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 засоби побудови захищених мережних інфраструктур для рішень від провідних виробників»

Виконав: студент 2-го курсу групи КБмп-24-1
спеціальності 125 «Кібербезпека та захист інформації»
_____ Олександр ДМИТРІЄВ
Керівник: старший викладач кафедри КІ та КБ
_____ Олександра ПОКОТИЛО
Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент
_____ Андрій ЄФІМЕНКО

Житомир – 2026

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
2 лютого 2026 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу магістра

Студент: Дмитрієв Олександр Геннадійович

Тема роботи: «Методи та засоби побудови захищених мережних інфраструктур для рішень від провідних виробників»

затверджена Наказом університету від 2 лютого 2026 р. №59/с

Термін здачі студентом закінченої роботи 27 березня 2026 р.

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

1. Об'єктом дослідженням є процес побудови корпоративної комп'ютерної мережі з багаторівневою системою захисту, сегментованої на чотири ізольовані функціональні зони (користувацьку, серверну, демілітаризовану та адміністративну), у якій одночасно застосовуються міжмережевий екран pfSense, комутатор Cisco IOSvL2 та централізований сервер управління ідентичностями FreeIPA.

2. Предметом дослідження є методи та засоби реалізації принципів архітектури нульової довіри (Zero Trust) у корпоративній мережі на базі зв'язки: pfSense CE (міжзонова фільтрація трафіку за схемою Router-on-a-Stick, система виявлення та запобігання вторгненням Snort IDS/IPS, інтеграція з LDAP), Cisco IOSvL2 (VLAN-сегментація, списки контролю доступу ACL, механізми захисту портів port-security) та FreeIPA (централізована автентифікація й авторизація на

3. базі Kerberos/LDAP, політики Host-Based Access Control), а також їхній вплив на рівень безпеки та керованість доступу до інформаційних ресурсів

Обладнання та програмне забезпечення:

1. Інструменти віртуалізації мережі GNS3 та Oracle VM VirtualBox.
2. Операційні системи CentOS Stream 9 (FreeIPA) та Ubuntu Server 22.04 LTS , Ubuntu 24.04.4 LTS Desktop
3. Програмний маршрутизатор та міжмережевий екран pfSense CE .
4. Cisco IOSvL2 15.2 — комутатор рівня L2 для реалізації VLAN-сегментації за стандартом IEEE 802.1Q.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Старший викладач кафедри КІ та КБ М. Хохлов	10.02.2026	11.02.2026
2	Старший викладач кафедри КІ та КБ М. Хохлов	12.02.2026	13.02.2026
3	Старший викладач кафедри КІ та КБ М. Хохлов	14.02.2026	15.02.2026

Студент _____ Олександр ДМИТРІЄВ

Керівник _____ Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз літератури та отримання завдання	02.02.2026	Виконано
2	Розробка теоретичного розділу (Розділ 1)	04.02.2026	Виконано
3	Проєктування системи захисту (Розділ 2)	05.02.2026	Виконано
4	Розгортання лабораторного стенду	07.02.2026	Виконано
5	Налаштування політик безпеки	18.02.2026	Виконано
6	Проведення експериментів (Розділ 3)	28.02.2026	Виконано
7	Оформлення пояснювальної записки	15.03.2026	Виконано
8	Захист кваліфікаційної роботи	27.03.2026	Виконано

Студент _____ Олександр ДМИТРІЄВ

Керівник _____ Олександра ПОКОТИЛО

АНОТАЦІЯ

Кваліфікаційна робота магістра містить 100 сторінок, 45 ілюстрацій, 23 таблиці, 1 додаток та 25 використаних джерел.

Метою роботи є розроблення та практична реалізація захищеної мережної інфраструктури на принципах архітектури нульової довіри із застосуванням мікросегментації, централізованого управління ідентичностями та міжзонової фільтрації трафіку, а також верифікація ефективності запропонованого рішення шляхом комплексного тестування.

Методи дослідження та апаратура: системний аналіз архітектурних рішень у сфері мережевої безпеки, порівняльний аналіз програмних засобів захисту, метод мережевого моделювання, метод «чорного ящика» при тестуванні захисних механізмів. Апаратна та програмна база включає маршрутизатор Cisco IOSv, міжмережевий екран pfSense 2.7 із системою виявлення вторгнень Snort, сервер FreeIPA та середовище моделювання GNS3.

Отримані результати: розроблено та реалізовано мережну інфраструктуру, сегментовану на чотири функціональні зони з ізоляцією на базі VLAN. Налаштовано централізовану автентифікацію та авторизацію через FreeIPA з HBAC-правилами. Інтегровано pfSense із FreeIPA та активовано автоматичне блокування загроз за допомогою Snort IDS/IPS. Проведене тестування підтвердило коректну роботу всіх 13 захисних сценаріїв та засвідчило відповідність реалізованої архітектури ключовим принципам моделі нульової довіри на високому рівні.

Рекомендації щодо використання результатів: розроблена відтворювана модель захищеної корпоративної мережі на базі відкритого програмного забезпечення може бути використана для побудови або модернізації систем захисту інфраструктур малих і середніх підприємств без витрат на комерційне ліцензування.

КЛЮЧОВІ СЛОВА: АВТЕНТИФІКАЦІЯ, БЕЗПЕКА, ЕКРАН, ІНФРАСТРУКТУРА, МІКРОСЕГМЕНТАЦІЯ.

ANNOTATION

The master's thesis contains 100 pages, 45 illustrations, 23 tables, 1 appendix, and 25 references.

The purpose of the work is the development and practical implementation of a secure network infrastructure based on Zero Trust architecture principles, utilizing microsegmentation, centralized identity management, and inter-zone traffic filtering, as well as the verification of the proposed solution's effectiveness through comprehensive testing.

Research methods and equipment: system analysis of architectural solutions in network security, comparative analysis of software security tools, network modeling method, "black box" method for testing security mechanisms. The hardware and software base includes a Cisco IOSv router, a pfSense 2.7 firewall with the Snort intrusion detection system, a FreeIPA server, and the GNS3 modeling environment.

Obtained results: a network infrastructure segmented into four functional zones with VLAN-based isolation was developed and implemented. Centralized authentication and authorization were configured via FreeIPA with HBAC rules. pfSense was integrated with FreeIPA, and automated threat blocking was activated using Snort IDS/IPS. The conducted testing confirmed the correct operation of all 13 security scenarios and proved the implemented architecture's high-level compliance with the key principles of the Zero Trust model.

Recommendations for the use of results: the developed reproducible model of a secure corporate network based on open-source software can be used to build or upgrade security systems for small and medium-sized enterprise infrastructures without commercial licensing costs.

KEYWORDS: AUTHENTICATION, FIREWALL, INFRASTRUCTURE, MICROSEGMENTATION, SECURITY.

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ АРХІТЕКТУРИ ZERO TRUST НА БАЗІ PFSENSE ТА ОБЛАДНАННЯ CISCO 11
1.1 Аналіз сучасного стану захисту мережних інфраструктур 11
1.2 Концепція Zero Trust як сучасна парадигма побудови захищених інфраструктур 14
1.3 Засоби периметрового захисту: аналіз та порівняння рішень 20
1.4 Засоби мережевої сегментації від провідних виробників 26
1.5 Управління ідентичностями як основа Zero Trust 31
РОЗДІЛ 2. ПРОЄКТУВАННЯ АРХІТЕКТУРИ ZERO TRUST НА БАЗІ PFSENSE ТА ОБЛАДНАННЯ CISCO 39
2.1 Постановка завдання та вимоги до інфраструктури 39
2.2 Обґрунтування архітектурних рішень 43
2.3 Проектування топології мережі 49
2.4 Вибір засобів реалізації та вимоги до середовища 55
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ZERO TRUST ТА ТЕХНОЛОГІЙ PFSENSE У ЛАБОРАТОРНОМУ СТЕНДІ 59
3.1. Розгортання середовища моделювання в GNS3 59
3.2. Налаштування компонентів інфраструктури 64
3.2.1. Cisco IOS — L2 сегментація 65
3.2.2. pfSense — периметр та міжзонова фільтрація 69
3.2.3. FreeIPA — централізоване управління ідентичностями 76
3.3. Тестування та верифікація захисних механізмів 79
3.4. Порівняльне оцінювання ефективності запропонованого рішення 85
3.4.1. Критерії та метрики оцінювання 85
3.4.2. Порівняння pfSense та OPNsense 86
3.4.3. Матриця відповідності архітектури принципам Zero Trust 88
3.4.4. Аналіз переваг та умов застосування рішення 88
ВИСНОВКИ 92
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 94
ДОДАТКИ 97

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API — Application Programming Interface (інтерфейс програмування застосунків)

CARP — Common Address Redundancy Protocol (протокол резервування IP-адрес)

DMZ — Demilitarized Zone (демілітаризована зона мережі)

DNS — Domain Name System (система доменних імен)

HA — High Availability (висока доступність)

IAM — Identity and Access Management (керування ідентифікацією та доступом)

IDS — Intrusion Detection System (система виявлення вторгнень)

IPS — Intrusion Prevention System (система запобігання вторгненням)

IPsec — Internet Protocol Security (набір протоколів захисту IP-трафіку)

Kerberos — протокол мережевої автентифікації

LDAP — Lightweight Directory Access Protocol (протокол доступу до служб каталогів)

MFA (2FA) — Multi-Factor Authentication (багатофакторна автентифікація)

NAT — Network Address Translation (перетворення мережевих адрес)

NIST — National Institute of Standards and Technology

NTP — Network Time Protocol (протокол синхронізації часу)

PEP — Policy Enforcement Point (точка примусового застосування політик)

SIEM — Security Information and Event Management (система керування подіями інформаційної безпеки)

SSO — Single Sign-On (єдиний вхід)

VLAN — Virtual Local Area Network (віртуальна локальна мережа)

VPN — Virtual Private Network (віртуальна приватна мережа)

ZTNA — Zero Trust Network Access

ZTA — Zero Trust Architecture

ВСТУП

Сучасні корпоративні мережі стикаються зі стрімким зростанням кіберзагроз, ускладненням інфраструктури та масовим переходом на віддалений доступ. За цих умов традиційна периметрова модель безпеки, що передбачає безумовну довіру до внутрішньої мережі, виявляється неефективною. Будь-яка компрометація одного вузла призводить до швидкого горизонтального поширення атаки. Це вимагає переходу до архітектури Zero Trust («ніколи не довіряй, завжди перевіряй»), яка базується на жорсткому розмежуванні доступу та мінімізації привілеїв.

Архітектура Zero Trust вимагає постійної перевірки автентичності, авторизації та контексту для кожного запиту, незалежно від розташування користувача. Практична реалізація цього підходу потребує поєднання мережевої мікросегментації, фільтрації трафіку, систем виявлення вторгнень (IDS/IPS) та централізованого керування ідентичностями. Ефективним і економічно доцільним шляхом є інтеграція відкритих рішень (pfSense, FreeIPA) із мережевим обладнанням корпоративного рівня (Cisco).

Об’єктом дослідження у даній магістерській роботі є процес побудови комп’ютерної мережі з багаторівневою системою захисту доступу, що використовує міжмережевий екран pfSense, сервер ідентифікації FreeIPA та мережеве обладнання Cisco.

Предметом дослідження є методи та засоби реалізації архітектури Zero Trust на базі pfSense (політико-орієнтована маршрутизація, фільтрація, IDS/IPS Snort), сервера FreeIPA (централізована автентифікація/авторизація) та обладнання Cisco (списки контролю доступу ACL), а також їхній вплив на захищеність і керованість мережі.

