувати пакети, що генеруються певними мережними службами відповідно до їх вмісту, потрібен шлюз прикладного рівня.

Так само як і шлюз сеансового рівня, шлюз прикладного рівня перехоплює вхідні та вихідні пакети, використовує програми-посередники, які копіюють та перенаправляють інформацію через шлюз, а також функціонує як сервер-посередник, виключаючи прямі з'єднання між довіреним сервером або клієнтом та зовнішнім хостом . Однак посередники, що використовуються шлюзом прикладного рівня, мають важливі відмінності від канальних посередників шлюзів сеансового рівня: по-перше, вони пов'язані з програмами, а по-друге, можуть фільтрувати пакети на прикладному рівні. На відміну від канальних посередників, посередники прикладного рівня пропускають лише пакети, які їм доручено обслуговувати. Наприклад, програма-посередник служби Telnet може копіювати, перенаправляти та фільтрувати лише графік, який генерується цією службою.

Якщо мережа працює лише шлюз прикладного рівня, то вхідні та вихідні пакети можуть передаватися лише тих служб, котрим є відповідні посередники. Так, якщо шлюз прикладного рівня використовує лише програми-посередники FTP і Telnet, він пропускатиме пакети цих служб, блокуючи у своїй пакети всіх інших служб. На відміну від шлюзів сеансового рівня, які копіюють і «сліпо»

перенаправляють всі пакети, що надходять, посередники прикладного рівня перевіряють вміст кожного пакета, що проходить через шлюз.

Ці посередники можуть фільтрувати окремі види команд або інформації протоколах прикладного рівня, які їм доручено. Утиліти цих шлюзів дозволяють фільтрувати певні команди, що використовуються цими службами (FTP, Telnet, HTTP тощо – razgovorodele.ru). Наприклад, можна налаштувати шлюз таким чином, щоб він запобігав використанню клієнтами команди FTP Put, яка дає можливість користувачеві, підключеному до FTP-серверу, записувати на нього інформацію. Багато мережних адміністраторів воліють заборонити використання цієї команди, щоб зменшити ризик випадкового пошкодження інформації, що зберігається на FTP-сервері, і ймовірність заповнення його гігабайтами хакерських даних, що пересилаються на сервер для заповнення його дискової пам'яті і блокування роботи.

На додаток до фільтрації пакетів багато шлюз прикладного рівня реєструють всі виконувані сервером дії і, що найважливіше, попереджають мережевого адміністратора про можливі порушення захисту. Наприклад, при спробах проникнення в систему ззовні «BorderWare Firewall Server» компанії «Secure Computing» дозволяє фіксувати адреси відправника та одержувача пакетів, час, у який ці спроби були здійснені, і протокол, що використовується. Продукт Black Hole компанії Milkyway Networks також реєструє всі дії сервера і попереджає адміністратора про можливі порушення, надсилаючи йому повідомлення електронною поштою або на пейджер.

Переваги:

– локальна мережа невидима з Internet;

– захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, знижуючи цим ймовірність злому з використанням дірок у програмному забезпеченні;

– при організації аутентифікації на рівні користувача може бути реалізована система негайного попередження про спробу злому.

Недоліки:

– вища, ніж для пакетних фільтрів вартість;

– продуктивність нижча, ніж для пакетних фільтрів.

Брандмауери експертного рівня поєднують у собі елементи всіх описаних вище категорій. Як і брандмауери з фільтрацією пакетів, вони працюють на мережному рівні, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес та номерів портів. Брандмауери експертного рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи пакети відносяться до відповідного сеансу. І, нарешті, брандмауери експертного рівня беруть він функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета відповідно до політики безпеки, виробленої у конкретній організації. Як і шлюз прикладного рівня, брандмауер експертного рівня може бути налаштований для відбраковування пакетів, що містять певні команди, наприклад команди Put та Get служби FTP.

Однак, на відміну від шлюзів прикладного рівня, при аналізі даних прикладного рівня такий брандмауер не порушує клієнт-серверної моделі взаємодії в мережі.

