

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

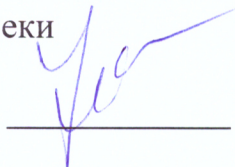
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту мережевої
інфраструктури на базі рішення pfSense з інтеграцією
MS Active Directory»

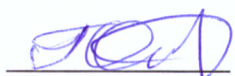
Виконав студент 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 А.М. Григорусь

Керівник старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 І.Г. Фальковський

Рецензент доцент кафедри комп'ютерної інженерії та
кібербезпеки, к.пед.н., доцент

 О.С. Головня

Житомир – 2024

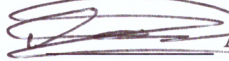
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Григорусь Антон Миколайович

Тема роботи: «Методи та технології захисту мережевої інфраструктури на базі рішення pfSense з інтеграцією MS Active Directory»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 26 грудня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

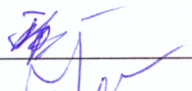
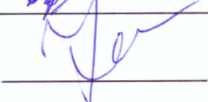
1. Топологія мережевої інфраструктури.
2. Використання pfSense та MS Active Directory

Обладнання та програмне забезпечення:

1. ОС Windows Server 2019
2. ОС Windows 10
3. Дистрибутив pfSense CE (v.2.7.2)

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О.О. Шелуха	17.09.2024	14.10.2024
2	О.О. Шелуха	15.10.2024	22.11.2024
3	О.О. Шелуха	23.11.2024	23.12.2024

Студент  А.М. Григорусь
Керівник  І.Г. Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024	Виконано
2	Аналіз літературних джерел	24.09.2024	Виконано
3	Огляд теоретичних аспектів MS Active Directory	01.10.2024	Виконано
4	Аналіз класифікації та призначення міжмережевих екранів	08.10.2024	Виконано
5	Порівняння безкоштовних рішень з відкритим кодом	15.10.2024	Виконано
6	Дослідження функціональних можливостей pfSense	22.10.2024	Виконано
7	Розробка топології та адресації	29.10.2024	Виконано
8	Вибір методів та механізмів захисту	05.11.2024	Виконано
9	Вибір обладнання	16.11.2024	Виконано
10	Налаштування мережі та обраних функцій захисту	05.12.2024	Виконано
11	Тестування працездатності мережі	15.12.2024	Виконано
12	Написання пояснювальної записки	23.12.2024	Виконано
13	Захист	26.12.2024	Виконано

Студент  А.М. Григорусь
Керівник  І.Г. Фальковський

АНОТАЦІЯ

Випускна кваліфікаційна робота складається з пояснювальної записки, що містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 78 сторінках друкованого тексту. Пояснювальна записка має 9 сторінок додатків. Список використаних джерел містить 22 найменування і займає 2 сторінки. В роботі наведено 63 рисунки та 2 таблиці. Загальний обсяг роботи 87 сторінки.

Метою кваліфікаційної роботи є дослідження методів та технологій захисту мережевої інфраструктури на базі рішення pfSense з інтеграцією MS Active Directory та проєктування мережевої інфраструктури з використанням згаданих рішень.

В ході роботи розглянуто теоретичні аспекти роботи Active Directory і його компоненти. Проаналізовано різновиди міжмережевих екранів, їх класифікацію та функціональні можливості. Проведено порівняння безкоштовних програмних маршрутизаторів і міжмережевих екранів з відкритим кодом, перераховано функціональні можливості та особливості pfSense.

Розроблено топологію та адресацію мережі організації. Виконано вибір методів та механізмів захисту для подальшої їх реалізації в проєкті і обрано необхідне обладнання для реалізації мережі.

Практично реалізовано та налаштовано проєкт мережі в емуляторі GNS3 із використанням VirtualBox. Протестовано наявність зв'язку між усіма компонентами. Здійснено налаштування додаткових функцій захисту та виконано їх тестування, яке підтвердило їх ефективність в захисті мережі та коректність всіх виконаних налаштувань проєкту.

КЛЮЧОВІ СЛОВА: MICROSOFT, ACTIVE DIRECTORY, МЕРЕЖА, МІЖМЕРЕЖЕВИЙ ЕКРАН, PFSense, ЗАХИСТ, ТОПОЛОГІЯ, ДОМЕН.

ANNOTATION

The final qualification paper consists of an explanatory note, which includes an introduction, three chapters, conclusions, a list of references, and appendices. The main text is presented on 78 pages of printed text. The explanatory note includes 9 pages of appendices. The list of references contains 22 entries and occupies 2 pages. The work includes 63 figures and 2 tables. The total volume of the paper is 87 pages.

The purpose of the qualification work is to study the methods and technologies for protecting network infrastructure based on the pfSense solution with MS Active Directory integration and to design a network infrastructure using these solutions.

The paper examines the theoretical aspects of Active Directory and its components. It analyzes various types of firewalls, their classification, and functional capabilities. A comparison of free software routers and open-source firewalls was conducted, listing the features and functionalities of pfSense.

The network topology and addressing for the organization were developed. Methods and mechanisms for protection were selected for further implementation in the project, and the necessary equipment for network deployment was chosen.

The network project was practically implemented and configured in the GNS3 emulator using VirtualBox. Connectivity between all components was tested. Additional security features were configured and tested, confirming their effectiveness in network protection and the correctness of all project settings.

KEYWORDS: MICROSOFT, ACTIVE DIRECTORY, NETWORK, FIREWALL, PFSense, SECURITY, TOPOLOGY, DOMAIN.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ACTIVE DIRECTORY ТА PFSense.....	10
1.1. Теоретичні аспекти роботи Active Directory	10
1.2. Різновид і призначення міжмережевих екранів.....	14
1.3. Порівняння відомих безкоштовних програмних маршрутизаторів/міжмережевих екранів	17
1.4. Відомості і функціональні можливості щодо pfSense	23
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПРОЄКТУ МЕРЕЖІ, МЕТОДІВ ЗАХИСТУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	29
2.1. Розробка топології та адресації	29
2.2. Вибір методів та механізмів захисту	35
2.3 Вибір обладнання для організації роботи мережі	38
РОЗДІЛ 3. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ	42
3.1. Базове налагодження проєкту мережі	42
3.2. Базове налагодження pfSense	52
3.3. Налаштування та перевірка додаткових функцій безпеки pfSense	56
3.4. Тестування діагностичних та моніторингових утиліт pfSense	66
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	77
ДОДАТКИ.....	79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – Операційна система

GDPR – General Data Protection Regulation

HIPAA – Health Insurance Portability and Accountability Act

MS – Microsoft

VPN – Virtual Private Network

NAT – Network Address Translation

DDoS – Distributed Denial of Service

AD – Active Directory

OU – Organizational Unit

SAML – Security Assertion Markup Language

SSO – Single Sign-On

DACL – Discretionary Access Control List

ADFS – Active Directory Federation Services

HTTP – Hypertext Transfer Protocol

NGFW – Next-Generation Firewall

IDPS – Intrusion Detection and Prevention Systems

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

LAN – Local Area Network

WAN – Wide Area Network

DHCP – Dynamic Host Configuration Protocol

PAT – Port Address Translation

PoE – Power over Ethernet

ВСТУП

Актуальність теми. Сьогодні, в умовах швидкої цифровізації бізнес-процесів і активного розвитку хмарних технологій, питання захисту мережевої інфраструктури стає критичним для забезпечення надійності й безперервності роботи організацій. Зростання кіберзагроз і поширення складних атак, таких як фішинг, атаки типу "відмова в обслуговуванні" (DDoS), а також зловживання привілеями користувачів, вимагають застосування сучасних підходів до захисту корпоративних мереж.

pfSense – це надійне рішення з відкритим кодом, яке дозволяє створити масштабовану систему безпеки з можливістю тонкого налаштування правил фільтрації, контролю трафіку та виявлення атак. Завдяки інтеграції з Microsoft Active Directory, pfSense надає організаціям можливість централізованого управління доступом і політиками безпеки, що є особливо важливим для середніх і великих компаній, де присутня значна кількість користувачів і складна внутрішня структура.

Використання Active Directory у поєднанні з pfSense дозволяє оптимізувати управління правами доступу до різних сегментів мережі, знижуючи ризик несанкціонованого доступу і підвищуючи ефективність контролю за активністю користувачів. Це особливо актуально для компаній з чутливими даними, які підпадають під регуляторні вимоги, такі як GDPR, HIPAA тощо.

Метою кваліфікаційної роботи є дослідження методів та технологій захисту мережевої інфраструктури на базі рішення pfSense з інтеграцією MS Active Directory.

Поставлена мета передбачає виконання таких завдань:

- Аналіз аспектів роботи Active Directory;
- Дослідження класифікації та призначення міжмережевих екранів;
- Порівняння безкоштовних рішень;
- Розробка топології мережі та вибір обладнання;
- Вибір методів та механізмів захисту;

– Налаштування проекту мережі та обраних рішень і перевірка ефективності їх роботи.

Об’єктом дослідження є процес проєктування захищеної мережевої інфраструктури організації.

Предметом дослідження є комплексні методи і технології захисту мережевої інфраструктури шляхом поєднання функціоналу pfSense з можливостями Microsoft Active Directory.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ACTIVE DIRECTORY ТА PFSense

1.1. Теоретичні аспекти роботи Active Directory

Active Directory (AD) – це сервіс каталогів від Microsoft, розроблений для організації і управління інформаційними ресурсами мережі. Основною функцією AD є централізоване управління доступом до ресурсів організації, включаючи користувачів, комп'ютери, принтери та інші мережеві об'єкти. Система Active Directory була вперше представлена в Windows 2000 Server і з того часу зазнала багатьох удосконалень. Основні функції AD включають аутентифікацію, авторизацію та управління ресурсами, що робить її одним із найпоширеніших рішень для корпоративних мереж.

Структура Active Directory

Active Directory є ієрархічною структурою, яка забезпечує зручне управління об'єктами в мережі. Її базова структура складається з декількох рівнів [1]:

1. Ліс (Forest) – це найвищий рівень структури Active Directory. Ліс об'єднує кілька доменів (Domains), кожен з яких представляє окрему одиницю управління. Всі домени в лісі мають спільну конфігурацію і схему, що дозволяє їм взаємодіяти один з одним. Ліс є логічною структурою, яка об'єднує всі домени в єдину екосистему.

2. Домен (Domain) – це основна одиниця в AD, яка об'єднує об'єкти, такі як користувачі, групи та комп'ютери. Домен забезпечує ізоляцію даних і політик, що спрощує управління та підвищує безпеку. Кожен домен має власну базу даних, яка зберігає інформацію про об'єкти, а також контролери домену, що відповідають за аутентифікацію і авторизацію.

3. Дерево (Tree) – це набір доменів, які мають загальний простір імен і можуть взаємодіяти між собою. Домен, доданий до дерева, автоматично успадковує властивості батьківського домену.

4. Одиниці організації (Organizational Units, OU) – це контейнерні об'єкти, які використовуються для організації ресурсів усередині домену. Вони дозволяють групувати об'єкти за функціональними або структурними ознаками, що спрощує управління доступом і політиками. Наприклад, відділи організації можуть бути представлені у вигляді окремих OU.

5. Об'єкти (Objects) – це основні елементи в Active Directory. Вони включають користувачів, комп'ютери, принтери, групи та інші ресурси. Кожен об'єкт має набір атрибутів (наприклад, ім'я, пароль, членство в групах), які визначають його властивості.

Функції Active Directory

Основними функціями Active Directory є:

- Аутентифікація користувачів і пристроїв – це процес перевірки особистості користувача або пристрою. Використання централізованої аутентифікації через AD дозволяє спростити процес входу користувачів у систему і забезпечує єдину точку доступу до всіх ресурсів в домені.

- Авторизація – визначення прав доступу користувача до ресурсів мережі на основі його ролей і налаштувань безпеки. Active Directory дозволяє налаштовувати різноманітні політики безпеки для різних об'єктів і груп, обмежуючи доступ до певних ресурсів на основі потреб користувача або пристрою.

- Управління об'єктами та ресурсами – AD дозволяє централізовано керувати всіма об'єктами мережі. Адміністратори можуть створювати, видаляти та змінювати об'єкти, а також призначати політики безпеки і доступу.

- Групові політики (Group Policy) – це механізм управління конфігурацією комп'ютерів і користувачів у домені. Політики дозволяють адміністратору налаштовувати параметри системи, зокрема безпеку, встановлення програмного забезпечення, параметри браузера тощо. Групові політики дозволяють швидко і централізовано застосовувати зміни для всіх комп'ютерів і користувачів у домені.

- Моніторинг і аудит – Active Directory забезпечує інструменти для відстеження подій, таких як входи в систему, зміни об'єктів чи політик, а також

спроби доступу до ресурсів. Це дозволяє адміністраторам аналізувати активність у мережі, виявляти потенційні загрози і забезпечувати відповідність вимогам безпеки.

Аутентифікація та безпека

Active Directory підтримує кілька методів аутентифікації, таких як:

- Kerberos – основний протокол для аутентифікації в AD, який забезпечує високий рівень безпеки завдяки використанню квитків доступу та криптографічних методів.

- NTLM (NT LAN Manager) – старіший протокол, який застосовується для сумісності зі старими версіями Windows [2]. Хоча NTLM не такий безпечний, як Kerberos, він все ще використовується в певних випадках.

- SAML (Security Assertion Markup Language) – це протокол для забезпечення єдиного входу (SSO) у сторонні додатки, що інтегрується з Active Directory Federation Services (ADFS) [3].

Управління безпекою в AD також передбачає налаштування групових політик, які дозволяють визначати різні обмеження та правила для користувачів і комп'ютерів. Наприклад, можна налаштувати вимоги до паролів, автоматичне блокування облікових записів у випадку підозрілої активності, обмеження доступу до певних файлів або програм.

Реплікація даних і контроль доступу

Active Directory підтримує реплікацію даних між контролерами домену, що забезпечує високу доступність і надійність системи. Реплікація дозволяє розподіляти оновлення інформації між усіма контролерами домену в домені або лісі, забезпечуючи актуальність даних на кожному вузлі. Це особливо важливо в розподілених мережах, де декілька фізичних локацій організації використовують одну і ту ж базу даних AD.

Для контролю доступу AD використовує дискреційні списки контролю доступу (DACL), які визначають права доступу до об'єктів. Кожен об'єкт має DACL, де вказано, які користувачі або групи мають право на читання, зміну або видалення цього об'єкта. Завдяки DACL можна налаштувати доступ на

детальному рівні, що підвищує безпеку і дозволяє застосовувати специфічні політики безпеки до різних об'єктів.

Логічна структура AD, яка включає ліс, домени, OU та об'єкти, спрямована на спрощення управління ресурсами в мережі та забезпечення чіткого поділу прав і ролей. Водночас AD має фізичну структуру, що відображає розподіл контролерів домену і зв'язків між ними.

- Сайти (Sites) – це елементи фізичної структури AD, які представляють собою фізичні локації мережі, наприклад офіси в різних містах. Сайти допомагають оптимізувати реплікацію, зменшуючи навантаження на мережу та покращуючи швидкість доступу до ресурсів.

- Контролери домену (Domain Controllers) – це сервери, які зберігають копії бази даних AD і відповідають за аутентифікацію, авторизацію та інші функції, пов'язані з безпекою [4].

Довірчі відносини між доменами

Active Directory підтримує створення довірчих відносин між доменами, що дозволяє користувачам одного домену отримувати доступ до ресурсів іншого домену. Це є важливим аспектом у великих організаціях, де існують кілька доменів. Довірчі відносини можуть бути односторонніми або двосторонніми, що визначає напрямок доступу між доменами. Вони також можуть бути транзитивними або нетранзитивними, що визначає можливість поширення довіри на інші домени в лісі.

Служби Federation Services і Lightweight Directory Services

Для додаткової функціональності Active Directory включає такі сервіси, як Active Directory Federation Services (ADFS) та Active Directory Lightweight Directory Services (AD LDS).

- ADFS дозволяє реалізувати єдиний вхід (SSO) і забезпечує доступ до сторонніх додатків за допомогою стандартів, таких як SAML, що полегшує інтеграцію з хмарними рішеннями та іншими сервісами.

- AD LDS надає функціональність каталогів, схожу на AD, але є легшим і призначеним для додатків, які потребують автономної бази даних без повної інфраструктури домену.

1.2. Різновид і призначення міжмережевих екранів

Міжмережеві екрани (або фаєрволи) є основним елементом захисту сучасних мережових інфраструктур. Вони виконують функцію фільтрації трафіку між мережами, дозволяючи або забороняючи доступ до ресурсів відповідно до заданих правил. Завдяки різноманітності технологій, сучасні міжмережеві екрани здатні забезпечувати захист не лише на основі простих правил, але й аналізувати поведінкові аспекти трафіку, виявляти шкідливі дії та протидіяти складним атакам. Далі розглянемо основні різновиди міжмережевих екранів та їх призначення [5].

Класифікація міжмережевих екранів за типом обробки трафіку

Залежно від способу обробки трафіку міжмережеві екрани поділяються на кілька основних типів [6]:

1. Пакетні фільтри (Packet Filters) – це один із найпростіших видів міжмережевих екранів, що працюють на мережевому та транспортному рівнях моделі OSI. Пакетні фільтри дозволяють або блокують трафік на основі IP-адреси, порту і протоколу. Основна перевага цього підходу – його висока швидкість обробки, однак такі екрани не можуть аналізувати зміст пакетів, що обмежує їхню здатність до виявлення складних атак.

2. Міжмережеві екрани стану (Stateful Firewalls) – це вдосконалена версія пакетних фільтрів, яка веде облік станів з'єднань. Вони перевіряють не тільки окремі пакети, а й стежать за контекстом з'єднань, дозволяючи відстежувати, чи є пакет частиною встановленого з'єднання. Така функція підвищує безпеку, оскільки знижується ризик проходження небажаного трафіку. Цей тип фаєрволів здатен захищати мережу від певних видів атак, таких як spoofing та DDoS [7].

3. Проксі-фаєрволи (Proxy Firewalls) – міжмережеві екрани цього типу виступають як посередники між кінцевими точками з'єднання. Вони приймають

запити від клієнта, аналізують їх і, при схваленні, передають на сервер. Проксі-фаєрволи можуть виконувати перевірку трафіку на рівні додатків, що підвищує рівень безпеки і дає можливість фільтрації небажаного контенту або додатків. Однак проксі-фаєрволи знижують швидкість роботи через необхідність обробки трафіку на додатковому рівні.

4. Міжмережеві екрани на рівні додатків (Application Layer Firewalls) – ці фаєрволи працюють на рівні додатків і можуть аналізувати вміст пакетів, визначаючи допустимість запитів залежно від специфіки додатків. Вони здатні захищати від атак, які зловживають протоколами рівня додатків, наприклад, від SQL-ін'єкцій або атак на основі HTTP. Такий тип екранів зазвичай використовують для захисту веб-додатків.

5. Гібридні міжмережеві екрани (Hybrid Firewalls) – комбінують у собі функції різних типів фаєрволів. Наприклад, вони можуть поєднувати можливості станового фаєрвола та проксі-функціонал для аналізу на рівні додатків. Завдяки цьому, гібридні фаєрволи забезпечують вищий рівень безпеки, дозволяючи одночасно фільтрувати трафік на кількох рівнях моделі OSI.

Міжмережеві екрани за місцем встановлення в мережі

За місцем установки в мережі, міжмережеві екрани також поділяються на різні категорії:

1. Периметрові фаєрволи (Perimeter Firewalls) – встановлюються на межі мережі, відокремлюючи її від зовнішнього середовища. Вони захищають внутрішню мережу від зовнішніх загроз, дозволяючи або блокуючи трафік залежно від заданих правил. Це найпоширеніший тип міжмережевих екранів, оскільки саме периметровий захист є першим рубежем безпеки організації.

2. Внутрішні фаєрволи (Internal Firewalls) – встановлюються всередині мережі для поділу різних сегментів, наприклад, між відділами організації. Внутрішні фаєрволи допомагають запобігати небажаному доступу між сегментами і можуть забезпечувати більш детальний контроль над доступом до ресурсів у внутрішній мережі. Вони є важливою частиною мережі, де застосовується концепція зон захисту.

3. Хмарні фаєрволи (Cloud Firewalls) – це міжмережеві екрани, які розгортаються в хмарних середовищах. Вони захищають віртуальні інфраструктури від зовнішніх загроз і дозволяють здійснювати фільтрацію трафіку на рівні хмарних додатків і сервісів. Хмарні фаєрволи особливо актуальні для організацій, які використовують моделі розподіленої обробки даних і хмарні ресурси.

Призначення міжмережевий екранів

Основне призначення міжмережевий екранів полягає в забезпеченні захисту мережі від несанкціонованого доступу і шкідливих впливів. Розглянемо ключові функції фаєрволів.

1. Контроль доступу – міжмережеві екрани регулюють доступ до мережі, дозволяючи або блокуючи з'єднання відповідно до заданих правил. Це допомагає обмежити доступ до конфіденційних ресурсів і знизити ризик проникнення злоумисників.

2. Захист від атак – завдяки функціям фільтрації та моніторингу трафіку фаєрволи можуть виявляти підозрілі дії та блокувати трафік, що може бути частиною атак, таких як DDoS, атаки типу "людина посередині" (Man-in-the-Middle), фішинг та інші.

3. Логування та моніторинг – фаєрволи ведуть журнали подій, які фіксують інформацію про всі з'єднання, що проходять через мережу. Це дозволяє аналізувати підозрілу активність і швидко реагувати на потенційні загрози.

4. Фільтрація контенту – проксі-фаєрволи можуть фільтрувати трафік на рівні додатків, що дозволяє обмежити доступ до певних веб-ресурсів або видів контенту, захищаючи організацію від небажаних веб-сайтів або шкідливого контенту.

5. Віртуальні приватні мережі (VPN) – багато міжмережевих екранів підтримують функцію VPN, що забезпечує безпечний віддалений доступ до мережевих ресурсів. VPN шифрує дані, що передаються через загальнодоступні мережі, тим самим захищаючи конфіденційність і цілісність переданих даних [8].

6. Захист від витоку даних – фаєрволи здатні запобігати передачі конфіденційної інформації за межі мережі за допомогою спеціальних політик фільтрації, що допомагає зберегти конфіденційність даних.

Міжмережеві екрани нового покоління (NGFW)

Новий етап розвитку міжмережевих екранів – це фаєрволи нового покоління (Next-Generation Firewalls, NGFW), які поєднують у собі функції традиційних фаєрволів з можливостями для захисту від сучасних загроз [9]. NGFW включають такі функції, як:

- Інспекція на рівні додатків – NGFW можуть розпізнавати та аналізувати специфічні додатки, навіть якщо вони використовують нестандартні порти або протоколи.

- Система запобігання вторгнень (IPS) – NGFW включають функції IPS, які дозволяють виявляти та блокувати підозрілу активність в режимі реального часу [10].

- Інтеграція з іншими системами захисту – NGFW можуть обмінюватися інформацією з системами антивірусного захисту, SIEM та іншими засобами безпеки для забезпечення комплексного захисту.

NGFW стали популярними завдяки своїй здатності забезпечувати захист від сучасних кіберзагроз, таких як кібер-шпигунство, шкідливе ПЗ, складні цільові атаки (Advanced Persistent Threats, APT) тощо.

1.3. Порівняння відомих безкоштовних програмних маршрутизаторів/міжмережевих екранів

Нижче наведено опис найбільш відомих міжмережевих екранів з відкритим вихідним кодом:

- 1) OPNsense – це програмне забезпечення з відкритим кодом для забезпечення мережевої безпеки та маршрутизації, розроблене на базі операційної системи FreeBSD. Воно є відгалуженням проєктів pfSense і m0n0wall. Головна мета спільноти розробників OPNsense – створення стабільної,

захищеної й адаптивної платформи з акцентом на зручність використання, регулярні оновлення компонентів безпеки та удосконалення інтерфейсу [11].

OPNsense надає широкий спектр інструментів для захисту мережі, маршрутизації, контролю доступу, аналізу та моніторингу трафіку. Подібно до pfSense, це рішення підходить для домашніх мереж, середніх і малих підприємств, а також великих корпорацій, де важливі високий рівень безпеки та простота керування.

Ключові функції обох платформ подібні: підтримка IDS/IPS, управління VPN, фільтрація трафіку, робота з VLAN, балансування навантаження та інтеграція з додатковими модулями, такими як Squid для кешування і проксі або Suricata для виявлення загроз. Відмінною рисою OPNsense є автоматичне оновлення системи та безпекових пакетів, що сприяє оперативному впровадженню виправлень і мінімізації ризиків.

Графічний інтерфейс OPNsense вирізняється сучасним дизайном і зручністю. Меню розташоване зліва, а функція пошуку за ключовими словами значно спрощує навігацію, особливо у великих мережах. У порівнянні з pfSense, де меню знаходиться зверху і пошуку немає, OPNsense пропонує більш інтуїтивний доступ до налаштувань, що робить його зручним для користувачів, які прагнуть ефективності та комфорту в адмініструванні.

2) pfSense – це програмне забезпечення з відкритим кодом для створення міжмережевого екрана та маршрутизатора, побудоване на основі операційної системи FreeBSD [12]. Воно є одним із провідних рішень у своїй категорії, яке пропонує комерційний рівень функціональності. Популярність pfSense пояснюється його високою продуктивністю, гнучкістю налаштувань і можливістю масштабування, що робить його універсальним для мереж будь-якого розміру та типу. Система включає широкий набір функцій для мережевої безпеки та маршрутизації, зокрема фільтрацію трафіку, підтримку VLAN, балансування навантаження, моніторинг і блокування небажаних з'єднань. Це забезпечує його ефективність у застосуванні як для домашніх мереж і малих

бізнесів, так і для великих корпоративних середовищ із підвищеними вимогами до безпеки та стабільності.

На відміну від багатьох комерційних рішень, pfSense доступний у кількох форматах: як апаратні пристрої від Netgate, як віртуальні пристрої для середовищ віртуалізації, а також у вигляді безкоштовної завантажуваної версії, яку можна встановити на серверне або звичайне обладнання. Це дозволяє користувачам вибрати найзручніший спосіб інтеграції pfSense у свою інфраструктуру залежно від технічних і фінансових потреб.

pfSense оснащений зручним веб-інтерфейсом, який спрощує налаштування та управління навіть для адміністраторів без глибоких знань FreeBSD. Інтерфейс дає змогу налаштовувати функції, як-от IDS/IPS для виявлення та запобігання вторгненням (з інтеграцією Snort або Suricata), створення та управління VPN (OpenVPN, IPsec, PPTP), політики брандмауера й NAT (Network Address Translation). Крім того, система підтримує численні додаткові модулі, такі як Squid для кешування веб-контенту або pfBlockerNG для контент-фільтрації, що дозволяє адаптувати її до специфічних потреб користувачів.

Завдяки широкому функціоналу, стабільності та здатності до масштабування pfSense є надійним рішенням для організацій, які прагнуть забезпечити високий рівень безпеки та управління трафіком без значних витрат на комерційні ліцензії.

3) IPFire – це дистрибутив керованого брандмауера на базі Linux, побудований на основі Netfilter, який поєднує функції мережевої безпеки, маршрутизації та фільтрації контенту [13]. Спочатку створений як форк IPCop, IPFire був переписаний із використанням Linux From Scratch, що дозволило оптимізувати його та зробити незалежною платформою. Завдяки цьому підходу система забезпечує високу продуктивність і стабільність навіть на скромному обладнанні.

IPFire підтримує широкий спектр апаратного забезпечення, включаючи пристрої з архітектурою ARM, наприклад Raspberry Pi, що робить його чудовим вибором для невеликих мереж, віддалених офісів або підприємств із

обмеженими ресурсами. Його ефективність проявляється у мінімальних вимогах до обладнання: для роботи IPFire достатньо лише 256 МБ оперативної пам'яті, що забезпечує доступність навіть для застарілих пристроїв.

Попри мінімалістичний підхід, IPFire пропонує базовий набір функцій, таких як веб-інтерфейс для управління, підтримка IDS/IPS, VPN, фільтрація веб-контенту та контроль доступу. Система активно використовується для захисту від веб-загроз, моніторингу трафіку та забезпечення безпеки локальних мереж. Додатково, IPFire підтримує функцію проксі-сервера з можливістю кешування даних, що сприяє оптимізації трафіку у мережах із обмеженою пропускнуою здатністю.

На відміну від більш потужних платформ, таких як pfSense або OPNsense, IPFire орієнтований на базові функції безпеки без розширеного набору модулів і плагінів. Цей фокус на простоті та легкості використання робить IPFire ідеальним вибором для завдань, де пріоритетом є швидка конфігурація, надійність та економія ресурсів. Однак останні оновлення включають підтримку TLS-перевірки та більш гнучкі можливості для фільтрації трафіку, що розширює його застосування навіть у більш складних мережах.