Метою магістерської роботи є розробка та експериментальне обґрунтування архітектури Zero Trust для корпоративної мережі на базі інтеграції pfSense, FreeIPA та Cisco, що забезпечує підвищений рівень безпеки, контроль доступу на рівні сегментів і гнучке керування політиками.

Для досягнення поставленої мети вирішуються такі основні завдання:

- проаналізувати сучасні підходи до побудови архітектури Zero Trust у корпоративних мережах;
- дослідити функціональні можливості pfSense (фаєрвол, VPN, Snort), FreeIPA (управління ідентичностями) та рішень Cisco (ACL) у контексті Zero Trust;
- спроєктувати топологію мережі з мікросегментацією та розподілом ролей між pfSense, FreeIPA і Cisco;
- розробити та налаштувати прототип системи захисту з використанням засобів ізоляції, IDS/IPS та централізованого керування доступом;
- провести експериментальне тестування рішення за критеріями ізоляції сегментів, виявлення атак та продуктивності;
- сформувати практичні рекомендації щодо впровадження запропонованої архітектури.

Практичне значення отриманих результатів полягає у створенні типової відтворюваної моделі побудови архітектури Zero Trust на базі pfSense, FreeIPA та Cisco для інфраструктур малих і середніх підприємств. Розроблений прототип, методики налаштування маршрутизації та інтеграції Snort із FreeIPA, а також результати тестування можуть бути безпосередньо використані адміністраторами мереж та фахівцями з кібербезпеки для впровадження багаторівневих політик доступу та підвищення стійкості мережі до сучасних кіберзагроз.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ АРХІТЕКТУРИ ZERO TRUST НА БАЗІ PFSENSE ТА ОБЛАДНАННЯ CISCO

1.1 Аналіз сучасного стану захисту мережних інфраструктур

Стрімкий розвиток інформаційних технологій та масштабна цифровізація бізнес-процесів зумовили кардинальну зміну ландшафту кіберзагроз. Якщо раніше основним вектором атак була зовнішня мережа, то сучасні зловмисники дедалі частіше діють зсередини периметра, використовуючи скомпрометовані облікові записи, ланцюги постачання програмного забезпечення та вразливості легітимного програмного забезпечення. За даними ФБР, у 2024 році було зафіксовано понад 859 000 скарг на кіберзлочини — на 33% більше порівняно з 2023 роком, а кількість витоків даних зросла на 75% у річному обчисленні. Кібератаки відбуваються в середньому кожні 39 секунд, що свідчить про безперервний і масштабний характер загроз для мережних інфраструктур. [1]

Класифікація актуальних загроз мережним інфраструктурам

Сучасні загрози мережним інфраструктурам організацій можна систематизувати за такими категоріями:

Несанкціонований доступ є базовим вектором більшості успішних атак. Зловмисники отримують початковий доступ через фішинг, експлуатацію вразливостей у публічно доступних сервісах (VPN-шлюзи, вебзастосунки) або використання скомпрометованих облікових даних. Зокрема, у 2024–2025 роках спостерігається значне зростання атак на VPN-апарати та граничні пристрої мережі — кожна п'ята витік даних пов'язана з непатченими вразливостями. [1]

Горизонтальне переміщення (Lateral Movement) є критично небезпечним тактичним прийомом, що дозволяє зловмиснику після отримання початкового доступу поширюватись по внутрішній мережі. За даними ReliaQuest Annual Threat Report 2025, горизонтальне переміщення може бути виконано за 27 хвилин з моменту первинного проникнення, а середній час становить 48 хвилин. Більш ніж 70% успішних зломів використовують техніки горизонтального переміщення. Середній час до виявлення атаки складає 95 днів — що надає зловмиснику тижні безперешкодного доступу до внутрішніх ресурсів. [2],[3],[4]

Розширені постійні загрози (APT — Advanced Persistent Threats) є найбільш небезпечним класом атак. APT-угруповання діють методично: проникнувши в мережу, вони можуть залишатись непоміченими місяцями, вивчаючи топологію мережі, збираючи облікові дані та готуючись до цільової атаки. Показовим прикладом є атака угруповання Volt Typhoon, яке тривалий час перебувало у мережах критичної інфраструктури США, та атака Black-Cat/ALPHV на Change Healthcare у лютому 2024 року, що завдала збитків понад 22 мільйони доларів. [3],[4]

Програми-вимагачі (Ransomware) набувають характеру домінуючої загрози: у 2024–2025 роках ransomware зафіксовано у 44% усіх інцидентів безпеки. Середній розмір викупу у 2024 році досяг 2 мільйони доларів, при цьому 94% організацій виплачують початково запитану суму. Ransomware-атаки нерідко поєднуються з горизонтальним переміщенням: зловмисники спочатку захоплюють якомога більше систем, а лише потім активують шифрування. [5],[6]

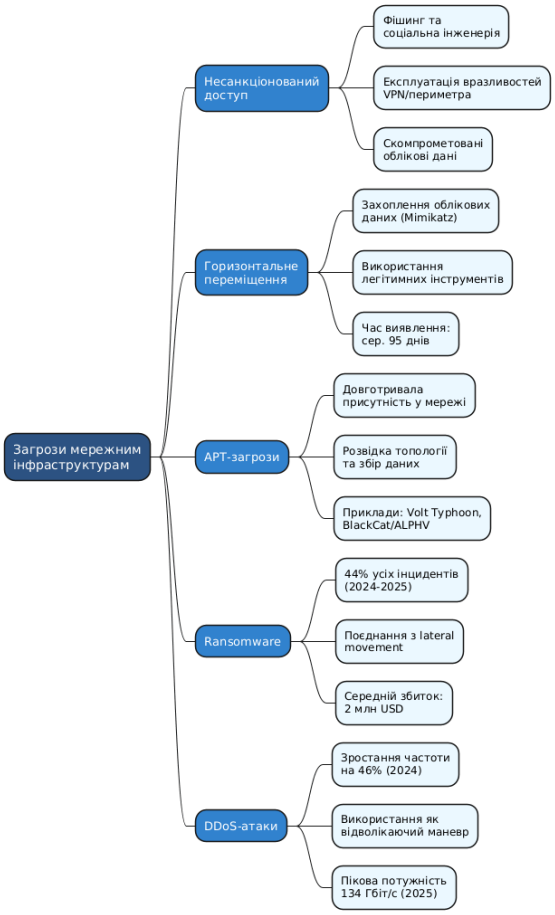


Рисунок 1.1—Класифікація актуальних загроз мережним інфраструктурам

Обмеженість класичного периметрального захисту

Традиційна модель безпеки базується на принципі «замку з ровом» (castle-and-moat): передбачається, що все всередині мережевого периметра є довіреним, а всі загрози надходять ззовні. Цей підхід мав логічне обґрунтування в епоху статичних корпоративних мереж, однак в умовах сучасного IT-середовища він демонструє критичні недоліки. [7]

Основні слабкості периметрального підходу полягають у наступному. По-перше, проблема неявної довіри: після успішного проходження периметрального захисту користувач або пристрій отримує широкий доступ до внутрішніх ресурсів без додаткової перевірки. По-друге, проблема інсайдерських загроз: 34% витоків даних пов'язані з внутрішніми акторами — легітимними користувачами, які або діють зловмисно, або чиї облікові дані було скомпрометовано. По-третє, розмивання периметра: масовий перехід на хмарні сервіси та дистанційну роботу зробив поняття «внутрішня мережа» умовним — 60% організацій відзначають труднощі із захистом віддалених працівників. По-четверте, неефективність проти горизонтального переміщення: традиційні міжмережеві екрани спроектовані для контролю периметрного (north-south) трафіку, але позбавлені механізмів контролю внутрішнього (east-west) трафіку між сегментами мережі. [8],[9],[10]

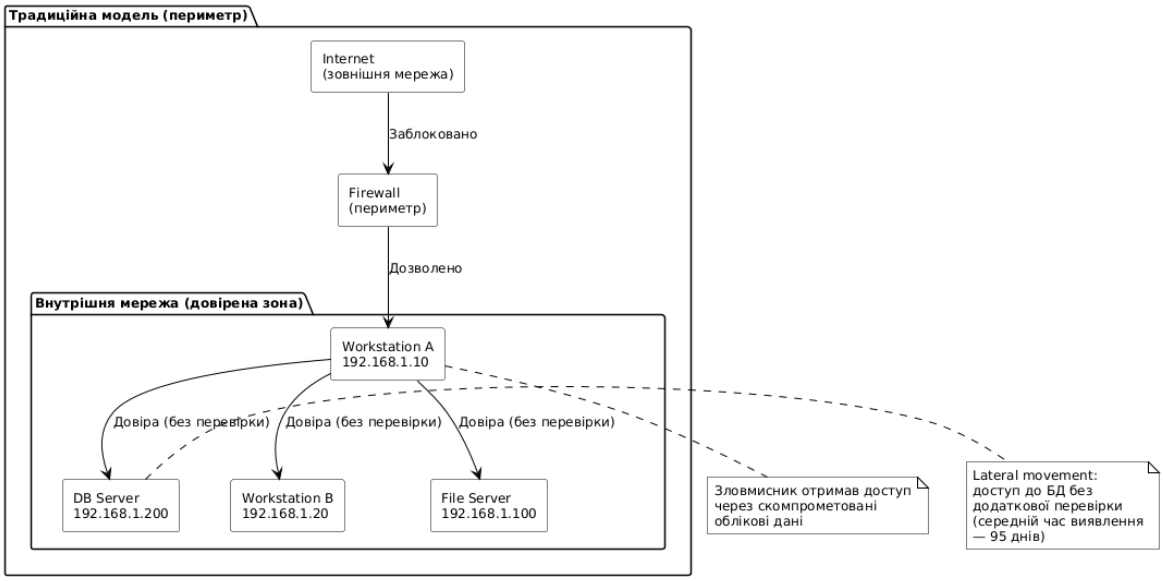


Рисунок 1.2—Порівняння традиційної периметральної моделі та наслідків її компрометації

Обґрунтування потреби у зміні підходу до побудови захищених інфраструктур

Аналіз сучасного ландшафту загроз свідчить про системну невідповідність між традиційними підходами до захисту мережних інфраструктур та реальними векторами атак. Зловмисники еволюціонували: сучасні APT-угруповання та ransomware-оператори цілеспрямовано обходять периметральний захист, використовуючи горизонтальне переміщення та легітимні інструменти адміністрування. [7]

Організації, що впровадили принципи Zero Trust, демонструють на 35% нижчі витрати від витоків даних та на 50% швидший час виявлення і реагування на загрози. Це підтверджує, що зміна парадигми з «довіряй, але перевіряй» на «ніколи не довіряй, завжди перевіряй» є не теоретичною концепцією, а практичною необхідністю для сучасних організацій. [8]

Таким чином, побудова захищеної мережної інфраструктури потребує комплексного підходу, що поєднує мікросегментацію мережі, централізоване управління ідентичностями та безперервну верифікацію кожного запиту на доступ — незалежно від його джерела. Реалізація цих принципів у практичному середовищі на базі рішень від провідних виробників є предметом дослідження даної роботи.