Шлюз прикладного рівня встановлює два з'єднання: одне – між авторизованим клієнтом та шлюзом, друге – між шлюзом та зовнішнім хостом. Після цього він просто пересилає інформацію між цими двома з'єднаннями. Незважаючи на високий рівень захисту, що забезпечується подібними шлюзами, така схема може позначитись на продуктивності роботи. На противагу цьому брандмауери експертного рівня допускають прямі з'єднання між клієнтами та зовнішніми хостами. Для забезпечення захисту такі брандмауери перехоплюють та аналізують кожен. Замість застосування пов'язаних із додатками програм-посередників, брандмауери експертного рівня використовують спеціальні алгоритми розпізнавання та обробки даних на рівні додатків.

За допомогою цих алгоритмів пакети порівнюються з відомими шаблонами даних, що теоретично має забезпечити більш ефективну фільтрацію пакетів. Оскільки брандмауери експертного рівня допускають пряме з'єднання між авторизованим клієнтом та зовнішнім хостом, деякі стверджують, що брандмауери цієї категорії забезпечують менш високий рівень захисту, ніж шлюзи прикладного рівня. Інші ж дотримуються протилежної думки – razgovorodele.ru. Проте брандмауери експертного рівня забезпечують один із найвищих на сьогоднішній день рівнів захисту корпоративних мереж, і, за твердженням фахівців, обдурити їх дуже не просто. Однак не варто забувати, що навіть ці надійні брандмауери не забезпечують 100% безпеки.

На рис.1 представлено типові схеми підключення міжмережевих екранів (firewall). У першому випадку (рис.1 а) міжмережевий екран встановлюється після маршрутизатору і захищає всю внутрішню мережу. Така схема застосовується, якщо вимоги у сфері захисту від несанкціонованого міжмережевого доступу приблизно однакові для всіх вузлів внутрішньої мережі. Наприклад, "дозволяти з'єднання, що встановлюються з внутрішньої мережі у зовнішню, і припиняти спроби підключення із зовнішньої мережі у внутрішню". Якщо вимоги для різних вузлів різні - наприклад, потрібно розмістити поштовий сервер, до якого можуть підключатися «ззовні», то подібна схема установки міжмережевого екрана не є достатньо безпечною. Наприклад, хакер у результаті реалізації мережевої атаки може отримати контроль над таким поштовим сервером і через нього вже отримає доступ до інших вузлів внутрішньої мережі.

У подібних випадках іноді перед міжмережевим екраном створюється відкритий сегмент мережі підприємства (рис.1, б), а мережевий екран захищає іншу внутрішню мережу. Недолік цієї схеми у тому, що підключення до вузлів відкритого сегмента міжмережевим екраном не контролюється.

Кращим у цьому випадку є використання міжмережевого екрану з трьома мережевими інтерфейсами (рис.1, в). Міжмережевий екран з трьома мережними інтерфейсами конфігурується таким чином, щоб правила доступу у внутрішню мережу були більш суворими, ніж у відкритий сегмент. У той же час, і внутрішня

мережа, і відкритий сегмент будуть контролюватись міжмережевим екраном. Такий відкритий сегмент часто зветься «демілітаризованою зоною» — DMZ.