4) VyOS – це програмне рішення для мережевої безпеки, побудоване на основі Linux, яке забезпечує функції брандмауера, маршрутизації та управління мережею [14]. Система була розроблена як універсальний інструмент для різних мережевих середовищ, з акцентом на простоту використання, гнучкість та масштабованість. Завдяки відкритому вихідному коду VyOS надає користувачам можливість адаптувати платформу до власних потреб, забезпечуючи високу продуктивність навіть на малопотужному обладнанні.

VyOS підтримує різноманітне апаратне забезпечення, включаючи пристрої з архітектурою ARM, що дозволяє використовувати його на таких пристроях, як Raspberry Pi. Це робить VyOS ефективним вибором для невеликих офісів, домашніх мереж і віддалених об'єктів, де важливо забезпечити надійний захист із мінімальними витратами. Система демонструє високий рівень економії

ресурсів: вона здатна працювати на обладнанні зі скромними характеристиками, забезпечуючи стабільність і швидкодію.

На відміну від потужних платформ, таких як pfSense або OPNsense, які пропонують широкий набір розширень, VyOS орієнтований на простоту та легкість використання. Цей підхід робить його зручним для завдань, де потрібно швидко налаштування та базовий рівень безпеки. Водночас останні оновлення системи розширили її функціонал, додавши можливість більш гнучкої фільтрації трафіку та покращення інструментів моніторингу.

Завдяки своїй відкритій архітектурі, мінімальним системним вимогам і зручному інтерфейсу, VyOS є ідеальним вибором для організацій, які прагнуть забезпечити базовий рівень мережевої безпеки та управління без значних витрат на обладнання чи ліцензування.

Для узагальнення інформації та виділення основних переваг і недоліків кожного з продуктів представлена порівняльна таблиця нижче, табл.1.1.

Таблиця 1.1

Порівняльна таблиця міжмережових екранів

	OPNsense	pfSense	IPFire	VyOS
Підтримка VPN	+	+	+	+
Фільтрація веб-змісту	+	+	+	+
IDS/IPS	+	+	+	+
Антивірусний захист	+	+	+	+
Балансування навантаження	+	+	—	+
Web Proxy	+	+	+	+
Додаткові функції	+	+	—	-

Обираючи pfSense, можна відзначити, що цей продукт забезпечує найбільш збалансований набір функцій безпеки, продуктивності та розширюваності, що робить його оптимальним рішенням для багатьох організаційних і технічних потреб.

Переваги вибору pfSense [15]:

1. Широкий функціонал без додаткових витрат – pfSense надає комплексний набір функцій для мережевої безпеки, включаючи підтримку VPN, IDS/IPS, антивірусний захист, фільтрацію веб-контенту, балансування навантаження та веб-проксі, що робить його потужним інструментом для всебічного захисту мережі. Важливо, що цей функціонал доступний без додаткових ліцензійних витрат.

2. Масштабованість і додаткові модулі – pfSense підтримує численні додаткові пакети, які можуть бути встановлені для розширення функціоналу залежно від специфічних потреб організації. Це включає пакети для захисту, моніторингу та оптимізації мережі, як-от Snort для додаткового рівня IDS/IPS або pfBlockerNG для розширеної фільтрації контенту. Порівняно з IPFire, який обмежений у розширенні функцій, pfSense пропонує більшу гнучкість.

3. Балансування навантаження – функція балансування навантаження забезпечує стабільну роботу мережі, що є важливим для організацій з великим обсягом трафіку або для середовищ з декількома інтернет-з'єднаннями. Ця можливість також доступна в OPNsense, але в IPFire вона відсутня, що робить pfSense кращим вибором для мереж, де потрібно підтримувати високу доступність.

4. Інтеграція з Active Directory – легко інтегрується з Microsoft Active Directory, що дозволяє централізовано управляти доступом користувачів і налаштовувати політики безпеки на рівні організації. Це є великою перевагою для компаній, що працюють у корпоративних середовищах і потребують єдиного контролю автентифікації.

5. Інтуїтивний інтерфейс та активна підтримка спільноти – має зручний веб-інтерфейс, який дозволяє навіть адміністраторам без глибоких знань у FreeBSD ефективно налаштовувати систему. Крім того, pfSense підтримується великою спільнотою користувачів і розробників, що забезпечує доступ до численних інструкцій, форумів та технічної підтримки.

Завдяки поєднанню безкоштовного, повнофункціонального рішення з активною підтримкою та розширюваністю, pfSense є оптимальним вибором для побудови безпечної, стабільної та масштабованої мережевої інфраструктури.

1.4. Відомості і функціональні можливості щодо pfSense

pfSense – це потужний міжмережевий екран з відкритим вихідним кодом, розроблений для побудови мережевих рішень, які можуть забезпечувати високий рівень безпеки. Він базується на операційній системі FreeBSD і надає користувачам гнучкі можливості управління мережевою інфраструктурою. pfSense є багатофункціональним інструментом, який включає в себе різні компоненти для захисту мережі, а також для її моніторингу і оптимізації [16].

Основні відомості про pfSense:

- Був розроблений як альтернатива дорогим апаратним міжмережевим екранам. Він став популярним завдяки своїй гнучкості, високій продуктивності, широкому функціоналу та активній спільноті. Його можна встановлювати на стандартне мережеве обладнання або спеціалізовані сервери, що робить його доступним для компаній різних масштабів – від малих офісів до великих корпоративних мереж.

- Підтримує конфігурацію через веб-інтерфейс, що робить його зручним у використанні навіть для ІТ-спеціалістів, які не є експертами у FreeBSD. Завдяки простому та зрозумілому інтерфейсу адміністратори можуть швидко налаштовувати правила безпеки, моніторити трафік і впроваджувати нові рішення для захисту мережі.

Функціональні можливості pfSense:

- Надає широкий спектр функціональних можливостей для забезпечення безпеки мережі, управління доступом та моніторингу мережевого трафіку.

- Надає функцію фільтрації трафіку, яка є основою для забезпечення безпеки мережі. Вона дозволяє створювати правила фільтрації на основі IP-адрес, портів та протоколів. Адміністратор може налаштовувати правила для конкретних мережевих інтерфейсів, контролювати вхідний і вихідний трафік та

обмежувати доступ до певних ресурсів. Це зрештою дозволяє блокувати шкідливий трафік і захищати мережу від несанкціонованого доступу.

- Однією з ключових функцій pfSense є Stateful Packet Inspection (SPI) – технологія, що відстежує стан з'єднань у мережі. На відміну від звичайної фільтрації пакетів, SPI дозволяє визначити, чи є пакет частиною існуючого з'єднання, або він надходить без відповідного дозволу. Це підвищує рівень захисту, знижуючи ризик пропуску небажаного трафіку.

- Підтримує Network Address Translation (NAT), що дозволяє змінювати IP-адреси в пакетах [17]. NAT допомагає приховати внутрішні IP-адреси мережі від зовнішніх джерел, забезпечуючи тим самим захист від прямого доступу до внутрішніх ресурсів. У pfSense підтримуються різні типи NAT, включаючи вихідний NAT і перенаправлення портів (Port Forwarding). Це дозволяє забезпечити більш гнучке управління доступом до внутрішніх ресурсів і обмежити зовнішній доступ до певних серверів.

- підтримує налаштування віртуальних приватних мереж (VPN), що дозволяє забезпечити безпечний віддалений доступ до корпоративної мережі. pfSense підтримує основні VPN-протоколи, такі як OpenVPN, IPsec, L2TP, що забезпечує надійне шифрування трафіку між віддаленими користувачами та мережею. Це особливо корисно для організацій з віддаленими співробітниками або офісами, які потребують безпечного доступу до ресурсів мережі.

OpenVPN – це один із найпопулярніших протоколів для створення VPN-з'єднань. Він відомий своєю гнучкістю та надійністю. OpenVPN підтримує шифрування на основі SSL/TLS, що забезпечує високий рівень захисту переданих даних. pfSense дозволяє налаштовувати OpenVPN для різних сценаріїв, включаючи точку-точку і клієнт-сервер.

IPsec – це ще один протокол, який підтримується в pfSense для забезпечення VPN-з'єднань. IPsec часто використовується для міжмережових з'єднань між офісами або для інтеграції з іншими мережевими рішеннями. Він забезпечує шифрування на рівні мережі, що робить його ефективним для забезпечення безпеки корпоративного трафіку.

pfSense підтримує балансування навантаження і резервування з'єднань. Це дозволяє розподіляти навантаження між декількома інтернет-каналами, що допомагає уникнути перевантаження одного каналу і забезпечує стабільний доступ до ресурсів. Крім того, pfSense підтримує налаштування резервного каналу, що забезпечує відмовостійкість. У випадку, якщо основний канал стає недоступним, трафік автоматично перенаправляється на резервний канал.

Наш міжмережевий може використовувати додаткові пакети для інтеграції з системами запобігання вторгнень, такими як Snort або Suricata. Ці системи дозволяють виявляти і блокувати підозрілу активність у мережі в режимі реального часу, що допомагає захистити мережу від різних атак, включаючи DDoS, фішинг і атаки на рівні додатків. Система IPS в pfSense аналізує мережевий трафік, використовуючи сигнатури відомих атак, і блокує небажаний трафік.

pfSense має потужні функції моніторингу і логування, що дозволяють адміністратору відстежувати стан мережі і контролювати активність користувачів. Логування подій дозволяє фіксувати всі з'єднання, що проходять через фаєрвол, зберігаючи інформацію про IP-адреси, порти, час з'єднань і інші важливі параметри. Це допомагає виявляти підозрілу активність і оперативно реагувати на потенційні загрози. Інтерфейс pfSense також надає графічне відображення трафіку та стану з'єднань, що полегшує адміністрування мережі.

Екран підтримує віртуальні локальні мережі (VLAN), що дозволяє сегментувати мережу на ізольовані сегменти. Сегментація за допомогою VLAN допомагає захистити конфіденційні дані, зменшуючи ризик поширення атак всередині мережі [18]. Наприклад, можна виділити окремі сегменти для різних відділів організації або для гостей користувачів, що знижує ймовірність несанкціонованого доступу до важливих ресурсів.

Інтеграція з Microsoft Active Directory

Інтеграція pfSense з Microsoft Active Directory є однією з ключових функцій для забезпечення централізованого управління доступом і автентифікацією. Це дозволяє організаціям використовувати існуючу інфраструктуру Active Directory

для управління правами доступу до мережевих ресурсів. Завдяки інтеграції з AD, адміністратори можуть контролювати доступ користувачів до ресурсів, застосовувати єдині політики безпеки і спрощувати процес автентифікації.

Інтеграція також дозволяє налаштувати одноразову автентифікацію (Single SignOn, SSO), що значно спрощує процес входу користувачів у систему. Це особливо корисно для організацій, які потребують єдиного способу управління доступом для зниження адміністративного навантаження. Крім того, можна впровадити двофакторну автентифікацію (2FA), яка додає додатковий рівень безпеки, вимагаючи підтвердження особи користувача через другий фактор, наприклад, одноразовий код або біометричні дані. Двофакторна аутентифікація є обов'язковою вимогою для доступу до критичних систем або публічних ресурсів.

Розширення можливостей за допомогою додаткових пакетів

pfSense підтримує встановлення додаткових пакетів, що дозволяє значно розширити його функціонал. Деякі з найпопулярніших пакетів включають:

- Snort і Suricata – системи виявлення та запобігання вторгнень (IDS/IPS), які дозволяють виявляти і блокувати підозрілу активність.
- pfBlockerNG – пакет для блокування небажаного контенту і фільтрації трафіку за географічними та іншими критеріями.
- Squid – проксі-сервер і кешуючий сервер, який може бути налаштований для контролю веб-трафіку, фільтрації контенту і економії пропускної здатності.
- Darkstat і BandwidthD – інструменти моніторингу, які надають докладну статистику про використання мережевих ресурсів.

Ці пакети дозволяють гнучко налаштовувати pfSense для відповідності специфічним потребам організації, забезпечуючи при цьому високий рівень захисту.

Фільтрація контенту:

pfSense дозволяє налаштовувати фільтрацію контенту на основі різних параметрів, зокрема з використанням пакета Squid для контролю веб-трафіку. Це дозволяє обмежити доступ до певних веб-ресурсів, таких як соціальні мережі або

сайти з небажаним контентом, що може підвищити продуктивність співробітників і зменшити ризик доступу до шкідливих сайтів.

Переваги pfSense:

1. Відкритий код і безкоштовність – pfSense є продуктом з відкритим кодом, що робить його доступним для різних організацій без додаткових витрат на ліцензії.

2. Гнучкість і масштабованість – pfSense легко адаптується до різних вимог і може бути використаний як в малих офісах, так і в великих корпоративних мережах.

3. Підтримка безлічі функцій і пакетів – завдяки підтримці додаткових пакетів pfSense можна налаштувати відповідно до специфічних вимог організації.

4. Простота адміністрування – завдяки веб-інтерфейсу адміністратори можуть швидко налаштовувати і керувати мережею без необхідності вивчення складних команд FreeBSD.

pfSense є одним з найпопулярніших рішень для забезпечення безпеки мережі завдяки своїй гнучкості, широкому функціоналу і підтримці додаткових пакетів. Завдяки функціям фільтрації трафіку, підтримці VPN, системам запобігання вторгнень та інтеграції з Microsoft Active Directory, pfSense дозволяє створити надійну і керовану мережеву інфраструктуру, яка відповідає сучасним вимогам до безпеки. Це робить його ідеальним вибором для організацій різного масштабу, які прагнуть захистити свої ресурси і забезпечити безпечний доступ до даних.

Висновок до першого розділу

Було проведено теоретичний аналіз роботи Active Directory, що забезпечує централізоване управління доступом до ресурсів мережі. Розглянуто основні компоненти логічної та фізичної структури AD, включаючи ліс, домени, організаційні одиниці, об'єкти та контролери домену, а також функціональні можливості, такі як аутентифікація, авторизація, управління об'єктами та групові політики. Описано протоколи аутентифікації, зокрема Kerberos та NTLM,

механізми реплікації даних і довірчі відносини між доменами. Проаналізовано додаткові сервіси, такі як ADFS та AD LDS, які розширюють функціонал системи.

Виконано аналіз різновидів міжмережевих екранів та їх призначення. Розглянуто класифікацію фаєрволів за типом обробки трафіку. Також описано поділ міжмережевих екранів за місцем встановлення в мережі. Проаналізовано основні функції фаєрволів, такі як контроль доступу, захист від атак, логування, фільтрація контенту, підтримка VPN та запобігання витоку даних. Додатково розглянуто можливості фаєрволів нового покоління (NGFW), які інтегрують функції традиційних рішень із сучасними методами запобігання загрозам, таким, як інспекція на рівні додатків, IPS та інтеграція з іншими системами безпеки.

Проведено порівняння найпоширеніших безкоштовних програмних маршрутизаторів і міжмережевих екранів з відкритим кодом, а саме pfSense, OPNsense, IPFire та VyOS. Було визначено їхні основні функції, переваги та обмеження, а також представлено порівняльну таблицю. У результаті зроблено висновок, що pfSense є найбільш збалансованим рішенням для захисту корпоративних мереж завдяки широкому функціоналу, гнучкості та активній підтримці спільноти.

Наприкінці, було наведено відомості та функціональні можливості pfSense як одного з найефективніших програмних міжмережевих екранів з відкритим кодом. Висвітлено основні аспекти його роботи, включаючи можливості для забезпечення безпеки мережі, моніторингу, управління доступом і підтримки VPN-з'єднань. Розглянуто використання додаткових пакетів, які розширюють функціонал системи для виявлення загроз, фільтрації трафіку та контролю контенту. Зроблено висновок, що pfSense є гнучким, масштабованим та простим в адмініструванні рішенням, яке відповідає сучасним вимогам до безпеки корпоративних мереж.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПРОЄКТУ МЕРЕЖІ, МЕТОДІВ ЗАХИСТУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

2.1. Розробка топології та адресації

Вибір топології мережі є важливим етапом у створенні мережевої інфраструктури організації. Від правильно обраної топології залежить ефективність мережевого зв'язку, безпека даних та оптимізація використання ресурсів.

Проектування мереж може значно відрізнятися в залежності від розміру та вимог організацій. Наприклад, потреби в мережевій інфраструктурі для маленької організації з меншою кількістю пристроїв будуть менші, ніж для великої організації з великою кількістю пристроїв і підключень.

Однак, незалежно від розміру мережі чи вимог, важливим фактором для успішної реалізації будь-якої ІТ-інфраструктури є дотримання належних структурованих інженерних принципів. До них належать:

- **Модульність.** Поділяючи різні функції мережі на модулі, її проектування стає простішим. Cisco виділяє кілька таких модулів, зокрема кампусну мережу, блоки сервісів, дата-центр і край Інтернету.
- **Надійність.** Мережа повинна залишатися доступною для використання як в нормальних, так і в надзвичайних ситуаціях. Нормальні умови включають очікувані потоки трафіку та патерни трафіку, а також заплановані події, як от періоди технічного обслуговування. Надзвичайні ситуації охоплюють відмови апаратного чи програмного забезпечення, надмірне навантаження трафіку, незвичні патерни трафіку, атаки типу "відмова в обслуговуванні" (DoS), чи будь-які інші непередбачувані події.
- **Гнучкість.** Здатність змінювати частини мережі, додавати нові послуги або збільшувати її потужність без необхідності проведення великих оновлень (наприклад, заміни основного апаратного забезпечення).
- **Безпека.** Забезпечення захисту даних та мережі від несанкціонованого доступу та атак є основним аспектом будь-якої мережевої

інфраструктури. Це включає використання фаєрволів, систем виявлення вторгнень, шифрування даних та інших заходів, спрямованих на збереження конфіденційності, цілісності та доступності даних.

- **Управління та моніторинг.** Важливо мати можливість здійснювати ефективний моніторинг стану мережі та управляти її компонентами. Це включає використання засобів для виявлення проблем і аномалій, а також систем для централізованого керування мережею, що дозволяє швидко реагувати на збої або зміну умов.

- **Масштабованість.** Мережа повинна мати можливість масштабування без значних труднощів у разі зростання вимог або кількості користувачів. Це дозволяє зберігати високу ефективність та надійність навіть за умов розширення інфраструктури.

Тому, для задоволення всіх вищезазначених вимог, інженери з компанії Cisco запровадили використання трирівневої топології мережі (яку ще називають ієрархічна), яка включає в себе три основні рівні: рівень доступу, рівень розподілу та рівень ядра, рис.2.1. Така архітектура дозволяє ефективно розподіляти навантаження між різними частинами мережі, забезпечуючи оптимальний баланс між продуктивністю, масштабованістю та надійністю [19].

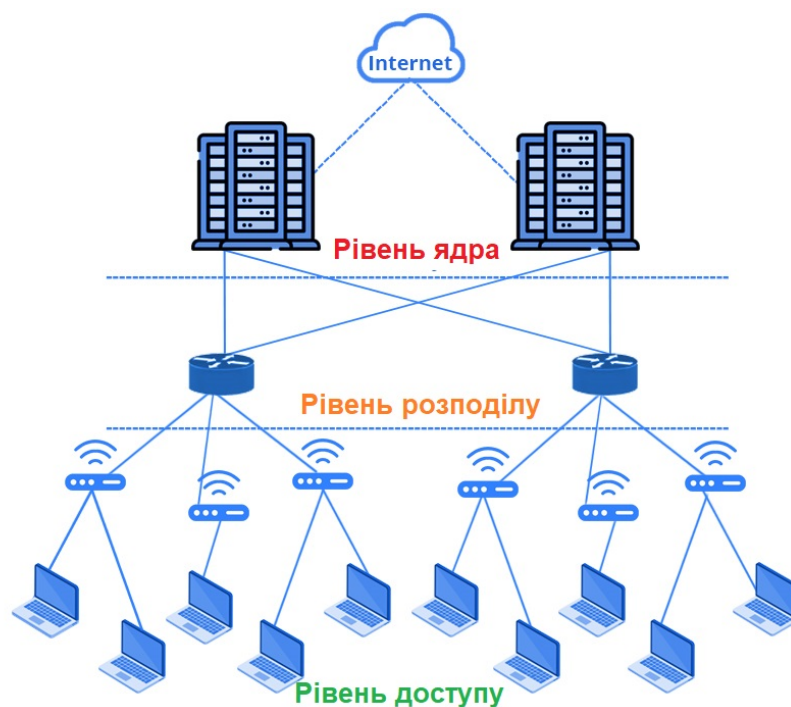


Рисунок 2.1 – Трирівнева топологія мережі

Подібне проєктування мережі передбачає поділ мережі на окремі рівні, кожен з яких виконує конкретні функції, що визначають його роль у загальній структурі мережі. Це дає можливість мережевому адміністратору оптимізувати вибір апаратного та програмного забезпечення, а також функцій, які відповідають за виконання специфічних завдань на кожному з рівнів. Такий підхід використовується, як до розробки LAN, так і WAN мереж.

Перевага поділу мережі на менші, більш керовані блоки полягає в тому, що локальний трафік залишається в межах локальних сегментів. Лише той трафік, який направляється в інші мережі, передається на вищий рівень.

Типове проєктування ієрархічної LAN-мережі для підприємства включає три основні рівні:

Рівень доступу відповідає за підключення кінцевих користувачів або робочих груп до мережі. Це точка входу в мережу для кінцевих пристроїв, таких як комп'ютери, телефони, принтери, а також інші кінцеві пристрої. На цьому рівні здійснюється контроль доступу до мережі, застосовуються політики безпеки та можуть бути впроваджені базові механізми для управління трафіком, наприклад, фільтрація або пріоритизація трафіку. Рівень доступу забезпечує підключення до інших частин мережі через розподільчі пристрої, такі як комутатори та точки доступу.

Рівень розподілу відповідає за зв'язок між різними сегментами мережі та надає можливість управління політиками, маршрутизації та фільтрації трафіку. Цей рівень визначає, як мережевий трафік буде розподілятися між різними підмережами і як будуть керуватися транзитні дані між рівнем доступу та ядром. Рівень розподілу також займається обробкою маршрутизації, фільтрацією трафіку та застосуванням політик безпеки, таких як доступ до певних ресурсів або сервісів. Він відіграє важливу роль у забезпеченні ефективної і безпечної взаємодії між різними сегментами мережі.

Рівень ядра є найвищим рівнем мережі і забезпечує швидку і надійну передачу даних між різними частинами мережі, зазвичай між різними розподільчими комутаторами в межах організації або між великими сегментами

мережі. Основна роль цього рівня – забезпечення високої пропускної здатності та швидкості обміну даними. Рівень ядра обробляє великий обсяг трафіку і є критичним для забезпечення стабільної роботи мережі, оскільки він підтримує зв'язок між віддаленими точками мережі та швидке переміщення даних. Важливо, щоб на цьому рівні були мінімальні затримки і максимальна надійність.

Тому, створення топології локальної мережі організації було проведено з дотриманням трирівневої моделі мережі. Проектування трирівневої мережевої структури передбачає врахування сучасних принципів забезпечення високої доступності та стійкості до відмов, що дозволяє мінімізувати ризики простою та збоїв у роботі системи. Проект представляє собою невелику локальну мережу організації на 30 кінцевих робочих станцій, рис.2.2.

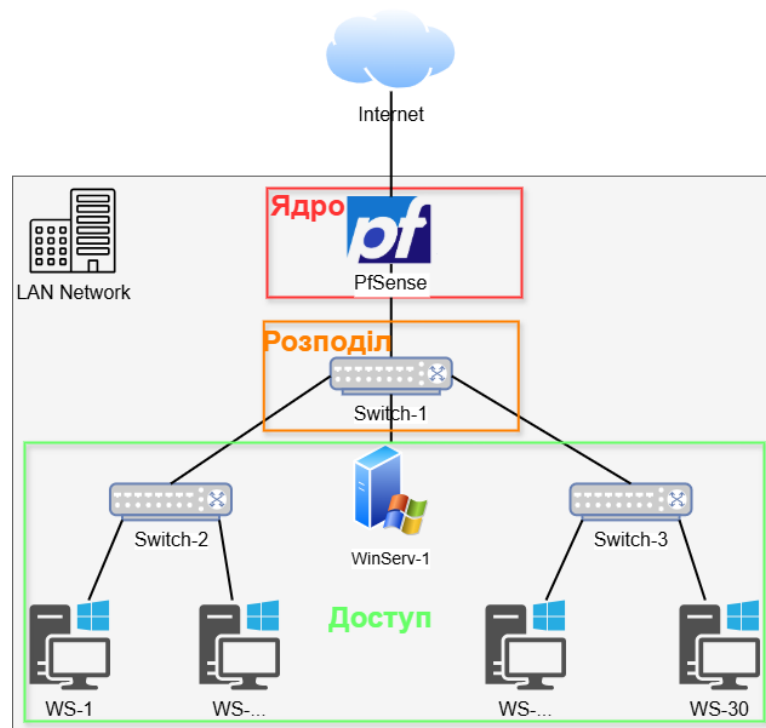


Рисунок 2.2 – Топологія мережі

Ядро відповідає за управління трафіком між корпоративною мережею та зовнішнім інтернетом. На цьому рівні встановлено маршрутизатор на базі pfSense, який одночасно виконує роль фаєрвола та маршрутизатора. Саме цей рівень є центральним для забезпечення захисту мережевої інфраструктури, контролю доступу та сегментації трафіку.

Розподіл представлений основним комутатором Switch-1, який є магістральним пристроєм, що забезпечує передачу трафіку між ядром мережі (pfSense) і підлеглими рівнями доступу. На цьому рівні також інтегрований сервер WinServ-1, що працює на Windows Server 2019. Він виконує роль контролера домену з використанням Microsoft Active Directory для централізованого управління користувачами, групами та політиками безпеки в корпоративній мережі.

Рівень доступу включає комутатори Switch-2 та Switch-3, які підключають кінцеві пристрої (робочі станції). Ці пристрої позначені як WS-..., і працюють під управлінням операційної системи Windows 10. Цей рівень забезпечує користувачам підключення до мережі, доступ до ресурсів, а також автентифікацію через контролер домену. Таким чином, кожен кінцевий пристрій отримує централізовано налаштований доступ до корпоративних сервісів і ресурсів.

Адресація

Наступним, не менш важливим кроком, є вибір підмереж та розподіл адресації. Для пристроїв локальної мережі передбачено використання адресного простір 192.168.1.0/24, який забезпечує до 254 доступних IP-адрес. Це ідеальний та типовий вибір для невеликої або середньої мережі, де важливо спростити управління мережею. Для автоматичного призначення IP-адрес кінцевим пристроям буде налаштовано сервер DHCP (Dynamic Host Configuration Protocol) на WinServ-1. Подібний підхід забезпечить ефективну роботу локальної мережі та спростить її розширення в майбутньому.

Маршрутизатор, тобто PfSense, буде налаштований для отримання IP-адреси динамічно від Інтернет-провайдера за допомогою протоколу DHCP. А доступ пристроїв локальної мережі до Інтернету буде забезпечуватись через налаштування механізму NAT (Network Address Translation), а точніше PAT (Port Address Translation), що водночас також сприятиме додатковій безпеці локальної інфраструктури.

Нижче на табл.2.1 наведено таблицю адресації пристроїв локальної підмережі, а на рис.2.3 продемонстровано топологію мережі із зазначенням розподілених адрес.