1.2 Концепція Zero Trust як сучасна парадигма побудови захищених інфраструктур

Традиційна модель мережевої безпеки, що панувала протягом десятиліть, ґрунтувалася на концепції «довіреного периметра»: все, що знаходиться всередині мережі організації, вважалось безпечним, а всі загрози — зовнішніми. Ця парадигма отримала назву «замок з ровом» (castle-and-moat) і передбачала зосередження захисних засобів на кордоні між зовнішньою та внутрішньою мережами. [7]

Перші концептуальні виклики цій моделі сформулювало міжнародне об'єднання Jericho Forum ще на початку 2000-х років, висунувши ідею «де-периметризації» — поступового розмивання меж між внутрішньою та

зовнішньою мережами внаслідок розвитку хмарних технологій, мобільних пристроїв та аутсорсингу. Переломним моментом стала операція Aurora у 2009 році — скоординована серія APT-атак на Google та понад 30 великих компаній, яка наочно продемонструвала неспроможність периметральної безпеки проти внутрішніх загроз. [11]

У 2009–2010 роках аналітик Forrester Research Джон Кіндерваг (John Kindervag) сформулював концепцію Zero Trust, ввівши термін, що став революційним для галузі. Кіндерваг запропонував замінити принцип «довіряй, але перевіряй» (trust but verify) на «ніколи не довіряй, завжди перевіряй» (Never Trust, Always Verify), стверджуючи, що сама по собі довіра є вразливістю. Ключова теза полягала в тому, що мережеве розташування ресурсу не може бути підставою для надання йому довіри — однакові вимоги до автентифікації та авторизації мають застосовуватись як до зовнішніх, так і до внутрішніх запитів. [12],[13],[14]

Паралельно Google у відповідь на Operation Aurora розробила внутрішню ініціативу BeyondCorp — практичну реалізацію Zero Trust-принципів у масштабах глобальної корпоративної інфраструктури. У 2017 році аналітики Gartner розвинули суміжну концепцію CARTA (Continuous Adaptive Risk and Trust Assessment), що наголошувала на необхідності безперервного адаптивного оцінювання ризику. Кульмінацією нормативного оформлення концепції стала публікація у 2020 році стандарту NIST SP 800-207 «Zero Trust Architecture» — першого офіційного документа, що систематизував архітектурні принципи та компоненти Zero Trust. [11],[15],[16] Хронологію розвитку концепції Zero Trust наведено на рисунку 1.3.



Рисунок 1.3—Еволюція концепції Zero Trust

Основні принципи Zero Trust

Концепція Zero Trust базується на трьох фундаментальних принципах, сформульованих Кіндервагом та розвинених у стандарті NIST SP 800-207 [17]:

Never Trust, Always Verify («Ніколи не довіряй, завжди перевіряй») — жоден користувач, пристрій або мережевий запит не отримує доступу до ресурсів без явної автентифікації та авторизації, незалежно від того, чи знаходиться джерело запиту всередині чи поза межами корпоративної мережі. Мережеве розташування перестає бути ознакою довіри. [17]

Least Privilege («Принцип мінімальних привілеїв») — кожен суб'єкт (користувач, сервіс, пристрій) отримує лише той рівень доступу, який є мінімально необхідним для виконання конкретного завдання у конкретний момент часу. Доступ надається динамічно і може бути відкликаний при зміні контексту. [12]

Assume Breach («Припускай злам») — система проектується з припущенням, що зловмисник вже знаходиться всередині мережі. Це зумовлює необхідність мікросегментації, шифрування внутрішнього трафіку, безперервного моніторингу та мінімізації радіуса ураження при компрометації. [17]

На основі цих принципів NIST SP 800-207 визначає сім тенетів Zero Trust Architecture [16],[17]:

1. Усі ресурси (дані, застосунки, пристрої) захищаються незалежно від їх розташування
2. Жодне мережеве розташування не є апріорі довіреним
3. Доступ до ресурсів надається на основі індивідуального запиту з урахуванням ідентичності та контексту
4. Принцип мінімальних привілеїв застосовується динамічно
5. Безперервний моніторинг та діагностика стану всіх активів
6. Журналювання та аналіз усіх запитів на доступ
7. Адаптивні політики, що базуються на телеметрії та даних про загрози

Архітектурні компоненти Zero Trust

Стандарт NIST SP 800-207 визначає логічну архітектуру Zero Trust через взаємодію трьох ключових компонентів, взаємодію яких зображено на рисунку 1.4 [17],[18]:

Policy Engine (PE) — Механізм політик виконує роль «мозку» системи: він аналізує запит на доступ, зіставляє його з поточними політиками безпеки, даними про ідентичність користувача, стан пристрою та контекст запиту, після чого виносить рішення — дозволити, заборонити або потребувати додаткової автентифікації. [18]

Policy Administrator (PA) — Адміністратор політик транслює рішення Policy Engine у конкретні команди для Policy Enforcement Point: створює або анулює сесію, налаштовує маршрути, генерує токени доступу. [18]

Policy Enforcement Point (PEP) — Точка застосування політик є операційним компонентом, що безпосередньо контролює з'єднання між суб'єктом запиту та ресурсом, застосовуючи рішення прийняте Policy Engine. У контексті мережної інфраструктури роль PEP можуть виконувати міжмережеві екрани, VPN-шлюзи, проксі-сервери та керовані комутатори. [17]

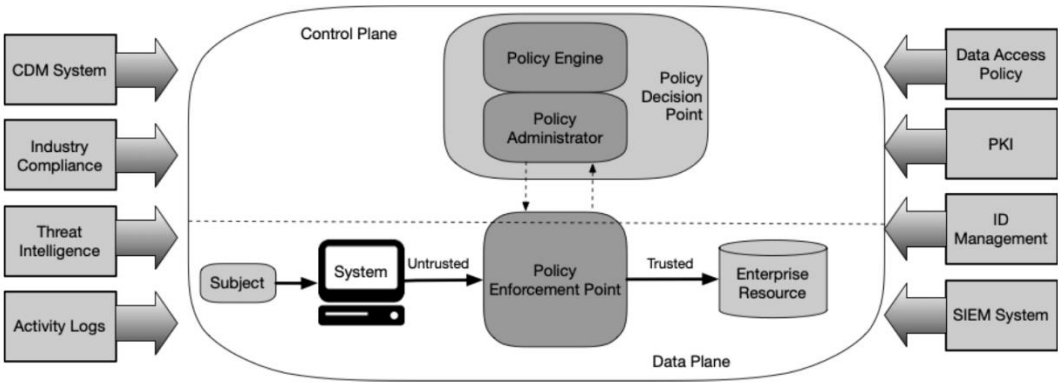


Рисунок 1.4—Архітектурні компоненти Zero Trust за NIST SP 800−207

Модель зрілості Zero Trust (CISA ZTMM)

Агентство з кібербезпеки та захисту інфраструктури США (CISA) у 2023 році опублікувало оновлену версію Zero Trust Maturity Model (ZTMM v2.0), що визначає практичний шлях впровадження Zero Trust через п'ять стовпів та чотири рівні зрілості. [19]

П'ять стовпів CISA ZTMM охоплюють усі домени, в яких необхідно застосовувати принципи Zero Trust, [19],[20] їх відповідність компонентам реалізованої у даній роботі архітектури наведено у таблиці 1.1.

Таблиця 1.1

П'ять стовпів CISA Zero Trust Maturity Model та їх реалізація у даній роботі

Стовп	**Зміст**	**Реалізація у даній роботі**
Identity (Ідентичність)	Верифікація кожного користувача незалежно від розташування	FreeIPA: LDAP, Kerberos, HBAC
Devices (Пристрої)	Інвентаризація та моніторинг стану пристроїв	Port security на Cisco IOS
Networks (Мережа)	Мікросегментація, шифрування трафіку	VLAN + pfSense firewall rules
Applications & Workloads	Контроль доступу до застосунків	Firewall rules pfSense між VLAN
Data (Дані)	Класифікація та захист даних	Централізоване журналювання, Syslog

Чотири рівні зрілості — Traditional, Initial, Advanced, Optimal — дозволяють організації оцінити поточний стан та визначити наступні кроки впровадження. Архітектура, реалізована у даній роботі, відповідає рівню Initial–Advanced: присутня мікросегментація, централізована автентифікація та журналювання подій, однак відсутня повна автоматизація реагування на інциденти та поведінковий аналіз трафіку. Графічне зображення п'яти стовпів CISA ZTMM наведено на рисунку 1.5. [19]

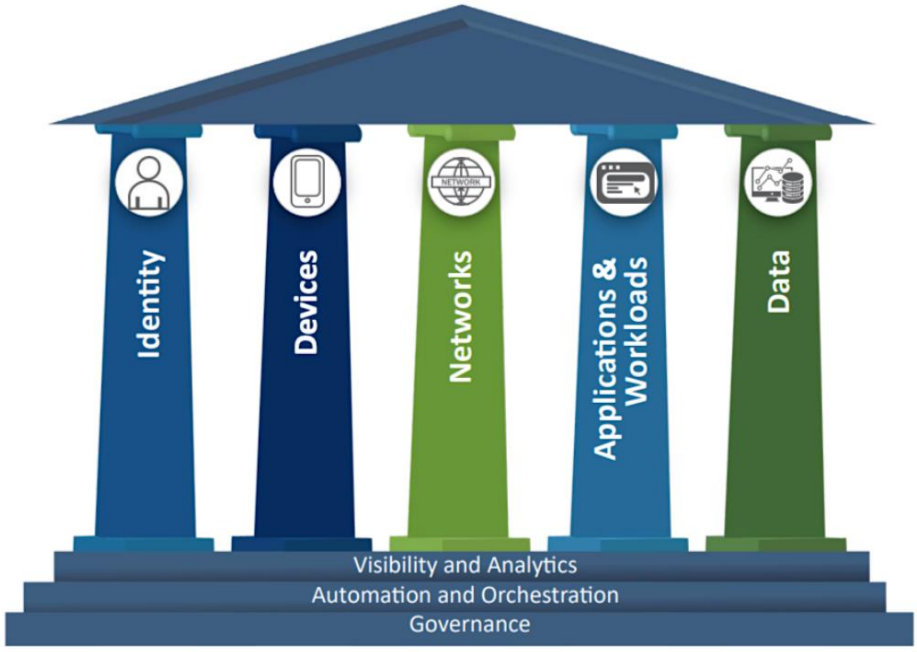


Рисунок 1.5 — П'ять стовпів CISA Zero Trust Maturity Model

Zero Trust є не продуктом чи технологією, а стратегічним підходом до проектування захищених інфраструктур. Його практична цінність підтверджується конкретними показниками: організації, що впровадили Zero Trust, демонструють на 35% нижчі витрати від витоків даних та вдвічі швидше виявляють інциденти безпеки. Аналіз стандарту NIST SP 800-207 та моделі CISA ZTMM (таблиця 1.1) свідчить, що ефективна реалізація Zero Trust вимагає інтеграції трьох ключових підсистем: засобів периметрового захисту (міжмережеві екрани, IDS/IPS), засобів мережевої сегментації (VLAN, ACL) та системи управління ідентичностями (Identity Provider). Саме така інтеграція є предметом дослідження та практичної реалізації у даній роботі.

1.3 Засоби периметрового захисту: аналіз та порівняння рішень

Класифікація міжмережевих екранів

Міжмережевий екран (ME, firewall) є ключовим компонентом периметрового захисту мережної інфраструктури, що здійснює контроль мережевого трафіку між зонами на основі визначених політик безпеки. Еволюція технологій ME відповідала зростанню складності мережевих загроз і пройшла кілька послідовних поколінь [21], що схематично відображено на рисунку 1.6.