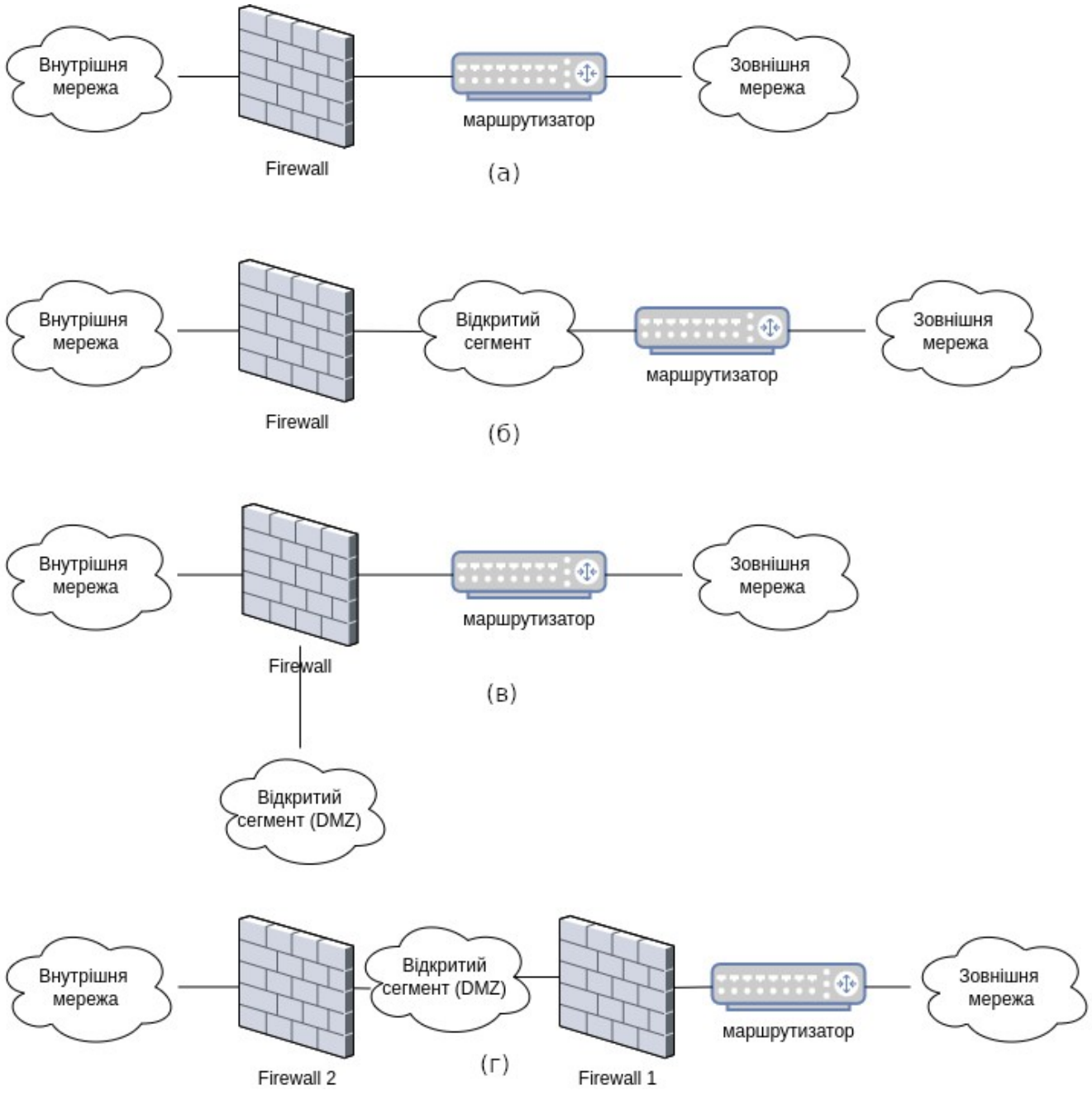


Рис. 1. Типові схеми підключення міжмережевих екранів (firewall):

а) підключення firewall із двома мережевими інтерфейсами; б) підключення firewall з двома мережевими інтерфейсами при виділенні відкритого сегмента внутрішньої мережі; в) підключення firewall з трьома мережевими інтерфейсами; г) підключення двох firewall.

Більш надійною для відкритого сегменту DMZ вважається схема, в якій для її захисту використовується два незалежних міжмережевих екрани (рис.1, г). Другий firewall реалізує набір правил фільтрації, що забезпечує захистом

внутрішню мережу, які більш жорсткі проти правил першого firewall, що контролює доступ до DMZ. Навіть успішна атака на перший firewall не зробить внутрішню мережу беззахисною.

Типовим стало встановлення програмного firewall на персональні комп'ютери або інші комп’ютери, що захищаються. Іноді такий firewall називають "персональним". Подібна схема дозволяє захиститися від загроз, що надходять не тільки із зовнішньої мережі, а й із внутрішньої. Особливо актуальним є застосування персональних firewall при безпосередньому підключенні комп'ютера до потенційно небезпечної мережі. Наприклад, при підключенні домашнього комп'ютера до Інтернету або ноутбуку до загально доступної мережі кафе, вокзалу, транспорту, тощо.

Практична частина

Файрвол у системі linux контролюється програмою iptables (для ipv4) та ip6tables (для ipv6). Для використання утиліти необхідні привілеї суперкористувача (root).

