МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет Магістерської підготовки

Кафедра Інформаційних технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: Аналіз та оптимізація роботи міжмережевих екранів на платформі Linux

Виконав студент 2 курсу групи МІС-19
спеціальності 122 Комп'ютерні науки

Нємцев Владислав Євгенович

Керівник д.т.н., професор
Казакова Надія Феліксівна

Рецензент засновник Компанії «UALinux»
Попов Володимир Леонідович

Одеса 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет _Магістерської підготовки_____
Кафедра _Інформаційних технологій_____
Рівень вищої освіти _магістр_____
Спеціальність 122 Комп'ютерні науки_____
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри_____
_____
" 26 " жовтня 2020 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

_____Нємцеву Владиславу Євгеновичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи __« Аналіз та оптимізація роботи міжмережевих екранів на платформі Linux»_____
_____
керівник роботи __Казакова Надія Феліксівна, д.т.н., професор_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від " 16 " жовтня № 194 «с»
2. Строк подання студентом роботи __7 грудня 2020р.
3. Вихідні дані до роботи_1. Аналіз існуючих рішень організації міжмереж-ного захисту_____
__2. Аналіз технологій IPTABLES, SHOREWALL._____
__3. Опис засобів для розгортання та налаштування екранів._____
_____
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
___Огляд існуючих рішень на ринку фаєрволів_____
___Дослідження технологій IPTABLES, SHOREWALL_____
___Покращення функціонального захисту мережі_____
___Розробка кінцевої схеми рішення фаервола_____
_____
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
____Слайди презентації_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання « 26 » жовтня 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Термін виконання етапів роботи	Оцінка виконання етапу	
			у %	за 4-х бальною шкалою
1.	Виконання огляду відомих рішень	**26.10.2020**	**70**	**задов**
2.	Аналіз методів та засобів виявлення уразливостей системи	30.10.2020	**70**	**задов**
3.	Дослідження технологій IPTABLES, SHOREWALL	4.10.2020	**70**	**задов**
4.	Установка та налаштування міжмережевих екранів	10.10.2020	**70**	**задов**
5.	Розробка рішення щодо покращення функціонального захисту мережі	12.10.2020	**70**	**задов**
	Рубіжна атестація	**19.11.2020**	**70**	**задов**
6.	Розробка кінцевої схеми рішення фаєрвола	22.11.2020	**70**	**задов**
7.	Додавання Ip телефонії, IPSEC тунелів	25.11.2020	**70**	**задов**
8.	Рекомендації про підвищення захищеності від уразливостей	3.12.2020	**70**	**задов**
	Подання роботи на кафедру	**07.12.2020**	**100**	**викон**
	Перевірка на плагіат	**08.12.2020**	**100**	**викон**
	Рецензування	**16.12.2020**	**100**	**викон**
	Інтегральна оцінка виконання етапів календарного плану (як середня по етапам)		**74**	**задов**

Студент _____ **Немцев В.Є.**
(підпис) (прізвище та ініціали)

Керівник роботи _____ **Казакова Н.Ф.**
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

на магістерську кваліфікаційну роботу
«Аналіз та оптимізація роботи міжмережевих екранів на платформі Linux»,
студента Нємцева Владислава Євгеновича

Актуальність теми магістерської кваліфікаційної роботи обумовлюється необхідністю підвищення рівня захищеності корпоративних інформаційних мереж та мереж державних установ. В першу чергу це стосується персональних даних та іншої інформації, необхідність захисту якої регламентована законодавчими та нормативними документами України.

Мета роботи – аналіз та оптимізація роботи міжмережевих екранів на платформі Linux.

Об’єкт дослідження – програмні міжмережні екрани, які виконують функції розмеження доступу у ОС linux.

Методи дослідження – емпіричний метод із використанням експертних оцінок, сучасних програмних продуктів та технологій.

Результати проведеного дослідження показало що кількість правил фільтрації чинять більш негативний вплив на продуктивність брандмауера Iptables ніж на Shorewall. Також у роботі створені правил доступу до мережі за допомогою міжмережевого екрану Shorewall..

Магістерська кваліфікаційна робота містить 77 сторінок, 15 рисунків, та 21 джерелО.

Ключові слова: ФАЄРВОЛ, ЕКРАН, МЕРЕЖА, МЕРЕЖЕВЕ СКАНУВАННЯ, ПЕНТЕСТИНГ, УРАЗЛИВІСТЬ.

SUMMARY

for a master's degree

"Analysis and optimization of firewalls on the Linux platform",

student Nemtsev Vladislav

The urgency of the topic of master's qualification work is due to the need to increase the level of security of corporate information networks and networks of government agencies. This primarily applies to personal data and other information, the need for protection of which is regulated by laws and regulations of Ukraine.

The purpose of the work is to analyze and optimize the operation of firewalls on the Linux platform.

The object of study is software firewalls, which perform the functions of access restriction in the Linux operating system.

Research methods - an empirical method using expert assessments, modern software products and technologies.

The results of the study showed that the number of filtering rules have a more negative impact on the performance of the Iptables firewall than on Shorewall. Also in the work rules of access to a network by means of the Shorewall firewall are created.

The master's thesis contains 77 pages, 15 figures, and 21 sources.

Keywords: FIREWORK, SCREEN, NETWORK, NETWORK SCANNING, PENTESTING, VULNERABILITY.

ЗМІСТ

ПЕРЕЛІК УМОВННХ СКОРОЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1. ОГЛЯД ВІДОМИХ РІШЕНЬ 12
1.1 Що таке брандмауер? 15
1.2 У чому полягає робота брандмауера? 15
1.3 Види брандмауерів 17
1.4 Перевага використання брандмауера 17
1.5 Рівень небезпеки 17
1.6 Міжмережевий екран як засіб від вторгнення з мережі інтернет 19
1.7 Функціональні вимоги і компоненти міжмережевих екранів 21
1.8 Фільтруючі маршрутизатори 22
1.9 Шлюзи мережевого рівня 24
1.10 Шлюзи прикладного рівня 25
1.11 Посилена автентифікація 27
1.12 Основні схеми мережевого захисту на базі міжмережевих екранів 29
1.13 Міжмережевий екран — фільтруючий маршрутизатор 30
1.14 Міжмережевий екран на базі двопортового шлюзу 30
1.15 Міжмережевий екран на основі екранованого шлюзу 31
1.16 Міжмережевий екран — екранована під мережа 31
РОЗДІЛ 2. ДОСЛІДЖЕННЯ IPTABLES, SHOREWALL 33
2.1 Опис мережі і вибір фаєрволів 33
2.2 Установка міжмережевих екранів 34
2.2.1. Iptables 34
2.2.2 Shorewall 34
2.3 Налаштування між мережевих екранів 35
2.3.1 Iptables 36
2.3.2 Shorewall 37
2.4 Пропускна здатність 38
2.5 Затримка 40

2.6 Оцінка установки з'єднання 42
2.7 Оцінка швидкості заборони. 42
2.8 Швидкість передачі HTTP 43
2.9 Споживання системних ресурсів 45
РОЗДІЛ 3. ПОКРАЩЕННЯ ФуНКЦІОНАЛЬНОГ0 ЗАХИСТУ МЕРЕЖІ 47
3.1 Пропускна здатність 48
3.2 Затримка 52
3.3 Оцінка установки з'єднання і розрив. 55
3.4 Швидкість передачі HTTP 58
3.5 Споживання системних ресурсів 59
3.6 Покращення результатів Shorewall 61
3.6.1 Базова настройка 61
3.6.2 Фільтрація трафіку 66
3.6.3 Введення додаткових можливостей 68
РОЗДІЛ 4.КІНЦЕВА СХЕМА РІШЕННЯ ФАЕРВОЛА 71
4.1 Додавання Ip телефонії 73
4.2 Додавання IPSEC тунелів 75
ВИСНОВКИ 77
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 78

ПЕРЕЛІК УМОВННХ СКОРОЧЕНЬ

TCP/IP Transmission Control Protocol, TCP (укр. Протокол керування передачею) один з основних мережевих протоколів Інтернету, призначений для управління передачею даних в мережах і під мережах TCP/IP.

FTP Протокол передачі файлів (англ. File Transfer Protocol, FTP) — дає можливість абоненту обмінюватися двійковими і текстовими файлами з будь-яким комп'ютером мережі, що підтримує протокол FTP.

HTTP HTTP (англ. HyperText Transfer Protocol - «протокол передачі гіпертексту») - протокол прикладного рівня передачі даних (спочатку - у вигляді гіпертекстових документів у форматі HTML, зараз використовується для передачі довільних даних).

VPN VPN (Віртуальна приватна мережа, Virtual Private Network) SMTP Simple Mail Transfer Protocol (Простий Протокол Пересилання Пошти) — це протокол, який використовується для пересилання електронної пошти до поштового сервера або з клієнта-комп'ютера, або між поштовими серверами.

UDP User Datagram Protocol, UDP (укр. Протокол дейтаграм користувача) — один із протоколів в стеку TCP/IP..

WWW Всесвітня мережа (англ. Wor1d Wide Web) — розподілена система, що надає доступ до пов'язаних між собою документів, розташованим на різних комп'ютерах, підключених до мережі Інтернет.

IMAP (англ. Internet Message Access Protocol) — протокол прикладного рівня для доступу до електронної пошти.

MITM — Атаки "людина посередині" (MITM) відбуваються, коли зловмисникові вдається розташуватися між законними сторонами в розмові. Зловмисник підробляє протилежну легітимну сторону, так що всі сторони вважають, що вони насправді розмовляють з очікуваними іншими, легітимними сторонами. Атака MITM дозволяє зловмиснику підслуховувати розмову між сторонами або активно втручатися в розмову, щоб досягти якогось незаконного кінця.

ВСТУП

Актуальність теми. Інтенсивний розвиток глобальних комп'ютерних мереж. Поява нових технологій пошуку інформації привертають все більше уваги до мережі Інтернет з боку приватних осіб і різних організацій. Багато організацій приймають рішення про інтеграцію своїх локальних і корпоративних мереж в глобальну мережу. Використання глобальних мереж у комерційних цілях, а також при передачі інформації, яка містить відомості конфіденційного характеру, тягне за собою необхідність побудови ефективної системи захисту інформації. Зі збільшенням опори на технології стає все більш важливим захищати всі аспекти онлайн-інформації та даних. У міру зростання Інтернету та збільшення комп’ютерних мереж цілісність даних стала одним із найважливіших аспектів для організацій.

Безпека мережі — це один з найважливіших аспектів, який слід враховувати при роботі через Інтернет, локальну мережу чи іншим способом, незалежно від того, наскільки малий чи великий ваш бізнес. Хоча немає мережі, яка захищена від атак, стабільна та ефективна система мережевої безпеки є важливою для захисту даних клієнта. Хороша система мережевої безпеки допомагає бізнесу зменшити ризик стати жертвою викрадення та саботажу даних.

Безпека мережі допомагає захистити ваші робочі станції від шкідливого шпигунського програмного забезпечення. Це також гарантує захист спільних даних. Інфраструктура мережевої безпеки забезпечує кілька рівнів захисту для запобігання атакам MITM, розбиваючи інформацію на численні частини, шифруючи ці частини та передаючи їх незалежними шляхами, таким чином запобігаючи таким випадкам, як прослуховування. Розвиток глобальних мереж привів до багаторазового збільшення кількості користувачів і збільшення кількості атак на комп'ютери, підключені до мережі Інтернет. Щорічні втрати, зумовлені недостатнім рівнем захищеності комп'ютерів, оцінюються десят-

ками мільйонів доларів. При підключенні до Інтернет локальної або корпоративної мережі необхідно подбати про забезпечення інформаційної безпеки цієї мережі. Глобальна мережа Інтернет створювалася як відкрита система, призначена для вільного обміну інформацією. У силу відкритості своєї ідеології Інтернет надає для зловмисників значно більші можливості в порівнянні з традиційними інформаційними системами. За цим питання про проблему захисту мереж і її компонентів ставати досить важливим та актуальним і цей час, час прогресу і комп'ютерних технологій. Багато країн нарешті зрозуміли важливість цієї проблеми. Відбувається збільшення витрат і зусиль спрямованих на виробництво і поліпшення різних засобів захисту. Основною метою реферату є розгляд, і вивчення функціонування одного з таких засобів мережевого захисту як брандмауер або міжмережевий екран. Який в даний час є найбільш надійним в плані захисту з пропонованих засобів.

Метою роботи є розгляд, і вивчення функціонування одного з таких засобів мережевого захисту як брандмауер або міжмережевий екран. Який в даний час є найбільш надійним в плані захисту з пропонованих засобів.

Для досягнення поставленої мети в роботі необхідно розв'язати такі завдання:

- Виконати огляд сучасних технологій захисту корпоративних мереж та методів впливу зловмисників на них. Проаналізувати та систематизувати одержані результати.
- Дослідити доцільність виконання кожного із розглянутих методів захисту за конкретних умов.
- Представити результати дослідження у зручному для користувача вигляді.

Об'єкт дослідження - міжмережеві екрани на платформі Linux

Предмет дослідження - покращення захисту мережі.

Методи дослідження.

У магістерській дипломній роботі розроблена методика, що дозволяє отримувати кількісну оцінку стану захищеності інформаційної системи, при

цьому враховуючи думки експертів, а також їхній досвід при оцінці системи захисту на підставі оцінки ймовірності загроз. Дана методика використовує напрацювання з області ризиків, дозволяючи будувати СЗІ за своїми характеристиками сумірною масштабом загроз. Таким чином, методика повинна дозволити вибирати засоби захисту оптимальні для кожної конкретної системи, що характеризується специфічним набором загроз, вимогами і моделлю порушника. Використання даної методики для оцінки існуючих систем а дозволить прийняти рішення про доцільність їх удосконалення, і дозволить уникнути неефективного використання коштів СЗІ при її проектуванні.

РОЗДІЛ 1. ОГЛЯД ВІДОМИХ РІШЕНЬ

Сучасна мережа передачі даних це безліч віддалених високопродуктивних пристроїв, що взаємодіють один з одним на деякій відстані. Однією з найбільш великомасштабних мереж передачі даних є комп'ютерна мережа інтернет. У ній одночасно працюють мільйони джерел і споживачів інформації по всьому світу. Разом з тим, загальний доступ до єдиних фізичних ресурсів відкриває доступ шахраям, вірусам та конкурентам, а це надає можливість заподіяти шкоду кінцевим користувачам: викрасти, спотворити, модифікувати, знищити збережену інформацію, порушити цілісність програмного забезпечення і навіть вивести апаратну частину кінцевої станції. [1][1)]

Через мережу Інтернет порушник може:

– вторгнутись у внутрішню мережу навчального закладу та отримати несанкціонований доступ до інформації;
– незаконно скопіювати важливу і цінну інформацію;
– отримати паролі, адреси серверів, а часом і їх вміст;
– входити в інформаційну систему навчального закладу під ім'ям зареєстрованого користувача.

Для запобігання небажаних впливів варто використовувати між мережеві екрани (Ipfw, , Iptables , Shorewall). Міжмережевий екран служить захисною стіною між локальною мережею та зовнішньою мережею і запобігає будь-яким загрозам. Він призначений для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі, дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти , спливаючі вікна та інше, не надсилати іншим "чужим" серверам інформацію про ваш комп'ютер, робить даремною роботу програм-троянів і засобів віддаленого адміністрування. Робота між мережевих екранів полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в

[1)] [1]Дилевский А. Фильтрация пакетов, firewall u маскарадинг в Линуксе [Електронний ресурс]. — Режим доступу: http://citforum.ru/operating_systems/articles/masquerade.shtml

залежності від результатів аналізу пропускає пакети у внутрішню мережу (сегмент мережі) або повністю їх фільтрує. Ефективність роботи між мережевого екрана, що працює під управлінням Linux, зумовлена тим, що він повністю заміщує реалізований стек протоколів TCP\IP, і тому порушення його роботи хакерами з допомогою спотворення протоколів зовнішньої мережі е неможливим. Між мережеві екрани виконують такі функції:

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

Розрізняють два типи між мережевих екранів: апаратний і програмний. Апаратний являє собою пристрій, який фізично підключається до мережі. Цей пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблюваного повідомлення, що забезпечує безпеку, допомагаючи запобігти небажаним проникненням в мережу або комп'ютер. Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який запущений на кінцевому комп'ютері або шлюзі (Рис.1). Найбільшого розповсюдження отримав програмний тип реалізації між мережевого екрану.

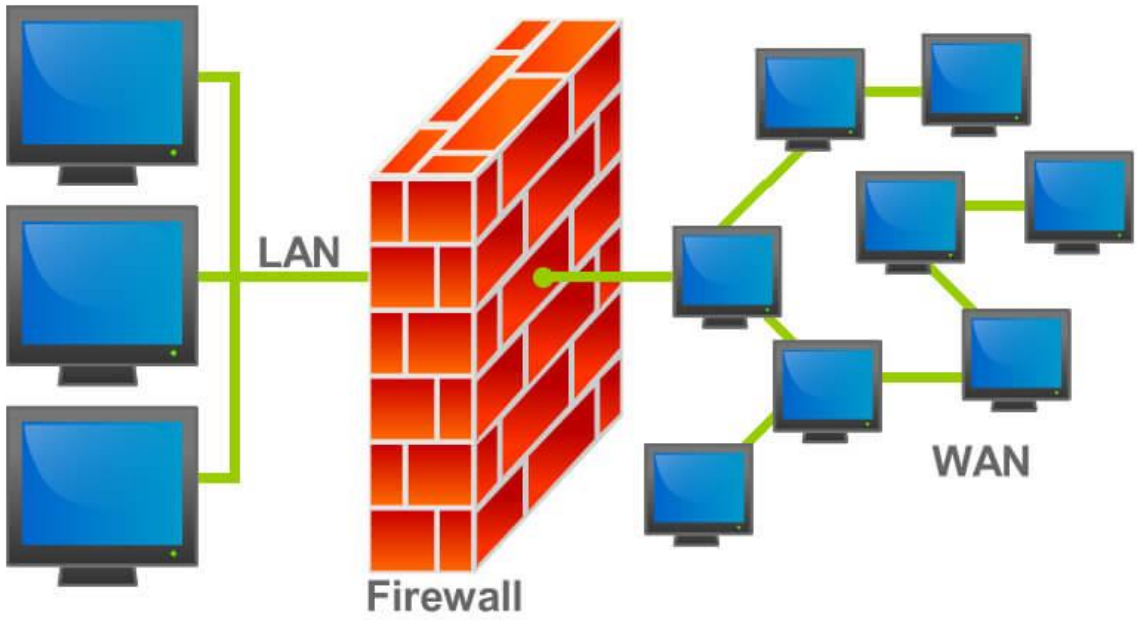

Рисунок 1. Загальна схема роботи локальної мережі з глобальною через міжмережевий екран

Міжмережеві екрани можуть працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP-адресам (наприклад, не пропускаються пакети з мережі Інтернет, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання)[2][1)]. На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів).