Пакетні фільтри (Packet Filtering Firewalls) — перше покоління ME, що з'явилося наприкінці 1980-х років. Принцип роботи базується на аналізі заголовків пакетів на мережевому рівні (L3) моделі OSI: IP-адреси джерела та призначення, протокол, порти. Рішення про пропуск або блокування приймається незалежно для кожного пакету без урахування контексту з'єднання. Перевагою є висока швидкість обробки, недоліком — відсутність розуміння стану з'єднання та неможливість виявлення атак на рівні застосунків.[21]

Stateful Inspection Firewalls (ME зі збереженням стану з'єднання) — друге покоління, що відстежує стан TCP/UDP-з'єднань у таблиці станів. ME аналізує не лише окремі пакети, а й контекст їхньої приналежності до конкретного з'єднання, що дозволяє блокувати пакети, які не відповідають жодному легітимному сеансу. Цей принцип реалізований у підсистемі pf (Packet Filter) операційної системи FreeBSD, на якій базуються pfSense та OPNsense.[21]

Міжмережеві екрани наступного покоління (NGFW — Next-Generation Firewall) — сучасне покоління, що поєднує stateful inspection з глибоким аналізом пакетів (DPI — Deep Packet Inspection) на рівні застосунку (L7), системами виявлення та запобігання вторгнень (IDS/IPS), SSL/TLS-інспекцією та інтеграцією з системами управління ідентичностями. Функціонал NGFW може бути реалізований на pfSense або OPNsense шляхом встановлення пакетів Snort або Suricata — це дозволяє отримати DPI та IDS/IPS-можливості на базі open-source платформи.[22]

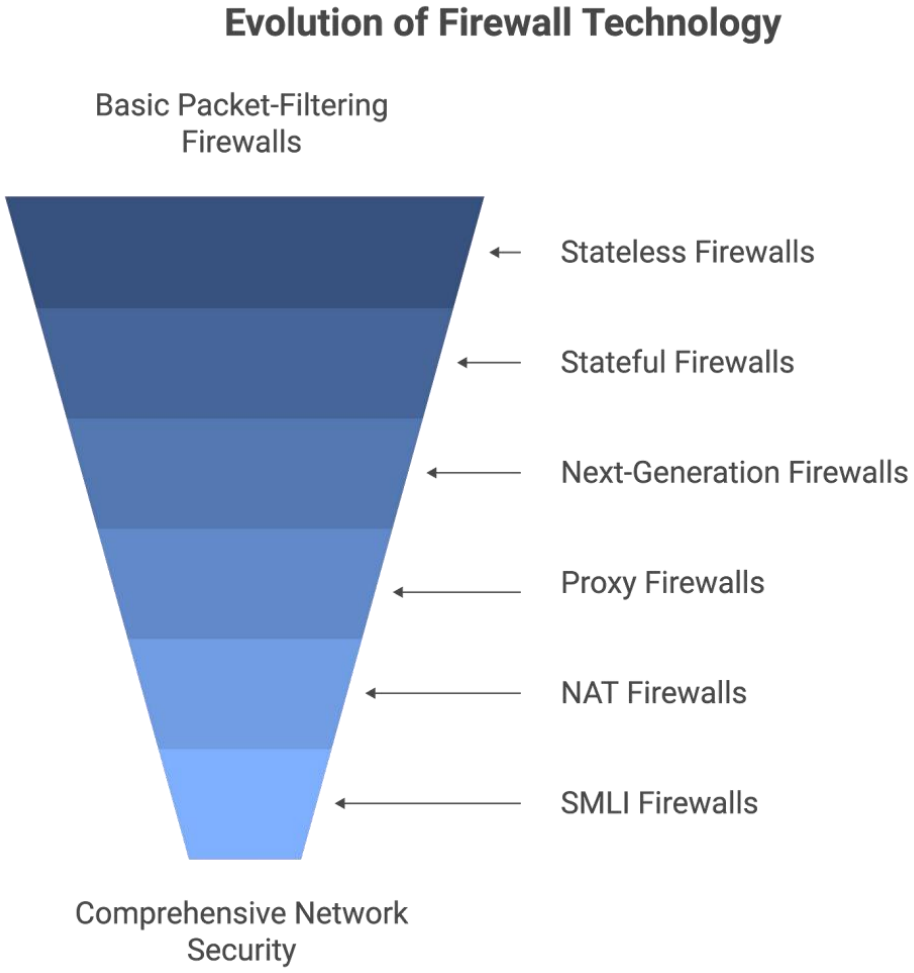


Рисунок 1.6 — Еволюція поколінь міжмережевих екранів

Огляд платформи pfSense

pfSense є відкритою операційною системою для міжмережевих екранів та маршрутизаторів, що базується на FreeBSD та підсистемі фільтрації пакетів pf. Проект розроблено компанією Netgate і поширюється у двох редакціях: Community Edition (CE) з відкритим вихідним кодом та pfSense Plus — комерційна версія з розширеними функціями та пріоритетною підтримкою.[23]

Ключові характеристики pfSense охоплюють широкий спектр мережевих функцій. У сфері маршрутизації та комутації платформа підтримує статичну маршрутизацію, VLAN (802.1Q), NAT/PAT, DHCP, DNS Resolver (Unbound), IPv6 та OSPF/BGP через пакет FRR. VPN-підсистема включає OpenVPN, IPsec IKEv2, L2TP та WireGuard (через плагін), що забезпечує широкі можливості для організації захищених тунелів. Функціонал IDS/IPS реалізується через пакети Snort та Suricata: обидва підтримують глибокий аналіз пакетів, набори правил Emerging Threats та Talos, а також інлайн-режим блокування. Моніторинг та журналювання забезпечуються вбудованим дашбордом, підтримкою Syslog, SNMP та пакетом ntopng для детального аналізу трафіку.

Важливим аспектом є зрілість екосистеми pfSense: платформа існує з 2004 року, має велику спільноту, значну кількість академічних та технічних публікацій, розгалужену документацію Netgate та широку підтримку у навчальних середовищах.

Огляд платформи OPNsense

OPNsense є відгалуженням (fork) pfSense, розробленим компанією Deciso у 2015 році з метою створення більш відкритої та регулярно оновлюваної альтернативи. Платформа розповсюджується виключно під ліцензією BSD з повністю відкритим вихідним кодом. [24]

OPNsense вирізняється сучаснішим підходом до архітектури та оновлень. Система виходить двічі на рік з великими релізами та регулярними патчами безпеки, тоді як pfSense CE оновлюється щорічно і отримує патчі безпеки із затримкою відносно комерційної Plus-редакції. IDS/IPS реалізований на базі Suricata як вбудований компонент — без необхідності окремої установки пакетів. Інтегрований MVC-фреймворк та REST API надають широкі можливості для автоматизації та інтеграції з зовнішніми системами. WireGuard підтримується як вбудований компонент без додаткових плагінів. [24]

Порівняльний аналіз pfSense та OPNsense

Для обґрунтованого вибору платформи периметрового захисту у даній роботі проведено порівняльний аналіз pfSense та OPNsense за ключовими

критеріями, що відповідають вимогам Zero Trust-архітектури. Результати порівняння наведено у таблиці 1.2.

Таблиця 1.2

Порівняльний аналіз pfSense та OPNsense за критеріями Zero Trust

Критерій	**pfSense CE**	**OPNsense**	**Перевага**
Ліцензія	Відкритий код (CE); Plus — пропрієтарний	Повністю відкритий код (BSD)	OPNsense
Базова ОС	FreeBSD	FreeBSD	Рівно
Інтерфейс управління	Функціональний, традиційне меню (top-bar)	Сучасний, бічна навігація (sidebar)	OPNsense
IDS/IPS	Snort або Suricata (встановлюється як пакет)	Suricata (вбудований за замовчуванням)	OPNsense
WireGuard VPN	Через плагін	Вбудований	OPNsense
Частота оновлень безпеки	CE отримує патчі після Plus (затримка)	Патчі виходять одразу після FreeBSD advisory	OPNsense
REST API	Обмежена підтримка	Повноцінний REST API (MVC-фреймворк)	OPNsense
Інтеграція з IdP (LDAP)	Підтримується (FreeIPA, AD)	Підтримується (FreeIPA, AD)	Рівно
Екосистема пакетів	Більша кількість сторонніх пакетів	Менша, але зростаюча	pfSense
Документація	Велика, зріла, багато академічних прикладів	Менша, але актуальніша	pfSense
Продуктивність (routing)	~938 Мбіт/с (WAN-to-LAN)	~940 Мбіт/с (WAN-to-LAN)	Рівно
Продуктивність (IDS увімкнено)	~670 Мбіт/с (-28%)	~680 Мбіт/с (-27%)	Рівно
Масштабованість	HA, CARP, Multi-WAN	HA, CARP, Multi-WAN	Рівно
Придатність для навчальних середовищ	Висока (велика база прикладів GNS3/VMware)	Середня	pfSense

Аналіз даних таблиці 1.2 дозволяє зробити такі висновки. OPNsense демонструє переваги у сфері відкритості коду, оперативності оновлень безпеки, вбудованого IDS/IPS та сучасного інтерфейсу, що робить його привабливим

вибором для нових розгортань у виробничому середовищі. pfSense, своєю чергою, переважає за обсягом документації, зрілістю екосистеми та широтою підтримки в академічних і лабораторних середовищах. Продуктивність обох платформ на ідентичному апаратному забезпеченні є практично однаковою — різниця не перевищує 1-2% як при маршрутизації, так і при увімкненому IDS.

Обґрунтування вибору pfSense для реалізації

На основі проведеного порівняльного аналізу для практичної реалізації у даній роботі обрано платформу pfSense CE з таких міркувань.

По-перше, зрілість документації та академічна підтримка: pfSense має значно більшу кількість задокументованих сценаріїв інтеграції з GNS3, FreeIPA та Cisco IOS, що є критичним для відтворюваності лабораторного середовища. По-друге, широта екосистеми пакетів: наявність Snort, Suricata, pfBlockerNG, ntopng та інших пакетів дозволяє реалізувати повний стек NGFW-функцій на єдиній платформі. По-третє, сумісність з середовищем моделювання: pfSense є стандартною платформою для мережевих лабораторій у середовищі GNS3+VirtualBox, що підтверджується значною кількістю готових конфігурацій та навчальних матеріалів.

Слід зазначити, що за умов промислового розгортання з вимогами до регулярних оновлень безпеки, вбудованого REST API та сучаснішого інтерфейсу управління — OPNsense є рівноцінною, а в деяких аспектах і кращою альтернативою, що підтверджується даними таблиці 1.2.

