МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

кафедра комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД ЗЛОВМИСНИКІВ

Виконав:студент групи 3К-21

Спеціальності

123 Комп’ютерна інженерія

Владислав БАСАРАБ

Керівник: Маргарита МЕДОЛИЗ

Черкаси 2024

АНОТАЦІЯ

У дипломній роботі розглядаються сучасні методи захисту комп'ютерних мереж від зловмисників, що є однією з найактуальніших проблем у сфері кібербезпеки. Метою дослідження є аналіз ефективності різних підходів до захисту мережевих інфраструктур та розробка рекомендацій для покращення рівня безпеки.

Результати дослідження показують, що комбіноване використання різних методів захисту, зокрема багаторівнева система безпеки, є найбільш ефективним підходом для протидії сучасним загрозам. Автоматизація процесів моніторингу та реагування на інциденти значно підвищує швидкість і точність виявлення та нейтралізації загроз.

Практичний результат роботи полягає у наданні рекомендацій для організацій щодо впровадження та оптимізації систем захисту комп'ютерних мереж, що сприятиме підвищенню рівня кібербезпеки та зниженню ризиків витоку даних та несанкціонованого доступу.

ABSTRACT

The thesis examines modern methods of protecting computer networks from intruders, which is one of the most urgent problems in the field of cyber security. The purpose of the study is to analyze the effectiveness of various approaches to the protection of network infrastructures and to develop recommendations for improving the level of security.

The results of the study show that the combined use of various protection methods, in particular a multi-level security system, is the most effective approach to combating modern threats. Automation of monitoring and incident response processes significantly increases the speed and accuracy of threat detection and neutralization.

The practical result of the work consists in providing recommendations for organizations on the implementation and optimization of computer network protection systems, which will contribute to increasing the level of cyber security and reducing the risks of data leakage and unauthorized access.

ЗМІСТ

ВСТУП

У сучасному світі, де інформаційні технології відіграють ключову роль у всіх сферах діяльності людини, питання захисту комп'ютерних мереж від зловмисників набуває особливої актуальності. З розвитком Інтернету та збільшенням кількості пристроїв, підключених до мережі, зростає і кількість загроз, що ставлять під ризик безпеку даних та функціонування інформаційних систем. Атаки зловмисників стають все більш складними та витонченими, використовуючи новітні методи і технології для досягнення своїх цілей.

Метою даної дипломної роботи є аналіз сучасних методів захисту комп'ютерних мереж від зловмисників. У роботі буде розглянуто різні підходи до забезпечення безпеки мережевої інфраструктури, включаючи як традиційні методи, так і інноваційні рішення, що з'явилися в останні роки. Особлива увага приділятиметься таким аспектам, як захист від мережевих атак, виявлення та протидія шкідливому програмному забезпеченню.

Актуальність даної теми зумовлена не тільки зростанням кількості атак на комп'ютерні мережі, але й постійною еволюцією методів атак, що вимагає постійного вдосконалення засобів захисту. Успішна реалізація ефективних заходів безпеки дозволяє не лише зберегти конфіденційність та цілісність даних, але й забезпечити безперервну роботу бізнесу.

Актуальність обраної теми визначається не лише зростанням кількості та складності кіберзлочинних атак, але й швидким розвитком технологій, що вимагають вдосконалення методів захисту. Існує необхідність у вивченні та аналізі сучасних підходів до захисту операційних систем з метою розробки більш ефективних та надійних стратегій. Швидкі темпи технологічного розвитку призводять до появи нових загроз та вразливостей, що робить безпеку комп’ютерних мереж надзвичайно важливою. Однією з найбільш наочних прикладів є зростання кількості кіберзлочинності та кібератак. Інциденти, пов'язані з витоками даних, розкриттям конфіденційної інформації, вимаганням викупу зашифрованих даних та інші види кіберзлочинності стають все поширенішими. Це підкреслює необхідність постійного вдосконалення заходів

захисту та розробки нових методів протистояння цим загрозам. Можливість захисту комп’ютерних мереж підтверджується і в контексті глобальних подій та тенденцій. Наприклад, пандемія COVID-19 зумовила значний ріст використання робочих віддалених станцій, що створило нові виклики для безпеки мереж та операційних систем. Зловмисники використовують такі ситуації для проведення специфічних атак, спрямованих на використання паніки та вразливостей в робочих оточеннях. Зростаюча кількість пристроїв, які стають частиною Інтернету речей, також створює нові виклики для безпеки. Критична інфраструктура, така як енергетичні системи, транспортні мережі та медичні пристрої, стають мішенями для кібератак, що може мати серйозні наслідки для громадської безпеки та здоров'я. Також важливо враховувати зростання кількості пристроїв та даних, які зберігаються у хмарних сервісах. Необхідність захисту цих даних стає все більш насущною, оскільки багато користувачів та організацій переходять до хмарних рішень для зберігання та обробки своїх даних. У висновку, актуальність теми захисту комп’ютерних мереж від зловмисників в сучасному світі неоспорима. Швидкий розвиток технологій, зростання кількості кіберзагроз та поширення нових технологічних рішень створюють необхідність у постійному вдосконаленні методів захисту та розробці нових стратегій протистояння цим загрозам.

У роботі буде проведено аналіз існуючих підходів до захисту комп'ютерних мереж, визначено їх переваги та недоліки, а також надано рекомендації щодо впровадження найефективніших з них у практичну діяльність. Результати даного дослідження можуть бути корисними як для фахівців у сфері інформаційної безпеки, так і для організацій, що прагнуть підвищити рівень захисту своїх мережевих інфраструктур.

Об'єкт та предмет дослідження були чітко визначені з метою ретельного аналізу сучасних методів захисту комп’ютерних мереж.

Об'єктом дослідження є сучасні методи захисту комп’ютерних мереж, а предметом - їхні можливості та обмеження. Дослідження спрямоване на вивчення проблем, пов'язаних з існуючими методами захисту та виявленням

можливостей для їх подальшого удосконалення. Дослідження враховує різноманітні потенційні загрози для кожного типу комп’ютерних мереж та спрямоване на розробку універсальних методів захисту, які можуть бути застосовані у різних середовищах. Також важливо враховувати специфічні вимоги та характеристики кожної операційної системи, а також потреби користувачів у забезпеченні безпеки та захисті їхніх даних.

У світі, де комп'ютеризація стає не лише нормою, але й невід'ємною частиною нашого повсякденного життя, захист комп’ютерних мереж від зловмисників стає надзвичайно актуальною та важливою проблемою. Різноманітність кіберзагроз та швидкий розвиток технологій вимагають постійного удосконалення методів захисту та розробки нових стратегій протистояння цим викликам.

Таким чином, дана дипломна робота сприятиме розширенню знань у галузі інформаційної безпеки, а також допоможе у виборі та впровадженні ефективних засобів захисту комп'ютерних мереж від зловмисників.

РОЗДІЛ 1

Мережеве обладнання

1.1 Види мережевого обладнання

Мережеве обладнання – пристрої, що забезпечують функціонування комп'ютерних мереж, до них відносять: маршрутизатор, комутатор, концентратор, патч-панель тощо.

Маршрутизатор – мережеве обладнання, призначене для з’єднання двох або більше мереж та керування процесом маршрутизації, цей процес являє собою передачу пакетів мережевого рівня між різними частинами мережі, відповідно до певних правил та наявної інформації про топологію.

Зазвичай маршрутизатор не тільки займається передачею пакетів між інтерфейсами, а також виконує такі функції як: захист локальної мережі від загроз зовні, обмеження доступу до глобальної мережі користувачам локальної мережі, призначення ір адрес, шифрування трафіку та інше.

Маршрутизатори функціонують на мережевому рівні моделі OSI, вони мають здатність передавати дані між різними мережами, використовуючи таблицю маршрутів, що також називається таблицею маршрутизації, вона може містити статичні записи маршрутів або може вивчати їх за допомогою протоколів динамічної маршрутизації.

Окрім того маршрутизатори можуть виконувати перетворення адрес відправника та одержувача (NAT, Network Address Translation), на основі певних правил фільтрувати пакети даних, що передаються, з метою обмеження доступу, шифрувати їх та виставляти приорітет порядку передачі в залежності від типу.