[1)] [2]Захаров И. Протокол TCP №1 [Електронний ресурс]. — Режим доступу: https://xakep.ru/2002/04/11/14943/

1.1 Що таке брандмауер?

Брандмауер, або міжмережевий екран, — це « напівпроникна мембрана», яка розташовується між що захищається внутрішнім сегментом мережі і зовнішньою мережею або іншими сегментами мережі Інтернет і контролює всі інформаційні потоки у внутрішній сегмент і з нього. Контроль трафіку полягає в його фільтрації, тобто у вибірковому пропущенні через екран, а іноді і з виконанням спеціальних перетворень і формуванням сповіщень для відправника, якщо його даним у пропуску відмовлено. Фільтрація здійснюється на підставі набору умов, попередньо завантажених в брандмауер і відображають концепцію інформаційної безпеки корпорації. Брандмауери можуть бути виконані у вигляді як апаратного, так і програмного комплексу, записаного в комутуючий пристрій або сервер доступу (сервер-шлюз, просто сервер, хост-комп'ютер і т.д.), вбудованого в операційну систему [3][1)]

1.2 У чому полягає робота брандмауера?

Робота брандмауера полягає в аналізі структури і вмісту інформаційних пакетів, що надходять із зовнішньої мережі, і в залежності від результатів аналізу пропуску пакетів у внутрішню мережу (сегмент мережі) або повному їх від фільтрування. Ефективність роботи між мережевого екрану, що працює під управлінням Linux, обумовлена тим, що він повністю заміщає реалізований стек протоколів TCP \ IP, і тому порушувати його роботу з допомогою спотворення протоколів зовнішньої мережі (що часто робиться хакерами) неможливо.

Міжмережеві екрани зазвичай виконують такі функції:

– фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі (внутрішньої під мережі) від зовнішніх каналів зв'язку;

[1)] [3]Iptables [Електронний ресурс]. — Режим доступу: http://uk.wikipedia.org/wiki/Iptables

– багатоетапну ідентифікацію запитів, що надходять в мережу (ідентифікація серверів, вузлів зв'язку про інших компонентів зовнішньої мережі);
– перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
– реєстрацію всіх запитів до компонентів внутрішньої під мережі ззовні;
– контроль цілісності програмного забезпечення і даних;
– економію адресного простору мережі (у внутрішній під мережі може використовуватися локальна система адресації серверів);
– приховування IP адрес внутрішніх серверів з метою захисту від хакерів.

Брандмауери можуть працювати на різних рівнях протоколів моделі OSI.

На мережевому рівні виконується фільтрація вступників пакетів, заснована на IP адреси (наприклад, не пропускати пакети з Інтернету, направлені на ті сервери, доступ до яких зовні заборонено; не пропускати пакети з фальшивими зворотними адресами або IP адресами, занесеними до (<чорного списку», і т.д.). На транспортному рівні фільтрація припустима ще й за номерами портів TCP і прапорів, що містяться в пакетах (наприклад, запитів на встановлення з'єднання). На прикладному рівні може виконуватися аналіз прикладних протоколів (FTP, HTTP, SMTP і т.д.) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь-яких типів файлів: рекламної інформації або виконуваних програмних модулів, наприклад).

Можна в брандмауері створювати та експертну систему, яка, аналізуючи трафік, діагностує події, що можуть становити загрозу безпеки внутрішньої мережі, та інформує про це адміністратора. Експертна система здатна також у разі небезпеки (спам, наприклад) автоматично посилювати умови фільтрації і т.д.[4][1)]

[1)] [4] https://www.gentoo.org/doc/ru/security/security-handbook.xml?part=1&chap=12#doc_chap1

1.3 Види брандмауерів

Брандмауери бувають апаратними або програмними. Апаратний брандмауер представляє собою пристрій, фізично підключається до мережі. Це пристрій відслідковує всі аспекти вхідного і вихідного обміну даними, а також перевіряє адреси джерела і призначення кожного оброблювано о повідомлення. Це забезпечує безпеку, допомагаючи запобігти небажаним проникнення в мережу або на комп'ютер. Програмний брандмауер виконує ті ж функції, використовуючи не зовнішній пристрій, а встановлену на комп'ютері програму.

На одному і тому ж комп'ютері можуть використовуватися як апаратні, так і програмні брандмауери.

1.4 Перевага використання брандмауера

Брандмауер представляє собою захисну кордон між комп'ютером (або комп'ютерною мережею) і зовнішнім середовищем, користувачі або програми якої можуть намагатися отримати несанкціонований доступ до комп'ютера. Зазвичай зломщики використовують спеціальні програми для пошуку в Інтернеті незахищених підключень. Така програма відправляє на комп'ютер дуже маленьке повідомлення. За відсутності брандмауера комп'ютер автоматично відповідає на повідомлення, виявляючи свою незахищеність. Встановлений брандмауер отримує такі повідомлення, але не відповідає на них; таким чином, зломщики навіть не підозрюють про існування даного комп'ютера.

1.5 Рівень небезпеки

Існує кілька шляхів звести нанівець або піддати ризику брандмауер захисту. І хоча вони всі погані, про деяких можна з упевненістю говорити як про

самих неприємних. Виходячи з того, що основною метою встановлення більшості брандмауерів е блокування доступу, очевидно, що виявлення будь-ким лазівки, що дозволяє проникнути в систему, веде до повного краху всієї захисту даної системи. Якщо ж несанкціонованому користувачеві вдалося проникнути в брандмауер і пере конфігурувати його, ситуація може прийняти ще більш загрозливого характеру.3 метою розмежування термінології приймемо, що в першому випадку ми маємо справу зі зломом брандмауер захисту, а в другому - з повним її руйнуванням. Ступінь впливу, який може спричинити за собою руйнування брандмауер захисту, визначити неймовірно складно. Найбільш повні відомості про надійність такого захисту може дати тільки інформація про діяльність, спробі злому, зібрана цим брандмауером. [5][1)] Найгірше відбувається із системою захисту саме тоді, коли при повному руйнуванні брандмауера не залишається жодних слідів, що вказують на те, як це відбувалося. У кращому ж випадку брандмауер сам виявляє спробу злому і ввічливо інформує про це адміністратора. Спроба при цьому приречена на провал.

Один зі способів визначити результат спроби злому брандмауер захисту — перевірити стан речей в так званих зонах ризику. Якщо мережа підключена до Інтернет без брандмауера, об'єктом нападу стане вся мережа. Така ситуація сама по собі не передбачає, що мережа стає вразливою для кожної спроби злому. Однак якщо вона приєднується до загальної не захищеної мережі, адміністраторові доведеться забезпечувати безпеку кожного вузла окремо. У разі утворення проломи в брандмауері зона ризику розширюється і охоплює всю захищену мережу.3ломщик, що отримав доступ до входу в брандмауер, може вдатися до методу "захоплення островів" і, користуючись брандмауером як базою, охопити всю локальну мережу. Подібна ситуація все ж дасть слабку надію, бо порушник може залишити сліди в брандмауері, і його можна буде викрити. Якщо ж брандмауер повністю виведений з ладу, локальна мережа стає

---

1) [5] W. Stallings, "Intruders," in Network Security Essentials, Applications and standards, Pearson, 2011, p. 319.

відкритою для нападу з будь-якої зовнішньої системи, і визначення характеру цього нападу стає практично неможливим.

Загалом, цілком можливо розглядати брандмауер як засіб звуження зони ризику до однієї точки пошкодження. У певному сенсі це може здатися зовсім не такою вже вдалою ідеєю, адже такий підхід нагадує складання яєць в один кошик. Однак практикою підтверджено, що будь-яка досить велика мережа включає, щонайменше, декілька вузлів, уразливих при спробі злому навіть не дуже досвідченим порушником, якщо у нього достатнього для цього часу. Багато великих компаній мають на озброєнні організаційну політику забезпечення безпеки вузлів, розроблену з урахуванням цих недоліків. Однак було б не надто розумним цілком покладатися виключно на правила. Саме за допомогою брандмауера можна підвищити надійність вузлів, направляючи порушника в такий вузький тунель, що з'являється реальний шанс виявити і вистежити його, до того як він наробить бід. Подібно до того, як середньовічні замки обносили кількома стінами, в нашому випадку створюється взаємно блокуючий захист.

1.6 Міжмережевий екран як засіб від вторгнення з мережі інтернет

Ряд завдань по віддзеркаленню найбільш ймовірних загроз для внутрішніх мереж здатні вирішувати міжмережеві екрани, у вітчизняній літературі до останнього часу використовувалися замість цього терміна інші терміни іноземного походження: брандмауер і firewall. Поза комп'ютерної сфери брандмауером (або firewall) називають стіну, зроблену з негорючих матеріалів і перешкоджає поширенню пожежі. У сфері комп'ютерних мереж міжмережевий екран є бар'єром, що захищає від фігуральної пожежі — спроб зловмисників вторгнутися у внутрішню мережу для того, щоб скопіювати, змінити або стерти інформацію або скористатися пам'яттю чи обчислювальною потужністю пра-

цюють у цій мережі комп'ютерів. міжмережевий екран покликаний забезпечити безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Міжмережевий екран (МЕ) — це система між мережевого захисту. дозволяє розділити загальну мережу на дві частини або більше і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальної) мережею підприємства і глобальною мережею Інтернет, хоча її можна провести і усередині корпоративної мережі підприємства. МЕ пропускає через себе весь трафік, приймаючи для кожного проходить пакету рішення — пропускати його або відкинути. Для того щоб МЕ міг здійснити це йому необхідно визначити набір правил фільтрації.

Зазвичай між мережеві екрани захищають внутрішню мережу підприємства від "вторгнень" з глобальної мережі Інтернет, однак вони можуть використовуватися і для захисту від "нападів" з корпоративної Інтернет мережі, до якої підключена локальна мережа підприємства. Жоден міжмережевий екран не може гарантувати повного захисту внутрішньої мережі при всіх можливих обставин. Однак для більшості комерційних організацій установка між мережевого екрану є необхідною умовою забезпечення безпеки внутрішньої мережі. Головний аргумент на користь застосування між мережевого екрану полягає в тому, що без нього системи внутрішньої мережі наражаються на небезпеку з боку слабо захищених служб мережі Інтернет, а також зондування і атакам з будь-яких інших хост-комп'ютерів зовнішньої мережі.

Проблеми недостатньої інформаційної безпеки є "вродженими" практично для всіх протоколів і служб Інтернет. Велика частина цих проблем пов'язана з історичною залежністю Інтернет від операційної системи UMX. Відомо, що мережа Arpanet (прабатько Інтернет) будувалася як мережа, що зв'язує дослідні центри, наукові, військові та урядові установи, великі університети США. Ці структури використовували операційну систему UNIX в якості пла-

тформи для комунікацій і вирішення власних завдань. Тому особливості методології програмування в середовищі UNIX та її архітектури наклали відбиток на реалізацію протоколів обміну і політики безпеки в мережі. Через відкритості та поширеності система UNIX стала улюбленою здобиччю хакерів. Тому зовсім не дивно, що набір протоколів TCP / IP, який забезпечує комунікації в глобальній мережі Інтернет і в які отримують все більшу популярність Інтернет мережі, має "вроджені" недоліки захисту. Те ж саме можна сказати і про ряд служб Інтернет.

Набір протоколів управління передачею повідомлень в Інтернет (Transmission Control Protocol / Інтернет Protocol - TCP / IP) використовується для організації комунікацій в неоднорідному мережевому середовищі, забезпечуючи сумісність між комп'ютерами різних типів. Сумісність — одна з основних переваг TCP / IP, тому більшість локальних комп'ютерних мереж підтримує ці протоколи. Крім того, протоколи TCP / IP надають доступ до ресурсів глобальної мережі Internet. Оскільки TCP / IP підтримує маршрутизацію пакетів, він зазвичай використовується в якості міжмережевогопротоколу.Завдяки своїй популярності TCP / IP став стандартом де факто для між мережевого взаємодії.

У заголовках пакетів TCP / IP зазначається інформація, яка може піддатися нападам хакерів.Зокрема, хакер може підмінити адресу відправника у своїх "шкідливих" пакетах, після чого вони будуть виглядати, як пакети, що передаються авторизованим клієнтом.

1.7 Функціональні вимоги і компоненти міжмережевих екранів

Функціональні вимоги до між мережевих екранів включають:

- вимоги до фільтрації на мережевому рівні;
- вимоги до фільтрації на прикладному рівні;
- вимоги по налаштуванню правил фільтрації та адміністрування;
- вимоги до засобів мережевої автентифікації;

– вимоги щодо впровадження журналів та обліку. Більшість компонентів між мережевих екранів можна віднести до однієї з трьох категорій:
– фільтруючі маршрутизатори;
– шлюзи мережевого рівня;
– шлюзи прикладного рівня.

Ці категорії можна розглядати як базові компоненти реальних між мережевих екранів. Лише деякі між мережеві екрани включають тільки одну з перерахованих категорій. Тим не менше, ці категорії відображають ключові можливості, що відрізняють між мережеві екрани один від одного.

1.8 Фільтруючі маршрутизатори

Фільтруючий маршрутизатор являє собою маршрутизатор або працює на сервері програму, сконфігурований таким чином, щоб фільтрувати вхідні і вихідні пакети. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP-і IP-заголовках пакетів.

Фільтруючі маршрутизатори звичайно може фільтрувати IP-пакет на основі групи наступних полів заголовка пакету:

– IP-адреса відправника (адреса системи, яка послала пакет);
– IP-адресу одержувача (адреса системи, яка приймає пакет);
– порт відправника (порт з'єднання в системі відправника);
– порт одержувача (порт з'єднання в системі одержувача);

Порт — це програмне поняття, яке використовується клієнтом або сервером для здійснення та отримання повідомлень; порт ідентифікується 16-бітовим числом.

В даний час не всі фільтруючі маршрутизатори фільтрують пакети по TCP / UDP — порт відправника, однак багато виробників маршрутизаторів почали забезпечувати таку можливість. Деякі маршрутизатори перевіряють, з якого мережевого інтерфейсу маршрутизатора прийшов пакет, і потім використовують цю інформацію як додатковий критерій фільтрації.

Фільтрація може бути реалізована в різний спосіб для блокування зв’язку з певними хост-комп'ютерами або портами. Наприклад, можна блокувати з’єднання, що надходять від конкретних адрес тих хост-комп'ютерів і мереж, які вважаються ворожими або ненадійними. [6][1)]

Додавання фільтрації по портів TCP і UDP до фільтрації по IP-адресами забезпечує більшу гнучкість. Відомо, що такі сервери, як домен TELNET, зазвичай пов'язані з конкретними портами (наприклад, порт 23 протоколу TELNET). Якщо міжмережевий екран може блокувати з’єднання TCP або UDP з певними портами або від них, то можна реалізувати політику безпеки, при якій деякі види з’єднань встановлюються лише з конкретними хост-комп'ютерами.

До позитивних якостей фільтруючих маршрутизаторів слід віднести:

– порівняно невисоку вартість;
– гнучкість у визначенні правил фільтрації;
– невелику затримку при проходженні пакетів.

Недоліками фільтруючих маршрутизаторів є:

– внутрішня мережа видно маршрутизується з мережі Інтернет правила фільтрації пакетів важкі в описі і вимагають дуже хороших знань технологій TCP і UDP;
– при порушенні працездатності брандмауера з фільтрацією пакетів всі комп'ютери за ним стають повністю незахищеними або недоступними;
– автентифікацію з використанням IP-адреси можна обдурити шляхом підміни IP-адреси (атакуюча система видає себе за іншу, використовуючи її IP- адреса);
– відсутня автентифікація на рівні користувача.

[1)] [6] V. У. P. B. Joe1 Sommers, "Toward Comprehensive Traffic Generation for Online IDS Evaluation," University of Wisconsin-Madison

1.9 Шлюзи мережевого рівня

Шлюз мережевого рівня іноді називають системою трансляції мережевих адрес або шлюзом сеансового рівня моделі OSI. Такий шлюз виключає, пряма взаємодія між авторизованим клієнтом і зовнішнім хост-комп'ютером Шлюз мережевого рівня приймає запит довіреної клієнта на конкретні послуги, і після перевірки допустимості запитаного сеансу встановлює з’єднання із зовнішнім хост-комп'ютером. Після цього шлюз копіює пакети в обох напрямках, не здійснюючи їх фільтрації.

Шлюз стежить за підтвердженням зв'язку між авторизованим клієнтом і зовнішнім хост-комп'ютером, визначаючи, чи е запитуваний сеанс зв'язку допустимим.

Фактично більшість шлюзів мережевого рівня не е самостійними продуктами, а поставляються в комплекті зі шлюзами прикладного рівня. Прикладами таких шлюзів е Gauntlet Інтернет Firewall компанії Trusted Information Systems, A1ta Vista Firewall компанії DEC і ANS Interlock компанії ANS. Наприклад, A1ta Vista Firewall використовує канальні посередники прикладного рівня для кожної з шести служб TCP / IP, до яких належать, зокрема, FTP, HTTP (Hyper Text Transport Protocol) і Telnet. Крім того, міжмережевий екран компанії DEC забезпечує шлюз мережевого рівня, що підтримує інші загальнодоступні служби TCP / IP, такі як Gopher і SMTP, для яких міжмережевий екран не надає посередників прикладного рівня.