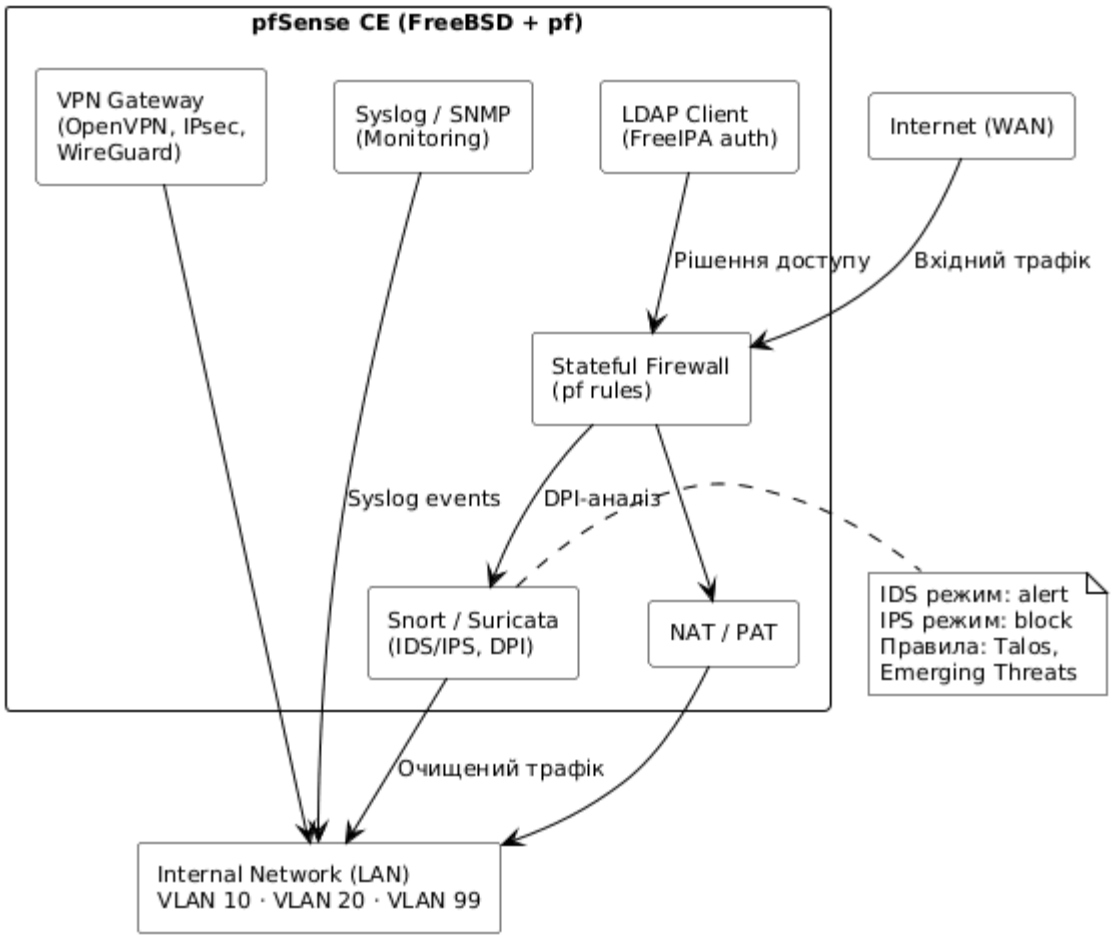


Рисунок 1.7 — Архітектура pfSense як засобу периметрового захисту

Підсумовуючи проведений аналіз засобів периметрового захисту, можна стверджувати, що сучасні вимоги до безпеки мережевої інфраструктури вимагають переходу від традиційних пакетних фільтрів до рішень класу NGFW. У контексті побудови архітектури нульової довіри (Zero Trust Architecture) міжмережевий екран відіграє критичну роль вузла контролю політик (Policy Enforcement Point), який повинен забезпечувати не лише фільтрацію за станом з'єднання, але й глибокий аналіз трафіку (DPI), роботу систем IDS/IPS та надійну інтеграцію з провайдерами ідентифікації.

Порівняння провідних відкритих платформ pfSense та OPNsense засвідчило, що обидва рішення володіють потужним функціоналом та демонструють паритетну продуктивність. Хоча OPNsense пропонує сучасніший архітектурний підхід, оптимізований для промислових розгортань завдяки вбудованому REST API та швидшим циклам оновлень безпеки, для цілей даного дослідження стратегічно виправданим є вибір pfSense.

Головними аргументами на користь pfSense для практичної реалізації стали неперевершена зрілість екосистеми пакетів, вичерпна документація та еталонна сумісність із середовищами віртуалізації та мережевого моделювання, такими як GNS3. Це дозволить безперешкодно розгорнути повноцінний тестовий стенд, налаштувати необхідний стек захисту (Snort/Suricata, VPN, Radius/LDAP) та ефективно змоделювати принципи мікросегментації і контролю доступу, що є фундаментальними для тестування моделі Zero Trust у подальших розділах роботи.

1.4 Засоби мережевої сегментації від провідних виробників

Роль мережевої сегментації у побудові захищених інфраструктур

Мережева сегментація є одним із фундаментальних механізмів реалізації принципів Zero Trust на рівні мережевої інфраструктури. Її сутність полягає у поділі єдиної мережі на ізольовані логічні або фізичні зони, між якими трафік дозволяється лише явно визначеними правилами. Дев'ять із десяти фахівців з інформаційної безпеки вважають мережеву сегментацію критично важливою для реалізації Zero Trust. Правильно налаштована сегментація обмежує поверхню атаки, унеможливлює вільне горизонтальне переміщення зловмисника та мінімізує радіус ураження при компрометації окремого вузла.

З точки зору Zero Trust-архітектури, сегментація реалізує принципи Least Privilege та Assume Breach: кожен сегмент отримує доступ лише до тих ресурсів, які необхідні для виконання його функцій, а компрометація одного сегменту не надає автоматичного доступу до решти інфраструктури. Відповідно до стовпа «Networks» моделі CISA ZTMM, мікросегментація є обов'язковим елементом зрілої Zero Trust-архітектури.

Cisco як провідний виробник засобів мережевої сегментації

Cisco Systems є світовим лідером у сфері мережевого обладнання: за даними аналітичної компанії IDC, частка компанії на ринку корпоративних комутаторів перевищує 50%. Лінійка продуктів Cisco для комутації охоплює серії Catalyst (корпоративний рівень), Nexus (центри обробки даних) та Small Business (серія SF/SG для малого та середнього бізнесу). Операційна система

Cisco IOS (Internetwork Operating System) забезпечує єдиний інтерфейс управління для всієї лінійки обладнання і є стандартом де-факто для корпоративної мережевої інфраструктури.

Позиція Cisco як провідного виробника підтверджується не лише ринковою часткою, а й глибиною інтеграції засобів безпеки безпосередньо в операційну систему. Cisco IOS реалізує повний стек засобів сегментації та контролю доступу: від базових ACL до розширених механізмів TrustSec із мітками Security Group Tags (SGT), що забезпечують динамічну ідентифікаційну сегментацію незалежно від топології.

VLAN як інструмент мікросегментації

VLAN (Virtual Local Area Network, IEEE 802.1Q) — це механізм логічного розділення мережі на рівні канального рівня (L2) моделі OSI. Кожен VLAN утворює окремий широкомовний домен: пристрої в різних VLAN не можуть безпосередньо взаємодіяти без явної маршрутизації через L3-пристрій, яким у даній архітектурі виступає pfSense.

Технологія VLAN реалізується на комутаторах Cisco через призначення портів до певного VLAN (access mode) або через тегування трафіку декількох VLAN на одному фізичному з'єднанні (trunk mode, 802.1Q). Trunk-з'єднання між комутатором Cisco та pfSense дозволяє передавати трафік усіх VLAN через єдиний фізичний канал, де pfSense виконує міжзонову фільтрацію на основі визначених правил.

З точки зору безпеки, правильно налаштована VLAN-сегментація значно знижує поверхню атаки: зловмисник, що скомпрометував пристрій у VLAN 10, не має мережевої видимості пристроїв у VLAN 20 без проходження через pfSense, де застосовуються firewall-правила. Архітектуру VLAN-сегментації у контексті Zero Trust наведено на рисунку 1.8.

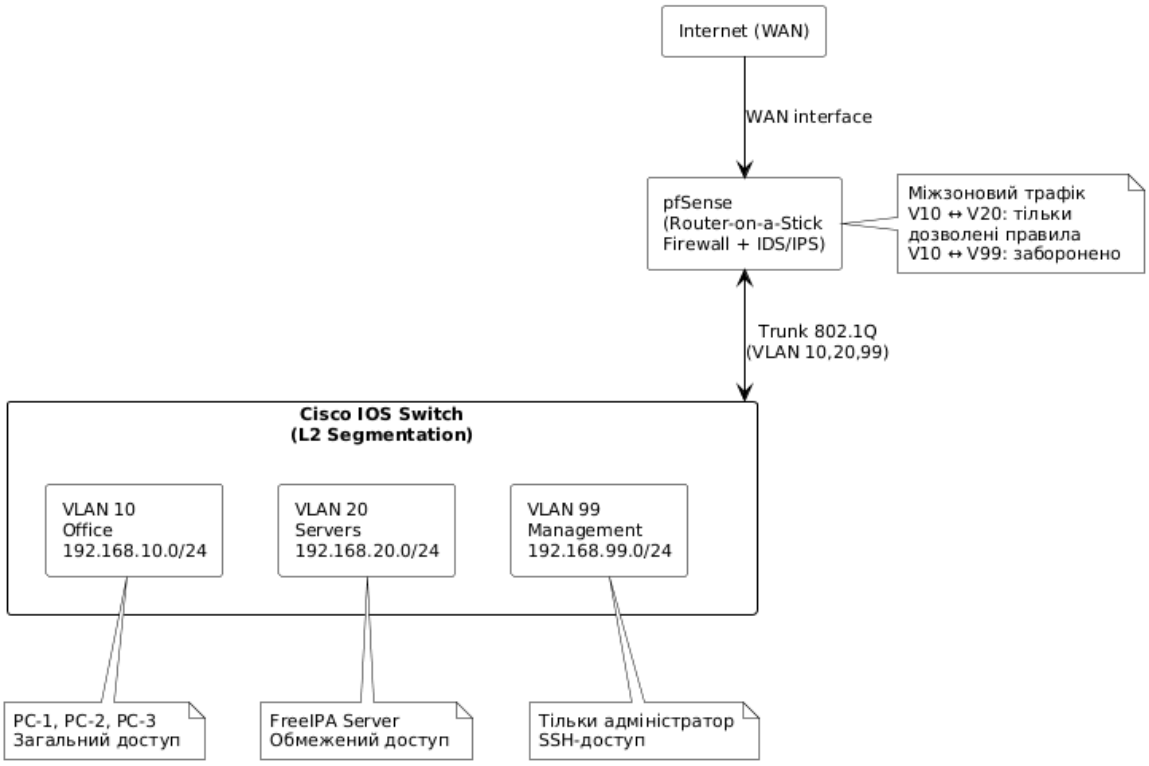


Рисунок 1.8 — VLAN-сегментація як засіб мікросегментації у Zero Trust-архітектурі

Механізми захисту Cisco IOS

Cisco IOS надає комплекс вбудованих механізмів захисту мережної інфраструктури, що безпосередньо реалізують вимоги Zero Trust на рівні access layer.

Списки контролю доступу (ACL)

Списки контролю доступу (Access Control Lists, ACL) є базовим механізмом фільтрації трафіку в Cisco IOS. ACL являє собою упорядкований набір правил «дозволити / заборонити», що застосовуються до трафіку на інтерфейсі комутатора або маршрутизатора у вхідному (in) або вихідному (out) напрямку.

Cisco IOS підтримує два типи ACL: стандартні ACL (Standard ACL, номери 1–99) фільтрують трафік лише за IP-адресою джерела; розширені ACL (Extended ACL, номери 100–199 або іменовані) аналізують IP-адреси джерела та призначення, протокол (TCP/UDP/ICMP/IP) і номери портів. Для захисту доступу до управлінського інтерфейсу комутатора (VTY lines) Cisco рекомендує

застосовувати ACL у поєднанні з командою access-class, що обмежує SSH-доступ до пристрою лише з визначеного Management VLAN.