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

Навантаження мережі зменшують за рахунок маршрутизаторів. Як правило їх застосовують, щоб об’єднати мережі різних типів, у тому числі несумісних за архітектурою і протоколам, наприклад для об’єднання різних локальних мереж, а також надання їх доступу до мережі Інтернет.

Функції маршрутизатора може виконувати не тільки спеціалізоване апаратне забезпечення, а й звичайний комп'ютер. За допомогою спеціального програмного забезпечення, як правило для операційних систем UNIX, робочу станцію або сервер з декількома мережевими платами можна перетворити на маршрутизатор.

Маршрутизатори розрізняють за певними класами: верхній, середній та нижній. Маршрутизатори верхнього класу, також їх ще називаються магістральними (backbone routers) – мають найбільшу продуктивність та об'єднують мережі підприємства, таким чином створюючи центральну мережу, яка може складатися з великої кількості локальних. Таке обладнання здатне обробляти кілька сотень тисяч або навіть кілька мільйонів пакетів за секунду. Вони мають підтримку багатьох протоколів та інтерфейсів. Значна увага приділяється надійності та відмовостійкості, що забезпечується завдяки системам терморегуляції, резервним джерелам живлення, та модулям, що підтримують швидку заміну під час роботи (hot swap).

Середній клас маршрутизаторів використовується для регіональних відділень, що з'єднують їх між собою та з центральною мережею. Мережа регіонального відділення, подібно до центральної мережі, може складатися з декількох локальних мереж. Таке обладнання зазвичай дещо простіше за своїм функціоналом та можливості в порівнянні з маршрутизаторами високого класу. Вони так само можуть працювати з популярними транспортними протоколами та протоколами маршрутизації. Представників цього класу найбільше, їх функціонал може досягати до можливостей магістральних маршрутизаторів або зменшуватись до рівня обладнання віддалених офісів.

Маршрутизатори нижнього класу призначені для використання у віддалених офісах, вони підключають невеликі офіси до мережі підприємства. Такі маршрутизатори можуть підтримувати досить небагато інтерфейсів локальних мереж, вони розраховані на виділені лінії з низькою швидкістю. Також в якості резервного каналу може використовуватись телефонна лінія зв'язку. Ці маршрутизатори мають велику популярність в організаціях, яким

необхідно розширити чинні міжмережеві зв’язки. Є дуже багато типів маршрутизаторіввіддалених офісів. Це обумовлено як великою кількістю потенційних споживачів, так і спеціалізацією такого типу пристроїв, що проявляється в підтримці одного конкретного типу глобального зв’язку.

Комутатор – це мережевий пристрій, який з’єднує кілька комп’ютерів в одну єдину локальну мережу. Сучасні комутатори мають дуже великий ряд функцій, які дуже сильно можуть полегшити подальшу роботу адміністратора. Від правильного вибору комутаторів залежить функціонування всієї локальної мережі й робота підприємства в цілому.

Комутатор функціонує на канальному (другому) рівні моделі OSI. Комутатори були створені для використання мостових технологій і досить часто розглядаються в якості мостів з великою кількістю портів. Комутатор передає дані лише безпосередньо одержувачеві, окрім широкомовного трафіку, що передається всім вузлам мережі, в той час як концентратор відправляє трафік від одного підключеного пристрою до всіх інших, не зважаючи на тип трафіку. Це дозволяє підвищити продуктивність і безпеку мережі, позбавляючи інші вузли мережі необхідності обробляти непризначені їм дані.

Комутатор має таблицю комутації, яку зберігає в асоціативній пам’яті, у ній міститься записи відповідності MAC-адреси вузла до порта комутатора. Оскільки після включення комутатора таблиця комутації порожня, він спочатку працює в режимі навчання, передаючи данні на всі інші порти, окрім того звідки вони надійшли. При цьому комутатор аналізує отримані фрейми (кадри), визначаючи MAC-адресу хоста-відправника та записує його до таблиці на певний час. Потім, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого уже є в таблиці, то такий кадр буде відправлено тільки на той порт.

Комутатори поділяють на такі, що:

– не мають можливості управління – це прості самостійні пристрої, які самі управляють передачею даних і не мають функцій ручного керування. Деякі моделі некерованих комутаторів мають вбудовані засоби моніторингу.

Недоліками таких комутаторів є відсутність знову ж таки засобів управління і низька продуктивність. Зважаючи на це, у великих мережах підприємств некеровані комутатори не використовуються, оскільки адмініструвати таку мережу досить складно і потрібно витрачати досить багато зусиль;

– керовані комутатори, вони також працюють в автоматичному режимі, але крім цього мають ручне керування. Ручне керування надає можливість дуже гнучко налаштувати роботу комутатора та полегшити життя системного адміністратора. Головним недоліком таких комутаторів є ціна, яка залежить від функціонала і продуктивності.

Встановлення та налаштування безпеки комутаторів

- **Використання сильних паролів**: Забезпечте використання складних паролів для доступу до комутаторів.
- **SSH замість Telnet**: Використовуйте SSH для захищеного доступу до комутатора, оскільки Telnet передає дані у відкритому тексті.
- **Захист консолі та віртуальних терміналів (VTY)**: використовуйте ACL(списки контролю доступу) для обмеження доступу доконсолі та VTY.

Захист від атак на рівні комутатора

- **DHCP Snooping**: Захист від підробки DHCP-серверів шляхом перевірки легітимності DHCP-повідомлень.
- **ARP Inspection**: Захист від атак ARP spoofing (атака на таблицю ARP) за допомогою Dynamic ARP Inspection (DAI).
- **IP Source Guard**: Захист від атак IP Spoofing шляхом перевірки джерела IP-адрес.

Оновлення та патчі

Регулярні оновлення прошивки та програмного забезпечення: Забезпечує регулярне оновлення комутаторів та мережевого обладнання для закриття відомих вразливостей.

Забезпечення безпеки комутаторів та мережі в цілому є критично важливим завданням для захисту даних та підтримки надійного функціонування інформаційних систем. Різноманітні методи та практики, такі як налаштування

безпеки комутаторів, використання ACL, VLAN, аутентифікація та авторизація, а також фізична безпека та моніторинг мережі, є основою для ефективної стратегії захисту.

Важливо постійно адаптувати стратегію безпеки до нових викликів та загроз, підтримуючи високий рівень обізнаності та готовності до реагування на інциденти. Такий комплексний підхід забезпечить надійну та безпечну роботу мережі, захист конфіденційної інформації та стабільність бізнес-процесів.

1.2 Методи захисту мережевого обладнання

Фізичний захист: розміщення обладнання у закритих приміщеннях, використання замків та камер відеоспостереження.

Апаратний захист: використання мережевих брандмауерів, систем виявлення вторгнень (IDS), систем запобігання вторгненням (IPS).

Програмний захист: встановлення антивірусного програмного забезпечення, оновлення ПЗ, налаштування політик безпеки.

Адміністративні заходи: розробка та впровадження політик безпеки, навчання персоналу, контроль доступу.

Більшість атак мережевого рівня пов’язані з використанням протоколу IP: підміна IP-адреси вузла, нав'язування хибного маршруту, перехоплення зловмисником діапазону IP-адрес та отримання інформа- ції про логічну структуру мережі (IP-адреси вузлів, доменні імена), проблеми одноразової ідентифікації за IP-адресою.

Можна виділити такі підходи до захисту від наведених атак:

• створення прив’язок IP – MAC-порт для запобігання підміні IP-адреси та несанкціонованому підключенню до мережі (базові підходи реалізуються на канальному рівні і їх було розглянуто у попередній статті циклу)

• використання технології трансляції мережних адрес (Network Address Translation – NAT) для приховання від зовнішніх зловмисників діапазону IP-адрес організації та логічної структури мережі,

• створення списків контролю доступу (Access Control List– ACL) для обмеження доступу до вузлів та протоколів/сервісів прикладного рівня.

1.3 Безпека мережі

Забезпечення безпеки мережі включає в себе встановлення захисних механізмів, таких як файрволи, системи виявлення і запобігання вторгненням (IDS/IPS), шифрування даних, аутентифікація користувачів та інші заходи. Включає в себе різноманітні заходи та стратегії для захисту мережевих ресурсів від несанкціонованого доступу, вірусів, атак з мережі та інших загроз.