Таблиця 2.1

Параметри адресації пристроїв мережі

Мережа/Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Префікс
Internet	–	DHCP		
LAN	–	192.168.1.0	255.255.255.0	/24
PfSense	Eth0	DHCP		
	Eth1	192.168.1.1	255.255.255.0	/24
Комутатор Switch-1	Інтерфейс Vlan 1	192.168.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	255.255.255.0	/24
Комутатор Switch-2	Інтерфейс Vlan 1	192.168.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	255.255.255.0	/24
Комутатор Switch-3	Інтерфейс Vlan 1	192.168.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	255.255.255.0	/24
Сервер Win-Serv-1	Eth0	192.168.1.10	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	255.255.255.0	/24
Робочі станції WS-1 – WS-30	Eth0	DHCP		
	Шлюз за замовчуванням			

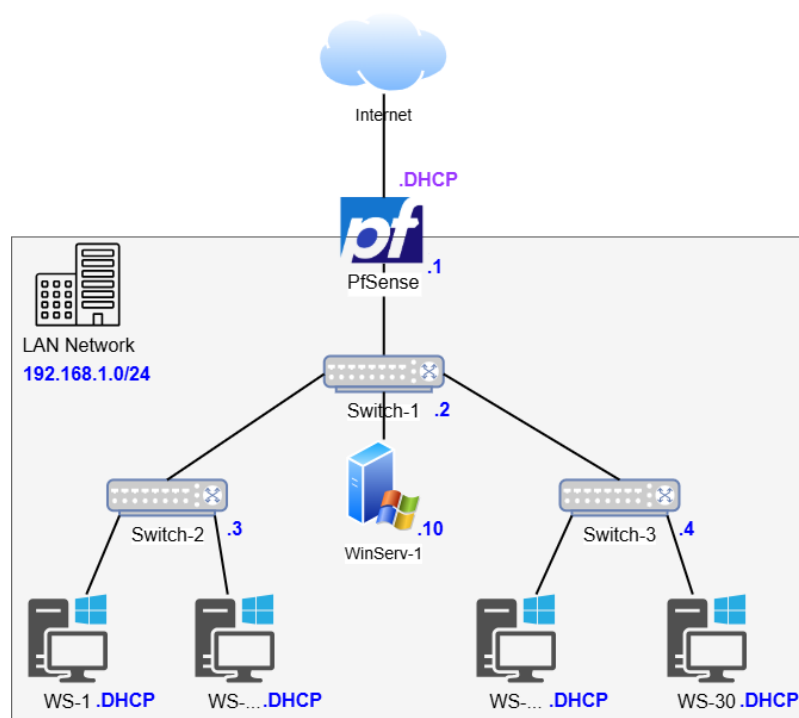


Рисунок 2.3 – Топологія мережі з адресацією пристроїв

2.2. Вибір методів та механізмів захисту

У сучасних умовах, коли мережі піддаються численним загрозам і атакам, важливо впроваджувати методи, які не тільки захищають від несанкціонованого доступу, але й зменшують площу атаки. Це передбачає застосування принципу багаторівневого захисту (Defense in Depth), що дозволяє локалізувати загрози і обмежити їх вплив на інші частини інфраструктури. Це означає, що навіть у разі успішної атаки на один з елементів мережі, зловмисник не матиме доступу до всіх ресурсів, оскільки кожен сегмент має свої власні рівні захисту. Такий підхід включає в себе як превентивні заходи, так і методи виявлення та реагування на інциденти безпеки, зокрема забезпечення конфіденційності, цілісності даних та доступності ресурсів. Вибір відповідних методів та механізмів захисту залежить від специфіки мережі, її масштабу та вимог до безпеки, а також враховує можливі загрози та ризики, з якими може зіткнутися організація.

Тому, для забезпечення відповідного рівня захисту мережі було вибрано низку рішень, які сприяють ефективному управлінню доступом, моніторингу подій та забезпеченню безпеки на всіх рівнях мережі.

Active Directory (AD) є зручним та відомим рішенням для управління доступом і захистом корпоративних мереж, забезпечуючи централізоване зберігання облікових записів користувачів, груп і ресурсів, а також політик доступу. Використовуючи протоколи LDAP, Kerberos, DHCP і DNS, AD дозволяє ефективно аутентифікувати користувачів і контролювати їх права через політики груп. AD також підтримує інтеграцію з іншими системами безпеки, що підвищує рівень захисту мережі. Крім того, AD дозволяє виконувати детальний аудит дій користувачів і надає можливість реалізовувати складні механізми ізоляції та розподілу прав доступу, що значно знижує ризики несанкціонованого доступу до важливих ресурсів.

Syslog є важливим протоколом для централізованого збору, зберігання та аналізу логів з різних пристроїв і систем у мережі. Використовуючи Syslog, адміністратори можуть ефективно моніторити події безпеки, реєструючи всі критичні дії та спроби несанкціонованого доступу. Це дозволяє оперативно

виявляти загрози, виконувати аудит та кореляцію подій, а також виконувати пошук тих чи інших подій. Інтеграція Syslog з системами моніторингу та виявлення вторгнень підвищує ефективність управління безпекою, забезпечуючи прозорість мережі та швидке реагування на потенційні загрози.

SSH (Secure Shell) – це протокол для безпечного віддаленого доступу до пристроїв та систем у мережі, який забезпечує шифрування даних, автентифікацію та цілісність повідомлень. SSH є критично важливим для адміністрування серверів, маршрутизаторів та інших мережевих пристроїв, оскільки він дозволяє здійснювати віддалену настройку та керування системами без ризику перехоплення або видозміни інформації. Протокол використовує криптографічні методи для забезпечення захисту даних, що передаються, і підтримує різні методи аутентифікації, зокрема за допомогою паролів і публічних ключів. Впровадження SSH у мережу забезпечить безпечний доступ до пристроїв, що робить його важливим інструментом для управління та підтримки безпеки в мережах будь-якого типу.

PfSense — це спеціалізований дистрибутив операційної системи на основі FreeBSD, який поєднує функції міжмережевого екрану і маршрутизатора. Цей продукт широко використовується для створення надійних та безпечних мережевих рішень як у малих, так і в середніх організаціях. PfSense забезпечує потужний набір інструментів для керування мережею, дозволяючи виконувати фільтрацію трафіку, маршрутизацію, створення віртуальних приватних мереж (VPN), а також здійснювати моніторинг і аналіз мережевого трафіку. Інтерфейс налаштувань є інтуїтивно зрозумілим і зручним для адміністраторів, що дозволяє швидко налаштовувати безпеку та ефективно управляти мережевими ресурсами. PfSense підтримує низку важливих функцій захисту, серед яких можна окремо виділити наступні, які будуть застосовані:

- Міжмережевий екран. PfSense дозволяє створювати детальні правила для фільтрації вхідного та вихідного трафіку, що допомагає захистити мережу від несанкціонованих доступів.

- NAT (Network Address Translation). Використовується для перетворення адрес на межі мережі, що дозволяє маскувати внутрішні IP-адреси та забезпечувати конфіденційність.
- Snort – це популярний інструмент виявлення та запобігання вторгненням (IDS/IPS), який доступний як додатковий пакет для платформи pfSense. Snort виконує функції аналізу мережевого трафіку в режимі реального часу та порівнює його з відомими шаблонами (сигнатурами) атак, щоб забезпечити безпеку мережі. В даному проєкті Snort буде виконувати перевірку вхідного трафіку з мережі Інтернет.
- Моніторинг та аналіз трафіку. Можливості дистрибутива дозволяють збирати дані про мережевий трафік, здійснювати його аналіз для виявлення аномалій або передавати ці дані для подальшого аналізу через вже згадай протокол Syslog або SNMP.

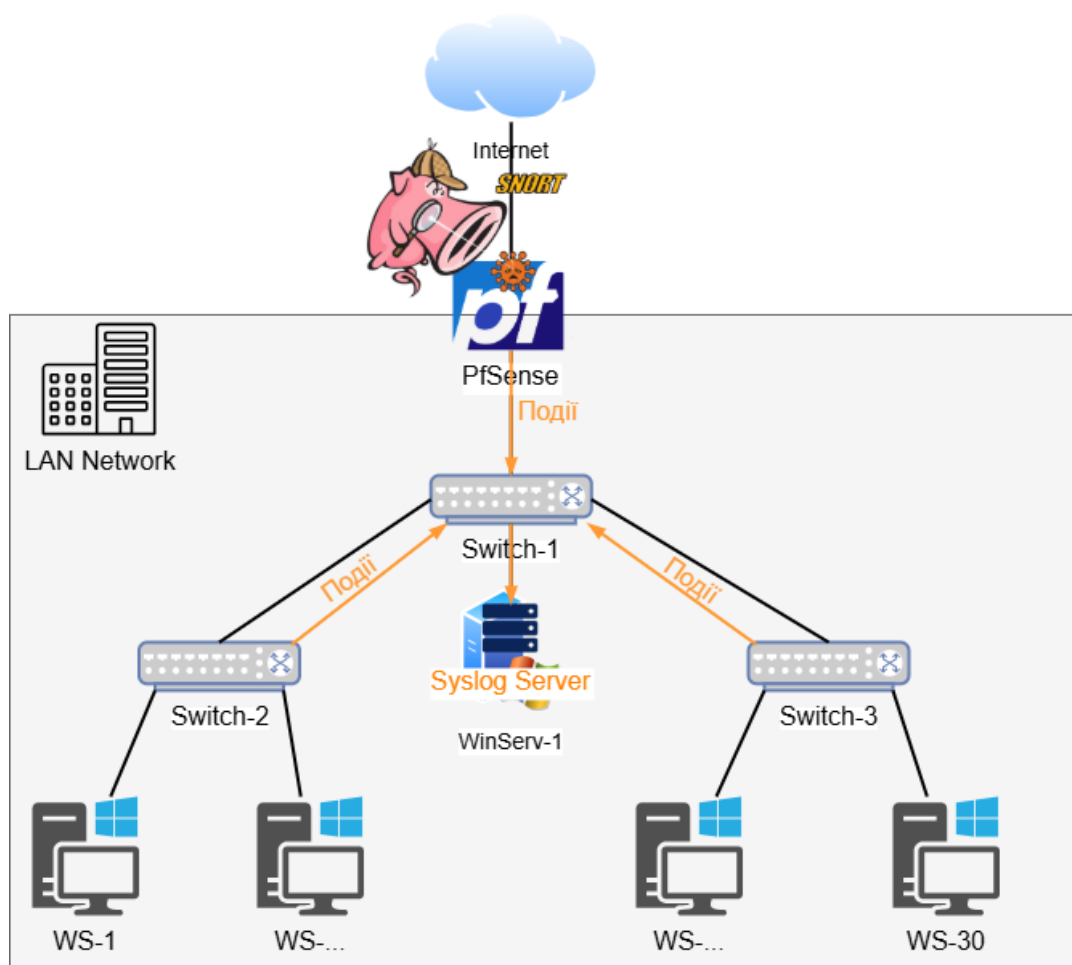


Рисунок 2.4 – Схема роботи Syslog та розміщення Snort в мережі

- **Packet Capture.** Інструмент для аналізу мережевого трафіку на рівні пакетів, що дозволяє адміністраторам вивчати вміст переданих даних, визначати джерело проблем або потенційні загрози.
- **Ping і Traceroute.** Використовуються для перевірки доступності хостів і діагностики маршрутів до них, що допомагає виявити проблеми з підключенням або затримками в мережі.
- **Nmap.** Інструмент для сканування мережі, що дозволяє виявляти відкриті порти та отримувати інформацію про запущені сервіси на хостах.
- **States і States Summary.** Інструменти для моніторингу стану з'єднань у реальному часі, які допомагають аналізувати використання ресурсів і з'єднань у мережі.
- **Monitoring.** Панель для моніторингу ресурсів мережевих інтерфейсів, що надає детальну інформацію про статистику трафіку, кількість помилок, швидкість передачі даних та інші ключові параметри роботи мережі.

2.3 Вибір обладнання для організації роботи мережі

Вибір пристрою для розгортання pfSense є критичним для забезпечення стабільної, безпечної та продуктивної роботи мережі. Сам PfSense підтримує широкий спектр функцій, таких як маршрутизація, VPN, фільтрація трафіку, фаєрвол та різні функції безпеки, тому обладнання має відповідати цим вимогам. Ключовими параметрами при виборі є продуктивність процесора, обсяг оперативної пам'яті для стабільної роботи при великій кількості з'єднань, а також швидкість і надійність мережевих інтерфейсів із підтримкою гігабітних портів. Важливими є також енергоефективність і система охолодження. Вибір має базуватися на аналізі поточних потребах мережі та враховувати майбутнє масштабування, щоб забезпечити надійність і довговічність інфраструктури.

Тому Netgate SG-1100 є оптимальним вибором для реалізації дистрибутива pfSense завдяки поєднанню потужності, компактності та енергоефективності. Цей пристрій спеціально розроблений для роботи з pfSense, що гарантує повну сумісність і стабільність роботи [20].



Рисунок 2.5 – Netgate SG-1100

Даний пристрій оснащений продуктивною та енергоефективною 64-розрядною системою на кристалі (SoC) Marvell ARMADA® 3720, що використовує двоядерний процесор ARM® Cortex®-A53. SG-1100 забезпечує пропускну здатність до 500 Мбіт/с у режимі міжмережевого екрана та до 1 Гбіт/с при роботі як маршрутизатор.

При виборі моделі комутатора важливо звернути увагу на такі параметри, як продуктивність, пропускну здатність та кількість портів. Крім того, варто враховувати можливість масштабування, енергоефективність та надійність обладнання.

Саме тому комутатор моделі Cisco SF200-24FP є відмінним вибором для задоволення основних вимог завдяки своїм 24 портам та підтримкою PoE. Це інтелектуальний комутатор Fast Ethernet серії Cisco Small Business 200, який поєднує вигідну ціну, високу продуктивність та функціональність. Він ідеально підходить для середніх офісних інфраструктур, забезпечуючи високий рівень безпеки і надійну продуктивність для мереж бізнес-класу. Цей розширений комутатор з підтримкою Fast Ethernet або Gigabit Ethernet надає основні функції керування, безпеки та якості обслуговування (QoS). Завдяки зручному веб-інтерфейсу користувача, Cisco SF200-24FP дозволяє швидко і легко налаштувати надійну мережу для організації, а також забезпечує масштабованість, що дозволяє адаптувати мережу до зростаючих потреб бізнесу.



Рисунок 2.6 – Комутатор Cisco SF200-24FP

У трирівневій мережевій структурі використання пристрою Netgate SG-1100 як мережевого екрана є актуальним і доцільним рішенням, враховуючи його ефективність у забезпеченні мережевої безпеки, підтримку сучасних функцій маршрутизації та розширені можливості фільтрації трафіку. Заплановане використання комутаторів Cisco SF200-24FP на другому та третьому рівнях забезпечить надійність та продуктивність мережі, створюючи збалансовану інфраструктуру, що відповідає вимогам сучасних корпоративних середовищ.

При виборі комп'ютера для встановлення Windows Server 2019 важливо враховувати наступні характеристики, що забезпечать ефективну роботу пристрою. Основним таким аспектом є продуктивність процесора, оскільки для операційної системи серверного типу є вкрай важливим наявність багатоядреного процесора з високою тактовою частотою, який здатний обробляти одночасно численні запити від користувачів. Наявність дискретної відеокарти не є вкрай важливим, оскільки більшість сучасних процесорів та материнський плат мають вбудований графічний інтерфейс, якого достатньо для більшості задач. Крім того, слід додати достатнього обсягу оперативної пам'яті, зазвичай це не менше 16 ГБ. Для зберігання даних важливий вибір швидких жорстких дисків або краще SSD, які забезпечать високу швидкість відгуку та роботи системи. Сервер обов'язково повинен мати підтримку гігабітного Ethernet для забезпечення швидкого обміну даними. Крім того, важливо, щоб комп'ютер мав достатньо портів для підключення периферійних пристроїв.

Висновок до другого розділу

В ході написання розділу було виконано розробку топології та адресації мережі організації відповідно до трирівневої моделі Cisco. Створено топологію

для мережі на 30 кінцевих робочих станцій, де маршрутизатор на базі pfSense реалізує функції фаєрвола та маршрутизатора. На рівні розподілу впроваджено комутатор Switch-1 і сервер WinServ-1 з інтеграцією Microsoft Active Directory для централізованого управління. На рівні доступу налаштовано комутатори Switch-2 і Switch-3 для підключення кінцевих пристроїв. Для адресації використано підмережу 192.168.1.0/24 з налаштуванням сервера DHCP для автоматичного розподілу IP-адрес. Спроектowana інфраструктура забезпечує централізоване управління, гнучкість та високий рівень безпеки.

Було виконано впровадження методів і механізмів захисту мережевої інфраструктури з використанням принципу багаторівневого захисту. У рамках цього підходу буде інтегровано Active Directory для централізованого управління обліковими записами та політиками доступу. Для моніторингу подій і аналізу логів буде впроваджено протокол Syslog. SSH використовуватиметься для захищеного віддаленого доступу до пристроїв. Основою безпеки мережі стане маршрутизатор/міжмережевий екран на базі дистрибутива pfSense, який виконуватиме функції міжмережевого екрану, NAT, а також IDS/IPS (з використанням Snort або Suricata). Також буде реалізовано моніторинг і аналіз трафіку, перехоплення пакетів через Packet Capture, діагностику мережевих маршрутів та стану pfSense з використанням різноманітних інструментів, а також сканування мережі за допомогою Nmap.

Було проаналізовано вимоги мережі до обладнання, та обрано Netgate SG-1100 для розгортання pfSense, Cisco SF200-24FP для комутаторів та сервер із багатоядерним процесором та наведено технічні параметри для сервера на ОС Windows Server 2019.

РОЗДІЛ 3. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ

3.1. Базове налагодження проєкту мережі

Проектування мережі було виконано в емуляторі GNS3, що дозволить максимально приблизно змодельовати мережеву інфраструктуру та протестувати її роботу в реальних умовах без потреби в фізичному обладнанні. При цьому для запуску операційних систем використовувався гіпервізор VirtualBox, що забезпечить віртуалізацію pfSense, сервера та робочих станцій. Зрештою це дозволяє створити повноцінне тестове середовище для перевірки та налаштування мережевих компонентів перед їх впровадженням у фізичній інфраструктурі. Топологія створеної мережі в GNS3 наведена нижче на рис.3.1 і також представлена на дод.А.

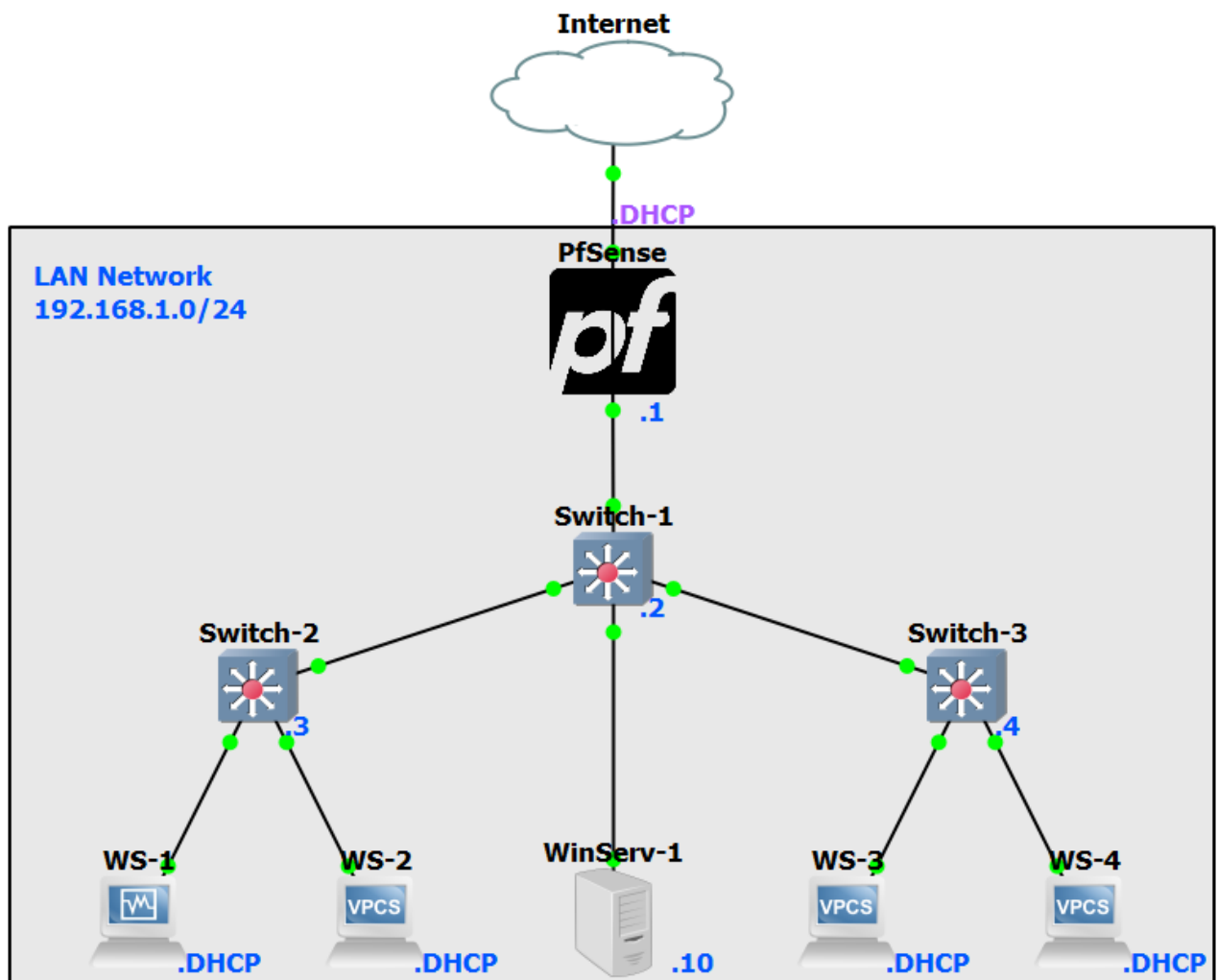


Рисунок 3.1 – Проєкт мережі в GNS3

Перш за все необхідно виконати базове налагодження параметрів адресації на дистрибутиві pfSense. Інтерфейс eth0 буде слугувати для підключення до Інтернету та за замовчуванням отримуватиме динамічні параметри адресації від провайдера, а eth1 призначений для локальної мережі і за замовчуванням має адресу 192.168.1.1/24, рис.3.2. Таким чином pfSense не потребує додаткових зміни в налаштуваннях.

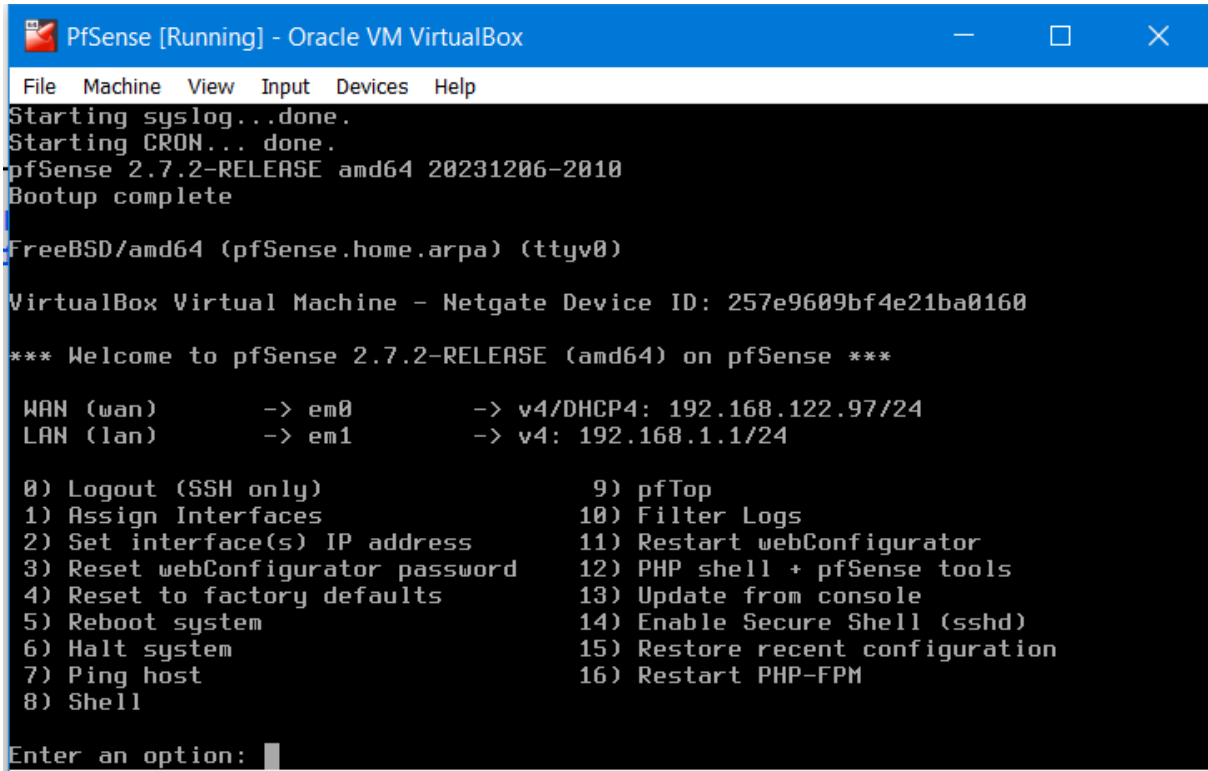
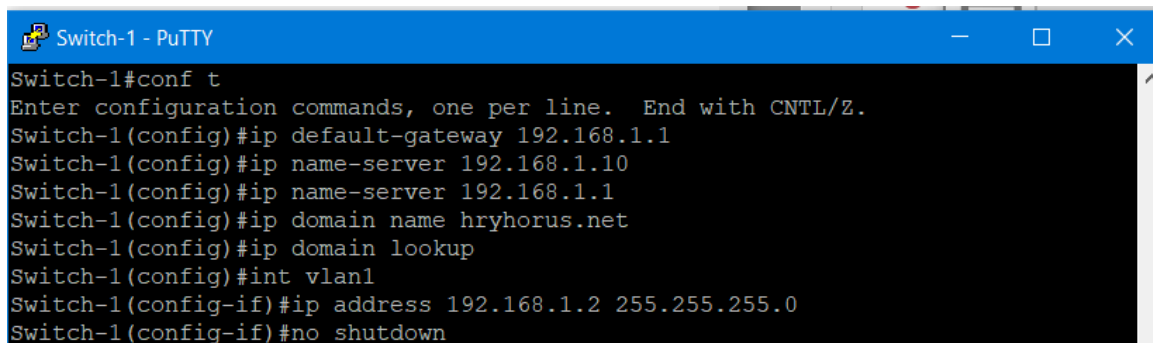


Рисунок 3.2 – Головне меню pfSense

Перейдемо до комутаторів. Нижче наведено сценарій налаштування для Switch-1, втім Switch-2 та Switch-3 налагоджуються за тим самим алгоритмом.

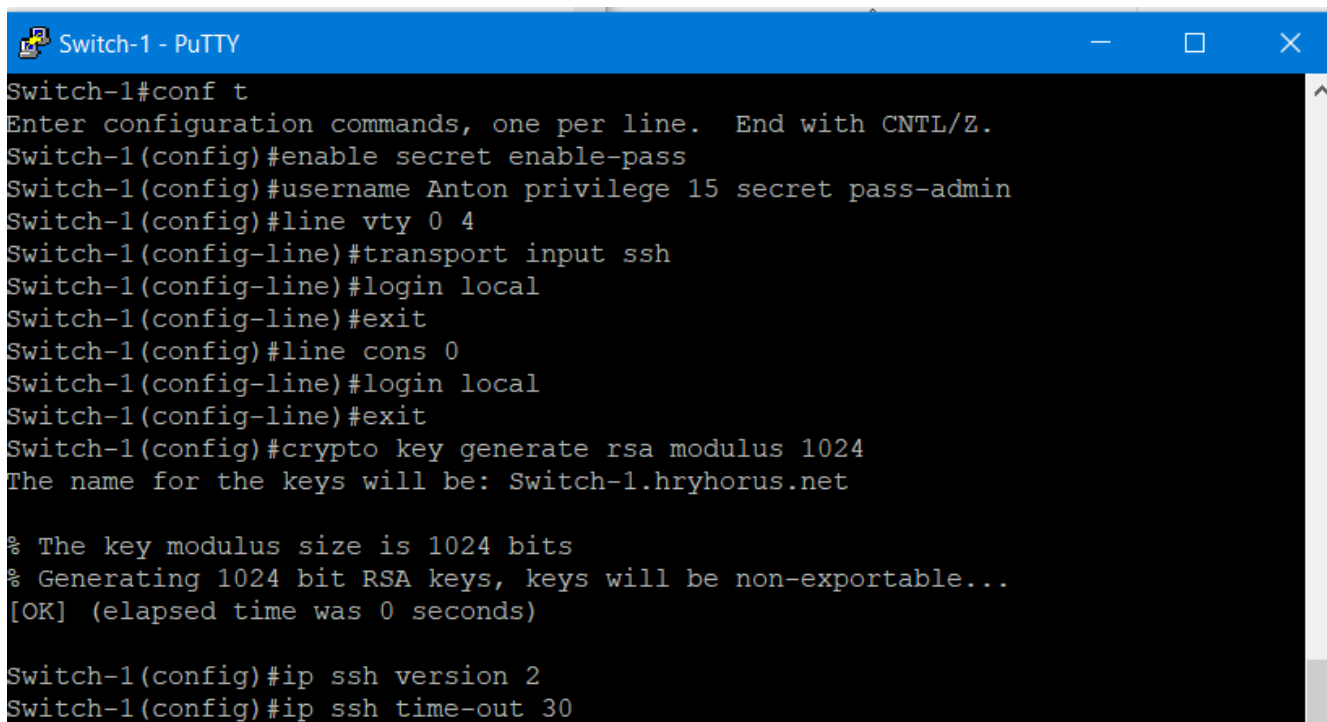
На було налаштовано шлюз за замовчуванням на адресу 192.168.1.1 для маршрутизації трафіку поза локальною мережею, вказано DNS-сервери з адресами 192.168.1.10 (адреса Winows Server) і 192.168.1.1 (адреса pfSense), задано доменне ім'я hryhorus.net, увімкнено функцію ip domain lookup для здійснення DNS-запитів, налаштовано інтерфейс vlan1 з IP-адресою 192.168.1.2 та маскою підмережі 255.255.255.0, а також активовано цей інтерфейс командою no shutdown, рис.3.3.



```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#ip default-gateway 192.168.1.1
Switch-1(config)#ip name-server 192.168.1.10
Switch-1(config)#ip name-server 192.168.1.1
Switch-1(config)#ip domain name hryhorus.net
Switch-1(config)#ip domain lookup
Switch-1(config)#int vlan1
Switch-1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch-1(config-if)#no shutdown
```

Рисунок 3.3 – Налаштування адресації на Switch-1

Далі на комутатора налагоджуємо базову аутентифікацію з використанням користувача та дозволяємо підключення до пристроїв з використання протоколу SSHv2. Таким чином тут було налаштовано пароль командою `enable secret enable-pass` для захисту режиму привілейованого доступу, створено користувача Anton з рівнем привілеїв 15 і паролем `pass-admin`, а також для ліній VTY 0-4 налаштовано використання лише SSH-протоколу, увімкнено локальну аутентифікацію за допомогою `login local` і аналогічно налаштовано консольний доступ. Згенеровано RSA-ключі для забезпечення SSH-з'єднань, активовано SSH-версію 2, а також встановлено тайм-аут для SSH-з'єднань у 30 секунд, рис.3.4. На цьому базове налагодження завершено.



```
Switch-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-1(config)#enable secret enable-pass
Switch-1(config)#username Anton privilege 15 secret pass-admin
Switch-1(config)#line vty 0 4
Switch-1(config-line)#transport input ssh
Switch-1(config-line)#login local
Switch-1(config-line)#exit
Switch-1(config)#line cons 0
Switch-1(config-line)#login local
Switch-1(config-line)#exit
Switch-1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Switch-1.hryhorus.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Switch-1(config)#ip ssh version 2
Switch-1(config)#ip ssh time-out 30
```

Рисунок 3.4 – Налаштування аутентифікації та SSHv2 на Switch-1

Перейдемо до контролера домену, тобто до WinServ-1. Для початку задаємо параметри статичної адресації згідно виконаного розподілу в розділі 2, рис.3.5.