У контексті Zero Trust, розширені ACL на Cisco IOS реалізують принцип Least Privilege на мережевому рівні: заборонений за замовчуванням трафік між VLAN з явним дозволом лише необхідних потоків.

Port Security

Механізм Port Security в Cisco IOS дозволяє обмежити кількість MAC-адрес, що можуть використовуватись на одному фізичному порті комутатора. При виявленні порушення (підключення несанкціонованого пристрою або перевищення ліміту MAC-адрес) порт може переходити у три режими: shutdown (адміністративно вимикається), restrict (пакети відхиляються, генерується SNMP-trap та Syslog-повідомлення) або protect (пакети з невідомими MAC відхиляються без сповіщення). Цей механізм реалізує принцип «Devices» зі стовпів CISA ZTMM — контроль пристроїв, що підключаються до інфраструктури.

Захищене адміністрування: SSH v2

Cisco рекомендує використовувати виключно SSH версії 2 для адміністративного доступу до мережевого обладнання. Протокол Telnet передає дані, включаючи паролі, у відкритому вигляді і має бути відключений на всіх пристроях. SSH v2 забезпечує шифрування сеансу, автентифікацію за ключем або паролем, а також підтримку AAA-інтеграції. Для генерації RSA-ключів Cisco рекомендує довжину не менше 2048 біт. У даній роботі SSH-доступ до комутатора обмежується лише з Management VLAN через ACL на VTY-лініях, що відповідає принципу мінімальних привілеїв.

Централізоване журналювання (Syslog)

Cisco IOS підтримує передачу системних повідомлень на централізований Syslog-сервер. Журналювання охоплює події безпеки: спрацювання ACL (за наявності ключового слова log), Port Security violations, зміни стану інтерфейсів, спроби авторизації. Рівні важливості Syslog (0-Emergencies до 7-Debugging) дозволяють гнучко налаштовувати деталізацію подій. У контексті Zero Trust,

централізований Syslog є реалізацією принципу «безперервного моніторингу» та стовпа «Data» моделі CISA ZTMM.

Місце Cisco у Zero Trust-архітектурі

У реалізованій архітектурі Cisco IOS виконує роль access layer — рівня доступу, що безпосередньо підключає кінцеві пристрої та забезпечує їх L2-ізоляцію за допомогою VLAN. Взаємодію компонентів та роль Cisco у загальній архітектурі відображено у таблиці 1.3.

Таблиця 1.3

Відповідність механізмів Cisco IOS принципам Zero Trust

Механізм Cisco IOS	**Принцип Zero Trust**	**Стовп CISA ZTMM**
VLAN-сегментація (802.1Q)	Assume Breach, мікросегментація	Networks
Розширені ACL (Extended ACL)	Least Privilege	Networks
Port Security	Never Trust, Always Verify	Devices
SSH v2 + ACL на VTY	Least Privilege	Identity
Syslog (централізоване журналювання)	Безперервний моніторинг	Data
Trunk 802.1Q до pfSense	Policy Enforcement Point	Networks

Важливо підкреслити: у даній архітектурі Cisco IOS виступає як Policy Enforcement Point (PEP) на рівні L2 — він ізолює трафік між VLAN та обмежує адміністративний доступ. Роль Policy Engine, що приймає рішення про міжзоновий доступ, виконує pfSense на основі визначених firewall-правил та даних автентифікації від FreeIPA. Такий розподіл відповідальності між компонентами забезпечує ешелонований захист (Defense in Depth) і є характерним для сучасних Zero Trust-архітектур на базі рішень провідних виробників. [25]

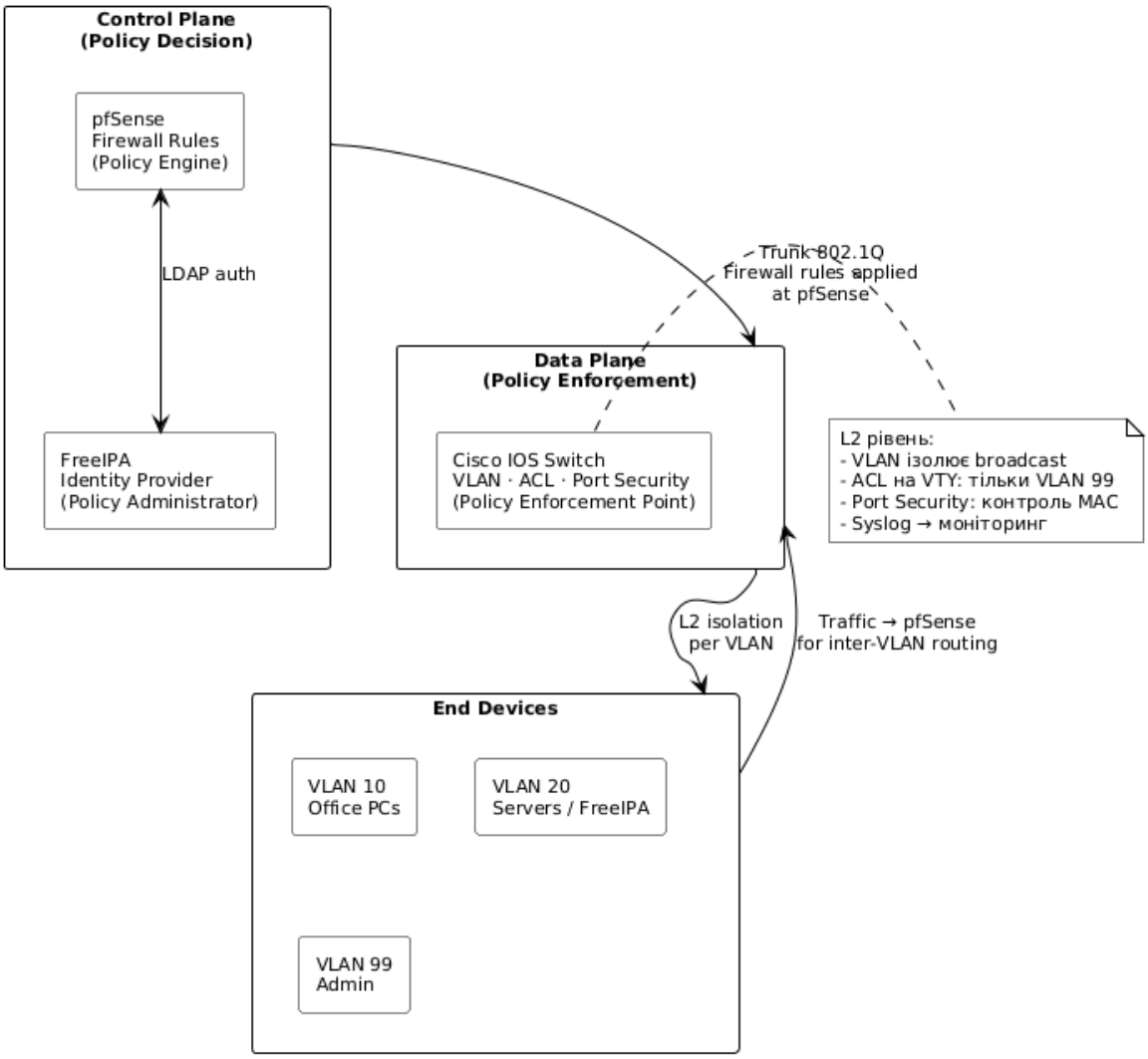


Рисунок 1.9 — Роль Cisco IOS у Zero Trust-архітектурі як Policy Enforcement Point

Таким чином, Cisco IOS у поєднанні з pfSense та FreeIPA формує повноцінну трирівневу архітектуру захисту: ідентичність верифікується через FreeIPA, рішення про доступ приймає pfSense, а фізична ізоляція сегментів забезпечується механізмами Cisco IOS. Саме такий розподіл відповідальності між рішеннями провідних виробників є предметом практичної реалізації та дослідницького аналізу у наступних розділах роботи.

1.5 Управління ідентичностями як основа Zero Trust

Принцип «Identity is the new perimeter»

Традиційна модель мережевої безпеки використовувала IP-адресу як основний ідентифікатор суб'єкта: якщо запит надходить з «внутрішньої» мережі

— він вважається легітимним. Zero Trust кардинально змінює цей підхід: ідентичність користувача, пристрою або сервісу замінює мережеве розташування як основу для прийняття рішень про доступ. Саме це лежить в основі концепції «Identity is the new perimeter» — периметром захисту стає не мережевий кордон, а система ідентифікації та авторизації.

У контексті Zero Trust Identity and Access Management (ZT IAM) кожен запит на доступ до ресурсу проходить три обов'язкові кроки: автентифікацію (підтвердження ідентичності), авторизацію (перевірку наявності прав) та аудит (журналювання події доступу). Ці три кроки мають виконуватись незалежно від того, звідки надходить запит — з внутрішньої мережі, VPN-тунелю або публічного Інтернету. Реалізація такого підходу вимагає централізованої системи управління ідентичностями — Identity Provider (IdP).

FreeIPA як Identity Provider для Linux-інфраструктури

FreeIPA є інтегрованим рішенням управління ідентичностями з відкритим вихідним кодом, розробленим компанією Red Hat та спільнотою Fedora. Назва є абревіатурою від «Free Identity, Policy, Audit». Платформа поєднує у єдиному рішенні низку компонентів, що окремо вимагали б встановлення та синхронізації: сервер каталогів 389 Directory Server (реалізація LDAP), центр розподілу ключів MIT Kerberos, DNS-сервер BIND, сервер сертифікатів Dogtag (вбудований CA), NTP-сервіс та веб-інтерфейс управління.

Архітектуру FreeIPA та взаємодію її компонентів наведено на рисунку 1.10.

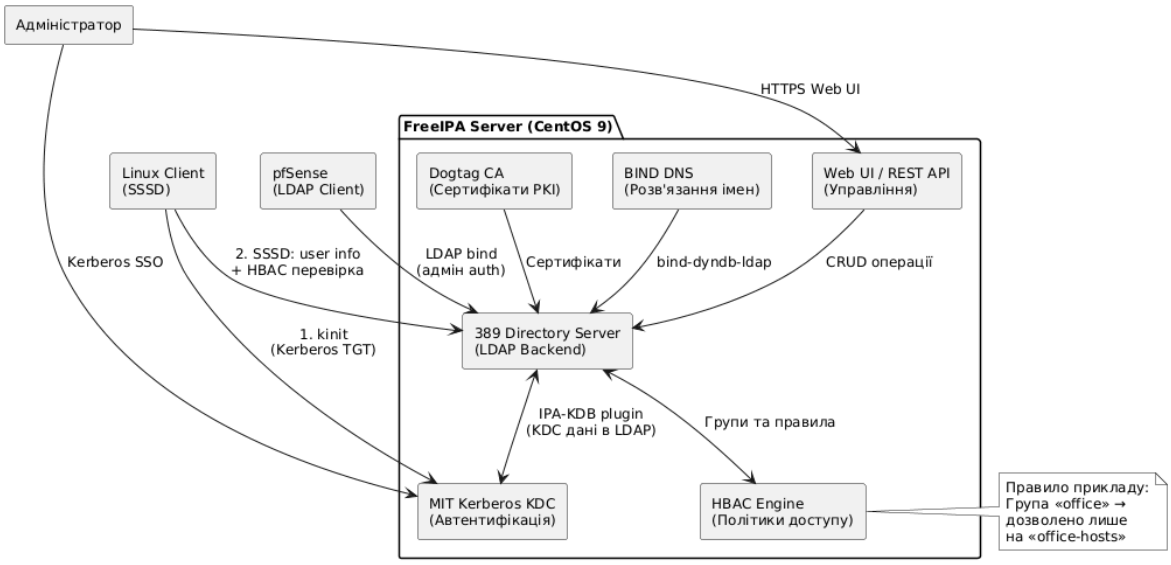


Рисунок 1.10 — Архітектура FreeIPA та взаємодія компонентів

Механізм автентифікації Kerberos

Kerberos є протоколом мережевої автентифікації, що використовує симетричне шифрування та систему «квитків» (tickets) для підтвердження ідентичності без передачі паролів мережею після початкового входу. Процес автентифікації складається з трьох кроків: клієнт звертається до Key Distribution Center (KDC) з ім'ям та зашифрованим запитом, KDC повертає Ticket Granting Ticket (TGT), після чого клієнт використовує TGT для отримання сервісних квитків (Service Tickets) до конкретних ресурсів без повторного введення пароля. Цей механізм реалізує принцип SSO (Single Sign-On) і забезпечує взаємну автентифікацію: не лише сервер перевіряє клієнта, а й клієнт перевіряє справжність сервера.