Мережеві розширення: Деякі маршрутизатори підтримують можливості розширення мережі, такі як підключення додаткових точок доступу для створення мережі з множинним доступом, розширення діапазону IP-адрес, підтримка

Деякі сучасні маршрутизатори мають розширені функції управління мережею, що дозволяють адміністраторам контролювати та моніторити мережу з використанням веб-інтерфейсу або спеціального програмного забезпечення. Це може включати керування пропускною здатністю, налаштування безпеки мережі, моніторинг мережевого трафіку та інші аспекти управління мережею.

1.4 Неявність або недостатня безпека мережевих пристроїв

Неявність або недостатня безпека мережевих пристроїв може стати серйозною загрозою для безпеки всієї мережі. Часто мережеві пристрої, такі як маршрутизатори або комутатори, мають захищені паролі для доступу до їхніх конфігурацій. Якщо паролі слабкі або не змінюються від заводських налаштувань, зловмисники можуть легко отримати доступ до цих пристроїв і внести зміни в їх конфігурацію або використовувати їх для перехоплення даних.

Мережеві пристрої працюють на операційних системах, які також можуть мати вразливості. Якщо ці вразливості не виправлені шляхом встановлення оновлень програмного забезпечення, зловмисники можуть використовувати їх для злому пристроїв та отримання несанкціонованого доступу.

1.5 Мережеві файрволи:

Файрволи (брандмауери) є важливими компонентами кібербезпеки, які контролюють і регулюють мережевий трафік на основі заздалегідь визначених правил безпеки. Вони можуть бути апаратними або програмними і

використовуються для захисту мереж від несанкціонованого доступу, атак і вірусів. Існує кілька типів файрволів, кожен з яких має свої особливості та призначення:

Пакетні фільтри: Контролюють трафік на основі IP-адрес відправника та одержувача, портів і протоколів.

Станові файрволи: Аналізують стан кожного з'єднання, дозволяючи або забороняючи трафік залежно від стану сесії.

Аплікаційні файрволи:

Proxy-сервери: Працюють на прикладному рівні, контролюючи трафік для певних додатків, таких як веб-браузери.

Веб-аплікаційні файрволи (WAF): Захищають веб-додатки, фільтруючи і моніторячи HTTP-запити, щоб виявити і запобігти атакам, таким як SQL-ін'єкції або XSS.

Некст-генераційні файрволи (NGFW):

Включають функціонал традиційних файрволів, а також додаткові функції, такі як інспекція на рівні додатків, інтеграція з системами запобігання вторгнень (IPS), та можливості глибокого аналізу пакетів (DPI).

Програмні файрволи:

Встановлюються безпосередньо на кінцеві пристрої (комп'ютери, сервери) і контролюють вихідний та вхідний трафік для цього конкретного пристрою. Програмні файрволи часто використовуються на персональних комп'ютерах і мобільних пристроях.

Гібридні файрволи:

Поєднують в собі риси кількох різних типів файрволів для забезпечення комплексного захисту.

Популярні рішення для файрволів включають такі продукти, як Cisco ASA, Palo Alto Networks, Fortinet FortiGate, Check Point, Sophos XG Firewall, ZoneAlarm, і багато інших. Кожен з них має свої особливості і може бути налаштований під конкретні потреби організації або користувача.

Налаштування мережевих файрволів

Пакетні фільтри:

1. **Збір інформації**: Визначте мережеві вимоги, включаючи IP-адреси, порти та протоколи, які будуть використовуватися.
2. **Створення правил фільтрації**:

- Визначте, які пакети повинні бути дозволені або заблоковані.
- Наприклад, дозволити HTTP-трафік (порт 80) і HTTPS-трафік (порт 443), але блокувати всі інші порти.

3. **Налаштування правил на файрволі**:

- Внесіть правила в конфігураційний файл або через інтерфейс користувача файрвола.
- Зазвичай це робиться через веб-інтерфейс або командний рядок.

4. **Застосування правил**:

- Активуйте правила і переконайтесь, що вони правильно працюють.
- Проведіть тестування, щоб переконатися, що дозволений трафік проходить, а небажаний блокується.+

РОЗДІЛ 2 ПОПУЛЯРНІ ПРОГРАМИ-БРАНДМАУЕРИ

Windows Firewall, або Брандмауер Windows, є вбудованим засобом безпеки операційної системи Windows, призначеним для контролю мережевого трафіку, що надходить на комп'ютер і виходить з нього. Його основна мета — захист комп'ютера від несанкціонованого доступу та шкідливих програм. Windows Firewall.

Брандмауер перевіряє всі мережеві з'єднання і дозволяє або блокує їх на основі налаштувань політики безпеки. Також він може блокувати невідомі або небезпечні з'єднання, що надходять із зовнішньої мережі, захищаючи таким чином систему від хакерських атак і вірусів. Windows Firewall веде журнали подій, що дозволяє адміністраторам відстежувати та аналізувати спроби доступу до мережі.

2.1 Компоненти Windows Firewall

1. **Основний Інтерфейс**: Дозволяє користувачам увімкнути або вимкнути брандмауер, а також налаштувати базові параметри.
2. **Розширені Налаштування (Windows Defender Firewall with Advanced Security)**: Дозволяють створювати детальні правила для вхідного та вихідного трафіку, налаштовувати безпекові політики та переглядати журнали подій.
3. **Профілі Безпеки**:
   - **Доменний Профіль**: Використовується, коли комп'ютер підключений до мережі домену.
   - **Приватний Профіль**: Застосовується, коли комп'ютер підключений до приватної мережі, наприклад, домашньої.
   - **Громадський Профіль**: Використовується, коли комп'ютер підключений до громадської мережі, наприклад, кафе чи аеропорту.

Використання Windows Firewall

Блокування Небажаного Трафіку:

Приклад: Компанія хоче заблокувати всі з'єднання з певною IP-адресою, яка була помічена у хакерській активності. Адміністратор створює правило в Windows Firewall, яке блокує всі вхідні та вихідні з'єднання з цією IP-адресою.

Блокування Вихідного Трафіку за Програмами:

1. Відкрийте **Windows Defender Firewall with Advanced Security**.
2. Перейдіть до розділу **Outbound Rules** (Правила для вихідного трафіку).
3. Виберіть **New Rule** (Нове правило).
4. Виберіть **Program** (Програма) і натисніть **Next**.
5. Виберіть **This program path** (Шлях до програми) і вкажіть шлях до програми, яку ви хочете обмежити.
6. У розділі **Action** (Дія) виберіть **Block the connection** (Блокувати з'єднання) і натисніть **Next.**
7. Виберіть профілі, до яких застосовується це правило, і натисніть **Next**.
8. Назвіть правило, додайте опис (якщо потрібно), і натисніть **Finish** (Завершити).

Дозвіл Трафіку для Конкретних Програм:

Користувач встановлює нову гру, яка потребує доступу до Інтернету. Windows Firewall запитує дозвіл на доступ для цієї гри. Користувач може створити правило, яке дозволяє цій грі вихідні та вхідні з'єднання через певні порти.

Фільтрація Трафіку за Протоколами та Портами:

Адміністратор мережі хоче обмежити доступ до певного сервісу, який використовує TCP порт 8080. Він створює правило, яке блокує всі вхідні з'єднання на цей порт, забезпечуючи додатковий рівень захисту для внутрішніх ресурсів.

Використання Windows Firewall для Захисту від DoS-атак

Хоча Windows Firewall не є спеціалізованим засобом для захисту від DoS-атак, він може допомогти зменшити ризики та наслідки таких атак. Ось як можна використовувати Windows Firewall для захисту від DoS-атак:

1. **Блокування Підозрілого Трафіку**:

- **Створення Правил для Блокування IP-адрес**: Виявивши підозрілу активність з певних IP-адрес, можна створити правило, яке блокує всі з'єднання з цих адрес.

2. **Обмеження Часу Сеансу**:

- **Налаштування Правил для Обмеження Сеансів**: Встановлення правил, які обмежують тривалість з'єднань, допомагає запобігти перевантаженню серверів.

3. **Використання Розширених Налаштувань**:

- **Створення Правил на Основі Протоколів та Портів**: Блокування невикористовуваних портів та протоколів зменшує можливість використання їх для атак.