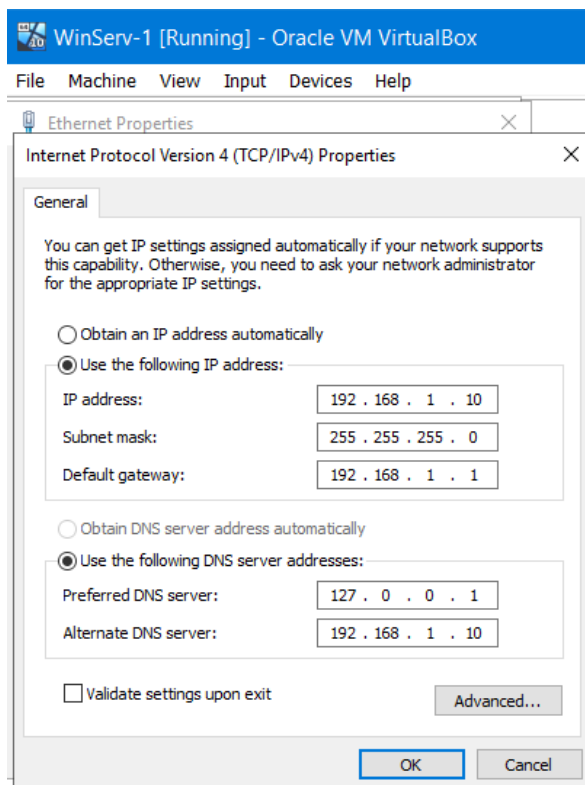


Рисунок 3.5 – Налаштування адресації на Windows Server

Далі виконуємо розгортання Active Directory з додаванням відповідних ролей, функцій та створення домену hryhorus.net, рис.3.6-3.8.

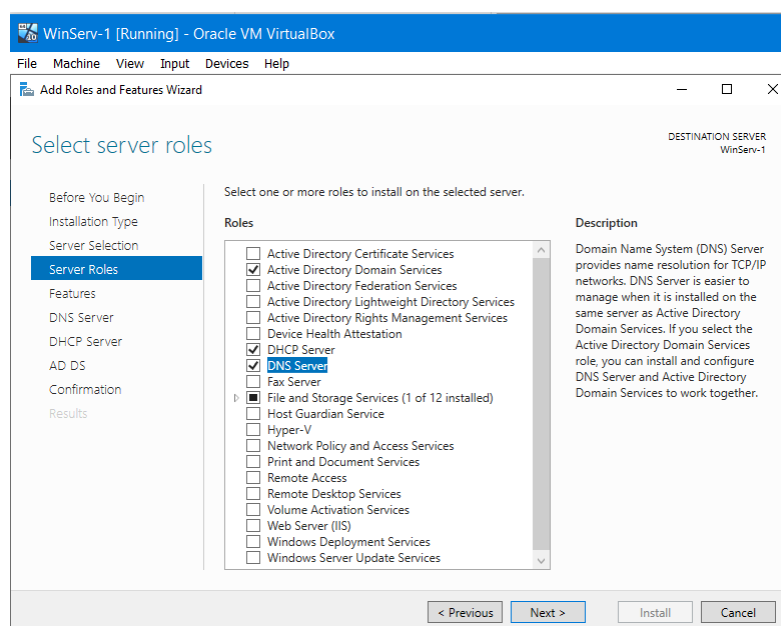


Рисунок 3.6 – Додавання відповідних ролей для контролера домену

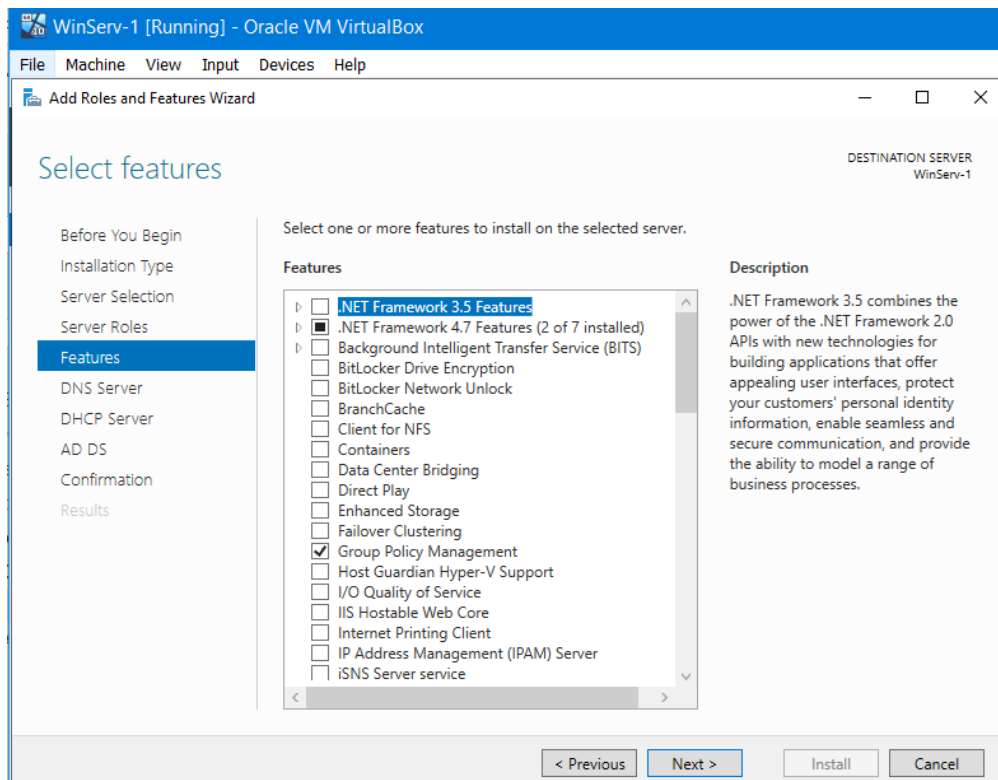


Рисунок 3.7 – Додання відповідних функцій для контролера домену

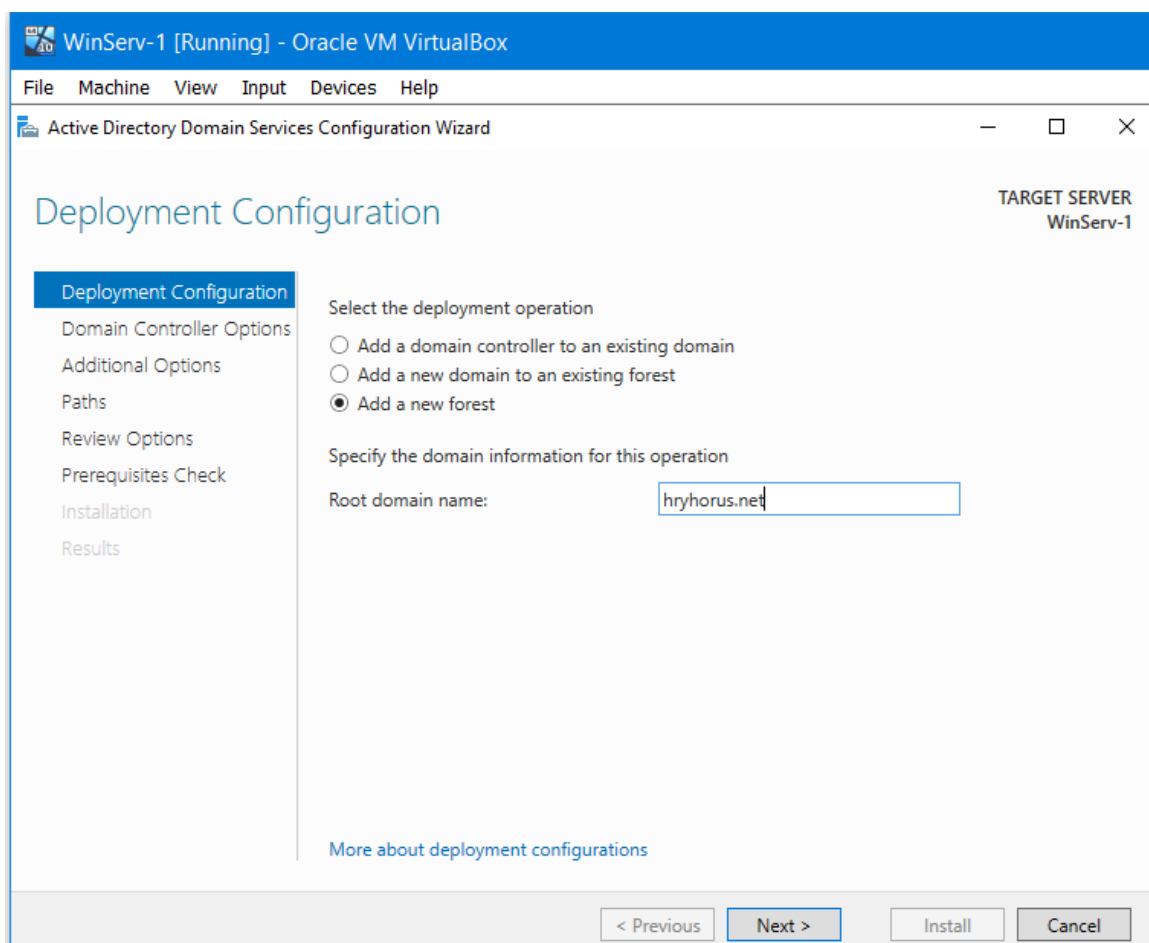


Рисунок 3.8 – Створення домену hryhorus.net

Після цього налагоджуємо роботу DHCP серверу на контролері домену. DHCP служить для автоматичного призначення IP-адрес і мережевих параметрів клієнтам, що спрощує адміністрування мережі, рис.3.9-3.10.

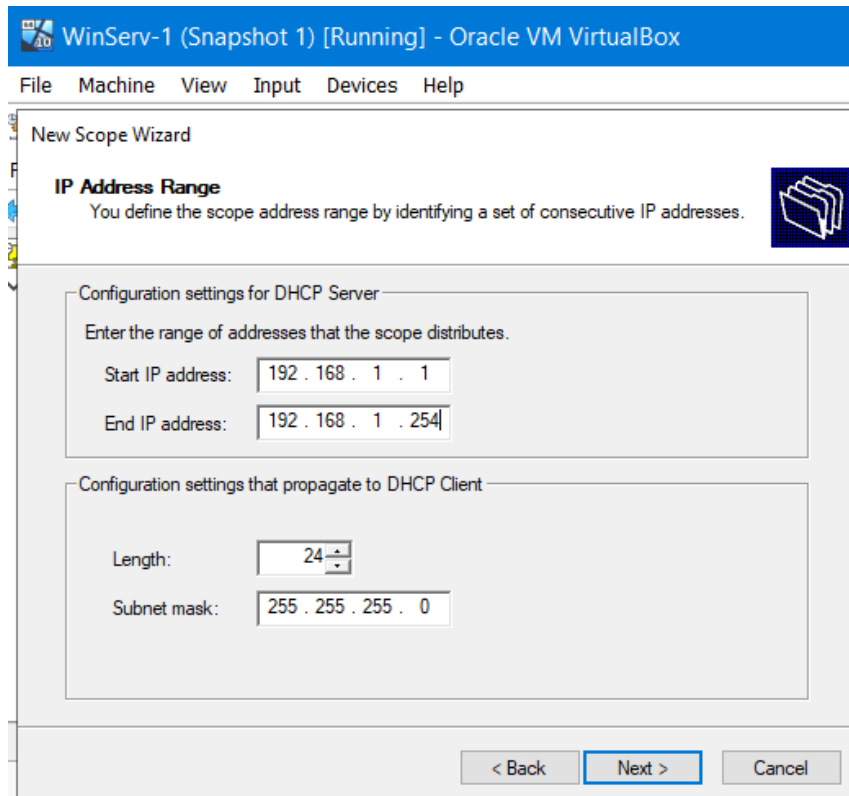


Рисунок 3.9 – Задання діапазону роздачі адрес клієнтам

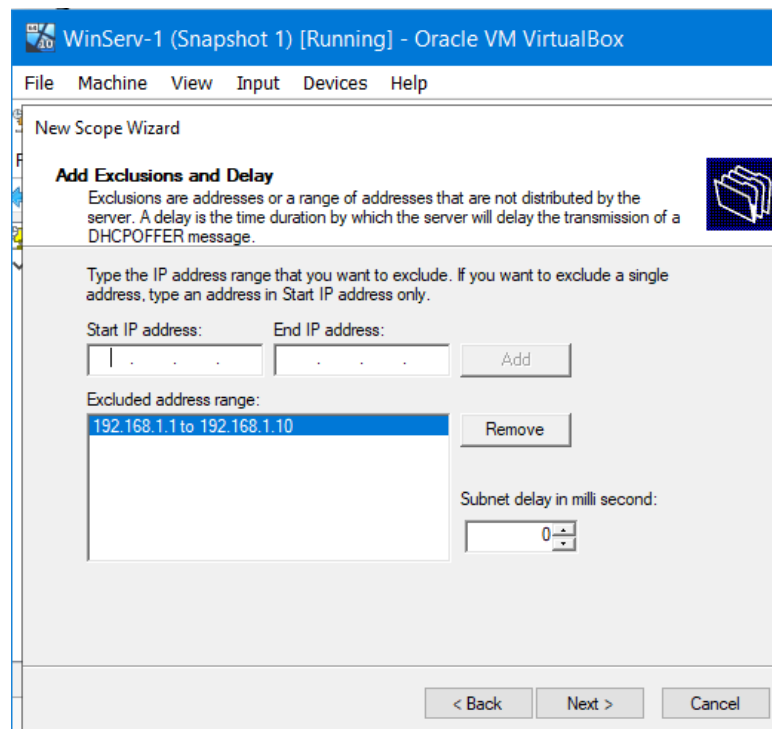


Рисунок 3.10 – Виключення статичних адрес з роздачі

Також налагодимо роботу DNS серверу шляхом додавання відповідних записів для пристроїв мережі. DNS сервер слугуватиме для перетворення доменних імен на IP-адреси, що зрештою забезпечить можливість зручно звертатись до пристроїв доменної інфраструктури за їх іменами, рис.3.11.

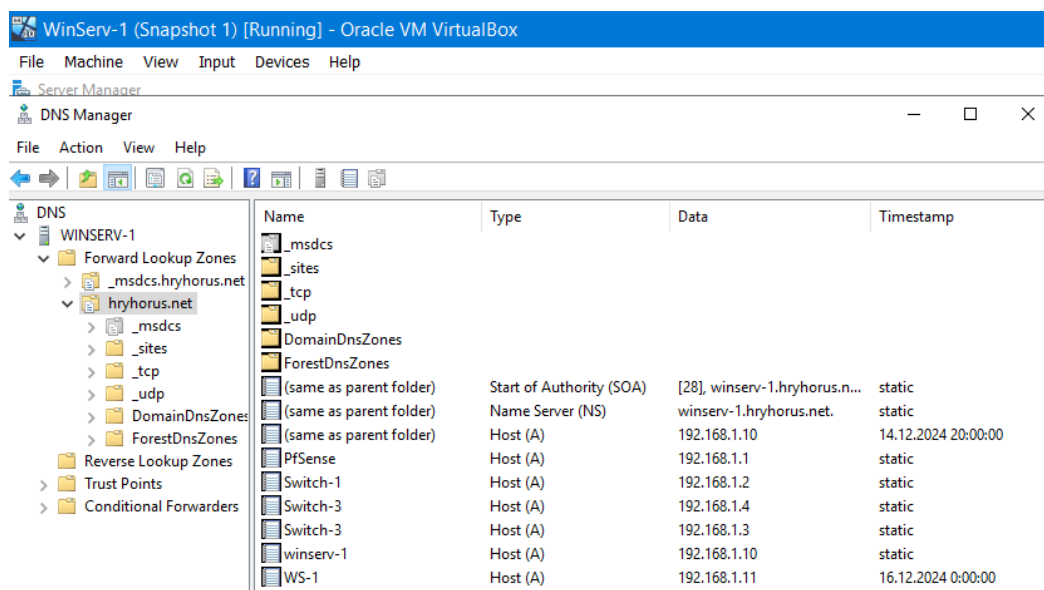


Рисунок 3.11 – Налаштування DNS серверу

На контролері домену лишається створити облікові записи користувачів, які будуть використовуватись клієнтами мережі для входу в систему на кінцевих станціях мережі, рис.3.12.

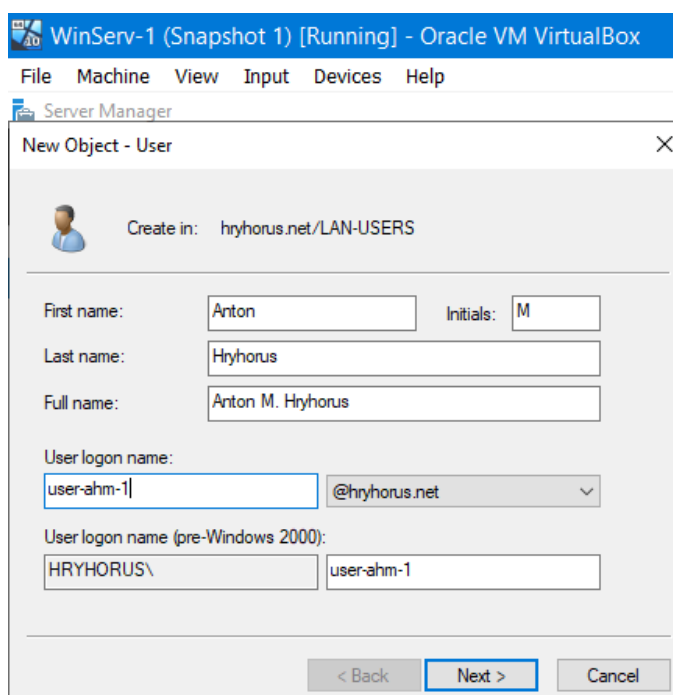


Рисунок 3.12 – Створення облікового запису користувача user-ahm-1

Перейдемо до кінцевих пристроїв Windows 10. Для прикладу розглянемо комп'ютер WS-1, втім інші вузли налаштовуються тим самим чином. Перш за все для даних пристроїв необхідно вказати динамічне отримання адрес від DHCP сервера, тобто від контролера домену WinServ-1 та перевірити коректність отриманих параметрів адресації, рис.3.13.

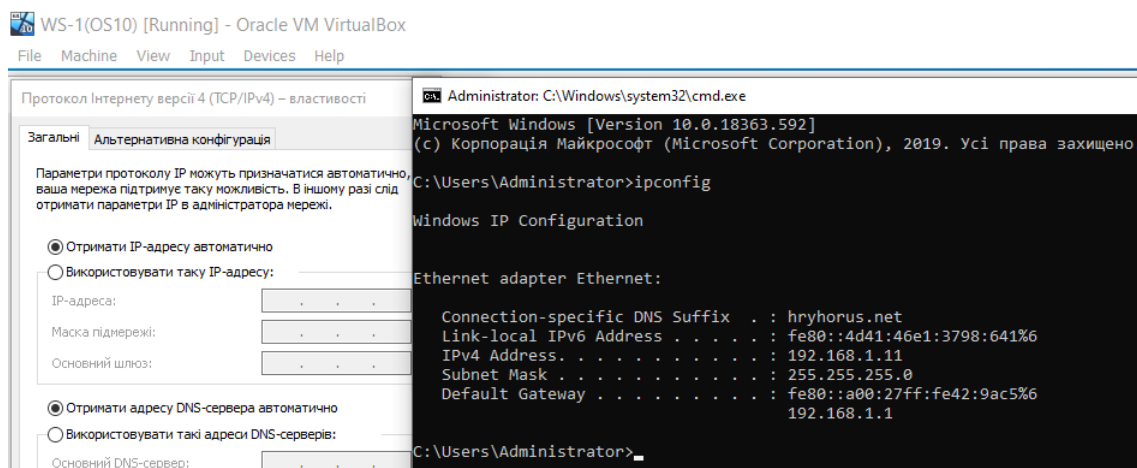


Рисунок 3.13 – Отримання динамічної адреси на WS-1

Після цього виконуємо приєднання пристрою до домену hryhorus.net з метою централізованого управління, застосування групових політик і забезпечення користувачам єдиного доступу до ресурсів доменної мережі, рис.3.14.

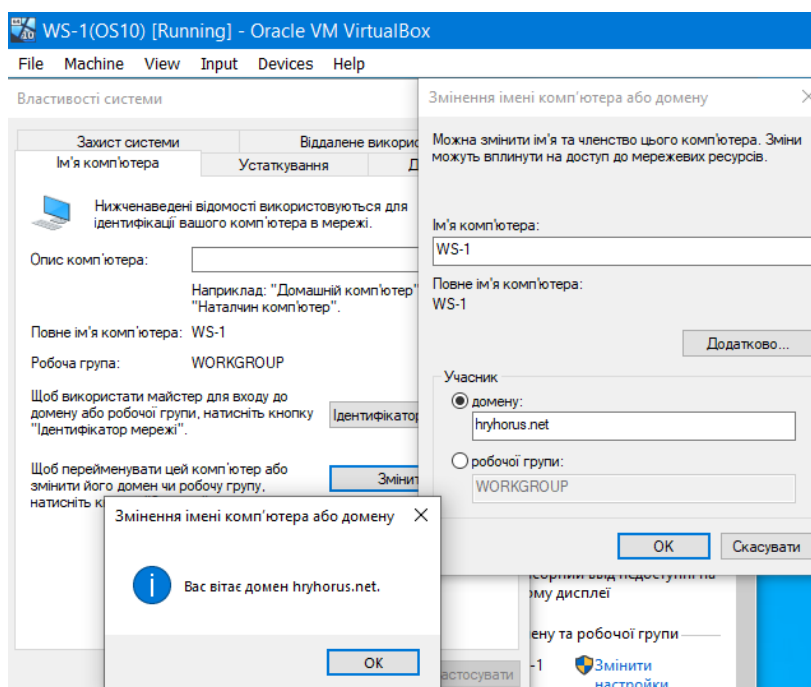


Рисунок 3.14 – Приєднання комп'ютеру до домену hryhorus.net

Syslog – це протокол для збору, зберігання та моніторингу повідомлень журналів подій з різних пристроїв і систем і використовується для централізованого управління логами, виявлення проблем, аудиту та безпеки в корпоративних мережах. В даному проєкті мережі роль Syslog сервера виконуватиме контролер домену, а клієнтами будуть комутатори та pfSense. Для прикладу, на сервері виконаємо встановлення безкоштовної утиліти «Visual Syslog Server» [21], яка дозволить отримувати і відображати зібрані події з пристроїв, рис.3.15.

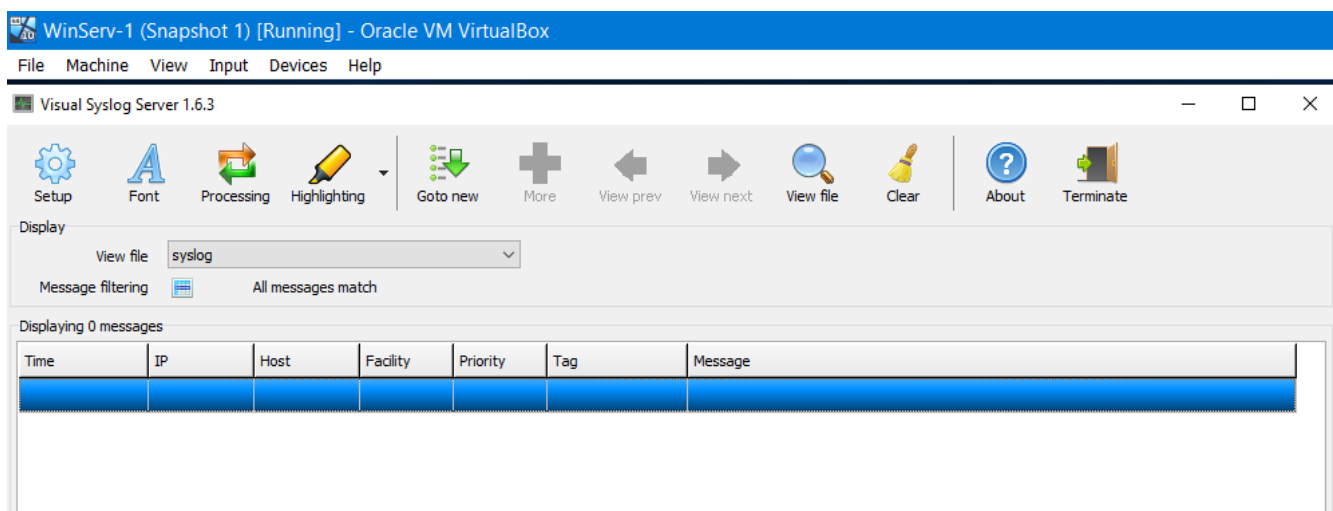


Рисунок 3.15 – Встановлена програма «Visual Syslog Server»

Тепер на комутаторах налаштуємо відправку подій до серверу Syslog. Нижче наведе сценарій налагодження для Switch-1, однак інші пристрої налагоджуються тим же чином рис.3.16.

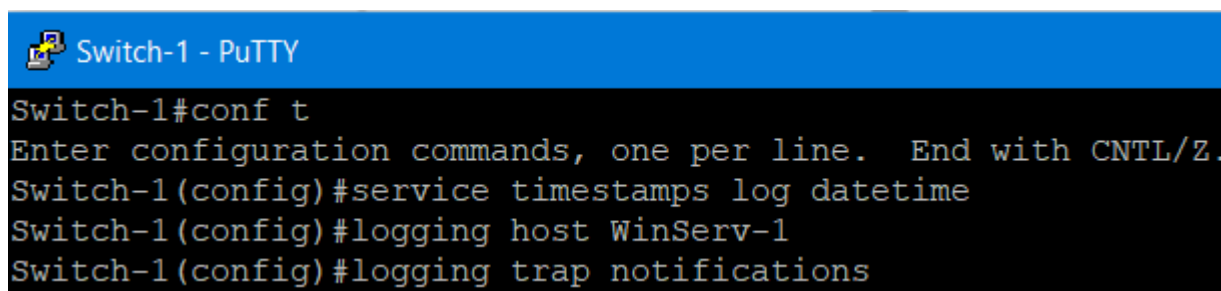


Рисунок 3.16 – Налаштування пересилки сповіщень до серверу Syslog

Перевірка роботи

З однієї з робочої станції мережі, для прикладу WS-1, виконаємо вхід в систему з використанням облікових даних користувача Anton Hryhorus.