Основними поняттями iptables є:

1. Правило, яке складається з критерію, дії та лічильника. Якщо пакет відповідає критерію, то до нього застосовується дія, і він враховується лічильником. Якщо критерій відсутній, то неявно передбачається критерій "усі пакети". Якщо відсутня дія, то правило працюватиме лише як лічильник. Критерієм є логічний вираз, що аналізує властивості пакета та/або з'єднання і визначає, чи підпадає даний конкретний пакет під дію поточного правила. Дія описує те, що потрібно зробити із пакетом і/або з'єднанням, якщо вони відповідають правилу. Лічильник забезпечує облік кількості пакетів, які потрапили під критерій правила. Він враховує сумарний обсяг таких пакетів у байтах.

2. Ланцюжок — це упорядкована послідовність правил. Ланцюжки можна розділити на власні та базові. Базовий ланцюжок створюється за замовчуванням при ініціалізації таблиці. Кожен пакет, залежно від того, чи призначений він самому хосту, згенерований ним або є транзитним, повинен пройти набір базових ланцюжків різних таблиць. Крім того, базовий ланцюжок відрізняється від користувальницького наявністю «за замовчуванням дії» (default policy). Ця дія застосовується до тих пакетів, які було оброблено іншими правилами цього ланцюжка і викликаних з нього ланцюжків. Імена базових ланцюжків завжди записуються у верхньому регістрі (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING). Ланцюжок, що створюється користувачем може використовуватись лише в межах своєї таблиці. Рекомендується не використовувати для таких ланцюжків імена у верхньому регістрі, щоб уникнути плутанини із базовими ланцюжками та вбудованими діями.

3. Таблицею є сукупність базових і користувальницьких ланцюжків, об'єднаних загальним функціональним призначенням. Імена таблиць (як і модулів

критеріїв) записуються в нижньому регістрі, тому що в принципі не можуть конфліктувати з іменами ланцюжків користувача. При виклику команди iptables таблиця вказується у форматі -t ім’я_таблиці. У разі відсутності явної вказівки, використовується таблиця filter.

Усі пакети пропускаються через певні послідовності ланцюжків. При проходженні пакетом ланцюжка до нього послідовно застосовуються всі правила цього ланцюжка у порядку їх розташування. Під застосуванням правила розуміється перевірка пакета на відповідність критерію і, якщо пакет цьому критерію відповідає, застосовується до нього зазначена дія. Дією може бути як елементарна операція (наприклад, ACCEPT, MARK), так і перехід до одного із ланцюжків користувача. Дії можуть бути термінальними та нетермінальними. Термінальні дії припиняють обробку пакета в рамках даного базового ланцюжка, наприклад, ACCEPT, REJECT. Нетермінальні дії не переривають процес обробки пакета, наприклад, MARK, TOS. Якщо пакет пройшов через весь базовий ланцюжок і до нього не було застосовано жодної термінальної дії, то до нього застосовується стандартна дія для даного ланцюжка, яка є обов'язково термінальною.

Наступна команда дозволяє вивести список правил, що діють:

```
# iptables -L -n -v
```

Для виведення списку правил для пакетів, що приймаються (INPUT) або відправляються (OUTPUT) застосовуються наступні команди

```
# iptables -L INPUT -n -v
# iptables -L OUTPUT -n -v
```

За допомогою наступних команд можна видалити усі або певні правила та ланцюжки:

```
# iptables -F
# iptables -X
# iptables -t nat -F
# iptables -t nat -X
# iptables -t mangle -F
# iptables -t mangle -X
# iptables -P INPUT ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD ACCEPT
```

де -F - видалити (flush) усі правила;
-X - видалити ланцюжок;
-t table_name - вибрати таблицю (nat або mangle) і видалити усі правила;
-P - вибрати дії за замовчуванням (такі, як DROP, REJECT або ACCEPT).

До усіх пакетів, які відносяться до вже встановлених з’єднань, застосовується термінальна дія ACCEPT — пропустити:

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

В якості дії для пакетів, що надходять, за замовчуванням встановлюється DROP — блокування пакету:

iptables -P INPUT DROP

Наступне дозволяє усі пакети, що виходять:

iptables -P OUTPUT ACCEPT

Тепер ланцюжок INPUT таблиці filter містить єдине правило, яке пропускає всі пакети, що стосуються вже встановлених з'єднань. До всіх інших вхідних пакетів буде застосовано стандартну дію — DROP. Ланцюжок OUTPUT взагалі не містить правил, тому до всіх вихідних пакетів застосовуватиметься дія за замовчуванням ACCEPT. Таким чином, хост, налаштований згідно з цим прикладом і підключений до Інтернету, буде недоступний ззовні (всі спроби встановити з'єднання зовні блокуються), проте з самого хоста доступ до Інтернету буде вільний (вихідні пакети дозволені, а відповіді на них уже відносяться до встановлених з'єднань).