Шлюз мережевого рівня виконує ще одну важливу функцію захисту: він використовується в якості сервера-посередника. Цей сервер-посередник виконує процедуру трансляції адрес, при якій відбувається перетворення внутрішніх IP-адрес в один "надійний" IP- адресу. Ця адреса асоціюється з між мережевим екраном, з якого передаються всі вихідні пакети. У результаті в мережі зі шлюзом мережевого рівня всі вихідні пакети виявляються відправленими з цього шлюзу, що виключає прямий контакт між внутрішньою (авторизованої)

мережею і потенційно небезпечної зовнішньої мережі. IP-адреса шлюзу мережевого рівня стає єдино активним IP-адресом, який потрапляє в зовнішню мережу. Таким чином, шлюз мережевого рівня та інші сервери-посередники захищають внутрішні мережі від нападів типу підміни адресу.

1.10 Шлюзи прикладного рівня

Для усунення ряду недоліків, властивих фільтруючим маршрутизаторам, між мережеві екрани повинні використовувати додаткові програмні засоби для фільтрації повідомлень сервісів типу TELNET і FTP. Такі програмні засоби називаються повноважними серверами (серверами-посередниками), а хост-комп'ютер, на якому вони виконуються, — шлюзом прикладного рівня.

Шлюз прикладного рівня виключає пряму взаємодію між авторизованим клієнтом і зовнішнім хост-комп'ютером. Шлюз фільтрує всі вхідні і вихідні пакети на прикладному рівні. Пов'язані з додатком сервери - посередники перенаправляють через шлюз інформацію, що генерується конкретними серверами.

Для досягнення більш високого рівня безпеки та гнучкості шлюзи прикладного рівня і фільтруючі маршрутизатори можуть бути об'єднані в одному між мережевому екрані. Як приклад розгляну мережу, в якій 38 допомогою фільтруючого маршрутизатора блокуються вхідні з’єднання TELNET і FTP. Цей маршрутизатор допускає проходження пакетів TELNET або FTP тільки до одного хост-комп'ютера - шлюзу прикладного рівня TELNET / FTP. Зовнішній користувач, який хоче з’єднатися з деякою системою в мережі, повинен спочатку з’єднатися зі шлюзом прикладного рівня, а потім вже з потрібним внутрішнім хост-комп'ютером.

На додаток до фільтрації пакетів багато шлюзи прикладного рівня реєструють всі виконувані сервером дії і, що особливо важливо, попереджають мережевого адміністратора про можливі порушення захисту. Наприклад, при спробах проникнення в мережу ззовні Border Ware Firewall Server компанії

Secure Computing дозволяє фіксувати адреси відправника і одержувача пакетів, час, в який ці спроби були зроблені, і використовуваний протокол. Міжмережевий екран B1ack Hole компанії Milkyway Networks реєструє всі дії сервера і попереджає адміністратора про можливі порушення, посилаючи йому повідомлення по електронній пошті або на пейджер. Аналогічні функції виконують і ряд інших шлюзів прикладного рівня.

Шлюзи прикладного рівня дозволяють забезпечити найбільш високий рівень захисту, оскільки взаємодія із зовнішнім світом реалізується через мало прикладних повноважних програм-посередників, повністю контролюють весь вхідний і вихідний трафік.

Шлюзи прикладного рівня мають ряд переваг у порівнянні зі звичайним режимом, при якому прикладної трафік пропускається безпосередньо до внутрішніх хост-комп'ютерів. Перерахую ці переваги.

– Невидимість структури мережі, що захищається з глобальної мережі Інтернет. Імена внутрішніх систем можна не повідомляти зовнішнім системам через DNS, оскільки шлюз прикладного рівня може бути єдиним хост-комп'ютером, ім'я якого повинно бути відомо зовнішнім системам.
– Надійна автентифікація та реєстрація. Прикладної трафік може бути автентифікований, перш ніж він досягне внутрішніх хост-комп'ютерів, і може бути зареєстрований більш ефективно, ніж за допомогою стандартної реєстрації.
– Оптимальне співвідношення між ціною і ефективністю. Додаткові або апаратні засоби для автентифікації або реєстрації потрібно встановлювати тільки на шлюзі прикладного рівня.
– Прості правила фільтрації. Правила на фільтруючому маршрутизаторі виявляються менш складними, ніж вони були б, якщо б маршрутизатор сам фільтрував прикладної трафік і відправляв його великому чи-

слу внутрішніх систем. Маршрутизатор повинен пропускати прикладної трафік, призначений тільки для шлюзу прикладного рівня, і блокувати весь інший трафік.

– Можливість організації великого числа перевірок. Захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, що знижує ймовірність злому з використанням "дірок" у програмному забезпеченні.

До недоліків шлюзів прикладного рівня відносяться:

– більш низька продуктивність у порівнянні з фільтруючими маршрутизаторами; зокрема, при використанні клієнт-серверних протоколів, таких як TELNET, потрібно двокрокова процедура для вхідних та вихідних з’єднань;
– більш висока вартість у порівнянні з фільтруючим маршрутизатором.

Крім TELNET і FTP шлюзи прикладного рівня зазвичай використовуються для електронної пошти, Windows і деяких інших служб.

1.11 Посилена автентифікація

Одним з важливих компонентів концепції між мережевих екранів е автентифікація (перевірка дійсності користувача). Перш ніж користувачеві буде надано право скористатися тим чи іншим сервісом, необхідно переконатися, що він дійсно той, за кого себе видає.

Одним із способів автентифікації е використання стандартних UNIX- паролів. Однак ця схема найбільш вразливе з точки зору безпеки - пароль може бути перехоплений і використаний іншою особою. Багато інциденти в мережі Інтернет відбулися почасти через уразливість традиційних паролів. Зловмисники можуть спостерігати за каналами в мережі Інтернет і перехоплювати що

передаються в них відкритим текстом паролі, тому схему автентифікації з традиційними паролями слід визнати застарілою. [7][1)]

Для подолання цього недоліку розроблено ряд засобів посиленою автентифікації: смарт-карти, персональні жетони, біометричні механізми і т.п. Хоча в них задіяні різні механізми автентифікації, загальним для них е те, що паролі, які генеруються цими пристроями, не можуть бути повторно використані порушником, що спостерігає за встановленням зв'язку. Оскільки проблема з паролями в мережі Інтернет с постійною, міжмережевий екран для з'єднання з Інтернет, не має в своєму розпорядженні засобами посиленою автентифікації або не використовує їх, втрачає всякий сенс.

Ряд найбільш популярних засобів посиленої автентифікації, що застосовуються в даний час, називаються системами з одноразовими паролями. Наприклад, смарт-карти або жетони автентифікації генерують інформацію, яку хост-комп'ютер використовує замість традиційного пароля. Результатом е одноразовий пароль, який, навіть якщо він буде перехоплений, не може бути використаний зловмисником під виглядом користувача для встановлення сеансу з хост-комп'ютером.

Так як між мережеві екрани можуть централізувати управління доступом в мережі, вони е підходящим місцем для установки програм або пристроїв посиленою автентифікації. Хоча кошти посиленою автентифікації можуть використовуватися на кожному хост-комп'ютері, більш практично їх розміщення на міжмережевому екрані. Якщо хост-комп'ютери не застосовують заходів посиленої автентифікації, зловмисник може спробувати зламати паролі або перехопити мережевий трафік з метою знайти в ньому сеанси, в ході яких передаються паролі.

У цьому випадку сеанси TELNET або FTP, що встановлюються з боку мережі Інтернет з системами мережі, повинні проходити перевірку за допомо-

---

[1)] [7] T. Aduolf, "systems, Department of technology enhanced learning information," protecting networks, vol. 1, no. University of North Carolina, p. 16, 2010.

гою засобів посиленою автентифікації, перш ніж вони будуть дозволені, Системи мережі можуть запитувати для дозволу доступу і статичні паролі, але ці паролі, навіть якщо вони будуть перехоплені зловмисником, не можна буде використовувати, тому що кошти посиленою автентифікації та інші компоненти між мережевого екрану запобігають проникнення зловмисника або обхід ними між мережевого екрану.

1.12 Основні схеми мережевого захисту на базі міжмережевих екранів

При підключенні корпоративної або локальної мережі до глобальних мереж адміністратор мережевої безпеки має вирішувати такі завдання:

- захист корпоративної або локальної мережі від несанкціонованого доступу з йоку глобальної мережі;
- приховування інформації про структуру мережі та її компонентів від користувачів глобальної мережі,
- розмежування доступу в мережу, що захищається з глобальної мережі і з мережі, що захищається в глобальну мережу.

Необхідність роботи з віддаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається. При цьому часто виникає потреба в організації у складі корпоративної мережі декількох сегментів з різними рівнями безпеки:

- вільно доступні сегменти (наприклад, рекламний WWW-сервер),
- сегмент з обмеженим доступом (наприклад, для доступу співробітникам організації з віддалених вузлів),
- закриті сегменти (наприклад, локальна фінансова мережа організації).

Для захисту корпоративної або локальної мережі застосовуються такі основні схеми організації між мережевих екранів:

- міжмережевий екран — фільтрvючий маршрутизатор;
- міжмережевий екран на основі двопортового шлюзу;

– міжмережевий екран на основі екранованого шлюзу;
– міжмережевий екран — екранована під мережа.

1.13 Міжмережевий екран — фільтруючий маршрутизатор

Міжмережевий екран, заснований на фільтрації пакетів, е поширеним і найбільш простим в реалізації. Він складається з фільтруючого маршрутизатора, розташованого між що захищається мережею і мережею Інтернет. Фільтруючий маршрутизатор налаштований для блокування або фільтрації вхідних і вихідних пакетів на основі аналізу їх адрес і портів. Комп'ютери, що знаходяться в мережі, що захищається, мають прямий доступ в мережу Інтернет, в той час як більша частина доступу до них з Інтернет блокується. Часто блокуються такі небезпечні служби, як X Windows, NIS і NFS.[8][1)]

1.14 Міжмережевий екран на базі двопортового шлюзу

Міжмережевий екран на базі двопортового прикладного шлюзу включає дводомний хост-комп'ютер з двома мережевими інтерфейсами. При передачі інформації між цими інтерфейсами і здійснюється основна фільтрація. Для забезпечення додаткового захисту між прикладним шлюзом та мережею Інтернет зазвичай розміщують фільтруючий маршрутизатор. У результаті між прикладним шлюзом та маршрутизатором утворюється внутрішня екранована підмережа. Цю під мережа можна використовувати для розміщення доступних ззовні інформаційних серверів.

[1)] [8] C. Berthelot, "Evaluation of a virtual firewall in a cloud environment," School of computing,

1.15 Міжмережевий екран на основі екранованого шлюзу

Міжмережевий екран на основі екранованого шлюзу об'єднує фільтруючий маршрутизатор і прикладної шлюз, дозволяються з боку внутрішньої мережі. Прикладної шлюз реалізується на хост-комп'ютері і має тільки один мережевий інтерфейс. [11][2)]

1.16 Міжмережевий екран — екранована під мережа

Міжмережевий екран, що складається з екранованої під мережі, являє розвиток схеми між мережевого екрану на основі екранованого шлюзу. Для створення екранованої під мережі використовуються два екрануючих маршрутизатора.Зовнішній маршрутизатор розташовується між мережею Інтернет і екранізованою під мережею, а внутрішній - між екранізованою під мережею і захищається внутрішньою мережею. Екранізована під мережа містить прикладної шлюз, а також може включати інформаційні сервери та інші системи, що вимагають контрольованого доступу. Ця схема між мережевого екрану забезпечує хорошу безпеку завдяки організації екранованої під мережі, яка ще краще ізолює внутрішню мережу, що захищається від Інтернет.

Отже можна зробити висновок наступне. На сьогоднішній день кращим захистом від комп'ютерних злочинців є брандмауер, правильно встановлений і підібраний для кожної мережі. І хоча він не гарантує стовідсотковий захист від професійних кібер злочинців, але зате ускладнює їм доступ до мережевої інформації, що стосується любителів, то для них доступ тепер вважається закритим. Також у майбутньому між мережеві екрани повинні будуть стати кращими захисниками для банків, підприємств, урядів, і інших спецслужб. Також

[2)] [11] http://wiki.kspu.kr.ua/index.php/Міжмережевий_екран#.D0.A0.D1.96.D0.B7.DO.BD.DO.BE.DO.B2.DO.B8.DO.B4.DO.BB.DO.BC.DO.B5.D1.80.DO.B5.DO.B6.DO.B5.DO.B2.DO.B8.D1.85_.DO.B5.DO.BA.D1.80.DO.BO.DO.BD.D1.96.DO.B2

е надія, що коли-небудь буде створено міжмережевий екран, який нікому не вдасться обійти. На даному етапі програмування можна також зробити висновок, що розробки по брандмауерів на сьогоднішній день обіцяють в недалекому майбутньому дуже непогані результати.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ IPTABLES, SHOREWALL

Всі інструменти і методи оцінки були детально обговорені для вимірювання продуктивності між мережевих екранів для порівняльного аналізу. Ця глава присвячена здійсненню всіх розроблених сценаріїв, включаючи конфігурацій, щоб отримати результати і прийти до висновку.

Для того, щоб зробити конфігурацію між мережевих екранів керівництва по налаштуванню малого офісу були проведені дослідження фаєрволів Iptable і Shorewall . Між мережеві екрани налаштовані відповідно до документації, доступної для них.

2.1 Опис мережі і вибір фаєрволів

В даному розділі я буду досліджувати між мережеві екрани Iptable і Shorewall, через те що ці між мережеві екрани дають високу продуктивність . Для того щоб перейти до роботи потрібна мережа. Використовуватися буде офісна мережа з виходом до Інтернет вказана на рисунку 2.1.

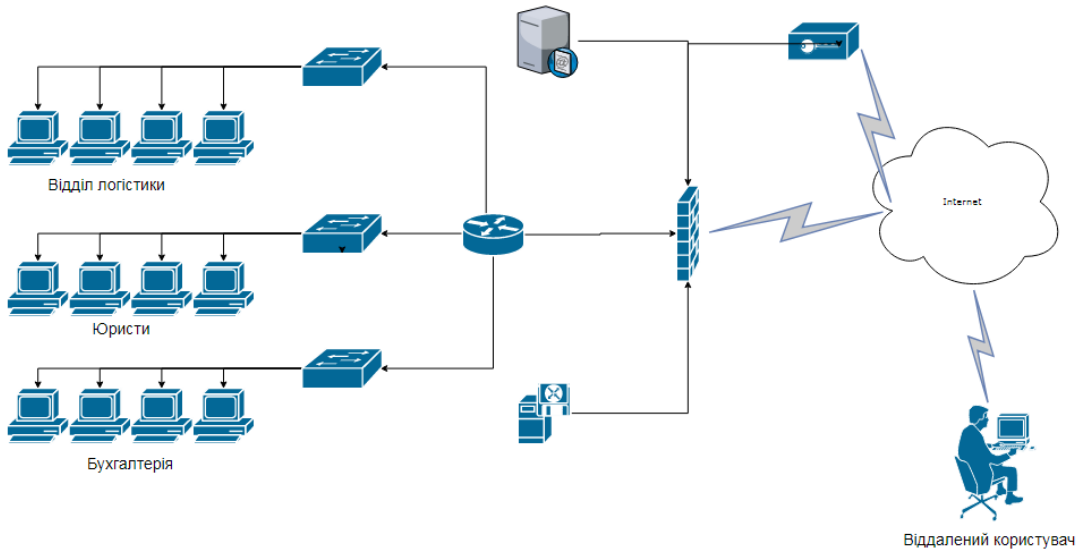

Рисунок 2.1 Офісна мережа з виходом до Інтернет

Мережа складається з 252 робочих місць, 3 комутаторів, 2 серверів, маршрутизатору та антивірусного шлюзу.

Наступним кроком буде встановлення між мережевих екранів. Котрими будуть Iptable та Shorewall.

Вибір заснований на тому що вони є найбільш продуктивні фаєрволи . Для подальшого дослідження вистачить взяти два комп'ютера з виходом до мережі Інтернет.

2.2 Установка міжмережевих екранів

Установка брандмауерів легкий крок. Оскільки обидва брандмауери можна завантажені в будь-який час з Інтернету.

2.2.1. Iptables

Система Linux встановлена на комп'ютері, тому Iptable стоїть по замовчуванням. Хоча всі настройки його не є по замовчуванням, тому всі види трафіку в будь-якому місці не допускаються. Крім того, на Ubuntu він може бути встановлений за допомогою команди, перерахованій нижче. Щоб переконатися, що брандмауер присутній в системі, використовуються наступні команди; де -1 виводить правила брандмауера і -v показує поточну версію. Установка Iptables виконується за допомогою наступної команди:

```
sudo apt-get install iptables
iptables -L
iptables -V
```

2.2.2 Shorewall

Shorewall не встановлений на системах Linux за замовчуванням. Користувач повинен завантажити та встановити його вручну з веб-сайту

shorewall.net. В Ubuntu він може бути встановлений командою, перерахованою нижче, і може бути перевірений за допомогою команд стану і версій. [9][1)]

```
sudo apt-get install shorewall
shorewall status
shorewall version
```

Після установки чи перевірки наявності фаєрволів на комп'ютерах, можна починати їх налаштування.

2.3 Налаштування між мережевих екранів

Перед початком налаштування будуть необхідні такі сервіси як: FTP, HTTP, WWW, SMTP, IMAP, Ip-телефонія.

IP-телефонія — це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відео зображень та факсів у режимі реального часу.

IMAP (англ. Internet Message Access Protocol — «Протокол доступу до інтернет-повідомлень») — мережевий протокол прикладного рівня для доступу до електронної пошти.

Simple MaiI Transfer Protocol (Простий Протокол Пересилання Пошти) — це протокол, який використовується для пересилання електронної пошти до поштового сервера або з клієнта-комп'ютера, або між поштовими серверами. FTP (File Transfer Protocol) — протокол передачі файлів, але при розгляді FTP як сервісу Інтернет мається на увазі не просто протокол, а саме сервіс-доступ до файлів у файлових архівах.

FTP — сервіс прямого поступу, що вимагає повноцінного підключення до Інтернет. Незважаючи на поширеність, FTP володіє істотними недоліками, головний з яких - відсутність простого й універсального засобу пошуку на серверах FTP.