У FreeIPA Kerberos є основним механізмом автентифікації: навіть операції з LDAP-каталогом виконуються через SASL/GSSAPI з використанням Kerberos-квитків, що забезпечує захист від перехоплення облікових даних.

Механізм авторизації HBAC

Host-Based Access Control (HBAC) є вбудованим механізмом авторизації FreeIPA, що дозволяє визначати детальні правила «хто може заходити на які хости і через які сервіси». Правило HBAC складається з чотирьох елементів: суб'єкт (користувач або група), цільовий хост (хост або група хостів), сервіс (SSH, sudo, login тощо) та дія (дозволити або заборонити).

HBAC є прямою реалізацією принципу Least Privilege у Zero Trust-архітектурі: замість надання широкого доступу всім автентифікованим користувачам, кожне правило явно визначає мінімально необхідний рівень доступу для конкретної групи. Наприклад, група office-users може мати дозвіл SSH лише до робочих станцій у VLAN 10, але не до серверів у VLAN 20 — і це правило застосовується централізовано без конфігурації кожного сервера окремо.

Вбудований центр сертифікації (CA)

FreeIPA включає вбудований центр сертифікації на базі Dogtag, що дозволяє видавати X.509-сертифікати для хостів та сервісів інфраструктури. Це забезпечує можливість взаємної TLS-автентифікації між компонентами, що відповідає принципу «Verify Explicitly» Zero Trust. Зокрема, сертифікати можуть використовуватися для автентифікації pfSense при LDAP-підключенні до FreeIPA замість простого пароля.

Порівняльний аналіз рішень управління ідентичностями

Для обґрунтування вибору FreeIPA як компонента IdP у реалізованій архітектурі проведено порівняння з основними альтернативами: Microsoft Active Directory та OpenLDAP. Результати порівняння наведено у таблиці 1.4.

Таблиця 1.4

Порівняльний аналіз рішень управління ідентичностями

Критерій	**FreeIPA**	**Microsoft Active Directory**	**OpenLDAP**
Ліцензія	Відкритий код (GPLv3)	Комерційна (Windows Server + CAL)	Відкритий код
Базова ОС	Linux (RHEL/CentOS /Fedora)	Windows Server	Крос-платформний
Протоколи автентифікації	Kerberos, LDAP, SASL	Kerberos, NTLM, LDAP	LDAP, SASL
Контроль доступу	HBAC (вбудований)	Group Policy (GPO)	Відсутній нативно
Вбудований CA (PKI)	Так (Dogtag)	Так (ADCS)	Ні

Продовження табл. 1.4

Порівняльний аналіз рішень управління ідентичностями

Критерій	**FreeIPA**	**Microsoft Active Directory**	**OpenLDAP**
Веб-інтерфейс управління	Так (вбудований)	Так (ADAC, ADUC)	Сторонні інструменти
REST API	Так (JSON-RPC API)	Обмежено (PowerShell)	Ні
Інтеграція з pfSense	LDAP (підтримується)	LDAP (підтримується)	LDAP (підтримується)
Підтримка Linux-клієнтів	Відмінна (рідна)	Задовільна (через winbind/sssd)	Хороша
Репліка / HA	Multi-master реплікація	Вбудована (DC реплікація)	Потребує ручного налаштування
Складність розгортання	Середня (автоматизований інсталятор)	Відносно проста (у Windows-середовищі)	Висока (ручне налаштування схем)
Вартість	Безкоштовно	Платна (ліцензія Windows Server)	Безкоштовно
Відповідність Zero Trust	Висока (HBAC, Kerberos, CA, LDAP)	Висока (GPO, Kerberos, ADCS)	Низька (тільки каталог)

Аналіз таблиці 1.4 дозволяє зробити наступні висновки. Microsoft Active Directory є найбільш зрілим та функціональним рішенням, однак вимагає ліцензування Windows Server та Client Access Licenses (CAL), що суттєво збільшує вартість інфраструктури. У Linux-орієнтованих середовищах AD потребує додаткових компонентів (winbind або sssd) для повноцінної інтеграції. OpenLDAP є максимально гнучким рішенням, однак позбавлений вбудованих механізмів Kerberos, HBAC та PKI, що вимагає ручного налаштування всіх цих компонентів та призводить до значного зростання складності адміністрування. FreeIPA займає оптимальну нішу: безкоштовне рішення, що нативно інтегрує LDAP, Kerberos, HBAC та CA в єдину систему з зручним веб-інтерфейсом, орієнтоване на Linux-середовища.

Інтеграція FreeIPA з мережевою інфраструктурою

У контексті реалізованої архітектури FreeIPA інтегрується з двома ключовими компонентами: pfSense та Linux-клієнтами.

Інтеграція з pfSense через LDAP. pfSense підтримує автентифікацію адміністраторів через зовнішній LDAP-сервер. При налаштуванні LDAP-підключення до FreeIPA pfSense виконує bind-запит до 389 Directory Server, перевіряє наявність користувача у визначеній групі (наприклад, cn=admins,cn=groups,cn=accounts,dc=lab,dc=local) та надає або відхиляє доступ до веб-інтерфейсу. Це забезпечує централізоване управління обліковими записами адміністраторів: блокування акаунту у FreeIPA миттєво позбавляє доступу до pfSense без окремого налаштування, що є прямою реалізацією принципу «Verify Explicitly».

Інтеграція з Linux-клієнтами через SSSD та Kerberos. На Linux-клієнтах встановлюється SSSD (System Security Services Daemon) — компонент, що забезпечує PAM/NSS-інтеграцію з FreeIPA. При вході користувача: SSSD звертається до Kerberos KDC за квитком автентифікації, отримує атрибути користувача з LDAP-каталогу та перевіряє HBAC-правила — чи має цей користувач право входу на даний хост через даний сервіс. Весь процес відбувається прозоро для користувача, забезпечуючи SSO в межах домену FreeIPA.

Схему інтеграції FreeIPA з компонентами інфраструктури наведено на рисунку 1.11.

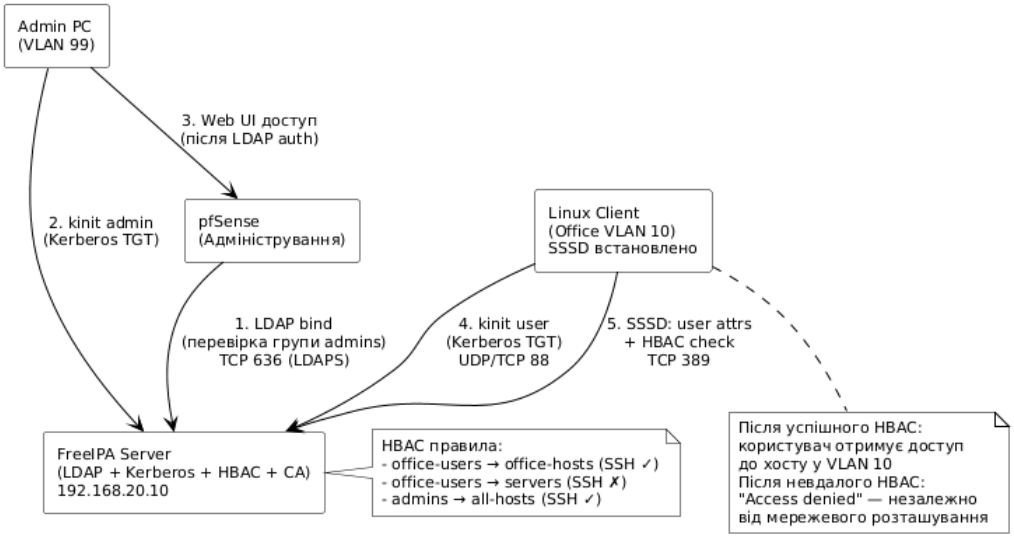


Рисунок 1.11 — Інтеграція FreeIPA з компонентами захищеної інфраструктури

Таким чином, FreeIPA у реалізованій архітектурі виконує роль **Identity Provider** — центрального компонента, що реалізує перший і найважливіший стовп моделі CISA ZTMM (таблиця 1.1). Поєднання Kerberos-автентифікації, HBAC-авторизації та вбудованого CA дозволяє забезпечити принцип «ніколи не довіряй, завжди перевіряй» на рівні кожного окремого запиту доступу незалежно від мережевого розташування суб'єкта. Саме інтеграція трьох підсистем — pfSense (периметровий захист), Cisco IOS (мережева сегментація) та FreeIPA (управління ідентичностями) — формує повноцінну Zero Trust-архітектуру, проектування та реалізація якої описуються у наступних розділах роботи.

Висновок до першого розділу

У першому розділі проведено комплексний аналіз сучасного стану захисту мережних інфраструктур, який довів неефективність традиційної периметральної моделі безпеки перед розширеними постійними загрозами, програмами-вимагачами та атаками з використанням горизонтального переміщення. Обґрунтовано, що стратегічною відповіддю на ці виклики є перехід до парадигми Zero Trust («нульової довіри»), стандартизованої у документах NIST та CISA. Ця концепція кардинально змінює підхід до кібербезпеки, спираючись на принципи безперервної верифікації кожного мережевого запиту, суворої мікросегментації та надання суб'єктам доступу

виключно мінімально необхідних привілеїв, незалежно від їхнього розташування в інфраструктурі.

На основі порівняльного аналізу рішень від провідних виробників спроектовано багаторівневу архітектуру захисту, що інтегрує три ключові підсистеми: засіб периметрового захисту та контролю політик на базі pfSense CE, механізми мікросегментації та ізоляції трафіку під управлінням Cisco IOS, а також систему управління ідентичностями FreeIPA як фундамент авторизації. Сформований теоретичний базис та обґрунтований вибір програмно-апаратного інструментарію створюють надійне підґрунтя для переходу до практичної частини дослідження — розгортання комплексного тестового стенда в середовищі мережевого моделювання, конфігурування обраних рішень та тестування ефективності політик доступу, що буде детально розглянуто у другому розділі.

РОЗДІЛ 2. ПРОЄКТУВАННЯ АРХІТЕКТУРИ ZERO TRUST НА БАЗІ PFSENSE ТА ОБЛАДНАННЯ CISCO

2.1 Постановка завдання та вимоги до інфраструктури

Предметом практичної реалізації у даній роботі є захищена мережна інфраструктура організації, що моделює типове корпоративне середовище з кількома функціонально відокремленими сегментами. Вибір сценарію обумовлений тим, що саме такий тип інфраструктури є найпоширенішим у реальних організаціях і водночас найбільш вразливим при застосуванні традиційного периметрального підходу: наявність декількох сегментів із різними вимогами до доступу вимагає чіткого міжзонового контролю, що є прямим застосуванням принципів Zero Trust, розглянутих у розділі 1.