Приклад Налаштування Windows Firewall

Створення правила для блокування підозрілих IP-адрес:

1. Відкриваємо **Windows Defender Firewall with Advanced Security**.
2. Потрібно перейти до розділу **Inbound Rules** (Правила для вхідного трафіку).
3. Вибираємо **New Rule** (Нове правило).
4. Вибираємо **Custom** (Користувацьке) і натисніть **Next**.
5. Вибираємо **All programs** (Всі програми) і натисніть **Next**.
6. У розділі **Protocol and Ports** (Протокол і порти) залишаємо налаштування за замовчуванням і натискаємо **Next**.
7. У розділі **Scope** (Область дії) вказуємо IP-адреси або діапазони, які хочемо заблокувати, у полі **Which remote IP addresses does this rule apply to?** (До яких віддалених IP-адрес застосовується це правило?).
8. У розділі **Action** (Дія) вибрали **Block the connection** (Блокувати з'єднання) і натискаємо **Next**.

9. Потрібно вибрати до яких профілів застосовується це правило (доменний, приватний, громадський), і натискаємо **Next.**

10. Називаємо правило, додаємо опис (якщо потрібно), і натискаємо **Finish** (Завершити).

Переваги та Недоліки Windows Firewall

Переваги:

- **Інтеграція з ОС**: Не потребує додаткового встановлення і тісно інтегрується з іншими компонентами Windows.
- **Зручність Налаштувань**: Простий інтерфейс для базових користувачів і розширені налаштування для адміністраторів.
- **Ефективність**: Забезпечує базовий рівень захисту без значного впливу на продуктивність системи.

Недоліки:

- **Обмежена Функціональність у Порівнянні з Платними Брандмауерами**: Деякі комерційні брандмауери пропонують більш розширені функції та налаштування.
- **Залежність від Правильних Налаштувань**: Недосвідчені користувачі можуть ненавмисно залишити систему вразливою, якщо неправильно налаштують брандмауер.

Windows Firewall є потужним інструментом для захисту від небажаних з'єднань. Він дозволяє створювати детальні правила для вхідного і вихідного трафіку, налаштовувати безпекові профілі та вести журнали подій для аналізу підозрілої активності. Використовуючи ці функції, можна значно підвищити рівень безпеки комп'ютера і мережі.

2.2 ZoneAlarm

Це програмний брандмауер для Windows, який надає різні рівні захисту та налаштування.

ZoneAlarm є програмним брандмауером для операційної системи Windows, розробленим для надання комплексного захисту комп'ютерів від шкідливих

програм та несанкціонованого доступу до мережі Інтернет. Він пропонує різні рівні захисту, включаючи відслідковування небезпечних IP-адрес, блокування небажаних веб-сайтів, виявлення та блокування шкідливих програм, контроль за даними, що виходять та входять, і багато іншого. Крім того, ZoneAlarm має можливості налаштування, що дозволяють користувачам настроювати захист з урахуванням їхніх потреб та вимог.

Крім основних функцій брандмауера, ZoneAlarm також може включати додаткові інструменти, такі як антивірусний захист, захист від шпигунського програмного забезпечення, захист від фішингу, а також можливості мережевого моніторингу для виявлення ненормальної активності в мережі. Крім того, він може надавати спеціалізовані інструменти для захисту від конкретних загроз, таких як захист від розповсюдження вірусів через електронну пошту або захист від витоку конфіденційної інформації. У вашій дипломній роботі ви можете дослідити якість захисту, продуктивність та вплив на продуктивність системи, а також порівняти ZoneAlarm з іншими аналогічними програмами для визначення його конкурентних переваг.

Технічні можливості ZoneAlarm включають:

Брандмауер: Здатність моніторити та контролювати вхідні та вихідні мережеві з'єднання, що дозволяє блокувати небажаний трафік та захищати комп'ютер від несанкціонованого доступу.

Антивірусний захист: Можливість виявлення та видалення вірусів, троянських програм, шпигунського програмного забезпечення та інших загроз для комп'ютерної безпеки.

Захист від фішингу: Вбудовані інструменти для виявлення та блокування фішингових веб-сайтів, що намагаються отримати конфіденційну інформацію від користувачів.

Контроль батьків: Функції, що дозволяють батькам встановлювати обмеження на доступ до Інтернету та контролювати використання комп'ютера дітьми.

Автоматичні оновлення: Можливість автоматичного оновлення програм та баз даних, що забезпечує постійну актуальність захисту.

Контроль даних: Функції, що дозволяють моніторити та контролювати передачу даних в мережі, щоб уникнути витоку конфіденційної інформації.

Ці технічні можливості забезпечують високий рівень захисту та контролю над мережевою активністю комп'ютера, що робить ZoneAlarm популярним інструментом для захисту комп'ютерів під управлінням операційної системи Windows.

Ефективність ZoneAlarm полягає у його здатності ефективно виявляти та блокувати різноманітні загрози для комп'ютерної безпеки, такі як віруси, шкідливе програмне забезпечення, фішингові атаки та несанкціонований доступ до мережі. Ця програма пропонує комплексний підхід до захисту, об'єднуючи в собі брандмауер, антивірусний сканер, інструменти контролю батьків та інші функції для максимальної безпеки.

Вплив ZoneAlarm на безпеку полягає в його здатності запобігати успішним атакам та захищати конфіденційні дані користувачів. Шляхом блокування шкідливого трафіку та виявлення потенційно небезпечних дій, ZoneAlarm допомагає зменшити ризик інцидентів з безпекою та забезпечує спокійний режим роботи для користувачів. Враховуючи швидкість реакції на нові загрози та регулярні оновлення, ZoneAlarm допомагає забезпечити високий рівень безпеки для користувачів операційної системи Windows.

ZoneAlarm впливає на продуктивність системи через додаткове програмне навантаження, яке він накладає на операційну систему. Оскільки ZoneAlarm постійно моніторить мережеву активність, виконує антивірусний скан та проводить інші заходи безпеки, це може призвести до певного сповільнення роботи комп'ютера, особливо на старих або менш потужних пристроях.

Проте, важливою є збалансованість між безпекою та продуктивністю. В багатьох випадках невелике сповільнення роботи комп'ютера може бути

прийнятним компромісом для забезпечення надійного захисту від потенційних загроз.

Для дослідження впливу ZoneAlarm на продуктивність системи можна провести тестування швидкості роботи системи з та без програми, а також проаналізувати відгуки користувачів та різні експертні огляди.

налаштування ZoneAlarm:

Встановлення ZoneAlarm:

Потрібно завантажити інсталяційний файл з офіційного сайту ZoneAlarm.

Запустить інсталяційний файл і дотримуватись інструкцій на екрані для завершення встановлення.

Після встановлення потрібно перезавантажити комп'ютер.

Основні налаштування: Відкриваємо ZoneAlarm: Після встановлення запускаємо програму ZoneAlarm.

Налаштування брандмауера:

Переходимо до вкладки "Firewall".

Увімкніть або вимкніть брандмауер, якщо це необхідно.

Вибираємо рівень захисту (наприклад, High, Medium, або Low).

Додайте виключення для певних програм або портів, які повинні мати доступ до мережі.

Налаштування антивірусу:

Переходимо до вкладки "Antivirus & Anti-Spyware".

Встановлюємо частоту автоматичного сканування (наприклад, щоденно або щотижнево).

Увімкаємо реальний захист для автоматичного виявлення загроз у режимі реального часу.

Контроль програм:

У вкладці "Application Control" можна налаштувати доступ програм до інтернету.

Встановлюємо правила для кожної програми (дозволити, блокувати, запитувати).

Захист мережі:

У вкладці "Advanced Firewall" можна налаштувати детальні параметри мережевого захисту.

Встановлюємо фільтри для вхідного та вихідного трафіку, налаштуйте блокування портів.

Логи та звіти:

У вкладці "Logs" переглядаємо історію виявлених загроз та блокувань.

Налаштовуємо автоматичне надсилання звітів на вашу електронну пошту.

Приклади використання ZoneAlarm:

1. **Блокування небажаних програм**:

- Якщо ви виявили програму, яка намагається підключитися до інтернету без вашого дозволу, ви можете заблокувати її у вкладці "Application Control".
- Це дозволить вам уникнути потенційно небезпечного трафіку.

2. **Захист від нових загроз**:

- ZoneAlarm регулярно оновлює базу даних вірусів і шпигунських програм.
- Переконайтесь, що автоматичне оновлення ввімкнено, щоб завжди мати актуальний захист.