[1)] [9]Руководство по Shorewall

Система гіпермедіа WWW (World Wide Web) — сервіс прямого доступу, що вимагає повноцінного підключення до Інтернет і дозволяє взаємодіяти з представленим на web-серверах змістом (машинна взаємодія). Це найсучасніший, зручний і перспективний сервіс мережі Інтернет.

Налаштування фаєрволів відбувається за допомогою правил, а саме правил дозволу і заборони до сервісів. Добре налаштований брандмауер може заперечувати або відкидати трафік на основі правил. Конфігурація обох брандмауерів буде відрізнятися одна від одної.

2.3.1 Iptables

Конфігурація брандмауера Iptables досить легка і проста, ніж у Shorewall. Файл конфігурації iptables.rules, знаходиться в корені/ etc / iptables.rules. Для зручності був використаний інструмент конфігурації веб системи для Linux Webmin. Це дозволило додавати, видаляти або змінювати сценарії.[10][1)] Правила зберігаються у файлі конфігурації, згаданого вище. Нижче скрипт для вирішення всіх типів трафіку.

```
#!/bin/sh
iptables –F INPUT
iptables –F OUTPUT
iptables –F FORWARD
iptables –P INPUT ACCEPT
iptables –P OUTPUT ACCEPT
iptables –P FORWARD ACCEPT
```

Команда –F — очищає весь зміст, а –P — задає прийняти політику вхідного/ вихідного ланцюга .

[1)] [10] H. Haas, "Network Address Translation," NAT, vo1. 1.0, no. Cisco Systems Inc., p. 43, 2005.

2.3.2 Shorewall

Конфігурація Shorewall не така проста, як в Iptbles, тому що, Shorewall має різні налаштування конфігурації включаючи зони, інтерфейсу, політики rules11. Всі конфігураційні файли знаходяться в кореневому каталозі / etc / Shorewall. Зони можуть бути встановлені шляхом зміни файлу зони, який знаходиться в кореневій папці / etc / Shorewall / zones.

Цей файл буде мати вигляд:

```
#ZONE TYPE OPTIONS IN OPTIONS OUT OPTIONS
#
fw firewall
net ipv4
1oc ipv4
#LAST LINE - ADD YOUR ENTRIES ABOVE REMOVE THIS ONE - DO NOT REMOVE
```

Наступний крок полягає в додаванні фізичного інтерфейсу комп'ютера в тих зонах. Зоні LOC відповідає відкритий інтерфейс який буде відображати чисту зону. Команда (Ifconfig) Linux була використана, щоб переконатися, що eth1 це фізичний інтерфейс комп'ютера. Інтерфейс встановлюється відповідно з комп'ютерною системою.

```
#ZONE INTERFACE BROADCAST OPTIONS
neteth1 detect
loc lodetect
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Файл політики Shorewall визначить, які є правила за замовчуванням для брандмауера. Для того, щоб встановити політику, файл політики повинен бути відрегульований. Він розташований в корені / etc / Shorewall / policies. Відповідно до політики файл тестових сценаріїв встановлений, як показано нижче:

```
#SOURCE DEST POLICY LOG LEVEL LIMIT:BURST CONNLIMIT:MASK
Fw net ACCEPT
Fw loc ACCEPT
Net fw ACCEPT
```

```
Loc fw ACCEPT
net all DROP info
# THE FOLLOWING POLICY MUST BE LAST
all all REJECT info
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Створення правил був остатнім кроком для конфігурації Shorewall. Правила розповідають брандмауеру, що робити з конкретним проханням. Файл правило також знаходиться в/ etc / Shorewall / rules. Нижче вказані правила, які дозволяють весь трафік.

```
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/ MARK
PORT  PORT(S)    DEST  LIMIT      GROUP
ACCEPT net       fw    all
ACCEPT fw  net   all
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Як було сказано раніше, з веб-програмним забезпеченням конфігурації системи Webmin настроювати легше і простіше тому воно було застосоване і для Shorewall. Після налаштування всіх файлів, сервер готовий до використання.

Отже після налаштування двох фаєрволів за правилами час робити дослідження і згодом порівнювати їх, для того щоб вибрати один фаєрвол для офісної мережі.

2.4 Пропускна здатність

Пропускну здатність було проведено перевіркою Netperf. Netperf посилає TCP або UDP потік на вказану IP-адресу, на яку встановлено брандмауер. [11] Пропускна здатність UDP розраховується за таким же методом шо і TCP, за винятком UDP STREAM. За допомогою Netserver було отримано трафік від клієнта. Нижче показано команди, використані для запуску Netperf на серверних і клієнтських хостах.

```
Server (IP: 194.47.155.156)
```

```
root@labcomputer:# netserver
Starting netserver with host 'IN(6)ADDRANY' port '12865' and family
AF UNSPEC
Client
root@labcomputer :# netperf -l 30 -t TCP_STREAM –H 194.47.155.156
-S 16K -m 64
MIGRATED TCP STREAM TEST from 0.0.0.0 0 port 0 AF INET to
194.47.155.156 ( )
port 0 AF_INET
Recv Send Send
Socket Socket Message Elapsed
Size Size Size Time Throughput
Bytes bytes bytes secs. 10^6bits/sec
32768 32768 64 30.00 605.06
```

У Netperf опція клієнта -1 використовується, щоб вказати тривалість часу, який триває до 30 секунд; -t вказує, що буде TCP трафік, -H дає можливість вказати IP-адрес сервера, -s чекає 26 секунд між тестом і запуском перевірки, який є при відправці байта розміру гнізда; -S Встановлено SO_KEEPALIVE який може побачити в отриманих байтах розмір гнізда ; -m використовується для зміни розміру пакета в байтах. У наведеному випробуванні розмір пакета встановлено 64 байт.

```
Server (IP: 194.47.155.157)
root@labcomputer:# netserver
Starting netserver with host 'IN(6)ADDR ANY' port '12865' and
family AF UNSPEC
Client
root@labcomputer:# netperf -1 30 -t UDP STREAM -H 194.47.155.157 -
s
16384 -S 16K -m 512
MIGRATED UDP STREAM TEST from 0.0.0.0 () port 0 AF INET to
194.47.155.157 () port 0 AF_INET
Socket Message Elapsed Messages
Size Size Time Okay Errors Throughput
```

```
Bytes bytes secs       #   #   10^6bits/sec
32768 512 30.00  3955459   0   540.05
32768     30.00  2287221       312.28
```

Вище показано пропускний розрахунок UDP. UDP розмір пакета пропускної спроможності встановлений в 512 байт. Графічне представлення результатів обговорюється в наступному розділі.

2.5 Затримка

Тест затримки виконувався за допомогою Netperf. Функція запиту / відповіді з Netperf вже докладно розрахувала затримку. Команди тестування затримки брандмауерів наведені нижче. Розрахунок затримки UDP є таким самим, як TCP, за винятком того, що UDP_RR Netperf буде генерувати UDP трафік.

```
Server (IP: 194.47.155.156)
root@labcomputer:# netserver
Starting netserver with host 'IN(6)ADDR ANY' port '12865' and
family AF_UNSPEC
Client
root@labcomputer:# netperf -H 194.47.155.156 -1 30 -t TCP_RR -- -
r64,1024
MIGRATED TCP REQUEST/RESPONSE TEST from 0.0.0.0 () port 0
AF INET to 194.47.155.156 () port 0 AF INET : first burst 0
Local /Remote
Socket Size Request Resp. Elapsed Trans.
Send Recv Size Size Time Rate
bytes Bytes bytes bytes secs. per sec
16384 87380 64 1024 30.00 6650.46
16384 87380
```

Команда -H використовується, щоб вказати IP-адресу сервера; -l дає інформацію про тривалість часу випробування; -t TCP_RR показує, що використовується функція запит/відповідь в TCP; -r використовується для зміни розміру запиту / відповіді.

```
Server (IP: 194.47.155.156)
root@labcomputer:# netserver
Starting netserver with host 'IN(6)ADDR ANY' port '12865' and
family AF_UNSPEC
Client
root@labcomputer:# netperf -T 1 -H 194.47.155.156 -l 30 -t UDP_RR
-r32,1024
MIGRATED UDP REQUEST/RESPONSE TEST from 0.0.0.0 () port 0
AF INET to 194.47.155.156 () port 0 AF INET : first burst 0 :
cpu bind
Local /Remote
Socket Size Request Resp. Elapsed Trans.
Send Recv Size Size Time Rate
bytes Bytes bytes bytes secs. per sec
112640 112640 32 1024 30.00 7284.23
112640 112640
```

В UDP команда -T використовується, щоб переконатися, що Netperf і Netserver швидко пересувається на даному процесорі. На малюнку вище розмір запит / відповідь зводиться до 32/1024 байт.[12][1)] Результати обох брандмауерів TCP і UDP затримки обговорюється в наступному розділі в графічному форматі з затримкою кількості транзакцій в секунду оцінюється по осі ординат і кількості правил фільтрації по осі абсцис.

[1)] [12] http://digincore.org/index.php/dokumentatsiya/ur1-digincore-ubuntu/iptables

2.6 Оцінка установки з'єднання

Метод розрахунку швидкості установки з'єднання через функцію Netperf TCP_CRR вже зрозуміло. Команда Netserver говорить, що сервер повинен бути запущений разом з брандмауером. Команда -H використовується, щоб вказати IP-адресу сервера; -l показує тривалість тесту, в даному випадку він зберігається протягом 60 секунд; -t стверджує, що це підключення/ запит / функції TCP відгуку; -r використовується для зміни розміру запит/ відповідь, який зберігається в 32/1024.

```
Server (IP: 194.47.155.157)
root@labcomputer:# netserver
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and
family AF_UNSPEC
Client root@labcomputer:# netperf -H 194.47.155.157 -1 60 -t
TCP_CRR ---r32,1024
MIGRATED TCP Connect/Request/Response TEST from 0.0.0.0 () port 0
AF INET to 194.47.155.157 () port 0 AF INET
Local /Remote
Socket Size Request Resp. Elapsed Trans.
Send  Recv  Size  Size  Time  Rate
bytes Bytes bytes bytes secs. per sec
16384 87380 32    1024  60.00 3180.55
16384 87380
```

2.7 Оцінка швидкості заборони.

Для розрахунку швидкості заборони з'єднання використовується Netperf. Застосовуючи ті ж команди, розраховано швидкість встановлення з'єднання, а швидкість з'єднання демонтажу розраховується винятком, Netperf і TCP / закриття / підключення тестом. Нижче можна побачити результат.

```
Server (IP: 194.47.155.156)
root@labcomputer:# netserver
```

```
Starting netserver with host 'IN(6)ADDR_ANY' port '12865' and
family AF_UNSPEC
Client
root@labcomputer:# netperf -H 194.47.155.156 -1 60 -t TCP_CC ---
r32,1024
TCP Connect/Close TEST from 0.0.0.0 () port 0 AF INET to
194.47.155.156 () port 0 AF INET
Local /Remote
Socket Size Request Resp. Elapsed Trans.
Send   Recv Size    Size  Time    Rate
bytes  Bytes bytes  bytes secs.   per sec
16384  87380 32     1024  60.00   4273.89
16384  87380
```

2.8 Швидкість передачі HTTP

Щоб розрахувати швидкість передачі HTTP було змінено інструменти на: Iperf, Nmap і HTTPing. Команда -s Iperf використовується для запуску його в якості сервера, на якому брандмауер налаштований. Команда -c вказує IP-адресу сервера, який буде підключений до клієнта; -1 змінює розмір пакета, в цьому випадку команда передає 512 байт пакета на сервер; -t використовується для тривалості часу випробування.

```
Server (IP: 194.47.155.157)
root@labcomputer:# iperf -s
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
Client
root@labcomputer:# iperf -c 194.47.155.157 -1 512 -t 65
Client connecting to 194.47.155.157, TCP port 5001
TCP window size: 16.0 KByte (default)
[ 3] local 194.47.155.160 port 49724 connected with 194.47.155.157
port 5001
[ID] Interval Transfer Bandwidth
```

```
[ 3] 0.0-65.0 sec 2.14 GBytes 282 Mbits/sec
```

Команди показані вище для того щоб переконатися, що HTTP-сервер, що працює на між мережевому екрані, перевіряється командами Nmap.

```
Client (Nmap)
root@labcomputer:# nmap 194.47.155.157
Starting Nmap 5.00 ( http://nmap.org ) at 2012-09-27 09:04 CEST
Interesting ports on compc-2412-08.comlab.bth.se (194.47.155.157):
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcpopen ssh
80/tcpopen http
10000/tcpopen snet-sensor-mgmt
MAC Address: 00:19:B9:20:C6:C2 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

HTTPing використовується для відправки пінга брандмауера після перевірки веб-сервера HTTP на порту 80; -G опція використовується для відправки запиту GET; -b покаже швидкість передачі в кбіт / с; -g використовується, щоб вказати URL-адресу, це може бути IP-адреса; -c дозволяє кілька разів з'єднатися.

```
Client (HTTPing)
root@labcomputer:# httping -G -b -g http://194.47.155.157 -c 60
PING 194.47.155.157:80 (http://194.47.155.157):
connected to 194.47.155.157:80, seq=0 time=1.29 ms 206554KB/s
connected to 194.47.155.157:80, seq=1 time=1.21 ms 157269KB/s
Continued...
connected to 194.47.155.157:80, seq=58 time=1.15 ms 317647KB/s
connected to 194.47.155.157:80, seq=59 time=1.50 ms 2219KB/s
--- http://194.47.155.157 ping statistics ---
60 connects, 60 ok, 0.00% failed
round-trip min/avg/max = 1.1/1.5/4.1 ms
Transfer speed: min/avg/max = 2219/224093/321235 KB
```

Результат цієї метрики тесту обговорюється в наступному розділі. Де вісь по осі абсцис представлятиме мінімальну швидкість передачі і кількість правил фільтрації.

2.9 Споживання системних ресурсів

Для того, щоб побачити, який брандмауер споживатиме більше системних ресурсів в Linux є (SAR). Утиліта яка використовується для відображення середнього ЦП і ОЗУ під час руху. Для обидвох брандмауерів застосована велика кількість правил, щоб побачити їх поведінку і зробити порівняння між ними. [13][1)]

Характеристики комп'ютерів одинакові. На фрагменті коду нижче відображений метод обчислення ЦП і ОЗУ протягом 30 секунд. Команда показує використання в кожну секунду і відображає середнє значення використання після закінчення часу.

На малюнку опція -u відображає всі показники використання CPU протягом 30 секунд; -r показує статистику використання пам'яті. Досліди обох брандмауерів зберігаються на обох комп'ютерах в текстовому файлі для того, щоб можна було оцінити який з мережевих екранів е кращим.

```
Linux [sar] command
root@labcomputer:#       sar       –u       1       30       >>
/home/student/Documents/sar_cpu_shorewall_1000
root@labcomputer:#       sar       –r       1       30       >>
/home/student/Documents/sar_rnem_shorewall_1000
```

Пропускна здатність, швидкість затримки, встановлення з'єднання і розрив показали, що кількість правил фільтрації чинять негативний вплив на продуктивність Iptables брандмауер на відміну від Shorewall. Так як обидва міжмережеві екрани не можуть виявити повторювані правила. Міжмережеві екрани обробили правила зверху вниз. Порядок правил, в якому вони записані

[1)] [13] http://pro-spo.ru/linux-for-beginner/1576--iptables-

також важливий. Обидва брандмауери показують, що малі розміри пакетів не впливають на продуктивність брандмауера. Shorewall добре зарекомендував себе при навантаженнях.

РОЗДІЛ 3. ПОКРАЩЕННЯ ФуНКЦІОНАЛЬНОГ0 ЗАХИСТУ МЕРЕЖІ

За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або зловмисних програм (наприклад хробаків) через мережу або Інтернет. Крім того, брандмауер запобігатиме надсиланню зловмисних програм із вашого комп'ютера на інші.

Всі інструменти і методи оцінки були детально обговорені для вимірювання продуктивності між мережевих екранів для порівняльного аналізу. Ця глава присвячена здійсненню всіх розроблених сценаріїв, включаючи конфігурацій, щоб отримати результати і прийти до висновку. [14][1)]

Проводячи експеримент над Iptable і Shorewall було вияснено що Shorewall дає більш високу продуктивність, ніж Iptables, коли число правил фільтрації збільшуються. Обидва брандмауери піддавалися аналогічних випробувань, на додаток з специфікації системи, ряд правил, дизайну і методів. Тим не менш, конфігурація Shorewall відрізняється від Iptables.

Shorewall є гнучкою програмою і ділить вхідні пакети на різні категорії. Це дозволяє користувачеві встановити інтерфейс, який є на цій машині.

Shorewall може використовуватися на спеціалізованій системі брандмауера і на окремій системі GNU / Linux. Shorewall не використовує режим сумісності IP ланцюг NETFILTER і, таким чином, не дає скористатися перевагами державних з'єднань можливостей відстеження NETFILTER, які потім призводить до більш високої продуктивності в мережі .[15][2)]

В нашому випадку для потреб підприємства необхідно створити орієнтовано 2500 правил. Окремо слід відокремити демілітаризовану зону з публічно доступними серверами.

[1)] [14] А. Астахов. Анализ защищенности корпоративных автоматизированных систем / А. Асгахии. — Москва, 2010.

[2)] [15] Лукацкий А.В. Как работает сканер безопасности / Лукацкий А.В. - Hackzone, 2009.

Тому захисту своєї мережі я вибрав Shorewall бо він більш практичний і дає високу продуктивність.

3.1 Пропускна здатність

У будь-якій мережі, максимальна пропускна здатність дорівнює швидкості передачі даних, підтримуваної NIC, яка визначає теоретичну базову як 1000 Мбіт. Але на практиці ці теоретичні цифри не досяжні через різні чинники, в мережевих умовах. Результати обох брандмауерів показують, що менші розміри пакетів мають меншу пропускну здатність, ніж більші. Крім того збільшення правила фільтрації не впливає на менший розмір пакета взагалі. На рис. 3.1.1 зображено TCP пропускну спроможність Iptables брандмауера.