4. При короткочасовому підвищені навантаження на web-сервер з боку зовнішньої мережі дієвими є:

- обмеження кількості з’єднань з однієї IP адреси

iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 30 -j DROP

- блокування IP, наприклад, після 10 підключень до порту 80 на протязі 30 секунд

iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent -- set
iptables -I INPUT -p tcp --dport 80 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j DROP

5. При різкому збільшені вхідного UDP трафіку та виявлені вихідного трафіку з усіх відкритих UDP-портів, може вказувати на так званий UDP-Flood. Необхідно виставити обмеження на кількість підключень до відкритих портів і закрити порти, що не використовуються, за допомогою міжмережевих екранів. Додаються правила міжмережевого екрану:

- обмеження кількості підключень

iptables -I INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1

- дозволити підключення тільки перевіреним IP-адресам, наприклад, 1.2.3.4

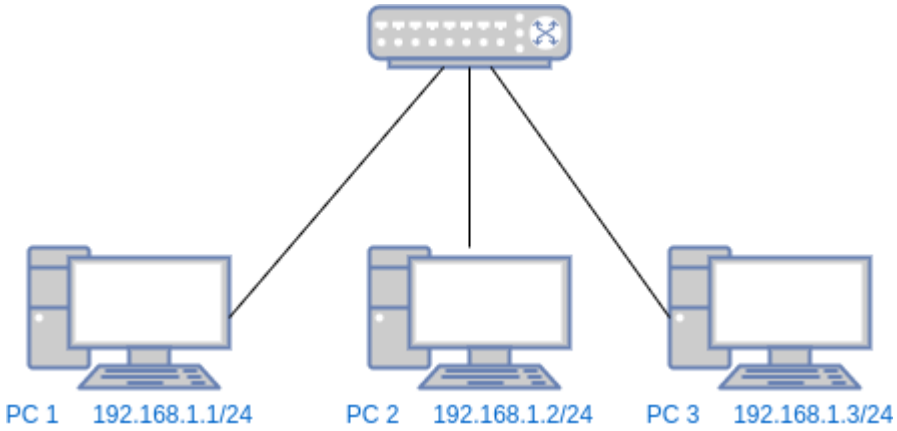
iptables -A OUTPUT -p udp --dport 53 -d 1.2.3.4 -j ACCEPT

- блокування інших портів

iptables -A OUTPUT -p udp -j DROP

Завдання до роботи

1. Реалізуйте мережу, що показано на рисунку.



На усіх комп’ютерах необхідно встановити або запустити ОС Linux
Налаштуйте робочі станції таким чином, щоб вони були у одній мережі, наприклад 192.168.1.0 маска 24 (255.255.255.0).
Перевірте утилітою ping зв’язок між комп’ютерами.

2. Встановіть, налаштуйте та запустіть на PC1 веб-сервер Apache

sudo apt-get install apache2

3. Запустіть на PC1 системний монітор і спостерігайте за навантаженням процесору та мережі. Послідовно з комп’ютерів PC 2 та PC 3 виконайте flood-атаку командою

ping -f -c 100000 192.168.1.1

Зафіксуйте навантаження (зробіть скрин-шот).

Повторіть flood-атаку командою
ping -f -c 100000 -s 1000 192.168.1.1

Зафіксуйте навантаження (зробіть скрин-шот).

4. Напишіть правило для iptables, що блокує такий тип flood-атак. Обґрунтуйте його і повторіть експеримет з фіксацією навантаження.

5. Підготуйте звіт.

Контрольні питання

1. Що визначає «ПРАВИЛО» в iptables?
2. Що визначає «ЛАЦЮЖОК» в iptables?
3. Що визначає «ТАБЛИЦЯ» в iptables?
4. Назвіть базові ланцюжки та їх налаштування.
5. Яке правило виконується останнім?
6. Наведіть приклад «ПРАВИЛА» в iptables.
7. Наведіть приклад «ЛАНЦЮЖКА» в iptables.
8. Наведіть приклад «ТАБЛИЦІ» в iptables.