3. **Моніторинг активності мережі**:

- Використовується функція моніторингу для перегляду активності мережі в режимі реального часу.
- Це допоможе вам виявити підозрілу активність і вчасно вжити заходів для її блокування.

ZoneAlarm є потужним інструментом для забезпечення безпеки вашої системи, який надає гнучкі налаштування та комплексний захист від різних типів загроз.

Додаткові рекомендації:

1. **Підтримуйте операційну систему та програмне забезпечення в актуальному стані**: Регулярно оновлюйте Windows та інші програми для виправлення вразливостей.
2. **Використовуйте сильні паролі**: Встановіть складні та унікальні паролі для всіх облікових записів.
3. **Будьте обережні з підозрілими електронними листами та посиланнями**: Не відкривайте електронні листи та посилання від невідомих відправників.
4. **Регулярно створюйте резервні копії даних**: Це допоможе відновити важливу інформацію в разі атаки або втрати даних.
5. **Навчайтесь основам кібербезпеки**: Підвищуйте обізнаність про сучасні загрози та методи захисту.

Використовуючи ZoneAlarm та дотримуючись цих рекомендацій, ви значно підвищите рівень безпеки вашого комп'ютера та особистих даних.

Comodo Firewall-це ефективний інструмент для захисту комп'ютера від шкідливих програм та небажаних підключень до Інтернету. Він працює на основі набору правил, що регулюють мережевий трафік. Кожне підключення або програма проходять через ці правила і перевіряються на відповідність зазначеним параметрам безпеки. Якщо певне з'єднання або додаток буде визнано потенційно небезпечним, Comodo Firewall заблокує його або направить користувачам повідомлення про потенційні ризики.

Крім основної функціональності захисту, Comodo Firewall може виявляти й блокувати різноманітні види загроз, такі як віруси, шпигунське програмне забезпечення, троянці та інші форми шкідливого коду. Він також має можливість налаштовувати правила для індивідуальних програм або процесів, щоб керувати їх доступом до мережі. Крім того, Comodo Firewall пропонує користувачеві різноманітні інструменти для моніторингу та аналізу мережевої активності, щоб виявляти потенційні загрози та вразливості в мережі.

Comodo Firewall може блокувати спроби підключення до вашого комп'ютера з невідомих IP-адрес або забороняти програмам відправляти дані на віддалені сервери без вашого дозволу. Крім того, він може реагувати на спроби встановлення з'єднання через вразливі мережеві порти та блокувати атаки типу "брутфорс", коли зловмисники намагаються вгадати паролі для входу на ваш комп'ютер. Всі ці функції допомагають забезпечити повноцінний захист вашого комп'ютера та конфіденційності ваших даних.

Наприклад, якщо ви спробуєте відкрити веб-сайт, що містить шкідливий код або відомий як джерело шкідливого програмного забезпечення, брандмауер Comodo заблокує доступ до цього веб-сайту.

Автоматична заборона

Коли ви встановлюєте нову програму, яка намагається отримати доступ до Інтернету, брандмауер Comodo може автоматично заблокувати цей доступ і попередити вас, щоб ви могли вирішити, дозволити або заблокувати цю програму для встановлення з'єднання.

Вбудований захист від загроз

Брандмауер Comodo виявляє спроби атаки на ваш комп'ютер через відкриті мережеві порти або використання вразливостей програмного забезпечення.

Розширені правила

Ви можете встановити свої власні правила для контролю доступу в Інтернет для кожної програми або служби на вашому комп'ютері, щоб точно налаштувати рівень захисту і конфіденційності.

Основні функції та можливості

Контроль мережевого трафіку:

Фільтрація вхідного та вихідного трафіку: Comodo Firewall контролює весь трафік, що проходить через мережевий адаптер, дозволяючи або блокуючи пакети на основі заданих правил.

Моніторинг активності додатків: Програма відстежує всі активні процеси і додатки, які намагаються отримати доступ до мережі, і надає можливість користувачу дозволити або заблокувати ці спроби.

Захист від вторгнень (HIPS):

Система виявлення та запобігання вторгнень (HIPS): Comodo Firewall включає систему HIPS, яка аналізує поведінку додатків і виявляє потенційно небезпечні дії, запобігаючи атакам нульового дня.

Захист портів та приховування системи:

Stealth Mode: Ця функція дозволяє приховати комп'ютер від сканування портів, ускладнюючи виявлення системи в мережі для потенційних зловмисників.

Віртуальні зони безпеки: Можливість створення віртуальних зон для різних типів мереж, що дозволяє налаштовувати різні рівні безпеки для домашньої, робочої та публічної мережі.

Журнали та звіти:

Детальні звіти: Comodo Firewall надає детальні журнали активності, які включають інформацію про спроби доступу, блокування та дозволені з'єднання.

Аналіз загроз: Інтерфейс дозволяє переглядати і аналізувати загрози та підозрілу активність.

Переваги та недоліки Переваги:

- Високий рівень захисту завдяки технологіям HIPS і фільтрації на рівні ядра.
- Безкоштовна версія з великим набором функцій.
- Інтеграція з хмарними технологіями для аналізу загроз.

Недоліки:

- Можливі конфлікти з іншими програмами безпеки.
- Високий рівень сповіщень може бути складним для недосвідчених користувачів. Налаштування для просунутих користувачів можуть вимагати значних знань про мережеві технології.

Висновок до другого розділу

У другому розділі були детально розглянуті три основні програмні засоби для налаштування брандмауерів у операційній системі Windows: Windows Firewall, ZoneAlarm та Comodo Firewall. Кожен з цих інструментів має свої унікальні характеристики, які роблять його відповідним для різних потреб користувачів.

Розглянуті програмні засоби для налаштування брандмауерів у Windows демонструють різні підходи до забезпечення мережевої безпеки, кожен з яких має свої переваги та особливості.

- **Windows Firewall** є простим та ефективним рішенням для базового захисту, яке інтегрується з операційною системою Windows і не потребує додаткових витрат.
- **ZoneAlarm** надає більш розширені можливості безпеки, включаючи антивірусний захист та VPN, що робить його хорошим вибором для користувачів, які шукають комплексний захист.
- **Comodo Firewall** пропонує найвищий рівень конфігурованості та додаткові функції безпеки, що робить його ідеальним для користувачів, яким потрібен детальний контроль над мережевим трафіком та захист від складних загроз.

Вибір конкретного брандмауера залежить від потреб та вимог користувача. Для базового захисту підійде Windows Firewall, тоді як ZoneAlarm або Comodo Firewall краще використовувати в середовищах, де потрібен більш високий рівень безпеки та можливість гнучкого налаштування. Розуміння можливостей та особливостей кожного з цих інструментів допомагає ефективніше захищати мережеву інфраструктуру від загроз та забезпечувати безпеку даних у сучасному цифровому світі.

РОЗДІЛ 3

pfSense — це відкрите програмне забезпечення, яке надає функціональні можливості для створення брандмауерів та маршрутизаторів. Розроблене на базі FreeBSD, pfSense може бути використане як на фізичних пристроях, так і у віртуальних середовищах.

Основні функції та можливості

Брандмауер:

Фільтрація пакетів: Використовує потужний механізм фільтрації пакетів, що дозволяє визначати, які пакети можуть пройти через мережу на основі різних критеріїв (IP-адреси, порти, протоколи тощо). Списки контролю доступу (ACL): Можливість створення детальних списків контролю доступу для керування мережевим трафіком.

Захист від DoS/DDoS-атак: Вбудовані механізми для виявлення та запобігання атак на відмову в обслуговуванні.

Маршрутизатор:

Статична та динамічна маршрутизація: Підтримка різних протоколів маршрутизації, таких як OSPF, BGP, RIP, що забезпечує ефективний обмін маршрутною інформацією між мережами.

Моніторинг та звіти:

Детальний журнал подій: pfSense надає розширені можливості для журналювання всіх мережевих подій, що дозволяє відстежувати та аналізувати мережеву активність.

Графіки та статистика: Інтерфейс включає в себе різноманітні інструменти для візуалізації мережевого трафіку та стану системи у режимі реального часу.

NetFlow та sFlow: Підтримка протоколів збору та аналізу мережевого трафіку.

Модульність та розширюваність:

- Система плагінів: pfSense підтримує установку додаткових плагінів для розширення функціональності, таких як Squid (проксі-сервер), Snort (система виявлення вторгнень) та інші.