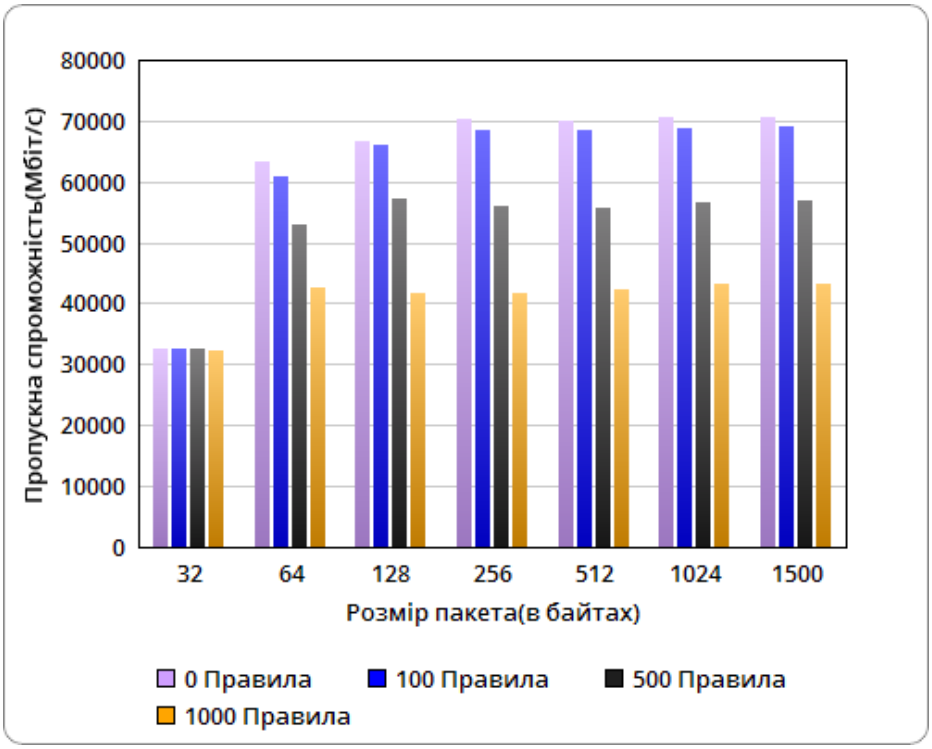

Рисунок 3.1.1: Пропускна спроможність Iptables TCP

UDP є протоколом, який визначає, як сформувати повідомлення, відправлені протягом IP. Пристрій, який посилає UDP-пакети припускає, що вони

досягають місця призначення. Там немає механізму, щоб повідомити відправнику, що пакет прибув. Це звичайно використовується для потокових мультимедіа додатків, в яких іноді втрата пакетів не має значення.

Результати Iptables брандмауер показують, що UDP-трафіку не залежить від кількості правил брандмауера. Менші розміри пакетів мають більш низький рівень пропускної спроможності і більше дає більш високу пропускну здатність. Тим не менш, на 1 кілобайт пакета він дав максимальну пропускну здатність, яку можна побачити з малюнка. Цей рівень знизився в 1,5 кілобайта пакету. Тест UDP_STREAM не має ніякого контролю потоку з кінця в кінець. [16][1)] Найбільший з цих наслідків це дані, при посиланні яких не можна буде отримати за допомогою приймача. На деяких платформах це може бути можливим. Для відправки, пропускну спроможність слід розглядати, як величину більшу, ніж максимальна швидкість лінії зв'язку. Це поширене тоді, коли процесор швидший, ніж мережі, і немає ніякого контролю потоку.

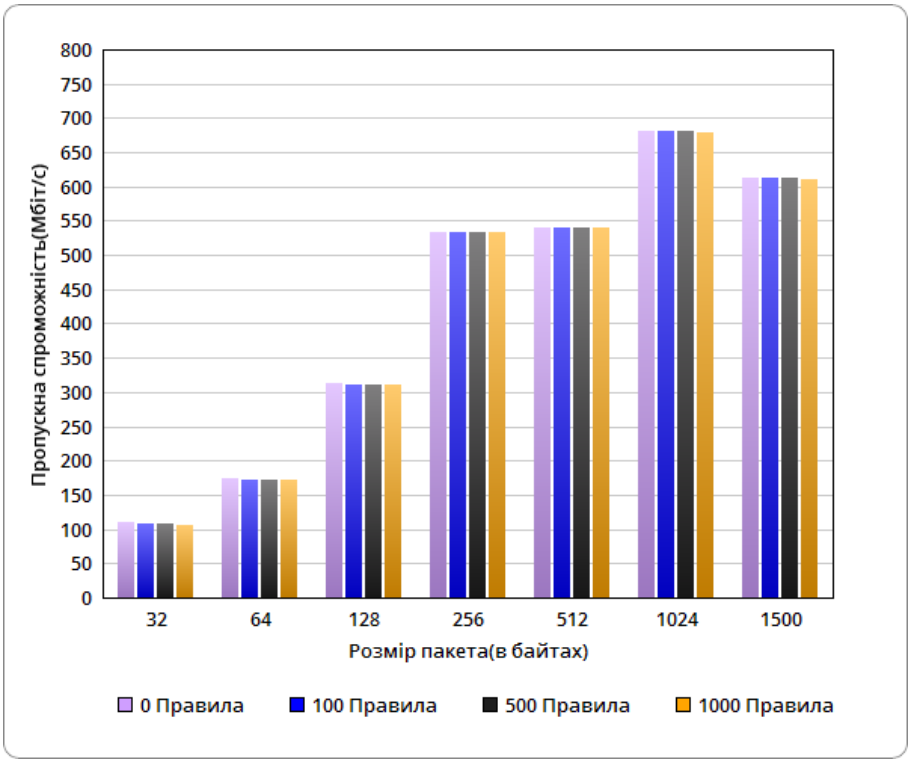

Рисунок 3.1.2: Пропускна спроможність Iptables UDP

[1)] [16] А. Астахов. IDS как средство управления рисками / А. Астахов : [Електронный ресурс]. — Режим доступу : URL http://www.globaltrust.ru/security/Pubs/Pub2part5. — Назва з екрану.

Все більше число правил фільтрації на брандмауерах, важливо визначити впливом на продуктивність. Брандмауери змушені перевіряти кожен пакет проти своїх правил; Це також відображається на роботі брандмауера під час годин пік, коли є багато навантаження на брандмауери у зверненні. Це добре видно з результатів TCP і UDP пропускної спроможності, що протокол TCP передає більше даних, у порівнянні з UDP. Загалом, UDP швидший, ніж TCP. TCP підтверджує набір пакетів, розрахованих з використанням розміру вікна TCP і туди-назад (RTT).

У цьому експерименті, TCP і UDP розміри вікон які були такі і можуть бути чітко видно з реалізації. Крім того, розмір вікна TCP і UDP також в процесі передачі різних пакетів. Причина більш пропускної спроможності TCP в тому, що TCP буфер даних заповнює сегмент мережі. Таким чином, більш ефективне використання доступної смуги пропускання. З іншого боку UDP ставить пакет в мережі, таким чином, відразу з'їдає весь мережевий трафік з великою кількістю невеликих пакетів.

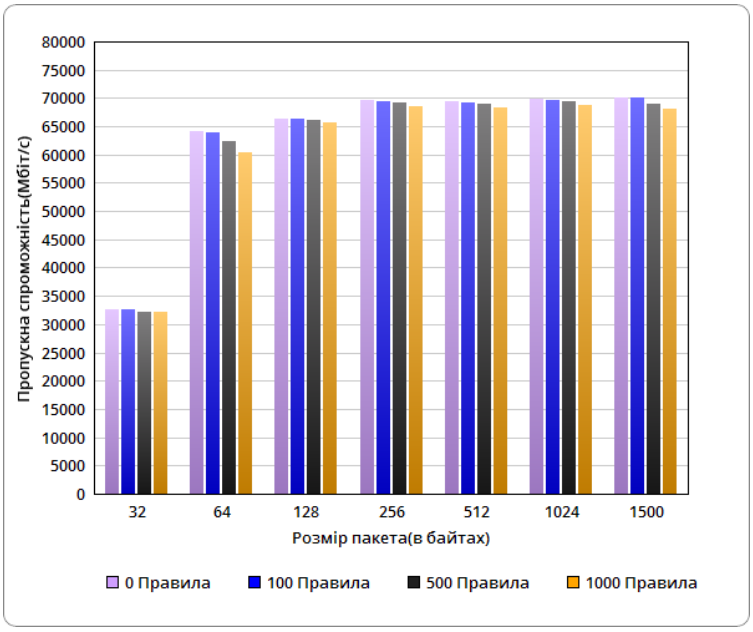

Рисунок 3.1.3: Пропускна спроможність Shorewall TCP

Рис. 3.1.3 показує пропускну спроможність TCP Shorewall. Продуктивність TCP Shorewall пропускна спроможність не розглядають на відміну з Iptables, хоча це було схоже випробування для обох брандмауерів. Велика різниця в обох між мережевих екранів пропускна спроможність . У 32 байт розмір пакета обидва брандмауери дають майже однакові результати. Але, ситуація змінюється, коли розмір пакета збільшується 64 байт тоді правила фільтрації є 1000.

Після порівняння обох результатів брандмауера, можна бачити, що Iptables погіршив свою ефективність, коли збільшилась кількість правил фільтрації, в той час як продуктивність Shorewall не піддалась впливу великої кількості правил фільтрації. Результат пропускної здатності Shorewall UDP схожий на пропускну Iptables UDP в якому чітко вказується, що UDP не залежить від кількості правил або типу брандмауера.

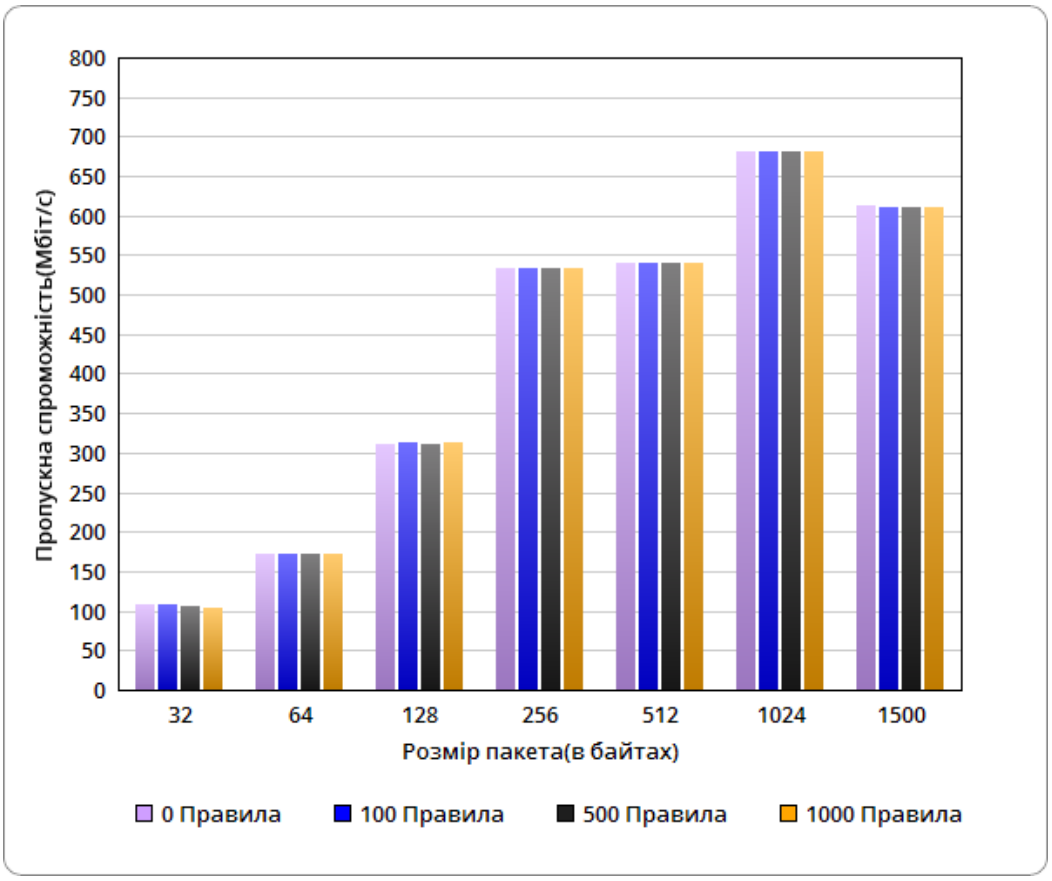

Рисунок 3.1 .4:Пропускна спроможність Shorewall UDP

3.2 Затримка

Затримка міжмережевих екранів вимірюється функцією запиту / відповіді Netperf. Чим більше розмір запиту / відповіді, тим нижче швидкість виконання транзакцій стає у брандмауера.

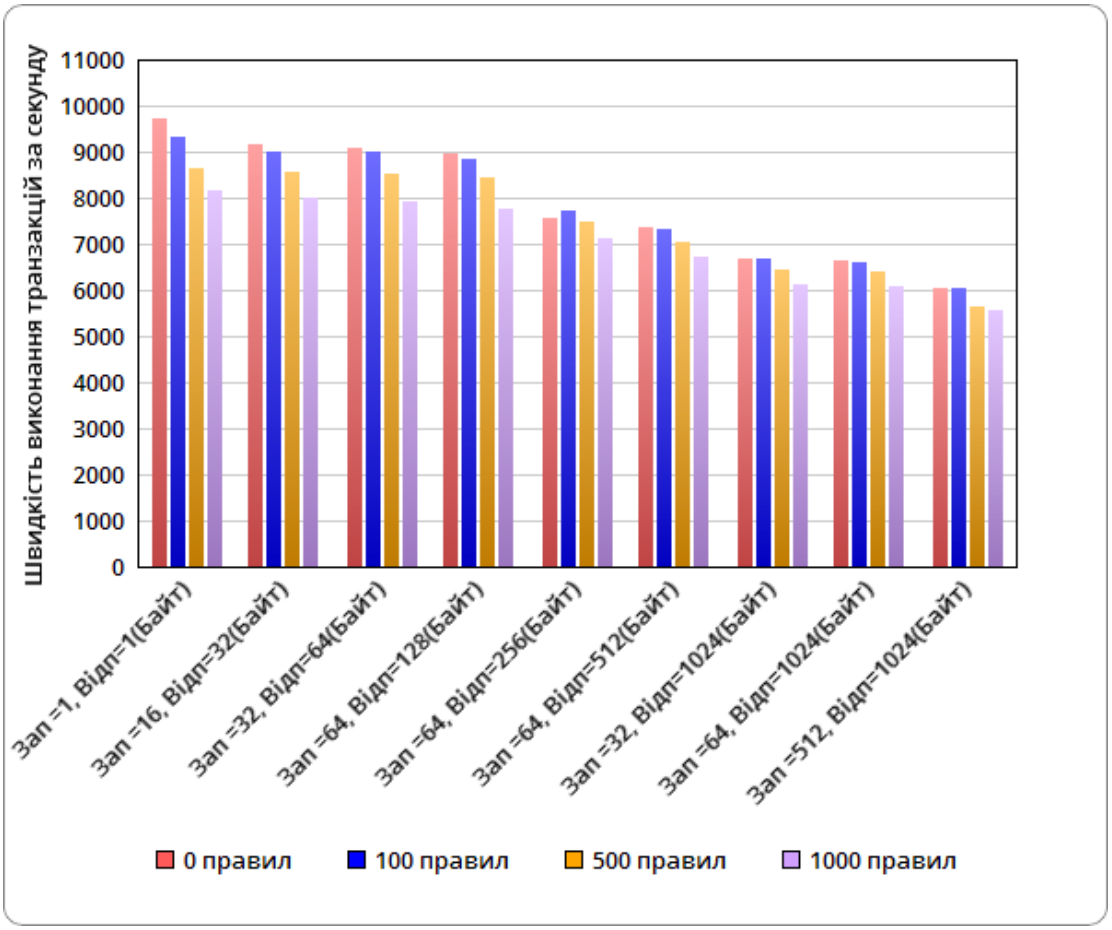

Рисунок 3.2.1: Затримка TCP Iptables

Результати показують, якщо ряд правил фільтрації збільшуються на брандмауерах є невелике зниження швидкості транзакцій, що доводить, що продуктивність деградує якщо правила збільшується.

Оскільки відправник пакетів UDP не вимагає яких-небудь знань про те, що місце отримало пакети, то UDP є відносно несприйнятливим до латентності. Єдиний ефект, що латентність на UDP потоці підвищена то відбувається затримка усього потоку. Правила фільтрації на брандмауері також вплинули на результати латентності UDP, тоді як в UDP правил фільтрації пропускна спроможність не впливає на продуктивність всіх брандмауерів. Важливо відзначити, що затримки та пропускна спроможність повністю незалежні з UDP трафіку. Іншими словами, якщо затримка йде вгору або вниз, UDP пропускна спроможність залишається та ж сама. Ця концепція має більше сенсу про вплив затримки на TCP-трафік.