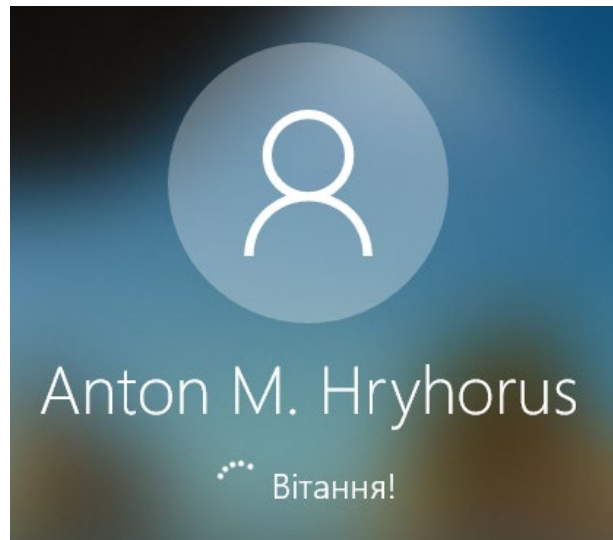


Рисунок 3.17 – Вхід в систему WS-1 під користувачем Anton Hryhorus

Виконаємо перевірку зв'язку з іншими пристроями локальної мережі з використання їх доменних імен. Також перевіримо можливість з'єднання з ресурсами мережі Інтернет, рис.3.18.

WS-1(OS10) [Running] - Oracle VM VirtualBox					
File	Machine	View	Input	Devices	Help
Windows PowerShell PS C:\Users\user-ahm-1.HRYHORUS> ping winserv-1 Pinging WinServ-1.hryhorus.net [192.168.1.10] with 32 bytes of data: Reply from 192.168.1.10: bytes=32 time=1ms TTL=128 Reply from 192.168.1.10: bytes=32 time=1ms TTL=128 Reply from 192.168.1.10: bytes=32 time=1ms TTL=128 Reply from 192.168.1.10: bytes=32 time=1ms TTL=128 Ping statistics for 192.168.1.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms PS C:\Users\user-ahm-1.HRYHORUS> ping pfsense Pinging pfsense.hryhorus.net [192.168.1.1] with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time=2ms TTL=64 Reply from 192.168.1.1: bytes=32 time=1ms TTL=64 Reply from 192.168.1.1: bytes=32 time=1ms TTL=64 Reply from 192.168.1.1: bytes=32 time=5ms TTL=64 Ping statistics for 192.168.1.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 5ms, Average = 2ms Windows PowerShell PS C:\Users\user-ahm-1.HRYHORUS> ping google.com Pinging google.com [142.251.39.14] with 32 bytes of data: Reply from 142.251.39.14: bytes=32 time=26ms TTL=113 Reply from 142.251.39.14: bytes=32 time=23ms TTL=113 Reply from 142.251.39.14: bytes=32 time=23ms TTL=113 Request timed out. Ping statistics for 142.251.39.14: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 23ms, Maximum = 26ms, Average = 24ms PS C:\Users\user-ahm-1.HRYHORUS> ping learn.ztu.edu.ua Pinging ztu.edu.ua [46.4.92.154] with 32 bytes of data: Reply from 46.4.92.154: bytes=32 time=46ms TTL=52 Reply from 46.4.92.154: bytes=32 time=37ms TTL=52 Reply from 46.4.92.154: bytes=32 time=39ms TTL=52 Reply from 46.4.92.154: bytes=32 time=40ms TTL=52 Ping statistics for 46.4.92.154: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 37ms, Maximum = 46ms, Average = 40ms					

Рисунок 3.18 – Перевірка мережевого зв'язку

З Windows Server виконаємо віддалене підключення до одного з комутаторів мережі з використання протоколу SSHv2 та утиліти PuTTY [22], рис.3.19. Для прикладу відімкнемо один з активних мережевих інтерфейсів і одразу в програмі для перегляду подій Syslog відобразились відповідні сповіщення про вимкнення інтерфейсу eth3/2. Виконані дії демонструють коректність роботи віддаленого підключення через SSH та правильну роботу Syslog.

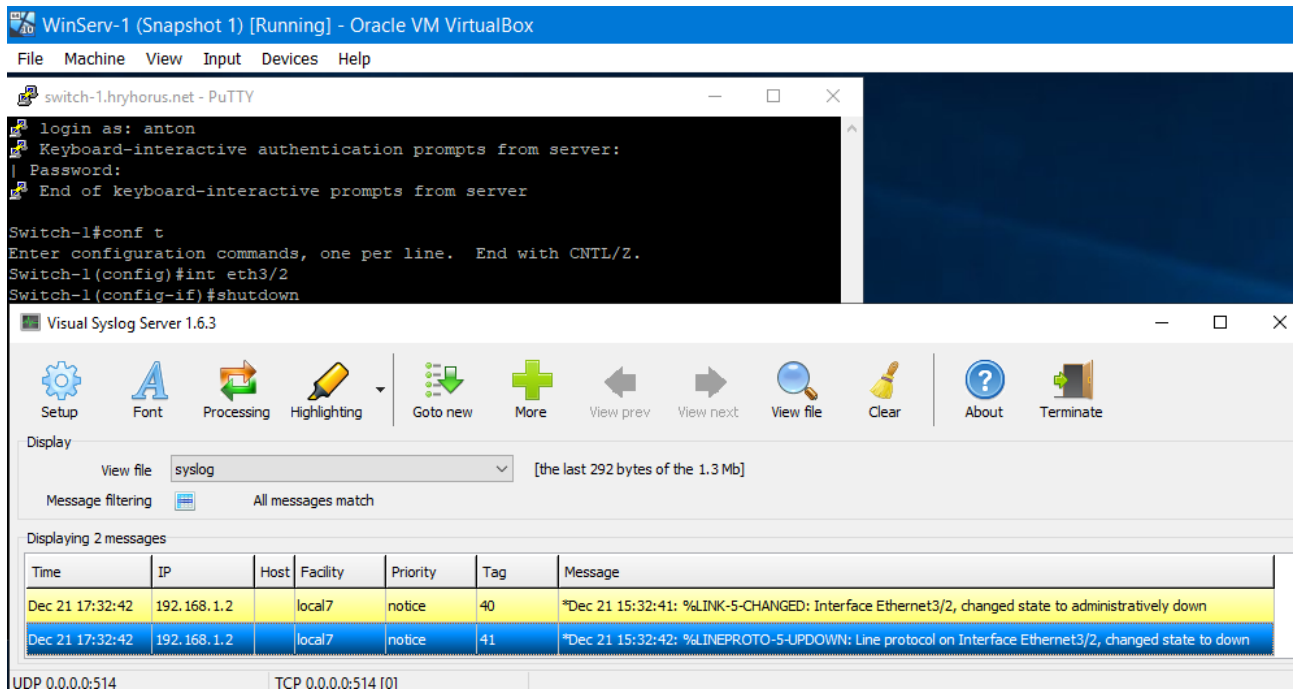


Рисунок 3.19 – Перевірка підключення через SSH та роботи Syslog

3.2. Базове налагодження pfSense

За замовчуванням доступ до веб-інтерфейсу pfSense можливий з використанням протоколу https, то за адресою <https://192.168.1.1> або <https://pfsense>, оскільки в мережі налаштовано роботу DNS серверу і є можливість звертатись до пристроїв за їх іменами. Тому з використання браузера переходимо за однією зі згаданою адресою. Нас зустрічає повідомлення про незахищене підключення, оскільки pfSense використовує самопідписаний сертифікат. Ігноруємо дане повідомлення та вводимо логін (admin) та пароль (pfsense) за замовчуванням, рис.3.20-3.21.

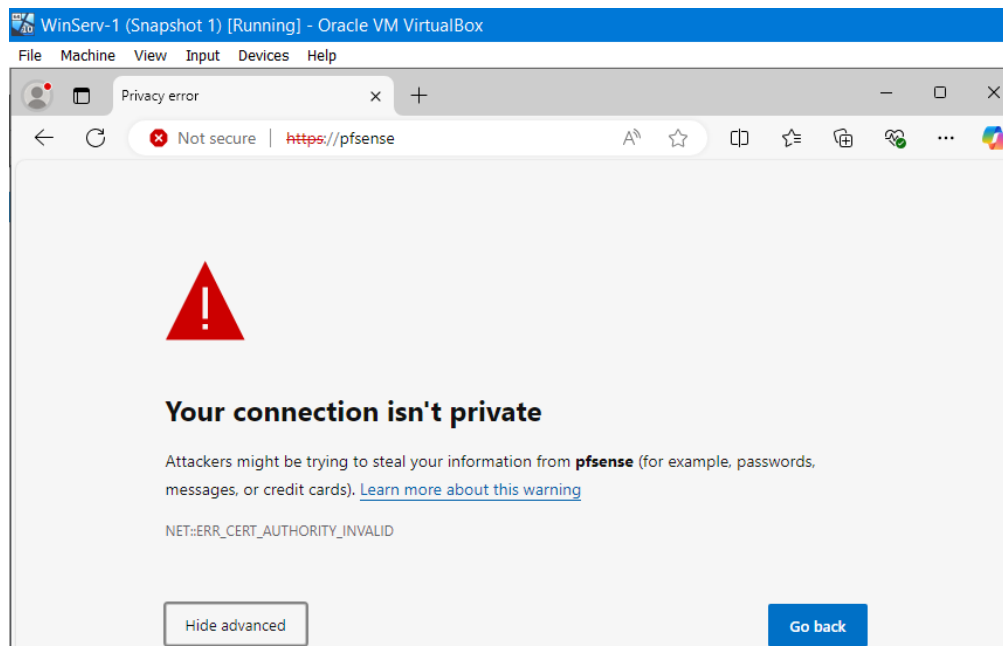


Рисунок 3.20 – Перехід за адресою pfSense у браузері

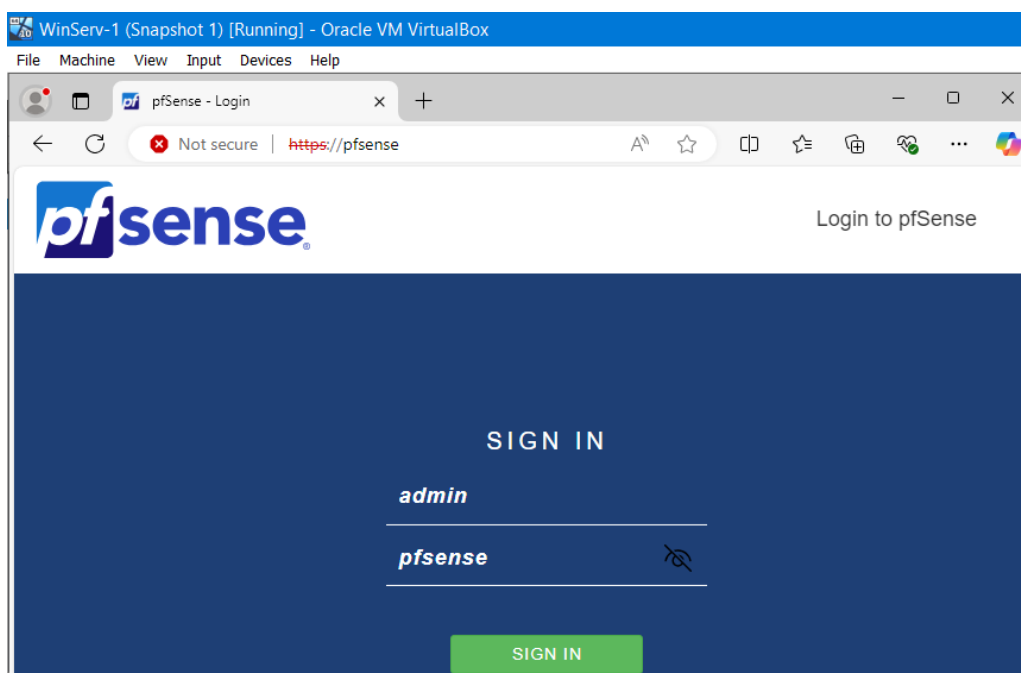


Рисунок 3.21 – Перехід за адресою pfSense в браузері

Якщо все було введено правильно, то відразу відобразиться вікно з майстром налаштувань, під час якого слід зазначити такі параметри, як ім'я домену, адресу NTP-серверу, часовий пояс та задати новий пароль адміністратора, рис.3.22-3.23. Інші пункти майстру налаштувань можна пропустити.

The screenshot shows the pfSense Setup Wizard at Step 2 of 9, titled "General Information". At the top, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb navigation is "Wizard / pfSense Setup / General Information". Below the step indicator, a section titled "General Information" contains the instruction: "On this screen the general pfSense parameters will be set." There are two input fields: "Hostname" with the value "pfSense" and "Domain" with the value "hryhorus.net". Descriptive text for the Hostname field reads: "Name of the firewall host, without domain part. Examples: pfsense, firewall, edgefw". Descriptive text for the Domain field reads: "Domain name for the firewall."

Рисунок 3.22 – Задання ім'я домену

The screenshot shows the pfSense Setup Wizard at Step 3 of 9, titled "Time Server Information". At the top, the same warning message is present. The breadcrumb navigation is "Wizard / pfSense Setup / Time Server Information". Below the step indicator, a section titled "Time Server Information" contains the instruction: "Please enter the time, date and time zone." There are two input fields: "Time server hostname" with the value "0.ua.pool.ntp.org" and "Timezone" with the value "Europe/Kyiv". Descriptive text for the Time server hostname field reads: "Enter the hostname (FQDN) of the time server." At the bottom of the form is a blue button labeled "Next".

Рисунок 3.23 – Задання адреси NTP-серверу та часового поясу

pfSense
COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

[Next](#)

Рисунок 3.24 – Задання нового пароля адміністратора

В пункті DNS Resolver- Domains Override задамо назву домену та відповідну адресу DNS-серверу завдяки чому pfSense зможе легко звертатися до пристроїв локальної мережі за їх іменами, рис.3.25.

pfSense
COMMUNITY EDITION

Services / DNS Resolver / General Settings / Edit Domain Override

Domains to Override with Custom Lookup Servers

Domain	hryhorus.net
Domain whose lookups will be directed to a user-specified DNS lookup server.	
IP Address	192.168.1.10
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.	
TLS Queries	☐ Use SSL/TLS for DNS Queries forwarded to this server
When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.	
TLS Hostname	
An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
Description	
A description may be entered here for administrative reference (not parsed).	

Рисунок 3.25 – Налаштування Domain Override

3.3. Налаштування та перевірка додаткових функцій безпеки pfSense

Налаштуємо відправку сповіщень до Syslog сервера для централізованого моніторингу подій і забезпечення оперативного реагування на потенційні проблеми, рис. 3.26.

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address Default (any) ▼
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4 ▼
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers WinServ-1:514 IP[:port] IP[:port]

Remote Syslog Contents

- ☐ Everything
- ☒ System Events
- ☒ Firewall Events
- ☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- ☒ General Authentication Events
- ☐ Captive Portal Events
- ☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- ☒ Gateway Monitor Events

Рисунок 3.26 – Налаштування відправки сповіщень до Syslog сервера

Перейдемо до правил фаєрвола. Міжмережевий екран pfSense за замовчуванням дотримується методологію "дозволити за замовчуванням" на LAN-інтерфейсі та "заборонити за замовчуванням" на WAN-інтерфейсі. Що означає дозвіл всього вихідного трафіку з LAN до Інтернету та блокування вхідного трафіку з Інтернету, рис.3.27-3.28. За можливістю користувач може

легко додати будь-які свої правила, втім для базової роботи мережі наявні правила є достатніми.

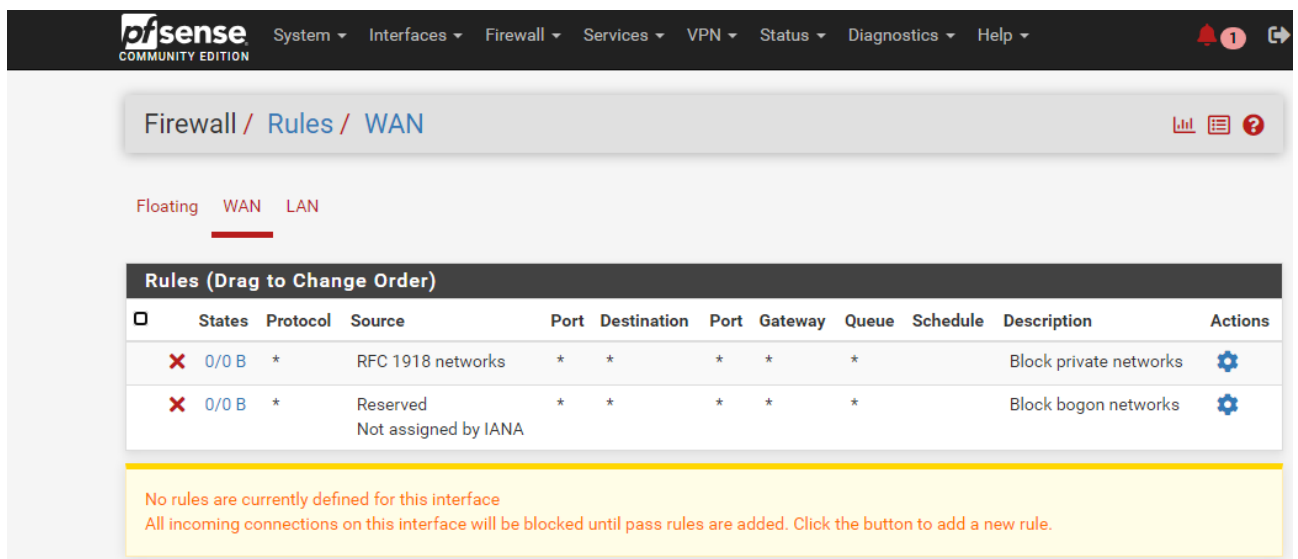


Рисунок 3.27 – Правила фаєрвола для інтерфейсу WAN

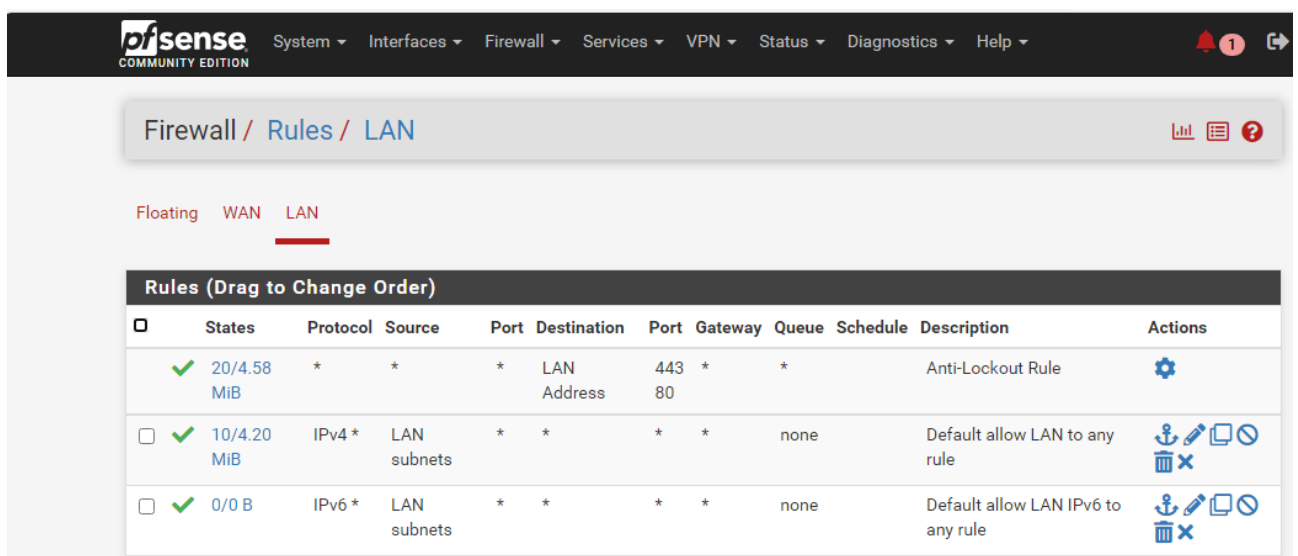


Рисунок 3.28 – Правила фаєрвола для інтерфейсу LAN

Налаштування і тестування Snort

Snort – це система виявлення та запобігання вторгненням (IDS/IPS), яка аналізує мережевий трафік у режимі реального часу, виявляє підозрілі активності та може блокувати атаки. У pfSense Snort можна встановити як додатковий пакет, що дозволяє інтегрувати потужний інструмент безпеки для моніторингу, фільтрації трафіку та запобігання кіберзагрозам, рис.3.29.

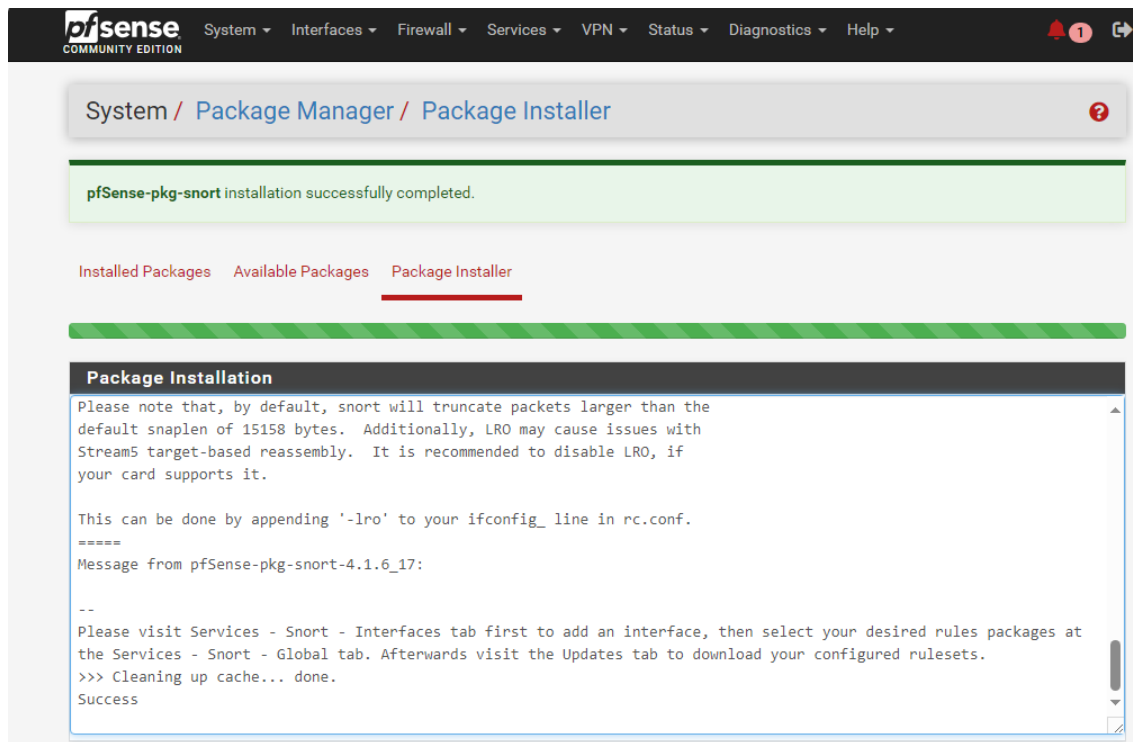


Рисунок 3.29 – Встановлення пакунку Snort на pfSense

Переходимо до глобальних налаштувань Snort. Перш за все необхідно обрати списки готових правил, які будуть використовуватись в роботі. Слід зауважити, що деякі списки надаються лише за платною підпискою, однак є і безкоштовні, рис.3.30.

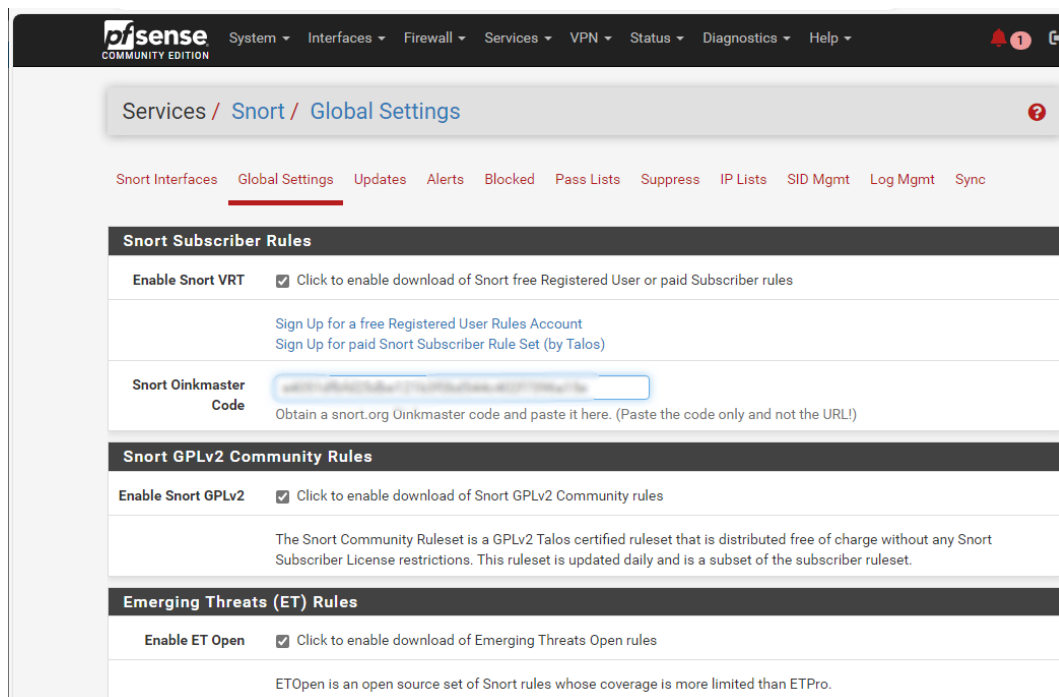


Рисунок 3.30 – Вибір списків правил

Тут же на сторінці можна зазначити інтервал автоматичного оновлення, в даному випадку це щодня, і зазначити термін блокування IP-адрес пристроїв у випадку порушень правил, що в даному випадку буде становити 1 годину, рис.3.31.

The screenshot displays the configuration interface for Snort, divided into two main sections: 'Rules Update Settings' and 'General Settings'.

Rules Update Settings:

- Update Interval:** A dropdown menu set to '1 DAY'. Below it, a note states: 'Please select the interval for rule updates. Choosing NEVER disables auto-updates.'
- Update Start Time:** A text input field set to '00:30'. Below it, a note explains: 'Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.'
- Hide Deprecated Rules Categories:** A checkbox that is checked. The note says: 'Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.'
- Disable SSL Peer Verification:** A checkbox that is unchecked. The note says: 'Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.'

General Settings:

- Remove Blocked Hosts Interval:** A dropdown menu set to '1 HOUR'. Below it, a note states: 'Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.'
- Remove Blocked Hosts After Deinstall:** A checkbox that is checked. The note says: 'Click to clear all blocked hosts added by Snort when removing the package. Default is checked.'
- Keep Snort Settings After Deinstall:** A checkbox that is checked. The note says: 'Click to retain Snort settings after package removal.'
- Startup/Shutdown Logging:** A checkbox that is unchecked. The note says: 'Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.'

Рисунок 3.31 – Налаштування інтервалу оновлень правил та блокування IP-адрес пристроїв

Далі необхідно безпосередньо виконати завантаження обраних списків правил, рис.3.32.

The screenshot shows the 'Updates' section of the Snort web interface. At the top, there is a navigation bar with links: 'Services / Snort / Updates'. Below this, a sub-navigation bar includes links: 'Snort Interfaces', 'Global Settings', 'Updates' (which is highlighted), 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'.

The main content area is titled 'Installed Rule Set MD5 Signature' and contains a table with the following data:

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	933de61b4fcc18617644c4e600dd2c28	Saturday, 21-Dec-24 18:33:25 EET
Snort GPLv2 Community Rules	5bc43fc972935ba67036bb4fd958e4a4	Saturday, 21-Dec-24 00:08:47 EET
Emerging Threats Open Rules	3f08fd219334d211e2517d1b102e6ec4	Saturday, 21-Dec-24 18:33:25 EET
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Below the table, there is a section titled 'Update Your Rule Set' which shows the 'Last Update' as 'Dec-21 2024 18:37' and the 'Result' as 'Success'. At the bottom, there is a button labeled 'Update Rules' with a checkmark icon and a 'Force Update' button with a download icon.