- Веб-інтерфейс: Інтуїтивно зрозумілий веб-інтерфейс для управління всіма аспектами системи, що полегшує налаштування та моніторинг.

Переваги та недоліки

Переваги:

- **Висока стабільність та безпека** завдяки базі FreeBSD.
- **Гнучкість та розширюваність** за допомогою плагінів.
- **Велика спільнота користувачів** та підтримка, що забезпечує постійний розвиток та поліпшення системи.
- **Веб-інтерфейс** робить налаштування та управління зручним навіть для користувачів з мінімальними технічними знаннями.

Недоліки:

- **Високі вимоги до апаратних ресурсів** у випадку великого навантаження або використання багатьох плагінів.
- **Складність налаштувань** для просунутих функцій може вимагати значних знань у сфері мережевих технологій.
- **Обмежена підтримка апаратних платформ** у порівнянні з комерційними рішеннями.

pfSense є потужним, гнучким і безкоштовним рішенням для створення брандмауерів та маршрутизаторів. Завдяки своїм розширеним можливостям, він підходить як для малих мереж, так і для великих корпоративних середовищ. Використання pfSense дозволяє забезпечити високий рівень безпеки та контролю мережевого трафіку, зберігаючи при цьому гнучкість налаштувань і простоту управління. Цей інструмент є відмінним вибором для організацій, які потребують надійного і економічного рішення для захисту своєї мережевої інфраструктури.

Налаштування pfSense може бути здійснене через інтуїтивно зрозумілий веб-інтерфейс. з налаштування pfSense.

1. Завантаження образу pfSense:

- Перейдіть на офіційний сайт pfSense (https://www.pfsense.org/).

- Завантажте ISO-образ для вашої платформи (наприклад, x86 або x64).

2. Створення завантажувального носія:

- Використовуємо програму для створення завантажувальних USB-носіїв, наприклад, Rufus для Windows або dd для Linux/Mac.
- Записуємо ISO-образ на USB-носій.

3. **Встановлення pfSense**:

- Встановлюємо USB-носій у сервер або комп'ютер, на який плануємо встановити pfSense.
- Перезавантажуємо систему і вибераємо завантаження з USB-носія.
- Дотримуйтесь інструкцій установника pfSense для завершення процесу інсталяції.

2. Початкове налаштування

1. **Перший запуск і базове налаштування**:

- Після успішного встановлення і перезавантаження системи ви побачите командний рядок pfSense.
- Введіть логін за замовчуванням (admin) і пароль (pfsense).

2. **Ініціалізація веб-конфігуратора**:

- Підключіть ваш комп’ютер до LAN-порту вашого pfSense пристрою.
- Відкрийте веб-браузер і введіть IP-адресу LAN-інтерфейсу pfSense (за замовчуванням це 192.168.1.1).
- Логіньтеся використовуючи логін (admin) і пароль (pfsense).

Додаткові налаштування

1. **Плагіни та розширення**:

- Перейдіть до **System** > **Package Manager**.
- Встановлюйте додаткові пакети для розширення функціональності pfSense, такі як Snort для виявлення вторгнень або Squid для проксі-сервера.

2. **Безпека та оновлення**:

- Переконайтеся, що ви використовуєте останню версію pfSense для забезпечення безпеки.
- Перевіряйте та встановлюйте оновлення через **System** > **Update**.

налаштувати pfSense як брандмауер та маршрутизатор для вашої мережі. Завдяки широкому спектру можливостей та гнучкості налаштувань, pfSense є потужним інструментом для забезпечення безпеки та ефективності мережевої інфраструктури.

iptables — це потужний і гнучкий інструмент для налаштування та управління правилами фільтрації мережевого трафіку в операційних системах на базі Linux. Використовується для створення брандмауерів, які допомагають забезпечити безпеку мережі, контролюючи доступ до ресурсів і блокуючи шкідливий трафік.

Модулі та розширення:

- iptables підтримує різноманітні модулі для розширення функціональності, наприклад, для обмеження швидкості, логування, встановлення маркерів на пакети тощо.
- **xtables-addons**: Пакет додаткових модулів для розширення можливостей iptables.

Інтерфейс та зручність користування

Командний рядок:

Основним способом налаштування iptables є використання командного рядка. Це дозволяє детально налаштовувати правила, але може вимагати значних технічних знань.

Приклади команд:

Додавання правила: iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Перегляд правил: iptables -L

Видалення правила: iptables -D INPUT 1

для автоматизації:

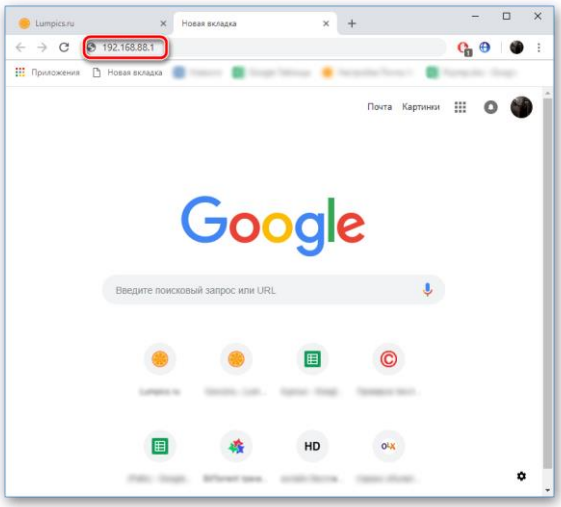
Правила iptables часто зберігаються у вигляді скриптів, які виконуються при завантаженні системи. Це спрощує управління та забезпечує стійкість налаштувань після перезавантаження.

Графічні інтерфейси:

Для спрощення налаштування iptables існують графічні інтерфейси, такі як Shorewall або GUFW, які роблять процес створення та управління правилами більш доступним для користувачів без глибоких знань командного рядка.

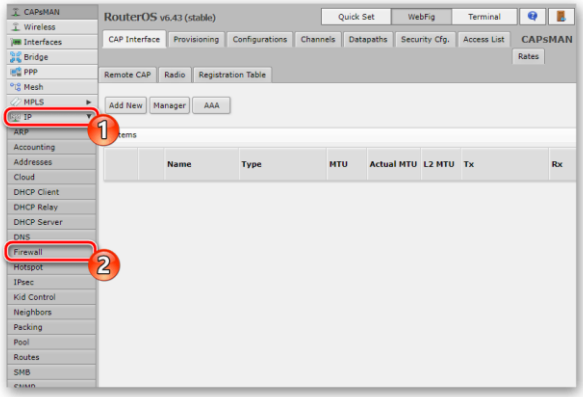
Налаштування firewall роутера Mikrotik

Потрібно перейти за адресою 192.168.88.



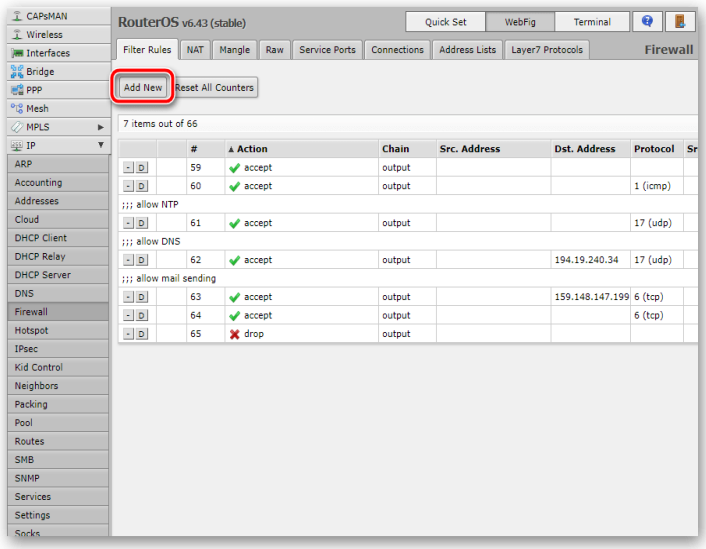
У стартовому вікні веб-інтерфейсу роутера вибераємо 171;Webfig&187;

Потрібно розгорнуть категорію «IP» і перейти до розділу «Firewall»



Видаляємо усі існуючі правила,натиснувши відповідну кнопку.Це необхідно зробити для того, щоб в майбутньому при створенні власної конфігурації не виникали конфлікти.