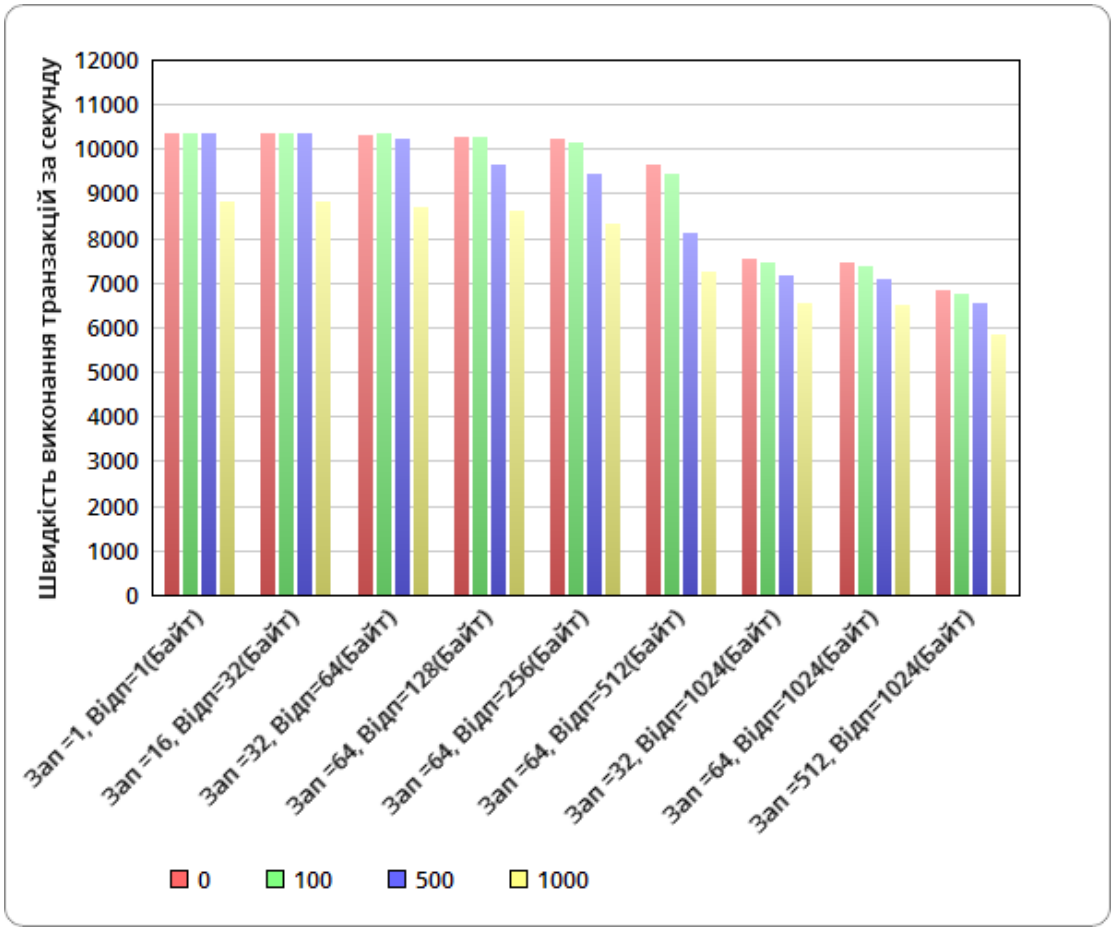

Рисунок 3.2.2: Затримка UDP Iptables

Затримка Shorewall TCP показує, що не затримує рух на відміну від Iptables, який може бути укладений після перегляду обох результатів. Швидкісна угода Shorewall ліпша ніж Iptables, яка показує, що це більш ефективно, ніж Iptables. На рис. 3.2.3 показано затримку Shorewall TCP. Менший запит / розмір реагування не впливає на кількість правил фільтрації на Shorewall, які можна побачити з малюнка. Беручи до уваги, що це не справа в Iptables. Зроблено висновок після аналізу результатів.

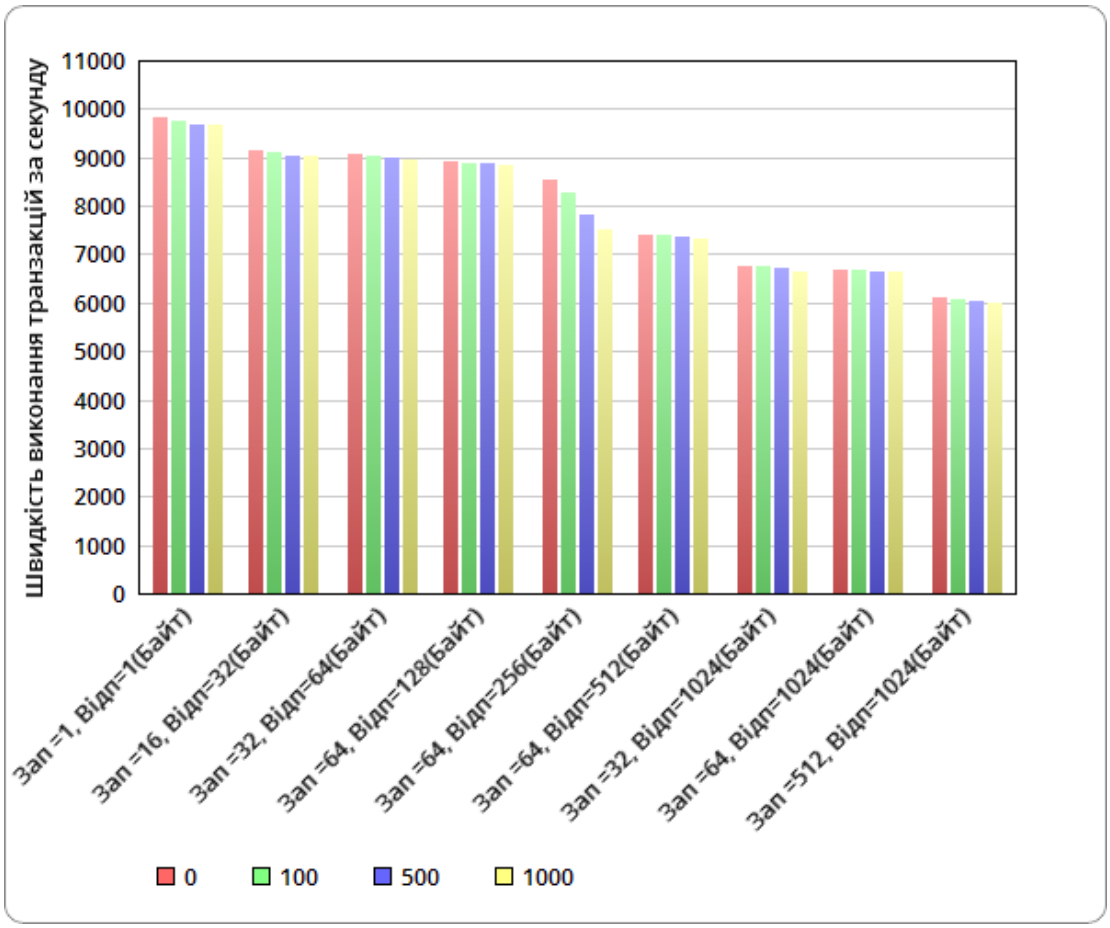

Рисунок 3.2.3:Затримка TCP Shorewall

Там немає ефекту затримки на передавальному пристрої з UDP-трафіку. Shorewall виконується краще в UDP-трафіку, а також в TCP. Зроблено висновок після аналізу результатів. Shorewall обробляє трафік добре, з великою кількістю правил фільтрації.

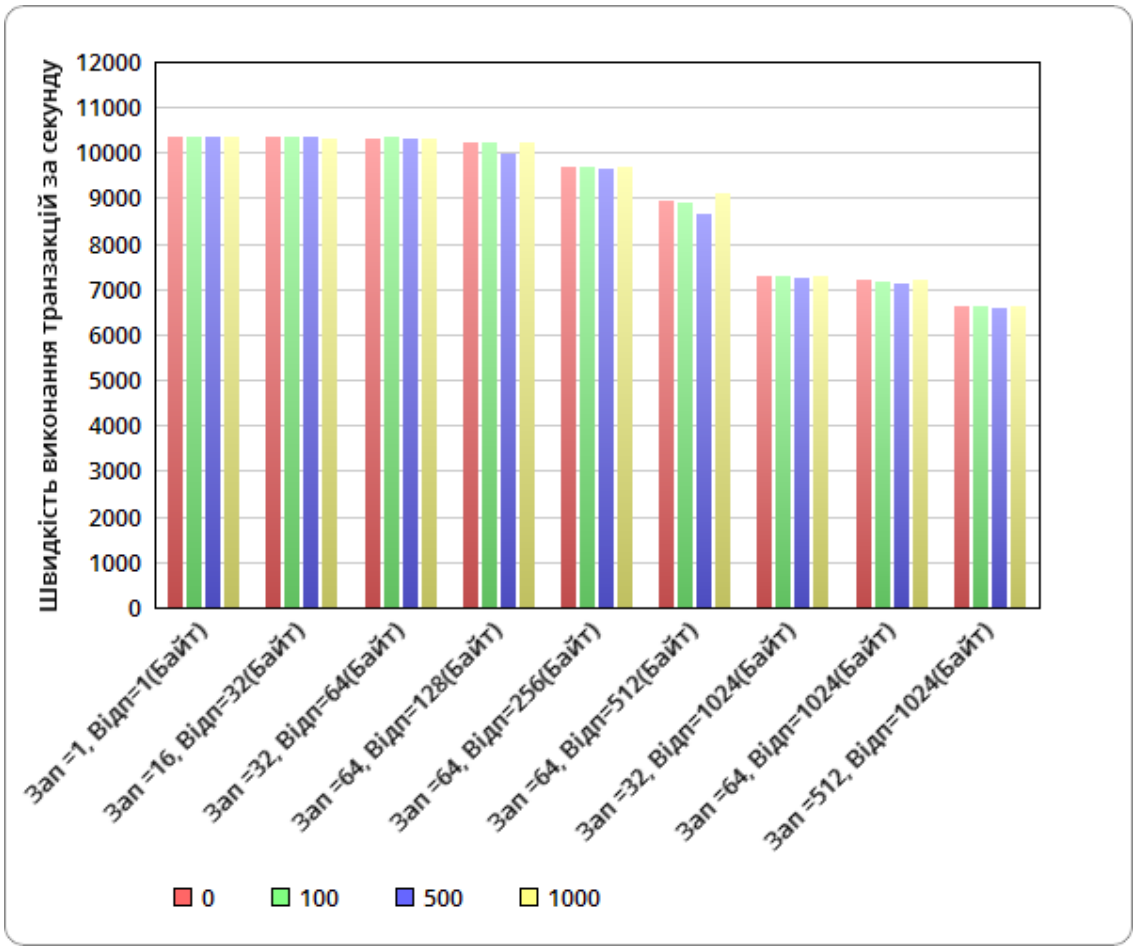

Рисунок 3.2.4:Затримка UDP Shorewall

3.3 Оцінка установки з'єднання і розрив.

Встановлені з'єднання TCP і швидкість демонтажу розраховуються за Netperf.

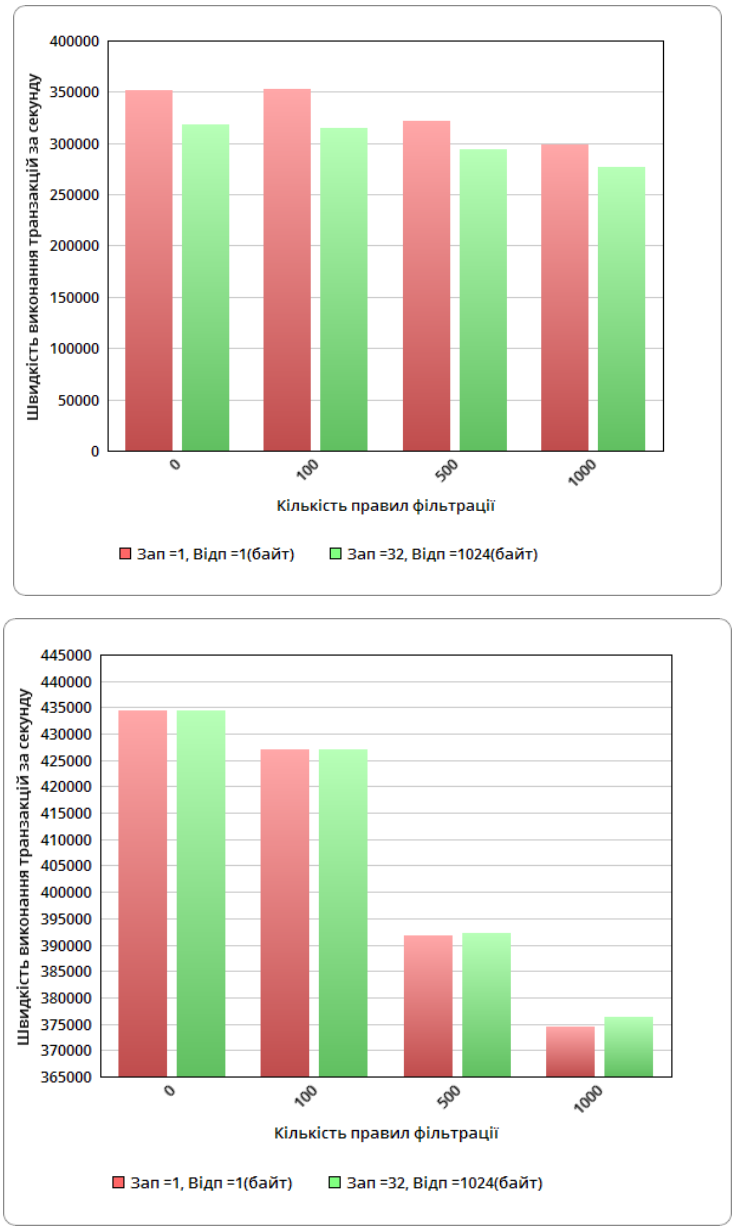

Рисунок 3.3.1: Iptables (підключити / запит / відповідь) і(підключити / закрити)

Значення запит/відповідь важливі завдяки швидкості передачі, де великі значення, отримані за низької швидкості транзакцій в секунду, а менші значення зберегли короткий час передачі. У цьому тесті, типовий запит/відповідь розміром 1/1 і 32/1024 використовується, щоб побачити ефект відкриття /з'єднання/закриття.

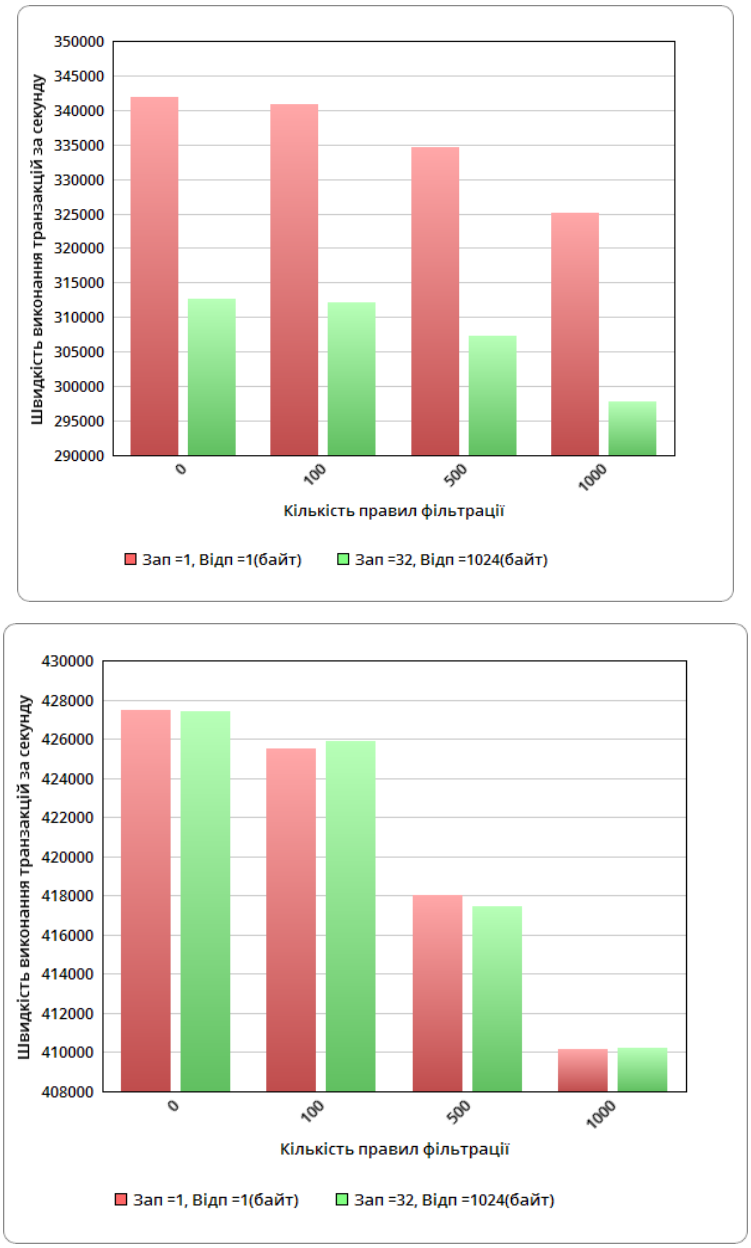

Рисунок 3.3.2: Shorewall (підключити / запит / відповідь) і(підключити / закрити)

Результати показують, що, є збільшення кількості правил фільтрації на обох брандмауерах коли знижена інтенсивність транзакцій, які укладають правила фільтрації на продуктивність брандмауера. Оскільки повинні перевірити кожен пакет, що надходять ззовні це є проти правил, які зберігаються в його конфігураційний файл для прийняття будь-якого рішення. На додаток до цього, існує значні зміни в продуктивності обох брандмауерів, коли є 1000 пра-

вил фільтрації в швидкості демонтажі з'єднання. Швидкість виконання транзакцій зменшується майже до половини в порівнянні від тоді, коли не було ніяких правил фільтрації, які можуть бути добре видно з графіків обох брандмауерів.

Результати показують, що Shorewall працює краще, ніж Iptables при встановлені і демонтажу з'єднання TCP.

3.4 Швидкість передачі HTTP

HTTPing використовується для відправки 60 пінг GET запитів обох брандмауерів. Це можна спостерігати за результатами графіку нижче, як є різке зниження у Iptables, коли кількість правил фільтрації стала 500.

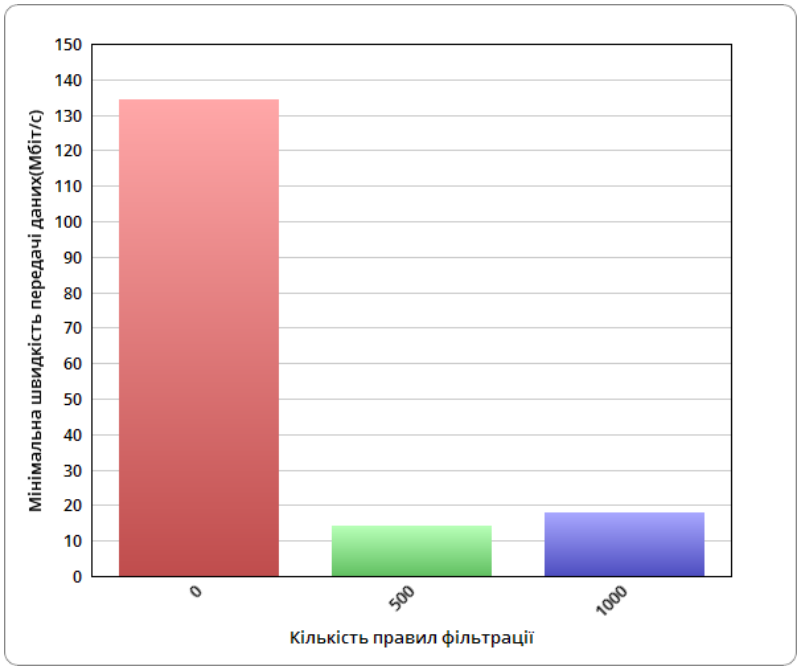

Рисунок 3.4.1: Швидкість передачі HTTP Iptables

Правила фільтрації також впливають на швидкість передачі HTTP в Shorewall, але не в порівнянні з Iptables, який різко дає погані результати при 500 правилах. Ще раз результати показали, що Shorewall працює краще, в цьому випадку, не знижуючи продуктивності різко. Отримані результати можуть бути видно на рис. 3.4.2.