Рисунок 3.32 – Завантаження обраних списків правил

Далі необхідно обрати інтерфейс на якому працюватиме Snort. В даному випадку це буде WAN, оскільки для нас більш важливо захистити мережу від зовнішніх загроз, рис.3.33.

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Services / Snort / WAN - Interface Settings'. Below this, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The 'WAN Settings' section is active. Under 'General Settings', the 'Enable' checkbox is checked. The 'Interface' dropdown is set to 'WAN (em0)'. The 'Description' field contains 'WAN'. The 'Snap Length' field contains '1518'.

Рисунок 3.33 – Налаштування роботи Snort на інтерфейсі WAN

Нижче на сторінці можна зазначити, щоб Snort автоматично генерував логи про спрацювання тривоги, які в подальшому будуть переадресовані до Syslog сервера, рис.3.34.

The screenshot shows the 'Alert Settings' section of the pfSense web interface. The 'Send Alerts to System Log' checkbox is checked. The 'System Log Facility' dropdown is set to 'LOG_AUTH'. The 'System Log Priority' dropdown is set to 'LOG_ALERT'. The 'Enable Packet Captures' checkbox is unchecked. The 'Enable Unified2 Logging' checkbox is unchecked.

Рисунок 3.34 – Налаштування генерації логів роботи Snort

Ще нижче є пункт «Block Offensice», який включає роботи Snort в режимі IPS (Intrusion Prevention System), тобто не лише виявлення, а і автоматичного блокування хостів у разі виникнення тривоги. Поки не будемо вмикати дану опцію і перевіримо роботу Snort в режимі IDS (Intrusion Detection System), рис.3.35.

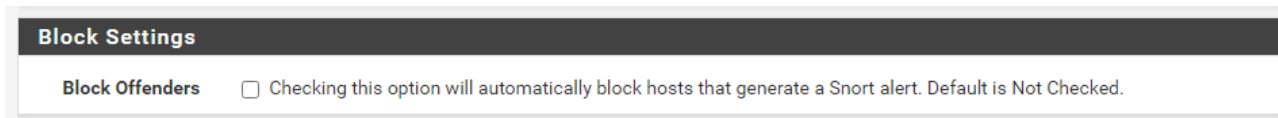


Рисунок 3.35 – Опція автоматичного блокування хостів (режим IPS)

Тепер необхідно обрати категорії правил, які будуть використані. Для «Snort Subscriber IPS Policy Selection» обираємо опцію «Balanced», яка забезпечить оптимальний набір правил. Для «Snort GPLv2 Community Rules (Talos certified)» та «Ruleset: ET Open Rules» вмикаємо всі категорії правил, рис.3.36. Повна ілюстрація сторінки представлена на дод.Б.1.

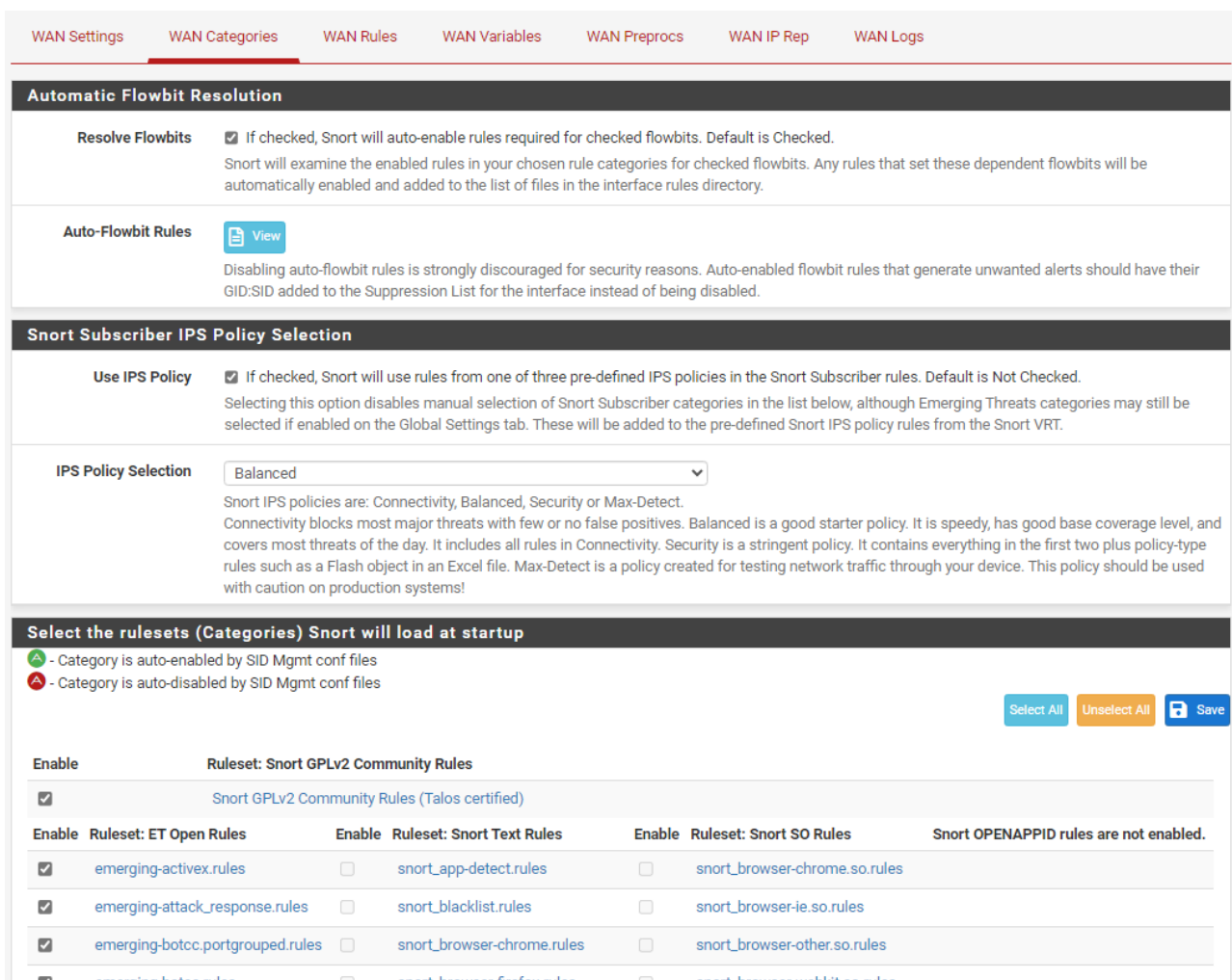


Рисунок 3.36 – Вибір категорія правил

Далі можна переглянути, які правила будуть використані та вручну виключити лишні. Однак залишимо всі правила включеними за замовчуванням, рис.3.37.

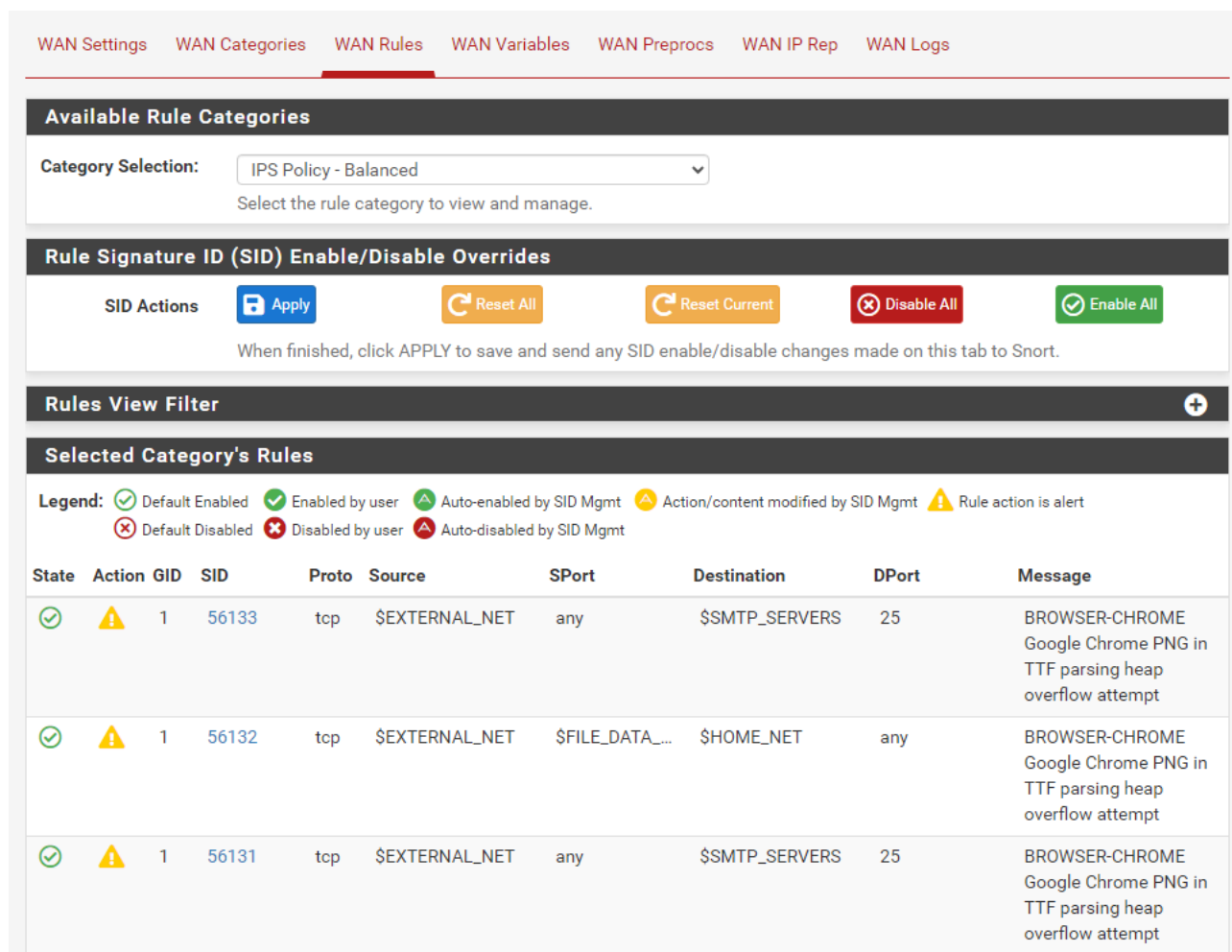


Рисунок 3.37 – Перегляд застосованих правил

Базові налаштування Snort виконано. Тепер запускаємо його роботу на інтерфейсі WAN, рис.3.38.

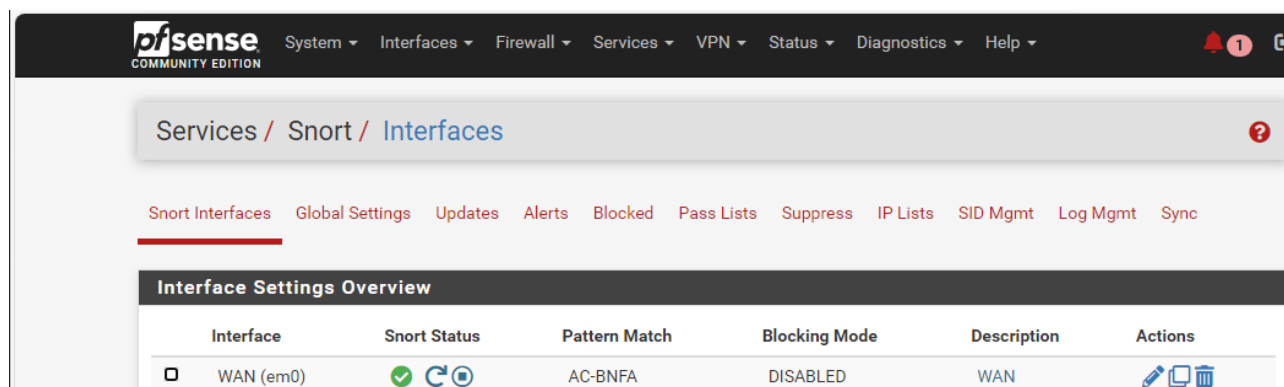
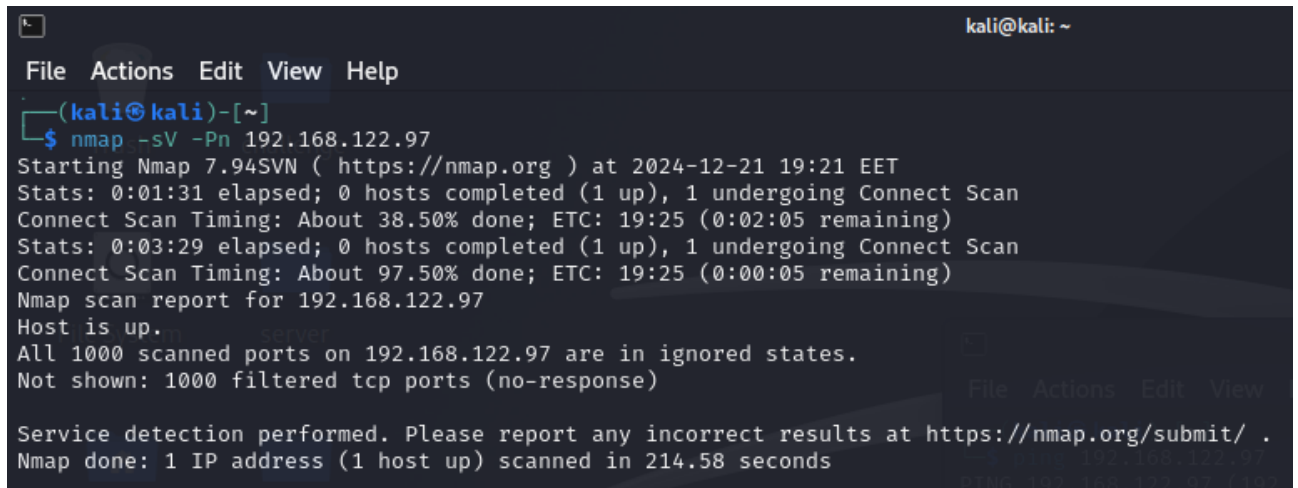


Рисунок 3.38 – Запуск роботи Snort на інтерфейсі WAN

Тестування роботи Snort

Nmap (Network Mapper) – це потужний інструмент для сканування мереж, який використовується для виявлення хостів, відкритих портів, запущених сервісів, їхніх версій і потенційних вразливостей. Його основна мета – аудит безпеки мережі та діагностика, втім часто використовується у зловмисних цілях. Для тестування роботи правил Snort буде використано Nmap, яка буде встановлена на умовну стацію зловмисника Kali з адресою 192.168.122.232. Далі виконаємо команду «nmap -sV -Pn 192.168.122.97», яка просканує зовнішній публічний (WAN) інтерфейс pfSense на наявність відкритих сервісів, що працюють на ньому. Після певного проміжку часу сканування завершилось без результатів, рис.3.39, оскільки правила фаєрвола pfSense на інтерфейсі WAN забороняють будь-які вхідні з’єднання.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV -Pn 192.168.122.97  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 19:21 EET  
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 38.50% done; ETC: 19:25 (0:02:05 remaining)  
Stats: 0:03:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 97.50% done; ETC: 19:25 (0:00:05 remaining)  
Nmap scan report for 192.168.122.97  
Host is up.  
All 1000 scanned ports on 192.168.122.97 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 214.58 seconds
```

Рисунок 3.39 – Результат сканування Nmap для виявлення сервісів на pfSense

Однак на pfSense в пункті «Alerts» надійшло 10 сповіщень з відмітками «Potentially Bad Traffic» та «Attempted Information Leak». Дані сповіщення мають в описі слово «ET SCAN», що означає виявлення сканування мережі на наявність відкритих портів і можливих вразливих сервісів, що і було виконано на попередньому кроці. Крім цього, можна дізнатись адресу та порти джерела і призначення, рис.3.40. Повна ілюстрація наведена на дод.Б.2.

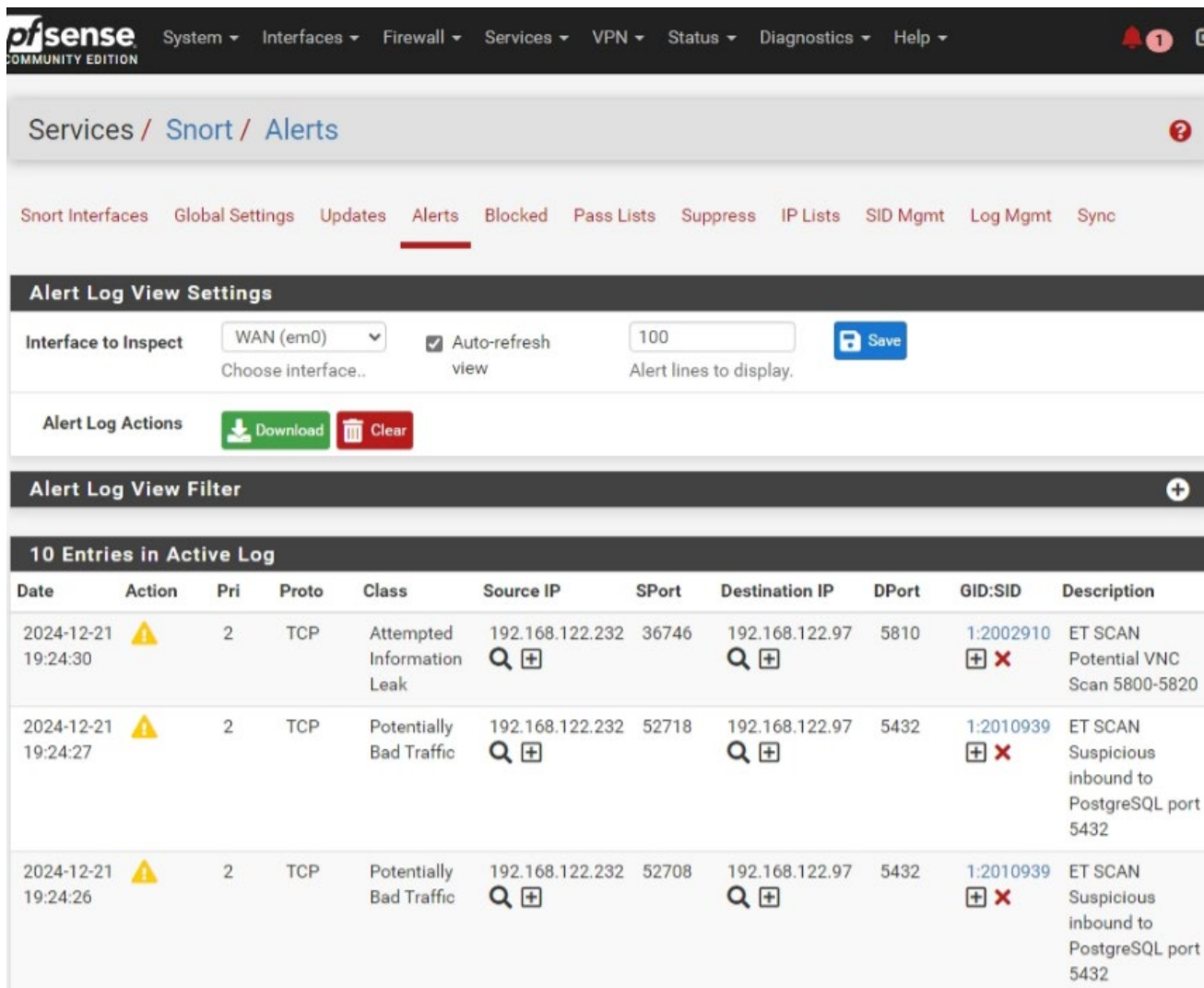


Рисунок 3.40 – Отримані сповіщення Snort про спробу сканування

Аналогічні повідомлення можна побачити і на Syslog сервері, що був налаштований на контролері домену, рис.3.41.

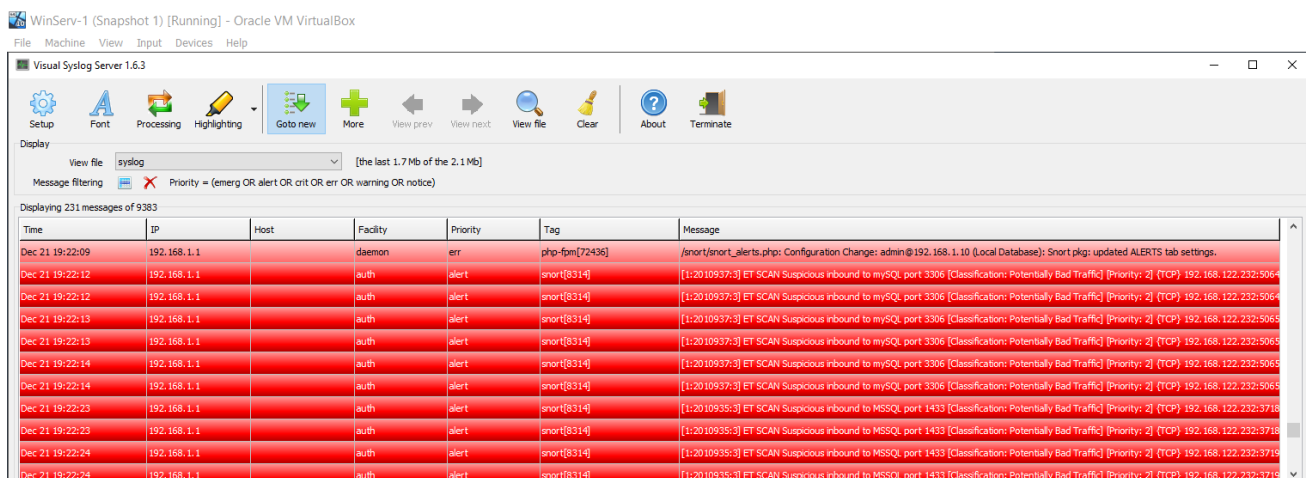
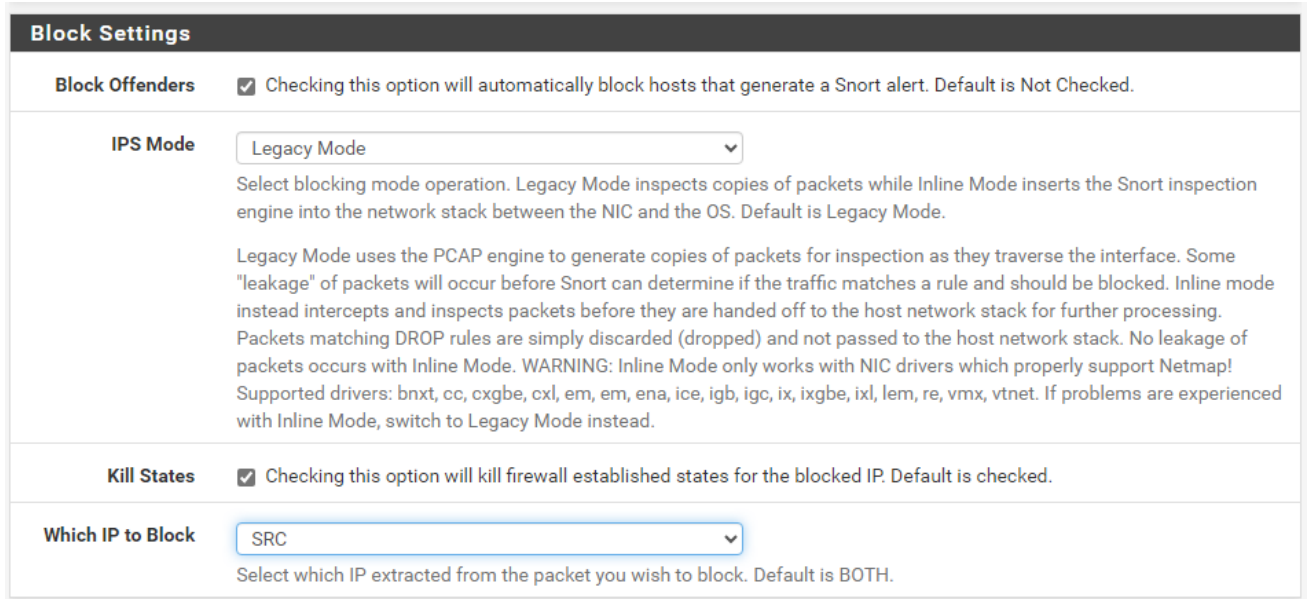


Рисунок 3.41 – Отримані сповіщення на Syslog сервері

Налаштування роботи Snort в режимі IPS

Повернемося до налаштувань Snort на інтерфейсі WAN і налаштуємо роботу системи в режимі IPS, тобто автоматичного блокування IP-адрес вузлів відправників пакетів, які провокують спрацювання сповіщень, рис.3.42.



Block Settings

Block Offenders ☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

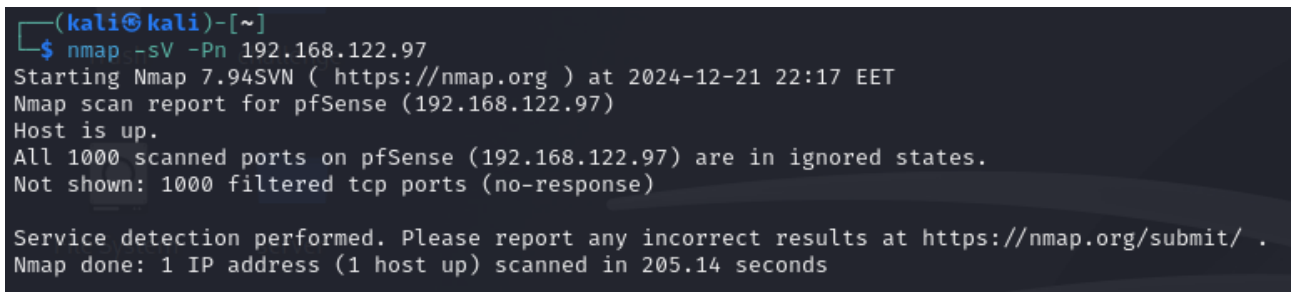
IPS Mode Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block SRC
Select which IP extracted from the packet you wish to block. Default is BOTH.

Рисунок 3.42 – Налаштування Snort в режимі IPS

Повторимо сканування pfSense з використанням утиліти Nmap, рис.3.43.