Якщо увійшли в меню через браузер, перехід до вікна створення настройки здійснюється через кнопку «Add»



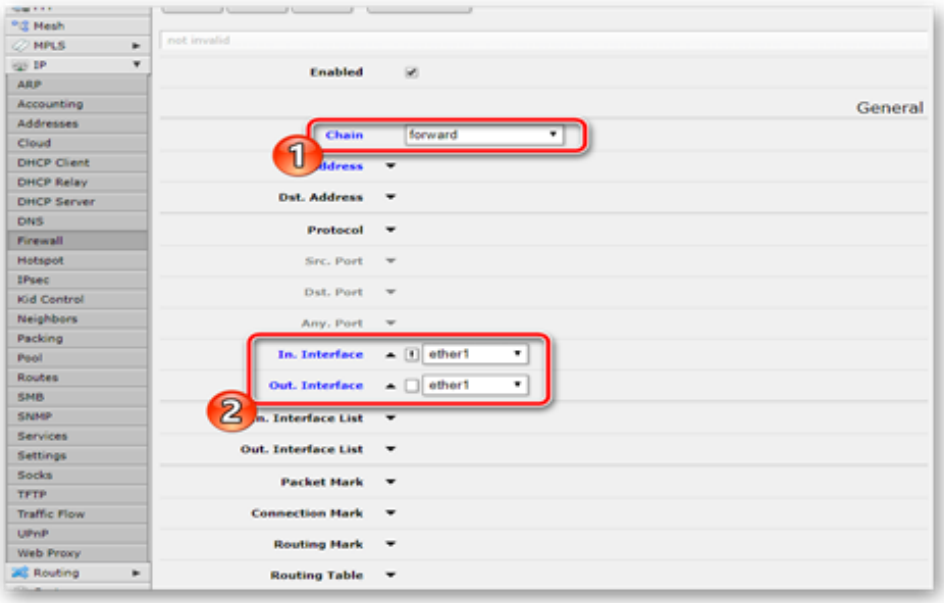
Перевірка зв'язку пристрою

З'єднаний з комп'ютером роутер іноді перевіряється операційною системою Windows на наявність активного підключення. Запустити такий процес можна і вручну, проте доступно це звернення буде тільки в тому випадку, якщо в фаєрволі присутній правило, що дозволяє зв'язок з ОС. Налаштовується воно наступним чином.

Дозвіл проходження трафіку з локальної мережі в інтернет

Робота в операційній системі RouterOS дозволяє розробляти безліч конфігурацій проходження трафіку. Ми не буде зупинятися на цьому, оскільки звичайним користувачам такі знання не знадобляться. Розглянемо тільки одне правило фаєрвола, що дозволяє проходити трафіку з локальної мережі в інтернет

Вибераємо «Chain» &8212; «Forward» . Задавати «In. Interface» і «Out. Interface» значення «Ether1» , після чого відзначте знаком оклику «In. Interface» .



Врозділі «Action» вибераємо дію «Accept»

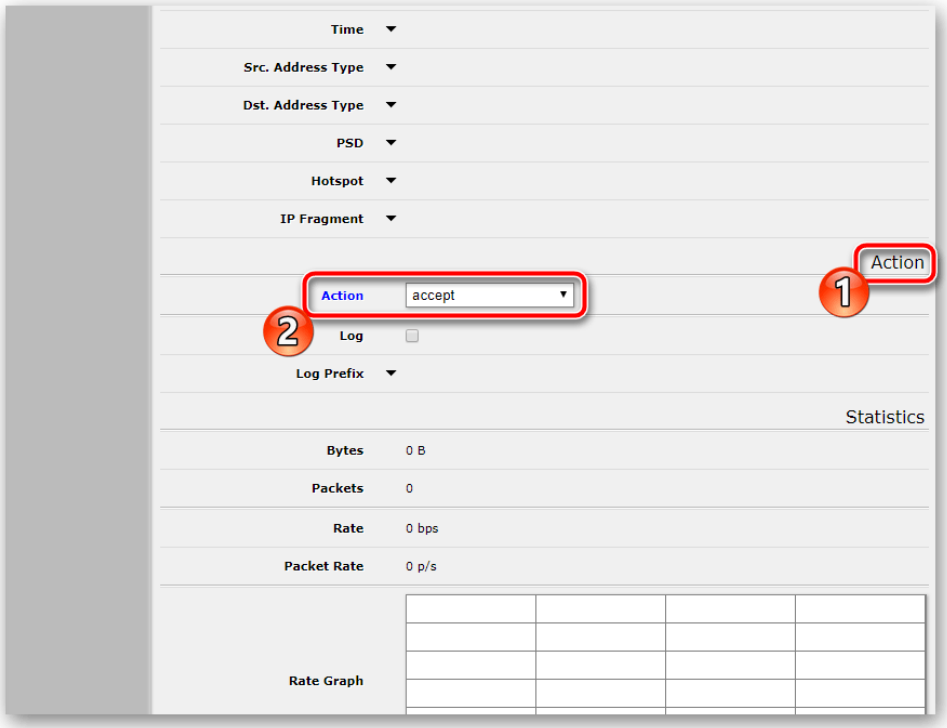
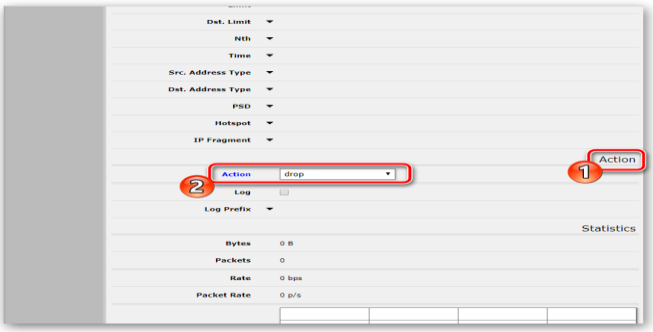


Рисунок 3. -

Рисунок 3. - В «Action» переконуємось, що варто «Drop»



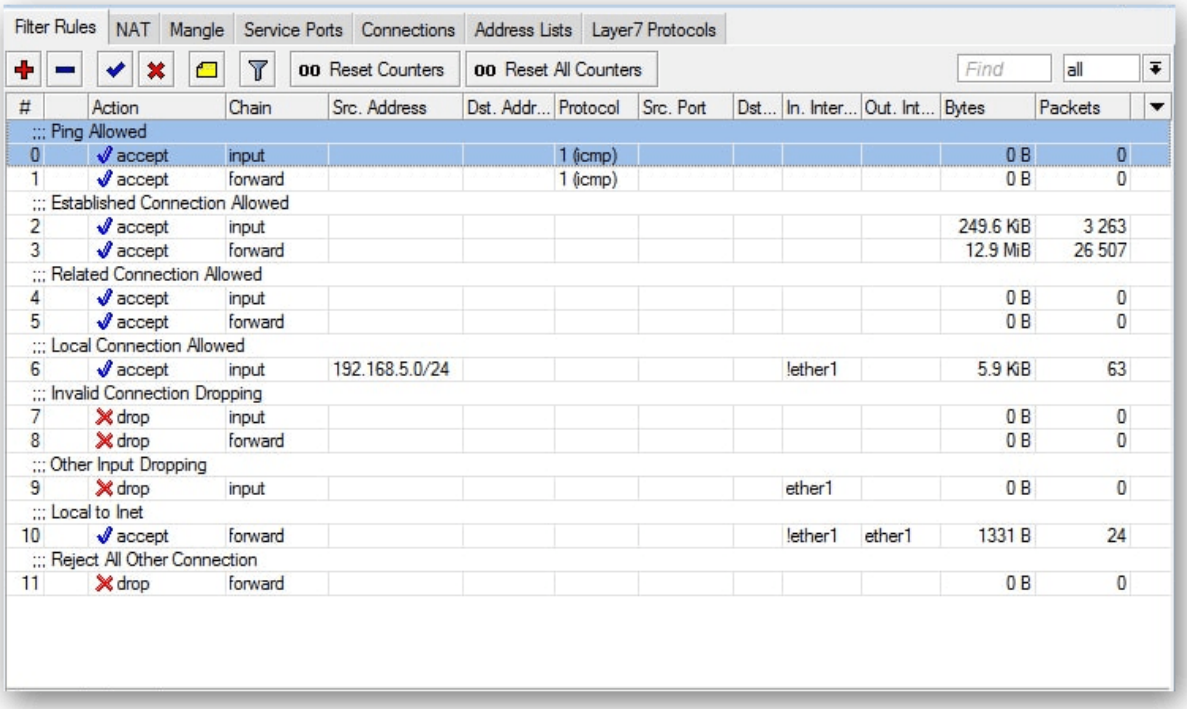


Рисунок 3. - схема firewall

Висновок до 3 розділу

У третьому розділі були детально розглянуті два потужні інструменти для налаштування та управління брандмауерами в системах на базі UNIX та Linux: pfSense та iptables. Кожен з цих інструментів має свої унікальні властивості, які роблять їх незамінними для забезпечення мережевої безпеки у різних середовищах.