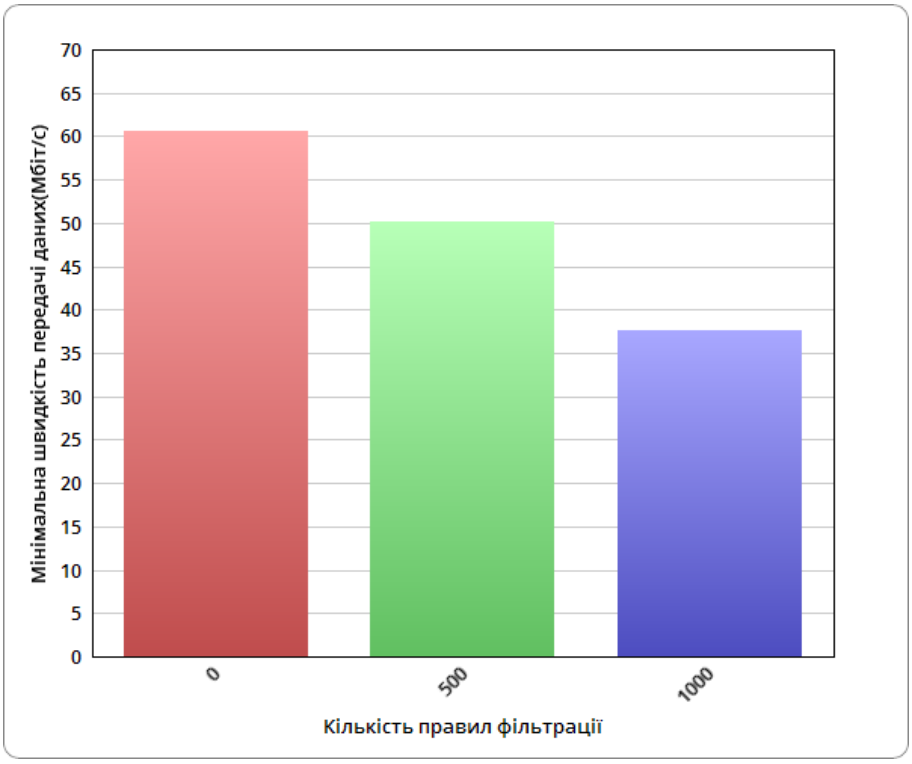

Рисунок 3.4.2: Швидкість передачі HTTP Shorewall

3.5 Споживання системних ресурсів

Linux (SAR) утиліта використовується для запису пам'яті і процесора споживання. Результат показує, відмінності брандмауерів. Існує невелика зміна в результатах використання процесора Shorewall, який можна побачити з графіків. Тим не менш, Shorewall споживає менше пам'яті порівняно з Iptables.

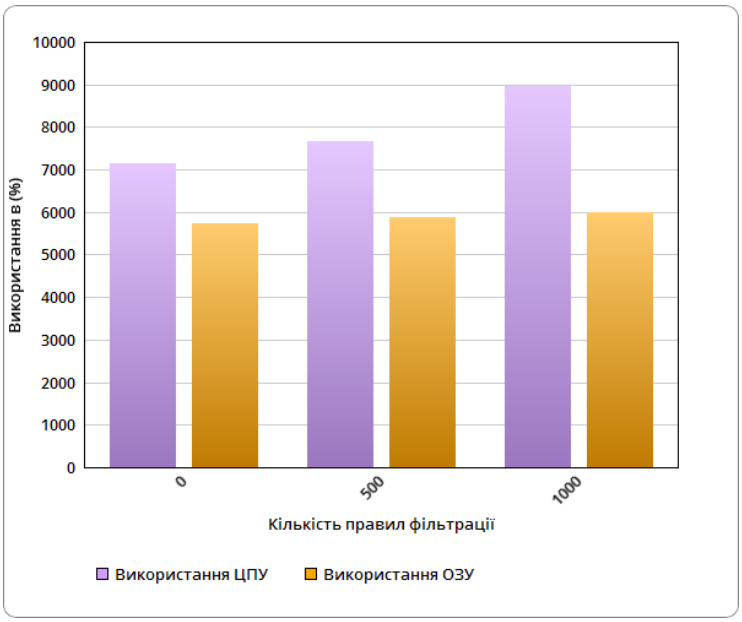

Рисунок 3.5.1: ЦПУ / ОЗУ Iptables

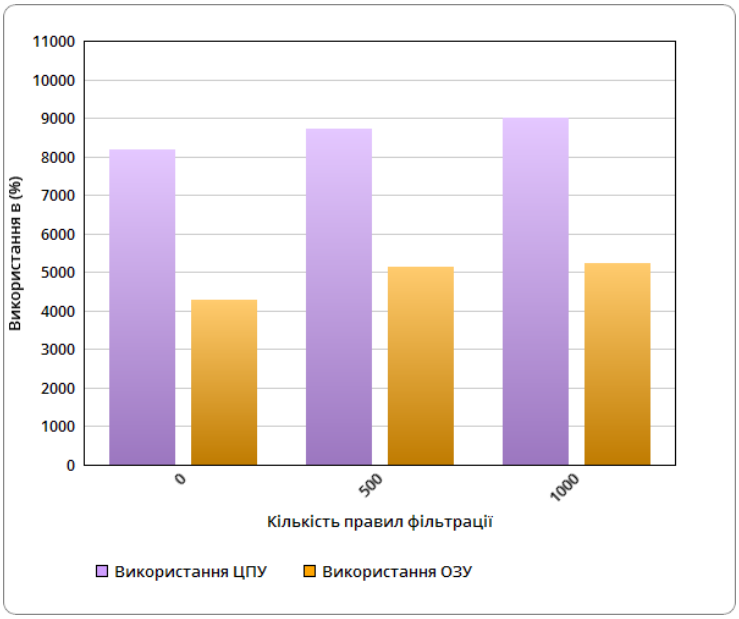

Рисунок 3.5.2: ЦПУ / ОЗУ Shorewall

Існує невелика зміна у використанні процесора, коли правила були 1000 на обох брандмауерах, але в 500 правил є незначні зміни в результатах.

Як вже зазначалося в конструкціях і методах розділу, системні вимоги, також мають значення в даному випадку. Таким чином обидва брандмауери розділяють майже рівну кількість системних ресурсів, але Shorewall споживає трохи більше CPU ніж Iptables і забезпечує більш високу продуктивність.

3.6 Покращення результатів Shorewall

В даних пунктах мова буде йти про налаштування між мережевого екрану а саме Shorewall під мережу малого офісу .

3.6.1 Базова настройка

Центральною концепцією при налаштуванні Shorewall є зона — логічна одиниця, яка об'єднує в собі однорідні (з точки зору доступу) вузли мережі. Класичними прикладами зон є локальна мережа, Інтернет і демілітаризована зона DMZ. Як правило, зони відображаються на мережеві інтерфейси за принципом 1:1, хоча подібний підхід жодним чином не нав'язується. [17][1)] Обмін трафіком між зонами контролюється так званими політиками. Природно, його можна дозволити (ACCEPT), заборонити (DROP) або відхилити (REJECT). В останньому випадку відправник отримає відповідне повідомлення (RST для TCP або ICMP Unreachable для інших протоколів). Тонка настройка проводиться за допомогою правил, що представляють собою виключення з раніше заданою політикою (наприклад, для пари зон "DMZ-локальна мережа" має сенс встановити політику DROP, але дозволити з'єднання з конкретними системами за певними протоколами прикладного рівня). Таким чином, настройка Shorewall в простому випадку зводиться до наступних кроків (тут і далі передбачається, що загальним коренем для конфігураційних файлів програми є / etc / shorewall; це значення може бути перевизначене параметром CONFIG_PATH в головному конфігураційному файлі /etc/shorewall/shorewall.conf):

- Визначити зони в/ etc / shorewall / zones.
- Поставити політику обміну трафіком між кожною парою зон в/ etc / shorewall / policy.

---

1) [17] А. В. Соколов. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. — 656с.

– Вказати "списковий склад" зон в/ etc / shorewall / interfaces і (в більш складних випадках / etc / shorewall / hosts). [18][1)] В принципі, призначення / etc / shorewall / interfaces більш широке, ніж може здатися з попереднього речення.
– Налаштувати правила пакетної фільтрації в/ etc / shorewall / rules.
– Опціонально: якщо в локальній мережі використовуються не маршрутизуемі ("сірі") адреси, активувати маскрадінг / SNAT в/ etc / shorewall / masq.

Для початку потрібно розібратися з зонами. В даному випадку їх знадобиться три штуки: одна для Інтернету (назвемо її net), одна для локальної мережі (1oc) і одна (fw) для самого брандмауера; наявність останньої зони е обов'язковим у всіх конфігураціях. Імена зон можна вибирати довільно (за вирахуванням зарезервованих ключових слів, на кшталт a11 і none), але в налаштуваннях за замовчанням вони не можуть бути довше п'яти символів. Ім'я зони брандмауера (у нашому прикладі - fw) зберігається в змінної $ FW, з якою ми ще не раз зустрінемося по ходу викладу. [19][2)]

Зони net і 1oc мають тип ipv4 (останні версії Shorewall підтримують також протокол IPv6, але ми не будемо говорити про нього в контексті даної дипломної роботи), для fw зарезервований спеціальний тип — firewall. У підсумку файл / etc / shorewall / zones прийме наступний вигляд:

```
#ZONE TYPE OPTIONS IN OUT
#     OPTIONS OPTIONS
fw firewall
net ipv4
loc ipv4
```

Коментарі видалені заради економії місця. Перейдемо до політики. В даному випадку вони зводяться до однієї-єдиної фрази: клієнти локальної мережі

[1)] [18] Hacker Dictionary [Electronic Resource]. — Mode of access : URL : http://www.robergraham.com/hacker-dictionary. — Назва з екрану.
[2)] [19] Крысин В.А. Безопасность предпринимательской деятельности / Крысин В.А. - М:Финансы и статистика, 2010.

можуть безперешкодно обмінюватися даними з Інтернетом, весь інший трафік заборонений, якщо не обумовлено інше. Іншими словами, для пари ioc-net встановлена політика ACCEPT, для всього іншого — REJECT. відповідний файл / etc / shorewall / policy може виглядати так:

```
#SOURCE DEST POLICY LOG LEVEL T:BURST
loc net ACCEPT
all all   REJECT info
```

Зверніть увагу на останній рядок: він цікавий по двох причинах. По-перше, в ньому задається політика за замовчуванням, яка діє, якщо для деякої пари зон не знайдена ніяка інша, по-друге, весь трафік, що задовольняє політиці за замовчуванням, протоколюється в syslog з рівнем info. Зазначений вид політики по замовчуванням є свого роду гарним тоном: вважається, що для всіх штатних ситуацій передбачені спеціальні політики і спрацьовування за замовчуванням є сигналом про підозрілу активність. Якщо заглянути все в той же каталог Samples, можна помітити, що пропонований авторами Shorewall набір політик виглядає трохи складніше, а саме:

```
#SOURCE DEST POLICY LOG LEVEL LIMIT:BURST
loc net ACCEPT
net all DROP info
all all REJECT info
```

Відмінність полягає в тому, що весь вхідний з Інтернету трафік ігнорується за допомогою DROP: розумний підхід до безпеки підказує, що не слід повідомляти потенційного зломщика про те, що ви існуєте і якось обробляєте його пакети. Протоколювання можна і вимкнути: навряд чи ви будете щодня продиратися через тисячі рядків журнальних файлів у пошуках потенційно небезпечних дій, а звичайний Snort впорається з цим завданням краще і швидше.

Якщо ж не просто заглянути в каталог Samples, а ще й прочитати файл two-interfaces / policy з усією ретельністю, можна помітити, що політик в ньому насправді не три, а десять. Як відзначають самі автори, це зроблено для біль-

шої деталізації повідомлень в журнальних файлах: функціональність, що у десяти, що у трьох, однакова; крім того, "розгортати" політики Shorewall може автоматично. Тому ми теж побережемо журнальний простір і перейдемо до інтерфейсів. Відповідний файл / etc / shorewall / interfaces виглядае так:

```
#ZONE INTERFACE BROADCAST OPTIONS
net th0 detect dhcp.tcpflags,routefilter,nosmurfs,loginartians
loc ethl detect tcpflas,nosmurfs
```

Як неважко здогадатися, локальна мережа в цьому прикладі підключена до інтерфейсу ethl, а вихід в Інтернет забезпечується через eth0. У колонці BROADCAST задається широкомовна адреса: в більшості випадків система здатна дізнатися його самостійно, а Shorewall-perl і зовсім розуміє тут тільки два значення: detect і "-". Інтерес представляють лише опції, а саме: dhcp — повідомляє, що на інтерфейсі виконується DHCP-клієнт або сервер; tcpflags — наказує перевіряти TCP-пакети, які надходять, на предмет наявності нелегальних комбінацій прапорів; routefilter, nosmurfs, logmartians — різні за своєю дією, але близькі по духу параметри, що змушують Shorewall звертати увагу на пакети, яких "точно не повинно бути на цьому інтерфейсі". Так, пакети з широкомовною адресою відправника відхиляються (nosmurfs), "марсіани" (пакети з некоректним вихідним адресом) протоколюються (logmartians).

Сюди ж можна віднести невикористану в даному прикладі опцію norfc 1918, що забороняє приймати пакети з не маршрутизованого адреса начебто 192.168.0.0/16 (точний список береться з/ etc / shorewall / rfci918). Параметр routefilter наказує включити в ядрі фільтрацію за маршрутом, але користуватися ним слід з обережністю: у схемі з кількома вихідними каналами можливі важко діагностовано несправності.[20][1)]

Варто відзначити, що наведена схема є можливою, але не самою оптимальною. Наприклад, для net є сенс вказати norfc 1918 (немаршрутизованих адрес там не повинно бути за визначенням), а logmartians встановити також і

---

1) [20] Аджиев В. Мифы о безопасности программного обеспечения / Аджиев В. — К: Уроки знаменитых катаетроф, 2005. — (Открытие системы).

для loc (щоб вчасно помітити в ній підозрілу активність і придушити її). Зрештою, все визначається рівнем безпеки та контролю, який ви хочете досягти. З інших опцій слід згадати optional, переважну помилку компіляції у випадку, якщо інтерфейс недоступний при запуску Shorewall (корисно для PPP-з'єднань) і routeback, змушує весь трафік, що прийшов через інтерфейс X, повертатися до відправника через нього ж(без цього практично не обійтися в ситуації, коли провайдерів декілька). Нарешті, щоб все це запрацювало, потрібно налаштувати маскрадінг. Для цього в файл / etc / shorewall / masq досить додати один рядок:

```
#INIERFACE SOURCE ADDRESS PROTO PORT(S) IPSEC MARK
eth0 eth1
```

Це може виглядати дивно, але насправді все просто. У колонці INTERFACE вказується вихідний інтерфейс, в нашому випадку це eth0 (він, нагадаю, підключений до Інтернету). У полі SOURCE перераховуються адреси, для яких потрібно застосувати SNAT-перетворення: тут, як і в багатьох реальних випадках, це просто eth1, тобто вся локальна мережа скопом.

При бажанні, ім'я інтерфейсу можна замінити явною вказівкою "сірих" адрес (наприклад, 192.168.0.0/24). Заборонити SNAT для обраних вузлів мережі можна за допомогою наступного синтаксису: eth1:! 192.168.0.1,192.168.0.3, до речі, він діє і в багатьох інших конфігураційних файлах Shorewall.

Колонка ADDRESS є необов'язковою і дозволяє вказати IP-адреси, які будуть використовуватися при маскардингу в якості вихідних (в переважній більшості випадків цього не потрібно). Решта колонки дозволяють відібрати пакети, що підлягають SNAT-перетворенню, більш точно.

Наостанок зазначимо, що якщо у вашій системі є більше двох інтерфейсів, число правил в / etc/ shorewall / masq відповідно збільшується (у загальному випадку в ньому повинні бути перераховані всі пари "локальний інтерфейс-зовнішній інтерфейс").

3.6.2 Фільтрація трафіку

Конфігурація, описана в минулому розділі, вже є працездатною, але не дуже корисною. Збагатимо її, внесши винятки зі стандартних політик в/ etc / shorewall / rules. Ось яким є цей файл Shorewall (коментарі опущені):

```
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/ MARK
#     PORT PORT(S) DEST LIMIT GROUP
DNS/ACCEPT $FW net
SSH/ACCEPT loc $FW
Ping/ACCEPT loc $FW
Ping/DROP net $FW
ACCEPT $FW loc icmp
ACCEPT $FW net icmp
```

По-перше наша політика забороняє всі з'єднання, крім створених між клієнтом в локальної мережі і сервером в Інтернеті: ні зв'язка "клієнт-брандмауер"; ні зв'язка "брандмауер-Інтернет" сюди не потрапляють. При цьому на шлюзі з Shorewall, досить імовірно, будуть запущені керуючий DNS-сервер (dnsmasq або BIND) і SSH-сервер для віддаленого адміністрування. Без правил в перших двох рядках вони будуть марними: брандмауер НЕ зможе зв'язатися з DNS-сервером, що відповідає за цікаву для вас зону, а sshd не побачить вхідне з'єднання. Альтернативний варіант (дозволити шлюзу вихід в Інтернет, а локальної мережі — довільний доступ до шлюзу) теж можливий і в ряді випадків навіть виправданий, але менш безпечний.