```
(kali㉿kali)-[~]
$ nmap -sV -Pn 192.168.122.97
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 22:17 EET
Nmap scan report for pfSense (192.168.122.97)
Host is up.
All 1000 scanned ports on pfSense (192.168.122.97) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.14 seconds
```

Рисунок 3.43 – Результат сканування Nmap для виявлення сервісів на pfSense

На pfSense, як і раніше, надійшли сповіщення про виявлення сканування, однак тепер у вкладці Blocked з'явився запис з адресою 192.168.122.232 та описом подій, через які дану IP-адресу було заблоковано для будь-якої взаємодії, рис.3.44. Згідно раніше налаштованих правил Snort даний вузол буде перебувати заблокований протягом години.

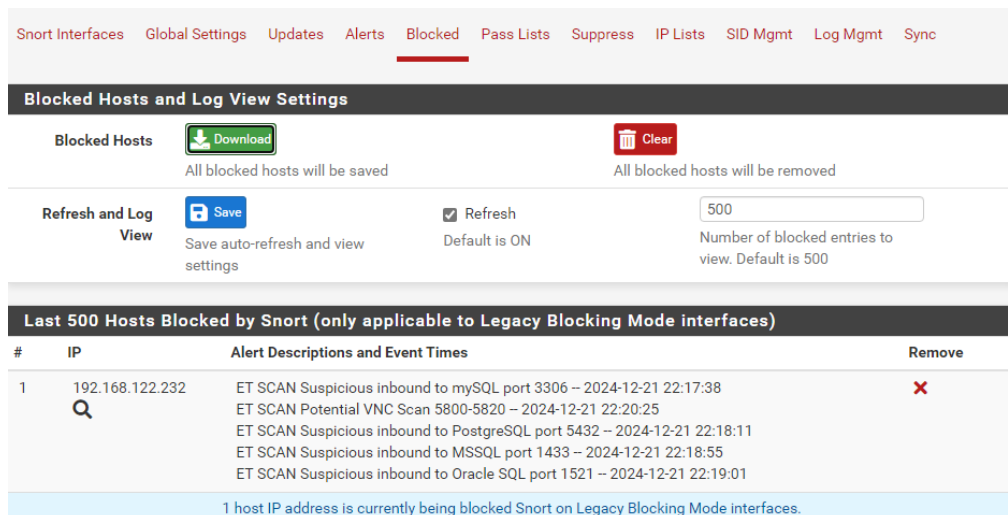


Рисунок 3.44 – Адреса комп’ютера, що проводив сканування була заблокована

3.4. Тестування діагностичних та моніторингових утиліт pfSense

Діагностичні інструменти

Дистрибутив надає великий перелік діагностичних інструментів, розглянемо основні з них.

Packet Capture – це інструмент для захоплення та аналізу мережевого трафіку, який проходить через маршрутизатор. Він дозволяє вибрати інтерфейс (LAN, WAN чи інший), налаштувати фільтри для збору даних за IP-адресами, портами чи іншими параметрами, а також зберігати трафік у форматі PCAP, що корисно для діагностики проблем із підключенням, маршрутизацією, VPN або фаєрволом, а також для виявлення шкідливих дій у мережі, рис.3.45-3.47.

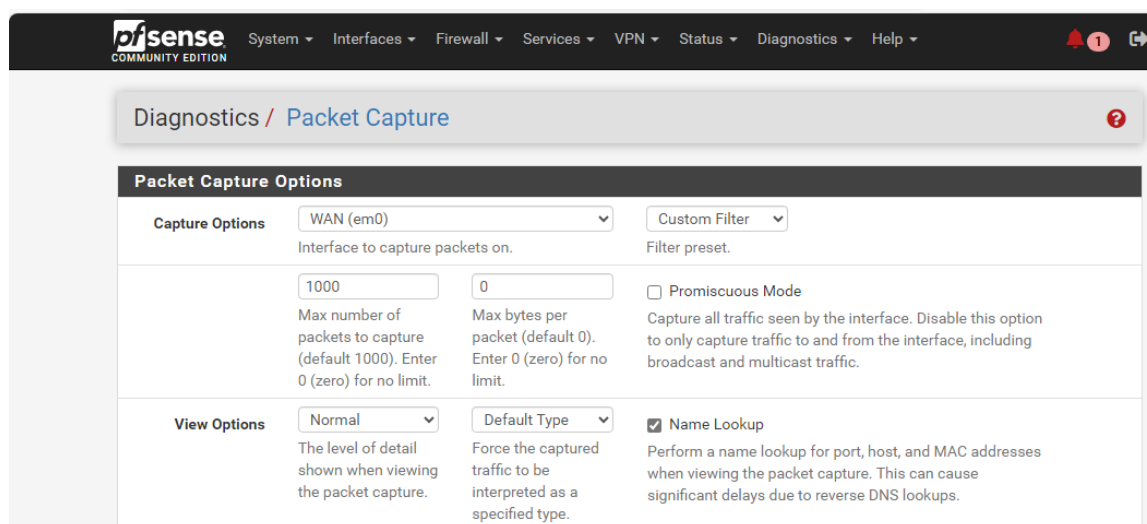


Рисунок 3.45 – Перехоплення трафіку через Packet Capture

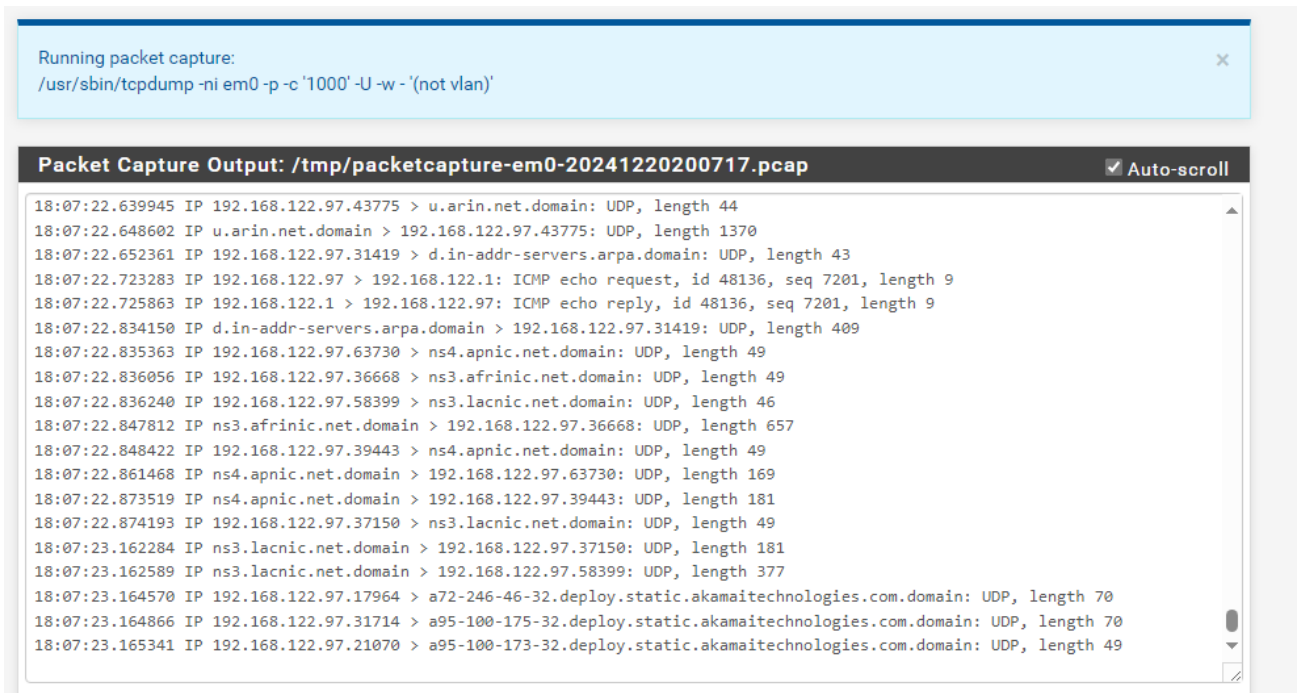


Рисунок 3.46 – Перехоплений трафік через Packet Capture

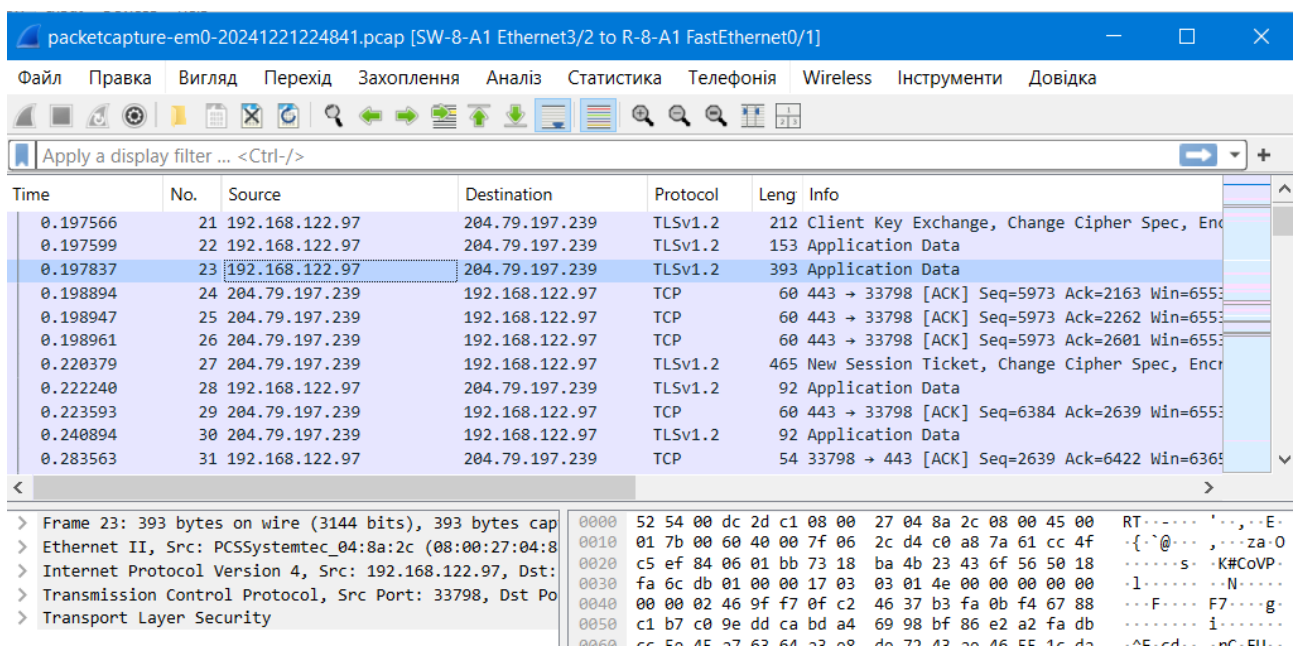


Рисунок 3.47 – Перегляд перехоплених пакетів через Wireshark

pfInfo – це інструмент, який надає зведену інформацію про стан системи, мережеві інтерфейси та налаштування. Він дозволяє переглядати ключові параметри, такі як використання процесора, пам'яті, стан з'єднань, статистику трафіку, активні сесії та інші діагностичні дані.

Diagnostics / pflInfo

Auto Update Page

Refresh
☒ Automatically refresh the output below

Output

```

Status: Enabled for 49710 days 05:34:32      Debug: Urgent

Hostid: 0x21ba0160
Checksum: 0xfbed52fffd7a33432f982e67f6c455c5

Interface Stats for em1
      IPv4      IPv6
Bytes In      2770629      7623
Bytes Out     42216738     2712
Packets In
  Passed      18194      34
  Blocked      7      0
Packets Out
  Passed      0      0
  Blocked     21      0

```

Рисунок 3.48 – Перегляд статистики pflInfo

Nmap в pfSense, виступає як діагностична утиліта для сканування мережі, визначення активних хостів, відкритих портів і доступних сервісів. Цей інструмент допомагає адміністраторам виявляти слабкі місця в конфігурації мережі, перевіряти доступність вузлів, а також діагностувати проблеми з підключенням. Для прикладу виконаємо сканування контролера домену, яке показало ряд відкритих портів, рис.3.49-3.50.

Diagnostics / Nmap

General Options

IP or Hostname

Enter the IP addresses or hostnames that you would like to scan.

Interface

Auto detect (default)

Select the source interface here.

Scan Type

TCP SYN

Select the scan type.

UDP Scan
☐ Combines an UDP scan (-sU) with a TCP scan method

Only possible if a TCP scan method was selected.

-Pn
☐ Treat all hosts as online (No ping).

Allow scanning of networks that do not answer echo requests.

-sV
☒ Attempt to identify service versions

Try to detect services running on discovered ports.

-O
☒ Enable Operating System detection

Try to identify remote host via TCP/IP fingerprinting.

Рисунок 3.49 – Налаштування сканування WinServ-1 через Nmap