pfSense:

- pfSense є відкритим програмним забезпеченням для налаштування брандмауерів та маршрутизаторів на базі FreeBSD.
- Відрізняється гнучкістю налаштувань, що дозволяє використовувати його як у малих домашніх мережах, так і в великих корпоративних середовищах.
- Пропонує широкий спектр функцій, таких як VPN, DHCP, DNS, NAT, що робить його багатофункціональним інструментом для мережевих адміністраторів.
- Інтуїтивно зрозумілий веб-інтерфейс забезпечує зручність налаштування і управління, що значно спрощує роботу навіть для користувачів без глибоких технічних знань.

iptables:

- iptables є інструментом для налаштування правил фільтрації мережевого трафіку в операційних системах на базі Linux.
- Відрізняється високою продуктивністю та надійністю завдяки інтеграції в ядро Linux.
- Забезпечує детальний контроль над мережевим трафіком завдяки можливості створення складних правил фільтрації та маршрутизації.
- Підтримує різноманітні модулі та розширення, що дозволяє налаштовувати правила відповідно до конкретних потреб мережі

Розглянуті інструменти pfSense та iptables демонструють різні підходи до забезпечення мережевої безпеки в системах на базі UNIX та Linux. Обидва інструменти мають свої переваги та можуть використовуватись у різних середовищах залежно від конкретних потреб.

pfSense є відмінним вибором для користувачів, які потребують зручний у використанні та багатофункціональний брандмауер з можливістю гнучкого налаштування та широким спектром підтримуваних сервісів.

iptables підходить для системних адміністраторів та досвідчених користувачів, які потребують високий рівень контролю над мережевим трафіком та готові працювати з командним рядком для створення складних правил фільтрації.

Таким чином, обидва інструменти є важливими складовими сучасної мережевої інфраструктури і забезпечують надійний захист від зовнішніх та внутрішніх загроз. Вибір між pfSense та iptables залежить від конкретних вимог та умов експлуатації, а розуміння їх можливостей дозволяє ефективно захищати мережі та дані у сучасному цифровому світі.

ВИСНОВКИ

У сучасному цифровому світі, де обсяг інформації та кількість користувачів комп'ютерних мереж постійно зростають, питання захисту інформації набуває надзвичайної важливості. В рамках цієї дипломної роботи проведено комплексний аналіз сучасних методів захисту комп'ютерних мереж від зловмисників, що дозволило виявити ключові тенденції, проблеми та ефективні стратегії у цій сфері.

Дослідження показало, що зловмисники постійно вдосконалюють свої методи атак, що робить традиційні методи захисту менш ефективними. Сучасні загрози, такі як розподілені атаки типу «відмова в обслуговуванні» (DDoS), фішинг, шкідливе ПЗ та атаки на основі соціальної інженерії, вимагають нових підходів до захисту. У зв'язку з цим, організації повинні інвестувати у постійне оновлення систем безпеки та навчання персоналу.

По-друге, було виявлено, що ефективний захист мережі базується на багатошаровому підході. Це включає використання різноманітних технологій та рішень, таких як міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень (IDS/IPS) Кожен з цих елементів має свої переваги і недоліки, але у поєднанні вони забезпечують високий рівень захисту.

Кожен з цих елементів має свої переваги і недоліки, але у поєднанні вони забезпечують високий рівень захисту.

У результаті проведеного дослідження можна зробити висновок, що ефективний захист комп'ютерних мереж від зловмисників вимагає комплексного підходу, який поєднує технічні, організаційні та правові заходи. Постійний розвиток технологій безпеки, впровадження інноваційних рішень та підвищення рівня обізнаності персоналу є ключовими факторами успішного захисту від сучасних загроз.

Таким чином, для забезпечення належного рівня безпеки комп'ютерних мереж організаціям необхідно здійснювати безперервний моніторинг і аналіз загроз, впроваджувати багаторівневі системи захисту, дотримуватись законодавчих вимог та постійно підвищувати кваліфікацію співробітників у

сфері кібербезпеки. Це дозволить мінімізувати ризики та забезпечити надійний захист інформаційних ресурсів від зловмисників.

Одним з ключових чинників успішного захисту мереж є навчання та підвищення обізнаності користувачів щодо кібербезпеки. Навіть найефективніші технічні рішення можуть виявитися недостатніми, якщо співробітники організації не дотримуються базових правил безпеки. Регулярні тренінги та симуляції атак допомагають користувачам розпізнавати фішингові повідомлення, небезпечні веб-сайти та інші загрози, що значно знижує ризик успішних атак.

Також необхідно враховувати аспекти фізичної безпеки, адже доступ до фізичної інфраструктури мережі може дозволити зловмисникам здійснювати атаки, які неможливо виявити засобами кібербезпеки. Забезпечення контролю доступу до серверних приміщень, використання камер відеоспостереження та інших заходів фізичної безпеки є невід'ємною частиною загальної стратегії захисту.

Можна зробити висновок, що захист комп'ютерних мереж від зловмисників – це складний і багатогранний процес, який вимагає комплексного підходу. Комбінування технічних, організаційних та правових заходів, впровадження передових технологій, таких як штучний інтелект та блокчейн, а також постійне навчання співробітників та оновлення систем безпеки є ключовими факторами успішного захисту.

У майбутньому важливо продовжувати дослідження та розвиток нових методів і технологій захисту, адже зловмисники не стоять на місці і постійно шукають нові способи обійти системи безпеки. Тільки завдяки постійному вдосконаленню та адаптації до нових викликів можна забезпечити надійний захист комп'ютерних мереж і мінімізувати ризики від Зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 1.Stallings, W. (2018). Network Security Essentials: Applications and Standards. Pearson Education.
2. 2.Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
3. 3.Bishop, M. (2005). Introduction to Computer Security. Addison-Wesley.
4. 4.Pfleeger, C. P., & Pfleeger, S. L. (2007). Security in Computing. Prentice Hall.
5. 5.Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
6. 6.Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94.
7. 7.Kizza, J. M. (2020). Guide to Computer Network Security. Springer.
8. 8.Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security. Cengage Learning.
9. 9.Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson.
10. 10.Shinder, D. L. (2013). Firewalls Don't Stop Dragons: A Step-by-Step Guide to Computer Security for Non-Techies. Apress.
11. 11.Mocanu, D. C., & Mocanu, E. (2018). Deep Learning for Network Security. Springer.
12. 12.Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82.
13. 13.Li, J., & Chen, H. (2019). Blockchain Technology and Its Applications in the Security Field. Springer.
14. 14.Tanenbaum, A. S., & Wetherall, D. J. (2010). Computer Networks. Pearson Education.
15. 15.Gollmann, D. (2011). Computer Security. Wiley.

16. 16.Viega, J., & McGraw, G. (2002). Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.

17. 17.ENISA. (2020). Threat Landscape 2020: Cyber Threats and Trends. European Union Agency for Cybersecurity.

18. 18.Goodrich, M. T., & Tamassia, R. (2011). Introduction to Computer Security. Addison-Wesley.

19. 19.Wagner, D., & Schneier, B. (1996). Analysis of the SSL 3.0 Protocol. USENIX Security Symposium.

20. 20.Cisco Systems. (2020). Cisco Firepower Next-Generation Firewall (NGFW) Data Sheet. Cisco Press.

21. 21.Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. Proceedings of the 25th Annual Network and Distributed System Security Symposium.

22. 22.Miller, M. (2016). The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World. Pearson Education.

23. 23.Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A Survey of Topics and Trends. Information Systems Frontiers, 17(2), 261-274.

24. 24.Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

25. 25.Gartner, Inc. (2021). Top Security and Risk Management Trends. Gartner Research.