У колонці ACTION (крім двох останніх записів) ми бачимо приклад використання макросів DNS, SSH і Ping. Макрос — це просто набір заздалегідь визначених правил, що приймає остаточну дію (наприклад, пропустити або відхилити пакет) в якості додаткового параметра. Макроси визначаються в файлах macro.імя_макроса в каталозі / usr / share / shorewall. Ось так, наприклад, виглядає макрос macro. DNS:

```
#ACTION SOURCE DEST PROTO DEST SOURCE USER/
#     PORT(S) PORT(S) LIMIT GROUP
```

```
PARAM -     -       udp 53
PARAM -     -       tcp 53
```

Як видно, це просто правила, що відбирають TCP / UDP-трафік на порт 53. При розгортанні макросу ключове слово PARAM замінюється фактичним значенням параметра: для нашого випадку це буде ACCEPT. Аналогічним чином, ми приймаємо ICMP Echo-запити, які виходять від локальних комп'ютерів на адресу маршрутизатора, але явно ігноруємо "пінг", що приходять з мережі. Цього можна було б і не робити (політика за замовчуванням виконує рівно те ж саме), але дане правило не створює ніяких записів у журнальних файлах і відповідно перешкоджає їх швидкого захаращення. Як було сказано вище, про корисності подібного підходу можна посперечатися (зрештою, раптова хвиля ping-запитів може свідчити про атаку), але тут слід зазначити для себе один факт: правила в / etc / shorewall / rules виконуються до дій, пов'язаних з політиками.

Останні два рядки дозволяють будь ICMP-трафік між брандмауером і комп'ютерами локальної мережі, а також між брандмауером та Інтернетом.

Думається, після всього вищесказаного скласти обіцяне правило для блокування ICQ не складе труднощів:

```
#ACTION SOURCE DEST
ICQ/LOG:info   loc:!192.168.0.10 net
ICQ/REJECT   loc:!192.168.0.10 net
```

В результаті будь-яка спроба "вийти в аську" буде протоколюватися і відхилятися з повідомленням на кшталт "Connection refused". Зазначимо, що це обмеження не стосується клієнта з адресою 192.168.0.10. Записи у файлі / etc / shorewall / rules (як, втім, і в багатьох інших в Shorewall, за винятком / etc / snorewall / tcruies) перевіряються до першого збігу - складаючи правила, треб мати це на увазі. Сказане не відноситься до дій LOG і QUEUE - вони не переривають обробку пакета.

Налаштування Shorewall завершена. щоб зміни вступили в силу, необхідно набрати команду:

```
# shorewall start
```

але щоб спочатку впевнитися, що ваші налаштування коректні. Це можна зробити командою:

```
# shorewall check
```

Вона виконає процес компіляції, але не стане запускати згенерований скрипт; ви ж зможете відловити всі помилки та попередження. Подивитися, які саме правила iptables були створені Shorewall від вашого імені, можна командою:

```
# shorewall show
```

Зрозуміло, "iptables -L" теж ніхто не відміняв.

3.6.3 Введення додаткових можливостей

Що ще можна зробити з нашою конфігурацією Shorewall. По перше — прозорий проксі-сервер: прийом, про порочність якого було сказано досить багато, але тим не менш широко поширений.

```
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL
#    PORT PORT(S) DEST
REDIRECT 1oc 3128 tcp www      -     ! 192.168.0.2
```

Дія REDIRECT передає пакет локальному (для шлюзу) процесу, прослуховують порт, зазначений у колонці DEST (у нас це 3128 — стандартну налаштування Squid і більшості інших HTTP-проксі). Правило задовольняє TCP-з'єднанням, що мають в якості порту призначення 80 (у прикладі використаний псевдонім www, заданий в/ etc / services), крім адресованих 192.168.0.2 (ймовірно, внутрішньому веб-серверу).

Розглянуте вище перенаправлення є окремим випадком DNAT- перетворення (в тому сенсі, що REDIRECT можна розглядати як DNAT на локальний IP-адреса), яке можна застосовувати з різними цілями. Наприклад, класичний кидок портів (port forwarding) Інтернет з'єднань на все той же внутрішній веб-сервер може бути організований таким чином:

```
#ACTION SOURCE DEST   PROTO DEST SOURCE ORIGINAL RATE
#                          PORT PORT(S) DEST LIMIT
DNAT net loc:192.168.0.2 tcp http     -     -     3/sec:10
```

Ми здійснюємо прозору передачу всіх TCP-з'єднань на 192.168.0.1:25 сервера з адресою 1.2.3.4. Тепер можна повідомити вашим користувачам, що для вихідної пошти потрібно вказати сервер 192.168.0.1.

Звичайно, такий прийом має ряд обмежень. По-перше, він буде погано працювати в тому випадку, коли для захисту з'єднання використовуються SSL-шифрування (отримавши сертифікат для несподіваного доменного імені, пристойний поштовий клієнт повинен, як мінімум, видати серйозне попередження), по-друге, редагувати адрес інтернет-сервера кожного разу при зміні провайдера — справа клопітна ("людський фактор" рано чи пізно дасть про себе знати). [21][1)] Тут може стати в нагоді ще одна особливість Shorewall — вміння отримувати параметри ззовні і працювати зі змінними. Центральна роль тут відводиться файлу / etc / shorewall / params: це сценарій на мові Shell, який копіюється в результуючий скрипт, генерований Shorewall в процесі компіляції. Він, наприклад, має такий вигляд:

```
ROUTER IP=192.168.0.1
SMTP=S(get_current_smtp)
```

Тут мається на увазі, що у вашій системі реалізована команда get_current_smtp, що повертає IP-адрес SMTP-сервера поточного провайдера. Тоді правило для "віртуального сервера" можна переписати наступним чином:

```
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL
#                          PORT PORT(S) DEST
DNAT- loc   net:$SMTP tcp 25 - $ROUTER_IP
```

Імена змінних рекомендується починати з великої літери - так ви гарантовано уникнете конфлікту імен з внутрішніми змінними Shorewall. Тепер при зміні провайдера досить просто виконати команду:

[1)] [21] Структура руководства по обеспечению информационной безопасности [Електронный ресурс]. — Режим доступу : URL : http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct. - Назва з екрану.

```
shorewall restart
```

Висновок: Shorewall дозволяє створювати конфігурації практично будь-якої складності: з декількома провайдерами (у тому числі розділяють один мережевий інтерфейс), мостами, шейпінгом і урахуванням трафіку, VPN. Також, його можна порівняно легко модифікувати під свої потреби, а ліцензія (GPLv2) дозволяє навіть поширювати змінені копії.

РОЗДІЛ 4.КІНЦЕВА СХЕМА РІШЕННЯ ФАЕРВОЛА

Для досягнення кінцевих результатів потрібно зробити такі дії:

– комп'ютери внутрішньої мережі мають адреси 192.168.1.0/24
– Розрахувати Directory Server, підключений до внутрішньої мережі через інтерфейс eth1 з встановленим IP адресою 192.168.1.1, і має вихід в інтернет через інтерфейс eth0 з встановленою IP адресою 1.2.3.4 (шлюз)
– в локальній мережі є поштовий сервер з адресою 192.168.1.10

Для початку визначити необхідні зони: net - інтернет, 1oc - локальна мережа, fw - CDS. В / etc / shorewall / zones поміщено записи:

```
###########################################
###################################
#ZONE TYPE OPTIONS IN OUT
# OPTIONS OPTIONS
fw firewall
net ipv4
1oc ipv4
```

Тепер вказано, що зона net обслуговується інтерфейсом eth0, а зона loc — інтерфейсом eth1. Вхідний трафік на обох інтерфейсах пропускається через фільтри: tcpflags, routefilter, nosmurfs, logmariians. В / etc / shorewall і interfaces поміщено записи:

```
#####################################################
#########################
#ZONE INTERFACE BROADCAST OPTIONS
net eth0   detect     tcpflags,nosmurfs,routefilter,logmartians
loc eth1   detect     tcpflags,nosmurfs,routefilter,logmartians
```

Описано правила за замовчуванням (політики) для трафіку які проходить через шлюз: локальної мережі (1oc) і шлюзу ($ FW) дозволений доступ у всі зони, пакети з мережі (net) скидається, до решти застосовується правило REJECT з логом. В/ etc / shorewall / policy поміщено записи:

```
###############################################################
##################
#SOURCE DEST POLICY LOG LIMIT: CONNLIMIT:
#LEVEL BURST MASK
loc all ACCEPT
$FW all ACCEPT
net all DROP
all all REJECT info
```

Додано маскарадинг для пакетів які виходять з локальної мережі в інтернет. В/ etc / shorewall / masq поміщено записи:

```
## ## #### #### ###### #### # # # # # ## ######## ## ## # # ### #
###### ## ###### ####### ###########
#INTERFACE:DEST SOURCE ADDRESS PROTO PORT(S) IPSEC
MARK USER/
#GROUP
eth0  192.168.1.0/24 1.2.3.4
```

Шлюз який забезпечує вихід в Інтернет локальної мережі готовий, тепер лишилось додати кілька правил:

– дозволимо ping шлюзу з Інтернету • дозволимо з'єднання по ssh зі шлюзом з Інтернету
– заборонемо вихід в Інтернет з діапазону адрес 192.168.1.100 - 192.168.1.254
– перенаправимо порти IMAP / IMAPS для доступу до поштового сервера з Інтернету
– перенаправимо порт SMTP до поштового сервера

В /etc/shorewall/rules помістити записи:

```
#####################################################
#####################################################
#####################################################
#####
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/ MARK
CONNLIMIT TIME HEADERS
```

```
PORT PORT(S) DEST LIMIT
GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
Ping/ACCEPT net $FW
SSH/ACCEPT net $FW
REJECT loc:192.168.1.100-192.168.1.254 net
IMAP/DNAT net loc:192.168.1.10
IMAPS/DNAT net loc:192.168.1.10
SMTP/DNAT net loc:192.168.1.10
```

Дозволимо запуск shorewall, для цього потрібно встановити параметр STARTUP_ENABLED = Yes у файлі /etc/shorewall/shorewail.conf.

4.1 Додавання Ip телефонії

– телефони підключені до основної мережі та їх ip адреси знаходяться в діапазоні 192.168.1.70-192.168.1.99
– на сервер 192.168.1.10 встановлюється asterisk

Оголосимо нову зону phone для телефонів. Змінимо / etc / shorewall / zones (зона phone повинна бути оголошена обов'язково перед зоною 1oc):

```
#ZONE TYPE OPTIONS IN OUT
# OPTIONS OPTIONS
fw firewall
net ipv4
phone ipv4 # Новий рядок
loc ipv4
```

Виділимо телефони із зони loc в зону phone. Помістимо в/ etc / shorewall / hosts

```
#######################################################
#########################
```

```
#ZONE HOST(S) OPTIONS
phone eth1:192.168.1.70-192.168.1.99
```

Опишемо політику заборони телефонів (phone) доступ до Інтернету (net). Змінимо / etc / shorewall / policy

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # #. ####.
# # # # # # # # # # # ##### ##########################
#SOURCE DEST POLICY LOG LIMIT: CONNLIMIT:
# LEVEL BURST MASK
phone net DROP # Новий рядок
loc all ACCEPT
$FW all ACCEPT
net all DROP
all all REJECT info
```

Прокинемо такі порти SIP та IAX на ip 192.168.1.10. Додамо до / etc / shorewall / rules

```
############################################################
############################################################
#############################################################
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/ MARK
CONNLIMIT TIME HEADERS
# PORT PORT(S) DEST LIMIT GROUP
#SECTION ESTABLISHED
#SECTION RELATED
SECTION NEW
SMTP/DNAT net loc:192.168.1.10
# SIP
DNAT net loc:192.168.1.10 udp 5060
# IAX
DNAT net loc:192.168.1.10 udp 4569
```

4.2 Додавання IPSEC тунелів

– Шлюз встановлює ipsec тунель з віддаленим шлюзом через інтернет, підключаючи сегмент 192.168.3 .0/24
– Віддалений шлюз має ip адреса 1.2.3.5

Додамо зону vpn для віддаленої підмережі. Змінюємо / etc / shorewall / zones

```
#########################################################
##########################
#ZONE TYPE OPTIONS IN OUT
# OPTIONS OPTIONS
fw firewall
vpn ipv4 # Новий рядок
net ipv4
phone ipv4
loc ipv4
```

Визначимо зону vpn (пакети, що надходять eth0 і знаходяться в під мережі 192.168.3.0/24). Змінюємо / etc / shorewall / hosts

```
#########################################################
##########################
#ZONE HOST(S) OPTIONS
phone eth1:192.168.1.70-192.168.1.99
vpn eth0:192.168.3.0/24 # Новий рядок
```

Опишемо тунель: ipsec, тунель проходить через зону net, ip адреса віддаленого шлюзу. Записуємо в/ etc / shorewall / tunnels

```
#TYPE ZONE GATEWAY GATEWAY ZONE
ipsec net 1.2.3.5
```

Відключимо маскарадинг. Пакети відправляються з локальний мережі (1oc) в віддалену під мережа (vpn). Змінюємо / etc / shorewall / masq:

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # # #
# # # # # # # # # # # # # # # # # # # ## ######################
#INTERFACE:DEST SOURCE ADDRESS PROTO PORT(S) IPSEC MARK USER/
```

```
# GROUP
eth0:192.168.3.0/24 192.168.1.0/24 1.2.3.4 # змінений рядок
```

Опишемо політику, дозволяючи з'єднання vpn з локальною зоною loc. Змінюємо / etc / shorewall / policy:

```
############.####################.####################
##########################
#SOURCE DEST POLICY LOG LIMIT: CONNLIMIT:
# LEVEL BURST MASK
phone net DROP
vpn loc ACCEPT # Новий рядок
loc all ACCEPT
$FW all ACCEPT
net all DROP
all all REJECT info
```

ВИСНОВКИ

При роботі в мережі Інтернет, для захисту інформації, на перше місце виходять міжмережеві екрани (firewalls) – найважливіший засіб захисту мережі організації. Вони контролюють мережевий трафік, що входить в мережу і що виходить з неї. Використовуючи інтерфейс налаштувань профілю доступу міжмережевого екрану, є можливість для кожного користувача створити свій профіль, який буде визначати не тільки права доступу цього користувача до мережі інтернет, але і права доступу до цього користувача з інтернету. Міжмережевий екран може блокувати передачу в мережу несанкціонованого трафіка та виконувати перевірки трафіка. Добре сконфігурований міжмережевий екран спроможний зупинити більшість відомих комп’ютерних атак. Результатами дослідження є такими, що пропускна здатність, швидкість затримки, встановлення з'єднання і розрив показали, що кількість правил фільтрації чинять більш негативний вплив на продуктивність брандмауера Iptables ніж на Shorewall. Міжмережеві екрани обробили правила зверху вниз. Порядок у якому записані правила також важливий. Обидва брандмауери показують, що малі розміри пакетів не впливають на продуктивність брандмауера. Shorewall добре зарекомендував себе при навантаженнях. Також Shorewall дозволяє створювати конфігурації практично будь-якої складності: з декількома провайдерами (у тому числі розділяють один мережевий інтерфейс), мостами, шейпінгом і урахуванням трафіку, VPN Завершальним етапом дипломної роботи є створення правил доступу до мережі за допомогою міжмережевого екрану Shorewall.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Дилевский А. Фильтрация пакетов, firewall и маскарадинг в Линуксе [Електронний ресурс]. — Режим доступу: http://citforum.ru/operating_systems/articles/masquerade.shtml
2. Захаров И. Протокол TCP №1 [Електронний ресурс]. — Режим доступу: https://xakep.ru/2002/04/11/14943/
3. Iptables [Електронний ресурс]. — Режим доступу: http://uk.wikipedia.org/wiki/Iptables
4. https://www.gentoo.org/doc/ru/security/security-handbook.xml?part=1&chap=12#doc_chap1
5. W. Stallings, "Intruders," in Network Security Essentials, Applications and standards, Pearson, 2011, p. 319.
6. V. У. P. B. Joe1 Sommers, "Toward Comprehensive Traffic Generation for Online IDS Evaluation," University of Wisconsin-Madison
7. T. Aduolf, "systems, Department of technology enhanced learning information," protecting networks, vol. 1, no. University of North Carolina, p. 16, 2010.
8. C. Berthelot, "Evaluation of a virtual firewall in a cloud environment," School of computing,
9. Руководство по Shorewall
10. H. Haas, "Network Address Translation," NAT, vo1. 1.0, no. Cisco Systems Inc., p. 43, 2005.
11. http://wiki.kspu.kr.ua/index.php/Міжмережевий_екран#.D0.A0.D1.96.D0.B7.DO.BD.DO.BE.DO.B2.DO.B8.DO.B4.DO.BB.DO.BC.DO.B5.D1.80.DO.B5.DO.B6.DO.B5.DO.B2.DO.B8.D1.85_.DO.B5.DO.BA.D1.80.DO.BO.DO.BD.D1.96.DO.B2
12. http://digincore.org/index.php/dokumentatsiya/ur1-digincore-ubuntu/iptables
13. http://pro-spo.ru/linux-for-beginner/1576--iptables-

14. А. Астахов. Анализ защищенности корпоративных автоматизированных систем / А. Асгахии. — Москва, 20 10.
15. Лукацкий А.В. Как работает сканер безопасности / Лукацкий А.В. - Hackzone, 2009.
16. А. Астахов. IDS как средство управления рисками / А. Астахов : [Електронный ресурс]. — Режим доступу : URL http://www.globaltrust.ru/security/Pubs/Pub2part5. — Назва з екрану.
17. А. В. Соколов. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. — 656с.
18. Hacker Dictionary [Electronic Resource]. — Mode of access : URL : http://www.robergraham.com/hacker-dictionary. — Назва з екрану.
19. Крысин В.А. Безопасность предпринимательской деятельности / Крысин В.А. - М:Финансы и статистика, 2010.
20. Аджиев В. Мифы о безопасности программного обеспечения / Аджиев В. — К: Уроки знаменитых катаетроф, 2005. — (Открытие системы).
21. Структура руководства по обеспечению информационной безопасности [Електронный ресурс]. — Режим доступу : URL : http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct. - Назва з екрану.