```
Scan Results

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Dec 20 20:20:48 2024 -- 1 IP address (1 host up) scanned in 32.28 seconds
# Nmap 7.94 scan initiated Sat Dec 21 23:02:51 2024 as: /usr/local/bin/nmap -sS -sV -O -oN /root/nmap.result --append-output winserv-1
Nmap scan report for winserv-1 (192.168.1.10)
Host is up (0.0023s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-12-21 21:03:13Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: hryhorus.net0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd?
514/tcp   open  shell?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: hryhorus.net0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:85:F0:99 (Oracle VirtualBox virtual NIC)
```

Рисунок 3.50 – Результат сканування WinServ-1

States – це інструмент для моніторингу станів з'єднань у таблиці станів фаєрволу. Він відображає всі активні сесії, включаючи інформацію про джерело, призначення, протокол і обсяг переданих даних. States дозволяє адміністраторам аналізувати поточний мережевий трафік, виявляти аномалії, діагностувати проблеми з підключенням і контролювати виконання правил фаєрволу. Повна ілюстрація наведена на дод.Б.3.

Diagnostics / States / States

States Reset States

State Filter

Interface all

Filter expression Simple filter such as 192.168, v6, icmp or ESTABLISHED

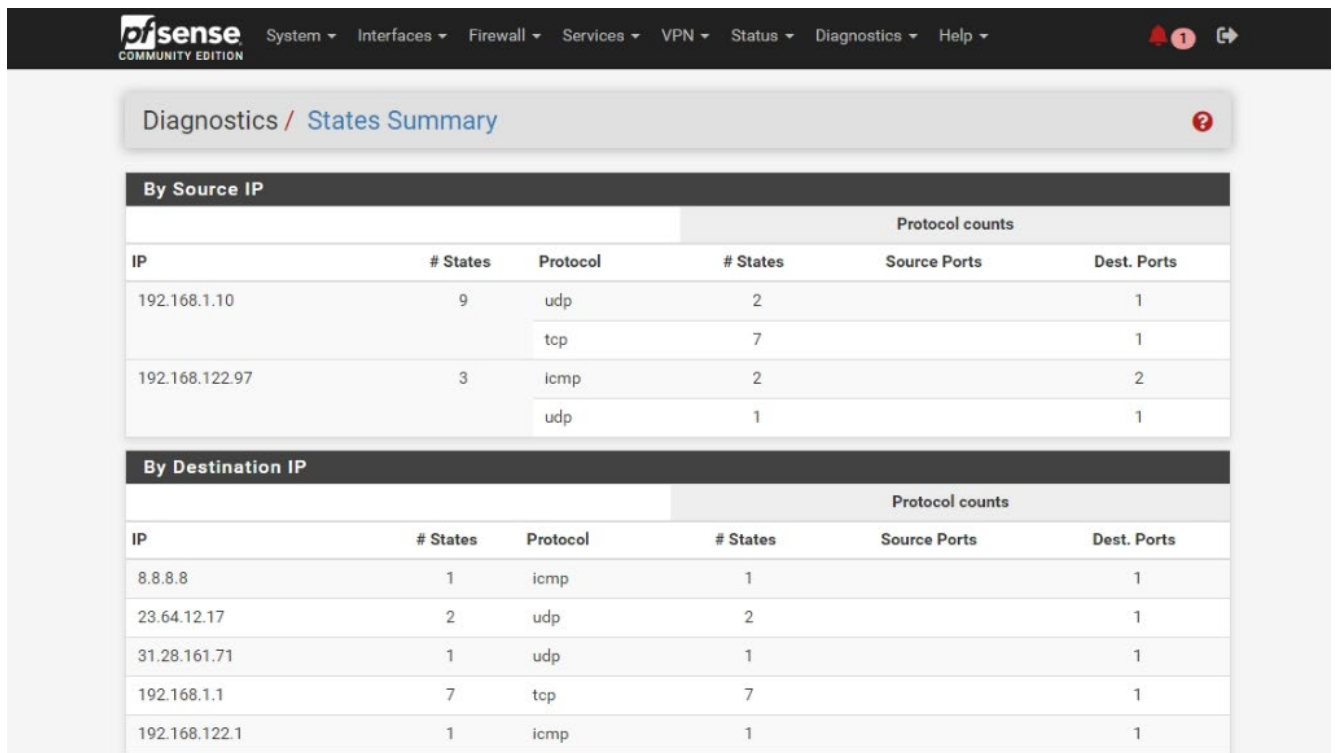
Rule ID Comma separated list of integer rule IDs

Filter

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)		State	Packets	Bytes
WAN	icmp	192.168.122.97:21044 -> 192.168.122.1:21044		0:0	9.086K / 8.541K	257 KiB / 242 KiB
WAN	icmp	192.168.122.97:39417 -> 8.8.8.8:39417		0:0	1.563K / 1.563K	128 KiB / 128 KiB
LAN	udp	192.168.1.10:55576 -> 23.64.12.10:443		MULTIPLE:MULTIPLE	9 / 11	4 KiB / 4 KiB
WAN	udp	192.168.122.97:61152 (192.168.1.10:55576) -> 23.64.12.10:443		MULTIPLE:MULTIPLE	9 / 11	4 KiB / 4 KiB

Рисунок 3.51 – Перегляд станів з'єднань

States Summary – це інструмент, який надає зведену інформацію про використання таблиці станів фаєрволу. Він відображає кількість активних з'єднань для кожного інтерфейсу, протоколу та IP-адреси. States Summary допомагає адміністраторам швидко оцінити завантаженість мережі, виявити джерела аномальної активності або підозрілий трафік, а також забезпечити ефективне управління ресурсами таблиці станів, рис.3.52. Повна ілюстрація наведена на дод.Б.4.



The screenshot shows the pfSense web interface with the 'States Summary' page under 'Diagnostics'. It features two tables: 'By Source IP' and 'By Destination IP'. Each table has columns for IP, # States, Protocol, # States (under Protocol counts), Source Ports, and Dest. Ports.

By Source IP					
IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
192.168.1.10	9	udp	2		1
		tcp	7		1
192.168.122.97	3	icmp	2		2
		udp	1		1

By Destination IP					
IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
8.8.8.8	1	icmp	1		1
23.64.12.17	2	udp	2		1
31.28.161.71	1	udp	1		1
192.168.1.1	7	tcp	7		1
192.168.122.1	1	icmp	1		1

Рисунок 3.52 – Перегляд загальної статистики з'єднань

Моніторинг pfSense

Дистрибутив pfSense також надає широкі можливості, щодо перегляду статистики роботи. Так на головній сторінці можна зручно побачити інформацію про основні параметри системи, використання системних ресурсів, IP-адрес. До того ж, дана панель може бути зручно налаштована користувачем під свої потреби, що і було виконано для зручного виводу сповіщень Snort, рис.3.53. Повна ілюстрація представлена на дод.Б.5.

Current date/time

Sat Dec 21 22:35:07 EET 2024

DNS server(s)

- 127.0.0.1
- 192.168.122.1
- 192.168.1.10

Last config change

Sat Dec 21 22:17:02 EET 2024

State table size

0% (31/147000) [Show states](#)

MBUF Usage

0% (4292/1000000)

Load average

0.67, 0.42, 0.36

CPU usage

4%

Memory usage

76% of 1474 MiB

SWAP usage

0% of 1024 MiB

Disks

Mount	Used	Size	Usage
> /	866M	7.4G	11% of 7.4G (zfs)

(NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.122.97
LAN	↑	1000baseT <full-duplex>	192.168.1.1

Snort Alerts

Interface/Time	Src/Dst Address	Description
WAN Dec 21 22:34:...	192.168.122.232:44668 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:44668 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:44660 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:48802 192.168.122.97:5802	ET SCAN Potential VNC Scan 5800-5820
WAN Dec 21 22:34:...	192.168.122.232:37580 192.168.122.97:1433	ET SCAN Suspicious inbound to MSSQL port...

Рисунок 3.53 – Головне меню pfSense

Вкладка Interfaces дозволяє відстежувати статус і статистику роботи мережевих інтерфейсів маршрутизатора. Тут відображаються ключові параметри, такі як завантаження по вхідному та вихідному трафіку, кількість переданих і прийнятих пакетів, помилки та відкинуті пакети, рис.3.54.

Status / Interfaces

WAN Interface (wan, em0)

Status

up ↑

DHCP

up [Release WAN](#) ☐ Relinquish Lease

MAC Address

08:00:27:04:8a:2c - Oracle VirtualBox virtual NIC

IPv4 Address

192.168.122.97

Subnet mask IPv4

255.255.255.0

Gateway IPv4

192.168.122.1

IPv6 Link Local

fe80::a00:27ff:fe04:8a2c%em0

DNS servers

192.168.122.1

MTU

1500

Media

1000baseT <full-duplex>

In/out packets

56902/38713 (32.92 MiB/2.86 MiB)

In/out packets (pass)

56902/38713 (32.92 MiB/2.86 MiB)

In/out packets (block)

8683/0 (523 KiB/0 B)

In/out errors

0/0

Collisions

0

Interrupts

80004 (8/s)

LAN Interface (lan, em1)

Status

up ↑

MAC Address

08:00:27:42:9a:c5 - Oracle VirtualBox virtual NIC

IPv4 Address

192.168.1.1

Subnet mask IPv4

255.255.255.0

IPv6 Link Local

fe80::a00:27ff:fe42:9ac5%em1

MTU

1500

Media

1000baseT <full-duplex>

In/out packets

27703/61533 (4.67 MiB/45.43 MiB)

In/out packets (pass)

27703/61533 (4.67 MiB/45.43 MiB)

In/out packets (block)

71/50 (7 KiB/3 KiB)

In/out errors

0/0

Collisions

0

Interrupts

55097 (5/s)

Рисунок 3.54 – Перегляд вкладки Interfaces

Monitoring – це панель для відстеження та моніторингу стану системи і мережевої активності в реальному часі. Вона надає різноманітні інструменти для перегляду статистики роботи системи, трафіку, мережевих інтерфейсів та інших важливих параметрів. Однією з основних функцій є можливість переглядати дані про використання мережевих інтерфейсів, стан підключень, використання системних ресурсів, тощо, рис.3.55-3.57.

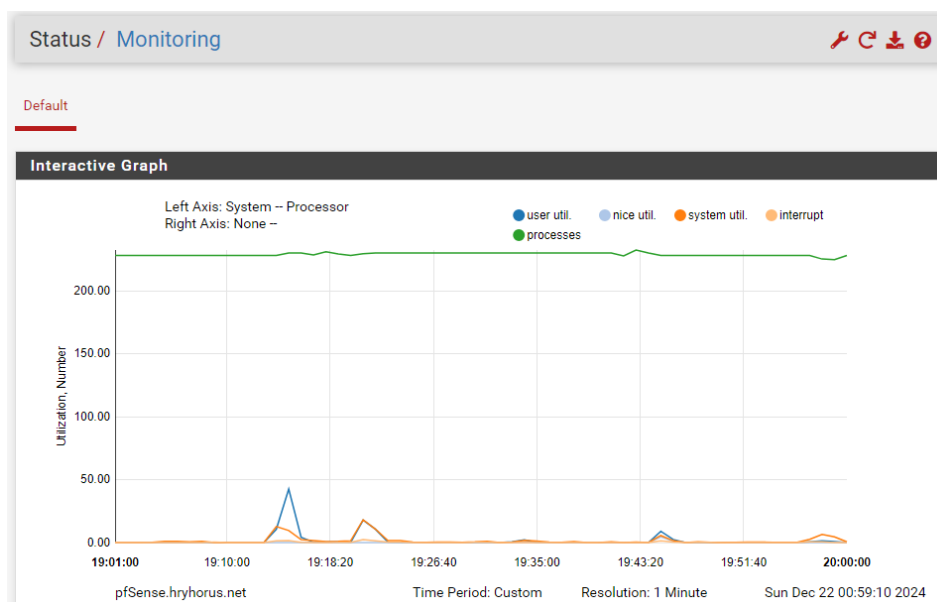


Рисунок 3.55 – Кількість активних процесів та використання процесорного часу

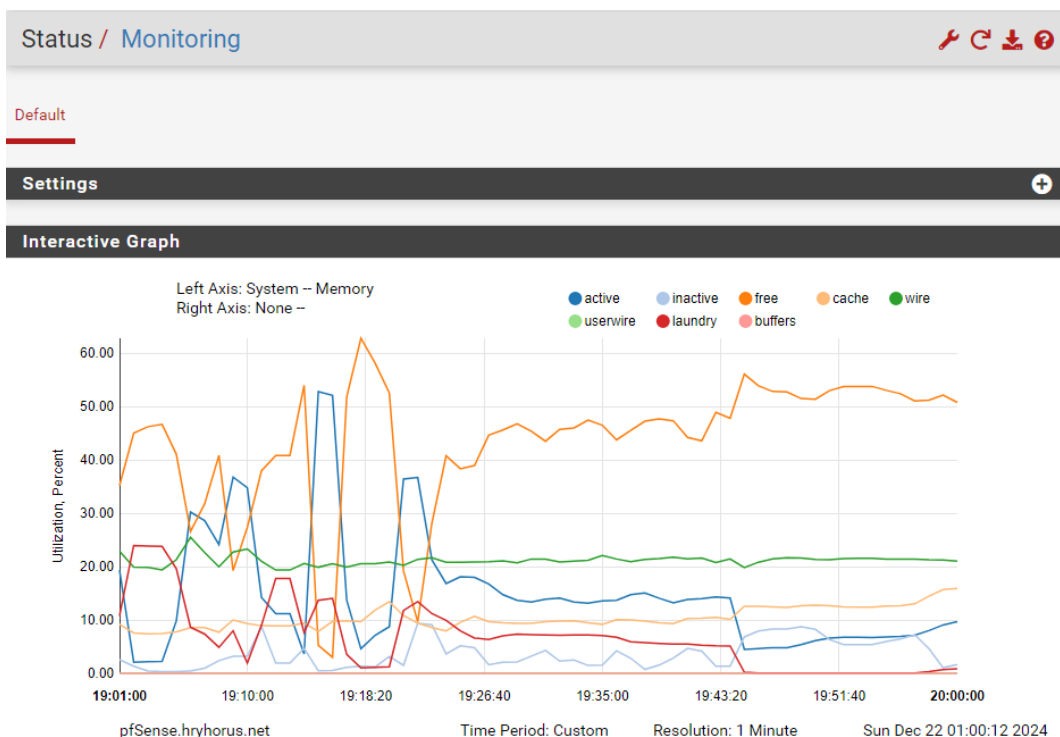


Рисунок 3.56 – Використання ОЗП

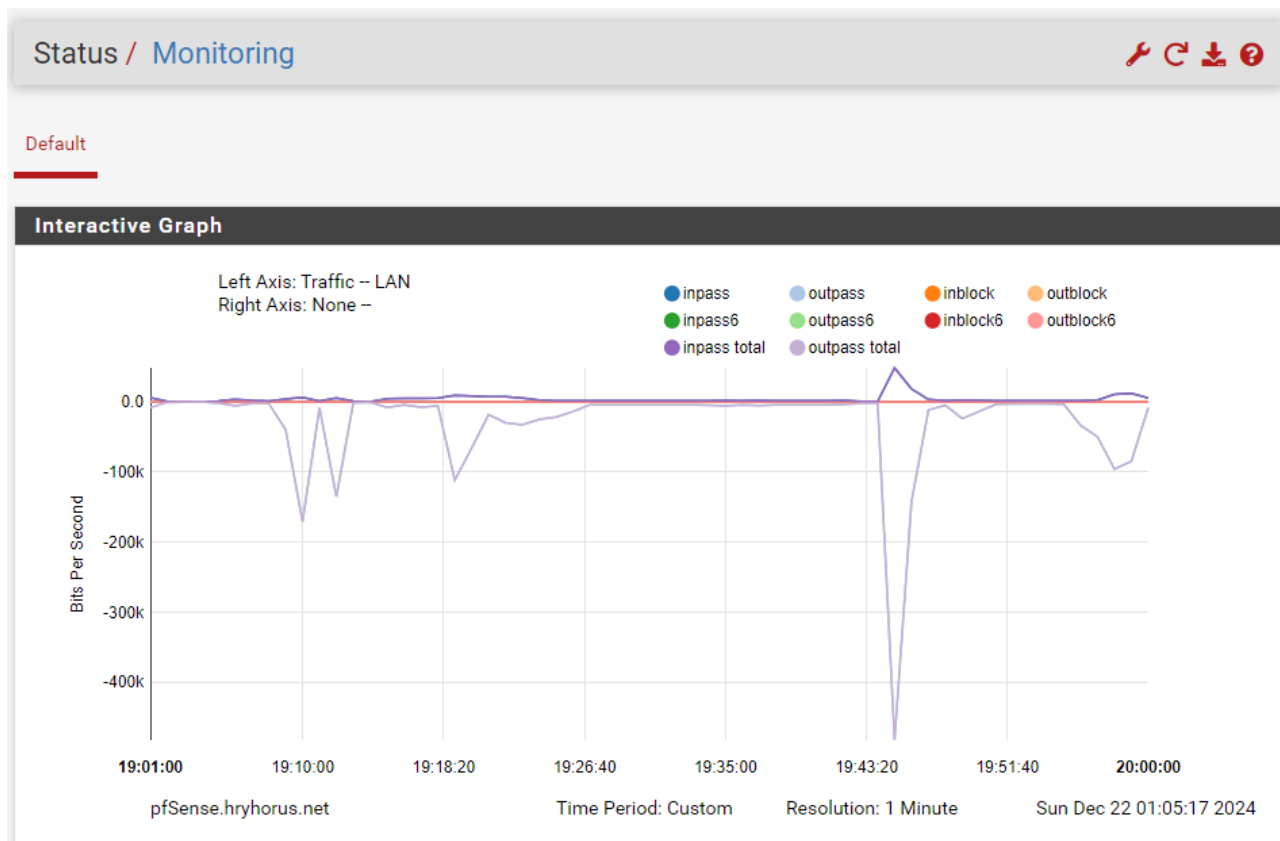


Рисунок 3.57 – Пропускна здатність за секунду

Висновок до третього розділу

В ході роботи було реалізовано проєкт мережі в емуляторі GNS3 із використанням VirtualBox для віртуалізації pfSense, сервера та робочих станцій. Виконано базове налаштування pfSense, комутаторів з аутентифікацією та SSH. Виконано розгортання серверу Windows Server 2019 в ролі контролера домену з Active Directory та налаштованими сервісами DHCP і DNS. Робочі станції приєднано до домену. Для централізованого логування налаштовано Syslog із використанням Visual Syslog Server. Проведено тестування наявності зв'язку між пристроями мережі, авторизації користувачів на робочих станціях, роботи SSH та Syslog.

Було виконано базове налаштування pfSense з використанням веб-інтерфейсу. Додано ім'я домену, адресу NTP-сервера, часовий пояс, а також змінено пароль адміністратора. Для налаштування DNS Resolver вказано домен та відповідну адресу DNS-сервера, що дозволяє звертатися до пристроїв у локальній мережі за їх іменами.

Виконано налаштування та перевірку додаткових функцій безпеки pfSense. Спочатку налаштовано відправку сповіщень до Syslog сервера для централізованого моніторингу подій. Далі перевірено правила фаєрвола, де для інтерфейсу WAN встановлено блокування будь-якого вхідного трафіку. Для посилення безпеки встановлено пакет системи виявлення та запобігання вторгненням Snort та налаштовано його роботу з обраними списками правил. Після цього протестовано роботу Snort з використанням інструменту Nmap для виявлення мережових вразливостей. Сповіщення про потенційні загрози були зафіксовані в інтерфейсі pfSense та на Syslog сервері. Для подальшого посилення захисту на Snort було налаштовано режим IPS, що автоматично блокуватиме IP-адреси порушників після спрацювання сповіщень.

Виконано тестування діагностичних та моніторингових утиліт pfSense. Розглянуто основні інструменти, такі як Packet Capture для перехоплення мережевого трафіку, pfInfo для перегляду стану системи, а також Nmap для сканування мережі та виявлення активних хостів. Також було перевірено використання інструментів States та States Summary для моніторингу активних з'єднань і контролю стану таблиці фаєрволу. Додатково, вивчено можливості моніторингу стану системи через головну панель pfSense, а також вкладки для відстежування статистики мережових інтерфейсів та використання системних ресурсів.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було досліджено методи та технології захисту мережевої інфраструктури на базі рішення pfSense з інтеграцією MS Active Directory.

У першому розділі проведено детальний аналіз основних компонентів та функціональних можливостей системи Active Directory, а також проаналізовано різновиди міжмережевих екранів і їх класифікацію. Описано ключові аспекти роботи фаєрволів, зокрема контроль доступу, захист від атак, фільтрацію контенту та підтримку VPN, а також функції фаєрволів нового покоління. Проведено порівняння безкоштовних програмних маршрутизаторів і міжмережевих екранів з відкритим кодом, зокрема pfSense, OPNsense, IPFire та VyOS, і визначено, що pfSense є найбільш оптимальним рішенням для корпоративних мереж завдяки своїй гнучкості, функціональності та підтримці. Зроблено висновок, що pfSense є ефективним інструментом для забезпечення безпеки мережі, завдяки інтеграції з додатковими пакетами для виявлення загроз, фільтрації трафіку та контролю контенту.

У другому розділі було розроблено топологію та адресацію мережі організації. Створена топологія включає маршрутизатор на базі pfSense, комутатори для рівня доступу та розподілу, сервер з інтеграцією Microsoft Active Directory для централізованого управління та кінцеві робочі станції. Виконана адресація мережі з використанням DHCP для автоматичного розподілу IP-адрес для кінцевих пристроїв. Виконано вибір методів та механізмів захисту для подальшої їх реалізації в проєкті мережі. Окрім цього, було обрано необхідне обладнання для реалізації мережі.

У третьому розділі було реалізовано проєкт мережі в емуляторі GNS3 із використанням VirtualBox для віртуалізації pfSense, сервера та робочих станцій. Виконано базове налаштування pfSense, комутаторів, серверу Windows Server 2019. Робочі станції були приєднані до домену, а для централізованого логування налаштовано Syslog. Протестовано зв'язок між пристроями, авторизацію користувачів, роботу SSH і Syslog. Здійснено налаштування додаткових функцій

безпеки pfSense, включаючи сповіщення до Syslog, налаштування фаєрволу, інтеграцію Snort для виявлення вторгнень та тестування з інструментом Nmap. Окрім того, проведено налаштування режиму IPS для автоматичного блокування порушників та тестування діагностичних та моніторингових утиліт pfSense.

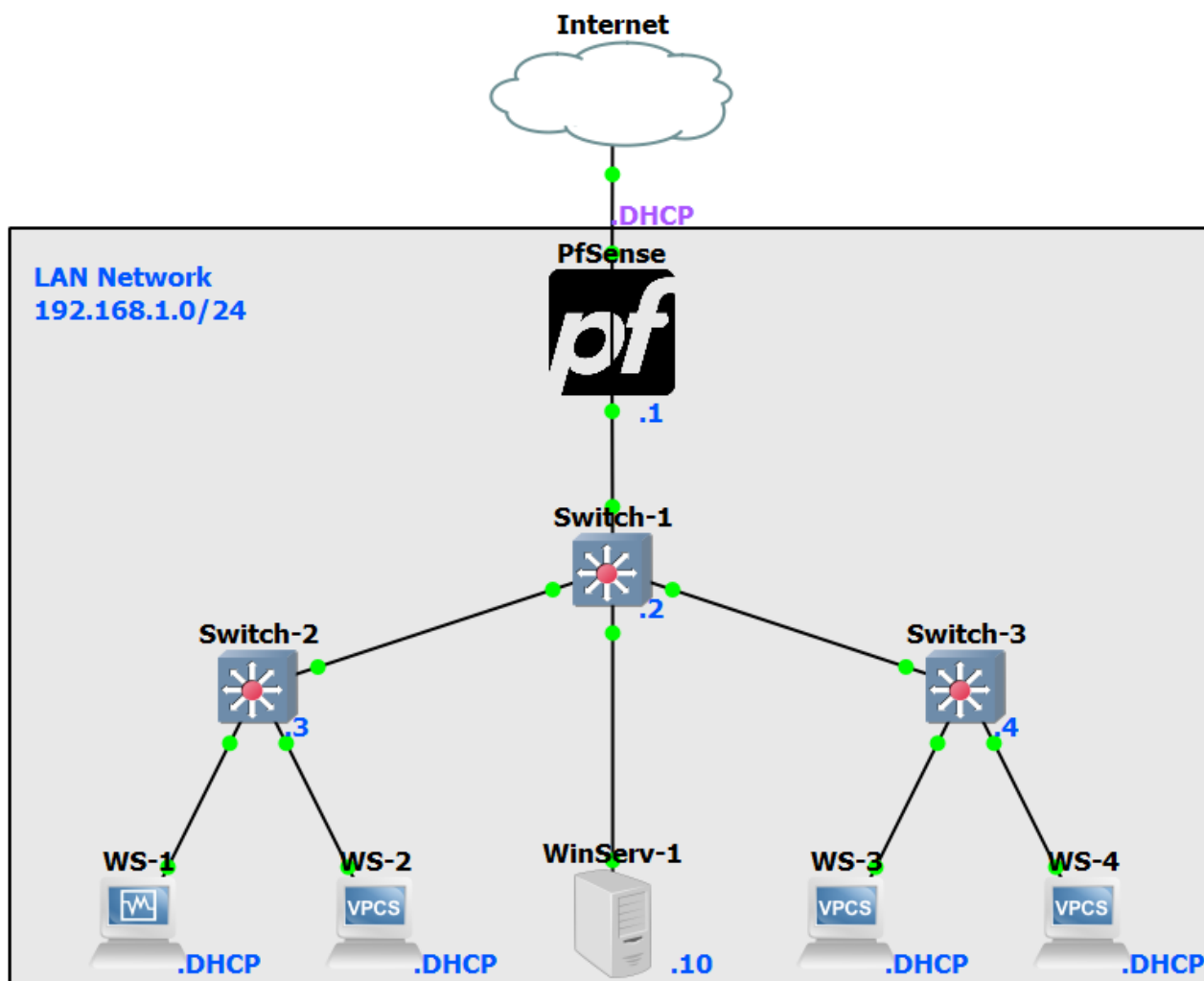
Результатом виконання роботи є створення ефективної та безпечної мережевої інфраструктури на базі рішень pfSense та MS Active Directory. Проведене дослідження дозволило детально вивчити основні компоненти та функціональні можливості Active Directory, а також проаналізувати різновиди міжмережевих екранів і фаєрволів. Окрема увага приділено функціональним можливостям pfSense. Розроблена топологія та адресація мережі забезпечили належний рівень безпеки та гнучкості інфраструктури. Реалізація проєкту в емуляторі GNS3 підтвердила коректність та ефективність використаних рішень. Всі поставлені завдання були виконані в повному обсязі. Подальші напрямки для дослідження та вдосконалення можуть включати інтеграцію додаткових механізмів захисту, таких як системи виявлення аномалій на основі машинного навчання або інтеграції зі системами SIEM.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Active Directory 101: A Step-by-Step Tutorial for Beginners [Електронний ресурс]. Режим доступу до ресурсу: <https://www.serveracademy.com/blog/active-directory-101-a-step-by-step-tutorial-for-beginners/>
2. Microsoft NTLM [Електронний ресурс]. Режим доступу до ресурсу: <https://learn.microsoft.com/uk-ua/windows/win32/secauthn/microsoft-ntlm>
3. What is Security Assertion Markup Language (SAML)? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-security-assertion-markup-language-saml>
4. What is a domain controller? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.techtarget.com/searchwindowsserver/definition/domain-controller>
5. Григорусь А. М., Фальковський І.Г. Аналіз типів міжмережевих екранів за їх призначенням і розміщенням в мережі // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
6. Types of Firewalls Defined and Explained [Електронний ресурс]. Режим доступу до ресурсу: <https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls>
7. What Is A Stateful Firewall? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.fortinet.com/resources/cyberglossary/stateful-firewall>
8. Що таке VPN? [Електронний ресурс]. Режим доступу до ресурсу: <https://nordvpn.com/uk/what-is-a-vpn/>
9. NGFW: Що це таке [Електронний ресурс]. Режим доступу до ресурсу: <https://softlist.ua/cases/ngfw>
10. Що таке IPS/IDS і де застосовується? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya>

11. Офіційна сайт OPNSense [Електронний ресурс]. Режим доступу до ресурсу: <https://opnsense.org/>
12. Офіційний сайт pfSense[Електронний ресурс]. Режим доступу до ресурсу: <https://www.pfsense.org/>
13. IPFire [Електронний ресурс]. Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/IPFire>
14. VyOS [Електронний ресурс]. Режим доступу до ресурсу: <https://docs.vyos.io/uk/latest/introducing/about.html>
15. Григорусь А. М., Фальковський І.Г. Функціональні можливості та переваги pfSense // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
16. PfSense features and functionality [Електронний ресурс]. Режим доступу до ресурсу: <https://www.miniserver.store/operating-system-pfsense>
17. Що таке NAT? [Електронний ресурс]. Режим доступу до ресурсу: <https://hyperhost.ua/info/uk/shcho-take-nat-dlya-chogo-vikoristovuyu-daniy-standart>
18. Що таке VLAN? [Електронний ресурс]. Режим доступу до ресурсу: <https://fiberroad.com/uk/resources/glossary/vlan-explained-what-is-vlan-how-does-it-work/>
19. What is three-tier architecture? [Електронний ресурс]. Режим доступу до ресурсу: <https://www.ibm.com/topics/three-tier-architecture>
20. Netgate SG-1100 Review [Електронний ресурс]. Режим доступу до ресурсу: <https://www.trenchesofit.com/2020/02/01/netgate-sg-1100-review/>
21. Visual Syslog Server for Windows [Електронний ресурс]. Режим доступу до ресурсу: <https://maxbelkov.github.io/visualsyslog/>
22. Download PuTTY - a free SSH and telnet client for Windows [Електронний ресурс]. Режим доступу до ресурсу: <https://www.putty.org/>

ДОДАТКИ



Додаток Б.1 – Включені категорії правил Snort

Select the rulesets (Categories) Snort will load at startup

Category is auto-enabled by SID Mgmt conf files

Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Enable

Ruleset: Snort GPLv2 Community Rules

Enable

Ruleset: ET Open Rules

Enable

Ruleset: Snort Text Rules

Enable

Ruleset: Snort SO Rules

Snort OPENAPPID rules are not enabled.

☒	emerging-activex.rules	☐	snort_app-detect.rules	☐	snort_browser-chrome.so.rules
☒	emerging-attack_response.rules	☐	snort_blacklist.rules	☐	snort_browser-ie.so.rules
☒	emerging-botcc.portgrouped.rules	☐	snort_browser-chrome.rules	☐	snort_browser-other.so.rules
☒	emerging-botcc.rules	☐	snort_browser-firefox.rules	☐	snort_browser-webkit.so.rules
☒	emerging-chat.rules	☐	snort_browser-ie.rules	☐	snort_exploit-kit.so.rules
☒	emerging-ciarmy.rules	☐	snort_browser-other.rules	☐	snort_file-executable.so.rules
☒	emerging-compromised.rules	☐	snort_browser-plugins.rules	☐	snort_file-flash.so.rules
☒	emerging-current_events.rules	☐	snort_browser-webkit.rules	☐	snort_file-image.so.rules
☒	emerging-deleted.rules	☐	snort_content-replace.rules	☐	snort_file-java.so.rules
☒	emerging-dns.rules	☐	snort_deleted.rules	☐	snort_file-multimedia.so.rules
☒	emerging-dos.rules	☐	snort_exploit-kit.rules	☐	snort_file-office.so.rules
☒	emerging-drop.rules	☐	snort_file-executable.rules	☐	snort_file-other.so.rules
☒	emerging-dshield.rules	☐	snort_file-flash.rules	☐	snort_file-pdf.so.rules
☒	emerging-exploit.rules	☐	snort_file-identify.rules	☐	snort_indicator-shellcode.so.rules
☒	emerging-ftp.rules	☐	snort_file-image.rules	☐	snort_malware-cnc.so.rules
☒	emerging-games.rules	☐	snort_file-java.rules	☐	snort_malware-other.so.rules
☒	emerging-icmp.rules	☐	snort_file-multimedia.rules	☐	snort_netbios.so.rules
☒	emerging-icmp_info.rules	☐	snort_file-office.rules	☐	snort_os-linux.so.rules
☒	emerging-imap.rules	☐	snort_file-other.rules	☐	snort_os-other.so.rules
☒	emerging-inappropriate.rules	☐	snort_file-pdf.rules	☐	snort_os-windows.so.rules
☒	emerging-info.rules	☐	snort_indicator-compromise.rules	☐	snort_policy-other.so.rules
☒	emerging-malware.rules	☐	snort_indicator-obfuscation.rules	☐	snort_policy-social.so.rules
☒	emerging-misc.rules	☐	snort_indicator-scan.rules	☐	snort_protocol-dns.so.rules
☒	emerging-mobile_malware.rules	☐	snort_indicator-shellcode.rules	☐	snort_protocol-nntp.so.rules
☒	emerging-netbios.rules	☐	snort_local.rules	☐	snort_protocol-other.so.rules
☒	emerging-p2p.rules	☐	snort_malware-backdoor.rules	☐	snort_protocol-scada.so.rules
☒	emerging-policy.rules	☐	snort_malware-cnc.rules	☐	snort_protocol-snmp.so.rules
☒	emerging-pop3.rules	☐	snort_malware-other.rules	☐	snort_protocol-ftp.so.rules
☒	emerging-retired.rules	☐	snort_malware-tools.rules	☐	snort_protocol-voip.so.rules
☒	emerging-rpc.rules	☐	snort_netbios.rules	☐	snort_pua-p2p.so.rules
☒	emerging-scada.rules	☐	snort_os-linux.rules	☐	snort_server-iaa.so.rules
☒	emerging-scan.rules	☐	snort_os-mobile.rules	☐	snort_server-mail.so.rules
☒	emerging-shellcode.rules	☐	snort_os-other.rules	☐	snort_server-mysql.so.rules
☒	emerging-smtp.rules	☐	snort_os-solaris.rules	☐	snort_server-oracle.so.rules
☒	emerging-snmp.rules	☐	snort_os-windows.rules	☐	snort_server-other.so.rules
☒	emerging-sql.rules	☐	snort_policy-multimedia.rules	☐	snort_server-webapp.so.rules
☒	emerging-telnet.rules	☐	snort_policy-other.rules		
☒	emerging-ftp.rules	☐	snort_policy-social.rules		
☒	emerging-tor.rules	☐	snort_policy-spam.rules		
☒	emerging-trojan.rules	☐	snort_protocol-dns.rules		
☒	emerging-user_agents.rules	☐	snort_protocol-finger.rules		
☒	emerging-voip.rules	☐	snort_protocol-ftp.rules		
☒	emerging-web_client.rules	☐	snort_protocol-icmp.rules		
☒	emerging-web_server.rules	☐	snort_protocol-imap.rules		
☒	emerging-web_specific_apps.rules	☐	snort_protocol-nntp.rules		
☒	emerging-worm.rules	☐	snort_protocol-other.rules		
☐		☐	snort_protocol-pop.rules		
☐		☐	snort_protocol-rpc.rules		
☐		☐	snort_protocol-scada.rules		
☐		☐	snort_protocol-services.rules		
☐		☐	snort_protocol-snmp.rules		
☐		☐	snort_protocol-telnet.rules		
☐		☐	snort_protocol-ftp.rules		
☐		☐	snort_protocol-voip.rules		
☐		☐	snort_pua-adware.rules		
☐		☐	snort_pua-other.rules		
☐		☐	snort_pua-p2p.rules		
☐		☐	snort_pua-toolbars.rules		
☐		☐	snort_server-apache.rules		
☐		☐	snort_server-iaa.rules		
☐		☐	snort_server-mail.rules		
☐		☐	snort_server-mysql.rules		
☐		☐	snort_server-mysql.rules		
☐		☐	snort_server-oracle.rules		
☐		☐	snort_server-other.rules		
☐		☐	snort_server-samba.rules		
☐		☐	snort_server-webapp.rules		
☐		☐	snort_sql.rules		
☐		☐	snort_x11.rules		

Додаток Б.2 – Сповіщення Snort про сканування мережі

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: WAN (em0) ☐ Auto-refresh view 100

Alert Log Actions

Alert Log View Filter

10 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-12-21 19:24:30		2	TCP	Attempted Information Leak	192.168.122.232	36746	192.168.122.97	5810	1:2002910	ET SCAN Potential VNC Scan 5800-5820
2024-12-21 19:24:27		2	TCP	Potentially Bad Traffic	192.168.122.232	52718	192.168.122.97	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2024-12-21 19:24:26		2	TCP	Potentially Bad Traffic	192.168.122.232	52708	192.168.122.97	5432	1:2010939	ET SCAN Suspicious inbound to PostgreSQL port 5432
2024-12-21 19:23:41		2	TCP	Potentially Bad Traffic	192.168.122.232	48510	192.168.122.97	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2024-12-21 19:23:40		2	TCP	Potentially Bad Traffic	192.168.122.232	48504	192.168.122.97	1521	1:2010936	ET SCAN Suspicious inbound to Oracle SQL port 1521
2024-12-21 19:22:23		2	TCP	Potentially Bad Traffic	192.168.122.232	37190	192.168.122.97	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2024-12-21 19:22:22		2	TCP	Potentially Bad Traffic	192.168.122.232	37186	192.168.122.97	1433	1:2010935	ET SCAN Suspicious inbound to MSSQL port 1433
2024-12-21 19:22:14		2	TCP	Potentially Bad Traffic	192.168.122.232	50650	192.168.122.97	3306	1:2010937	ET SCAN Suspicious inbound to MySQL port 3306
2024-12-21 19:22:13		2	TCP	Potentially Bad Traffic	192.168.122.232	50650	192.168.122.97	3306	1:2010937	ET SCAN Suspicious inbound to MySQL port 3306
2024-12-21 19:22:12		2	TCP	Potentially Bad Traffic	192.168.122.232	50646	192.168.122.97	3306	1:2010937	ET SCAN Suspicious inbound to MySQL port 3306

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾
 1


Diagnostics / States / States
?

States Reset States

State Filter
-

Interface

Filter expression

Rule ID



States					
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	192.168.122.97:21044 -> 192.168.122.1:21044	0:0	9.086K / 8.541K	257 KiB / 242 KiB
WAN	icmp	192.168.122.97:39417 -> 8.8.8.8:39417	0:0	1.563K / 1.563K	128 KiB / 128 KiB
LAN	udp	192.168.1.10:55576 -> 23.64.12.10:443	MULTIPLE:MULTIPLE	9 / 11	4 KiB / 4 KiB
WAN	udp	192.168.122.97:61152 (192.168.1.10:55576) -> 23.64.12.10:443	MULTIPLE:MULTIPLE	9 / 11	4 KiB / 4 KiB
LAN	tcp	192.168.1.10:64133 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	7 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64136 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	7 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64137 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	18 / 24	3 KiB / 14 KiB
LAN	tcp	192.168.1.10:64139 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	7 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64140 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	8 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64143 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	8 / 8	2 KiB / 2 KiB
LAN	tcp	192.168.1.10:64144 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	8 / 8	2 KiB / 2 KiB
LAN	tcp	192.168.1.10:64145 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	25 / 35	4 KiB / 19 KiB
LAN	udp	192.168.1.1:514 -> 192.168.1.10:514	SINGLE:NO_TRAFFIC	1 / 0	184 B / 0 B
LAN	tcp	192.168.1.10:64149 -> 48.209.144.71:443	FIN_WAIT_2:FIN_WAIT_2	18 / 21	6 KiB / 12 KiB
WAN	tcp	192.168.122.97:45783 (192.168.1.10:64149) -> 48.209.144.71:443	FIN_WAIT_2:FIN_WAIT_2	18 / 21	6 KiB / 12 KiB
LAN	tcp	192.168.1.10:64154 -> 204.79.197.239:443	FIN_WAIT_2:FIN_WAIT_2	13 / 17	3 KiB / 7 KiB
WAN	tcp	192.168.122.97:19046 (192.168.1.10:64154) -> 204.79.197.239:443	FIN_WAIT_2:FIN_WAIT_2	13 / 17	3 KiB / 7 KiB
LAN	tcp	192.168.1.10:64155 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	7 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64157 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	7 / 7	2 KiB / 546 B
LAN	tcp	192.168.1.10:64160 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	8 / 8	2 KiB / 2 KiB
LAN	tcp	192.168.1.10:64161 -> 192.168.1.1:443	FIN_WAIT_2:FIN_WAIT_2	8 / 8	2 KiB / 2 KiB


System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

 1


Diagnostics / States Summary 

By Source IP

IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
192.168.1.10	9	udp	2		1
		tcp	7		1
192.168.122.97	3	icmp	2		2
		udp	1		1

By Destination IP

IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
8.8.8.8	1	icmp	1		1
23.64.12.17	2	udp	2		1
31.28.161.71	1	udp	1		1
192.168.1.1	7	tcp	7		1
192.168.122.1	1	icmp	1		1

Total per IP

IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
8.8.8.8	1	icmp	1		1
23.64.12.17	2	udp	2		1
31.28.161.71	1	udp	1		1
192.168.1.1	7	tcp	7		1
192.168.1.10	9	udp	2		1
		tcp	7		1
192.168.122.1	1	icmp	1		1
192.168.122.97	3	icmp	2		2
		udp	1		1

By IP Pair

IP	# States	Protocol	Protocol counts		
			# States	Source Ports	Dest. Ports
192.168.122.97 -> 192.168.122.1	1	icmp	1		1
192.168.122.97 -> 8.8.8.8	1	icmp	1		1
192.168.1.10 -> 23.64.12.17	2	udp	2		1
192.168.1.10 -> 192.168.1.1	7	tcp	7		1
192.168.122.97 -> 31.28.161.71	1	udp	1		1


pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license.](#)



System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾
 1


Status / Dashboard
+ ?

System Information

Name	pfSense.hryhorus.net
User	admin@192.168.1.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 257e9609bf4e21ba0160
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 22:10:00 EET 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Sat Dec 21 21:50:34 EET 2024
CPU Type	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 48 Minutes 44 Seconds
Current date/time	Sat Dec 21 22:38:10 EET 2024
DNS server(s)	127.0.0.1 192.168.122.1 192.168.1.10
Last config change	Sat Dec 21 22:17:02 EET 2024
State table size	0% (27/147000) Show states
MBUF Usage	0% (4292/1000000)
Load average	0.45, 0.40, 0.35
CPU usage	3%
Memory usage	76% of 1474 MiB
SWAP usage	0% of 1024 MiB

Disks

Mount	Used	Size	Usage
/	866M	7.4G	11% of 7.4G (zfs)

Netgate Services And Support

Contract type
Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

Interfaces

WAN	1000baseT <full-duplex>	192.168.122.97
LAN	1000baseT <full-duplex>	192.168.1.1

Snort Alerts

Interface/Time	Src/Dst Address	Description
WAN Dec 21 22:34:...	192.168.122.232:44668 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:44668 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:44660 192.168.122.97:5432	ET SCAN Suspicious inbound to PostgreSQL...
WAN Dec 21 22:34:...	192.168.122.232:48802 192.168.122.97:5802	ET SCAN Potential VNC Scan 5800-5820
WAN Dec 21 22:34:...	192.168.122.232:37580 192.168.122.97:1433	ET SCAN Suspicious inbound to MSSQL port...

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

Додаток В – Лістинг конфігураційних файлів пристроїв мережі

SW-Distr-1:

```
!  
! Last configuration change at 16:09:38 UTC Fri  
Dec 20 2024  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime  
no service password-encryption  
service compress-config  
!  
hostname Switch-1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6  
msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 5  
$1$bDpr$yvzvN9oXJmKIuVOq2uvHV1  
!  
username Anton privilege 15 secret 5  
$1$nBb/$Jd6ByO94tgWw/ll4Vl7AH0  
no aaa new-model  
!  
!  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip domain-name hryhorus.net  
ip name-server 192.168.1.10  
ip name-server 192.168.1.1  
ip cef  
no ipv6 cef  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
!  
!  
!  
interface Ethernet0/0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2
```

```
!  
interface Ethernet0/3  
!  
interface Ethernet1/0  
!  
...  
interface Ethernet3/1  
!  
interface Ethernet3/2  
!  
interface Ethernet3/3  
!  
interface Vlan1  
ip address 192.168.1.2 255.255.255.0  
!  
ip default-gateway 192.168.1.1  
ip forward-protocol nd  
!  
ip tcp synwait-time 5  
ip http server  
!  
ip ssh time-out 30  
ip ssh version 2  
ip ssh server algorithm encryption aes128-ctr  
aes192-ctr aes256-ctr  
ip ssh client algorithm encryption aes128-ctr  
aes192-ctr aes256-ctr  
!  
!  
logging trap notifications  
logging host 192.168.1.10  
!  
!  
!  
control-plane  
!  
!  
line con 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
login local  
line aux 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
line vty 0 4  
login local  
transport input ssh  
!  
!  
!  
end
```

SW-Access-1:

! Last configuration change at 16:45:54 UTC Fri
Dec 20 2024

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime  
no service password-encryption  
service compress-config  
!  
hostname Switch-2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops 6  
msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
enable secret 5  
$1$jDyR$BTi5NESUWBT4ql27jSEJ41  
!  
username Anton privilege 15 secret 5  
$1$ZEx6$Yr0cf7nPmOhHT6fU8UKm70  
no aaa new-model  
!  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip domain-name hryhorus.net  
ip name-server 192.168.1.10  
ip name-server 192.168.1.1  
ip cef  
no ipv6 cef  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
interface Ethernet0/0  
!  
interface Ethernet0/1  
!  
interface Ethernet0/2  
!  
interface Ethernet0/3  
!  
interface Ethernet1/0  
!  
interface Ethernet1/1  
!
```

```
interface Ethernet1/2  
!  
interface Ethernet1/3  
!  
interface Ethernet2/0  
!  
...  
interface Ethernet3/0  
!  
interface Ethernet3/1  
!  
interface Ethernet3/2  
!  
interface Ethernet3/3  
!  
interface Vlan1  
ip address 192.168.1.3 255.255.255.0  
!  
ip default-gateway 192.168.1.1  
ip forward-protocol nd  
!  
ip tcp synwait-time 5  
ip http server  
!  
ip ssh time-out 30  
ip ssh version 2  
ip ssh server algorithm encryption aes128-ctr  
aes192-ctr aes256-ctr  
ip ssh client algorithm encryption aes128-ctr  
aes192-ctr aes256-ctr  
!  
!  
logging trap notifications  
logging host 192.168.1.10  
!  
!  
!  
control-plane  
!  
!  
line con 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
login local  
line aux 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
line vty 0 4  
login local  
transport input ssh  
!  
!  
!  
end
```