Модельоване середовище складається з чотирьох мережевих сегментів з різними рівнями довіри та вимогами до захисту:

- Сегмент Office (VLAN 10) — робочі станції співробітників організації. Користувачі цього сегменту потребують доступу до певних серверних ресурсів (файловий сервер, вебзастосунки), однак не повинні мати прямого доступу до інфраструктурних сервісів (FreeIPA, управлінські інтерфейси). Це сегмент з найменшим рівнем довіри — кінцеві пристрої є найбільш вразливими до компрометації через фішинг та зловмисне програмне забезпечення.
- Сегмент Servers (VLAN 20) — серверна інфраструктура, у тому числі сервер FreeIPA (Identity Provider). Доступ до цього сегменту суворо регламентований: лише дозволені потоки трафіку від Office VLAN (визначені сервіси) та повний доступ з Management VLAN.
- Сегмент Management (VLAN 99) — виключно для адміністративного доступу до мережевого обладнання та серверів. Цей сегмент має найвищий рівень привілеїв і є найбільш захищеним: доступ дозволено лише для окремих адміністративних облікових записів, автентифікованих через FreeIPA.
- DMZ (демілітаризована зона) — сегмент для публічно доступних сервісів. Ресурси DMZ ізольовані від внутрішніх сегментів: зовнішні користувачі

не можуть ініціювати з'єднання до Office або Servers VLAN, а DMZ-хости не мають доступу до внутрішньої мережі без явного дозволу.

Загальну концепцію сегментації модельованого середовища наведено на рисунку 2.1.

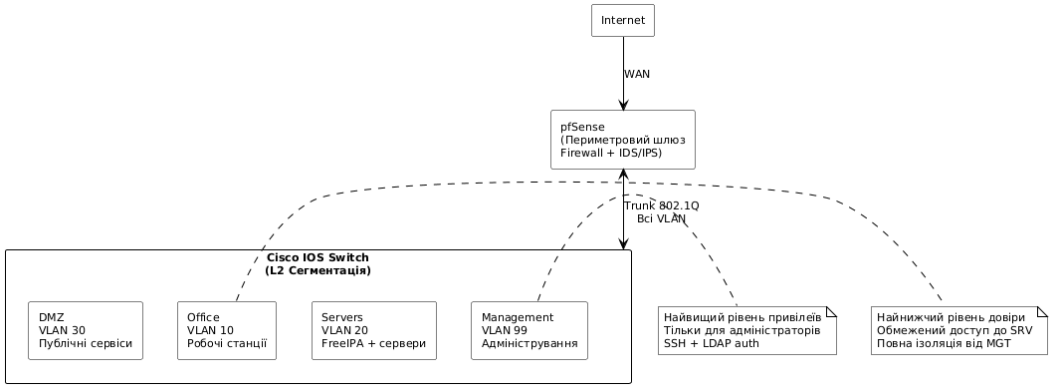


Рисунок 2.1 — Концептуальна схема сегментації мережі організації

Функціональні вимоги визначають конкретні можливості, якими має володіти реалізована інфраструктура. Вони сформульовані на основі принципів Zero Trust, розглянутих у підрозділі 1.2, та практичних потреб типового середовища організації.

Вимога Ф-1. Мережева сегментація. Інфраструктура повинна забезпечувати логічну ізоляцію не менше чотирьох мережевих сегментів (VLAN) з різними рівнями привілеїв. Трафік між сегментами має проходити виключно через pfSense, де застосовуються явні правила фільтрації. Широкомовний трафік (broadcast) кожного VLAN не повинен виходити за межі відповідного сегменту.

Вимога Ф-2. Міжзоновий контроль доступу. Правила firewall pfSense мають реалізовувати принцип «заборонено за замовчуванням» (default deny): весь міжзоновий трафік забороняється, якщо не визначений явний дозвільний правило. Дозволені лише конкретні потоки: VLAN 10 → VLAN 20 тільки для визначених портів (HTTP/S, SSH за потреби); VLAN 99 → усі сегменти (адміністративний доступ); VLAN 20 та VLAN 30 → обмежений вихід у WAN.

Вимога Ф-3. Централізована автентифікація. Автентифікація адміністраторів pfSense повинна виконуватися через FreeIPA за протоколом LDAP. Доступ Linux-хостів у сегменті Servers має контролюватися через HBAC-політики FreeIPA: користувачі групи office-users не повинні мати SSH-доступу

до серверів VLAN 20 навіть при наявності мережевого з'єднання. Локальні облікові записи адміністраторів pfSense мають використовуватися виключно як резервний засіб доступу.

Вимога Ф-4. Виявлення та запобігання вторгнень (IDS/IPS). На pfSense має бути налаштований Snort у режимі inline (IPS): при виявленні сигнатури мережевого сканування або відомої атаки — трафік блокується, генерується alert. Набори правил: Talos Community або Emerging Threats Open.

Вимога Ф-5. Централізоване журналювання. Cisco IOS та pfSense повинні передавати системні повідомлення на централізований Syslog-сервер. Журналювання охоплює: спрацювання ACL на Cisco (з ключовим словом log), Port Security violations, IDS-alerts від Snort, події автентифікації pfSense.

Вимога Ф-6. Захищене адміністрування мережевого обладнання. Доступ до CLI Cisco IOS дозволяється виключно через SSH v2 з VLAN 99 (Management). Протокол Telnet має бути вимкнений. Доступ до веб-інтерфейсу pfSense — тільки з VLAN 99 через HTTPS.

Нефункціональні вимоги до інфраструктури

Нефункціональні вимоги визначають якісні характеристики інфраструктури — не «що вона робить», а «як вона це робить».

Вимога НФ-1. Керованість. Усі компоненти мають бути керованими через централізовані інтерфейси: pfSense — через веб-GUI з VLAN 99; Cisco IOS — через SSH з VLAN 99; FreeIPA — через веб-інтерфейс з VLAN 99. Зміни в обліковому записі у FreeIPA мають негайно відображатися на всіх інтегрованих компонентах без ручного перезапуску сервісів.

Вимога НФ-2. Масштабованість. Архітектура повинна допускати розширення без принципової зміни дизайну: додавання нового VLAN-сегменту має вимагати лише конфігурації нового субінтерфейсу на pfSense, нового VLAN на Cisco та нової групи хостів у FreeIPA. Кількість хостів у межах одного VLAN може зростати без зміни топології.

Вимога НФ-3. Відтворюваність у лабораторному середовищі. Уся інфраструктура має бути відтворена у середовищі GNS3 + VirtualBox без

використання фізичного обладнання. Конфігурації всіх компонентів мають бути задокументовані у вигляді, що дозволяє повне відтворення стенду. Це вимагає використання образів, що є загальнодоступними: pfSense CE ISO (netgate.com), Cisco IOSvL2 (офіційний образ для GNS3), CentOS9, Ubuntu 22.04 LTS (ubuntu.com).

Вимога НФ-4. Мінімальний вплив на продуктивність. Увімкнення IDS/IPS (Snort) на pfSense не повинно знижувати пропускну здатність більш ніж на 30% від базового рівня маршрутизації, що відповідає типовим показникам для середнього навантаження мережі організації.

Узагальнення функціональних та нефункціональних вимог у вигляді структурованої таблиці наведено у таблиці 2.1.

Таблиця 2.1

Зведені вимоги до захищеної мережної інфраструктури

№	**Вимога**	**Тип**	**Компонент реалізації**
Ф-1	Мережева сегментація (≥4 VLAN)	Функціональна	Cisco IOS
Ф-2	Міжзоновий контроль (default deny)	Функціональна	pfSense
Ф-3	Централізована автентифікація LDAP+HBAC	Функціональна	FreeIPA
Ф-4	IDS/IPS (Snort, inline)	Функціональна	pfSense + Snort
Ф-5	Централізоване журналювання (Syslog)	Функціональна	Cisco + pfSense
Ф-6	Захищене адміністрування (SSH v2, HTTPS)	Функціональна	Cisco + pfSense
НФ-1	Централізована керованість	Нефункціональна	Усі компоненти
НФ-2	Масштабованість (VLAN, хости)	Нефункціональна	Cisco + pfSense
НФ-3	Відтворюваність (GNS3+VirtualBox)	Нефункціональна	Лабораторне середовище
НФ-4	Вплив IDS на продуктивність ≤30%	Нефункціональна	pfSense + Snort

Сформульовані вимоги є основою для прийняття архітектурних рішень у підрозділі 2.2 та проектування топології мережі у підрозділі 2.3. Кожне технічне рішення, що описується у наступних підрозділах, обґрунтовується через відповідність конкретним вимогам, визначеним у таблиці 2.1.

2.2 Обґрунтування архітектурних рішень

Архітектура захищеної мережної інфраструктури, що проектується у даній роботі, базується на трирівневій моделі безпеки, де кожен рівень відповідає за конкретний домен захисту відповідно до стовпів CISA ZTMM (підрозділ 1.2): периметровий захист (pfSense), мережева сегментація (Cisco IOS), управління ідентичностями (FreeIPA). Принциповою відмінністю від традиційного підходу є те, що жоден із цих рівнів не є самодостатнім: периметровий захист сам по собі не забезпечує ізоляції внутрішніх сегментів, а сегментація без централізованої автентифікації не гарантує контролю доступу на рівні ідентичності. Лише інтеграція трьох компонентів формує повноцінну Zero Trust-архітектуру.

При виборі конкретних рішень для кожного рівня враховувались такі критерії: відповідність вимогам, визначеним у підрозділі 2.1; доступність у лабораторному середовищі GNS3 + VirtualBox; наявність документації та академічних прецедентів використання; можливість інтеграції між компонентами. Результатом є архітектура, що складається з чотирьох активних компонентів: pfSense CE, Cisco IOSvL2, FreeIPA на CentOS Stream 9 та набору Ubuntu 22.04 LTS-серверів і клієнтів.

pfSense як периметровий шлюз та router-on-a-stick

Роль у архітектурі

pfSense виконує у проектованій архітектурі дві нерозривно пов'язані функції. По-перше, це периметровий шлюз — єдина точка входу та виходу для трафіку між внутрішніми сегментами та мережею WAN (Internet). Весь трафік, що покидає або входить до внутрішніх VLAN, проходить через pfSense, де застосовуються правила stateful firewall, NAT та IDS/IPS (Snort). По-друге, pfSense є router-on-a-stick — маршрутизатором, що обслуговує міжзонову

маршрутизацію між усіма внутрішніми VLAN через єдиний фізичний або віртуальний інтерфейс за допомогою субінтерфейсів (VLAN Parent Interface + VLAN subinterfaces).

Концепція router-on-a-stick

Технологія router-on-a-stick передбачає підключення маршрутизатора (у даному випадку — pfSense) до комутатора через єдиний trunk-канал 802.1Q. На стороні pfSense для кожного VLAN створюється окремий субінтерфейс з власною IP-адресою, яка стає шлюзом за замовчуванням для хостів відповідного VLAN. Трафік між VLAN 10 і VLAN 20, наприклад, надходить з комутатора на pfSense із тегом VLAN 10, де pfSense приймає рішення на основі firewall-правил та перенаправляє пакет назад на комутатор із тегом VLAN 20. Це означає, що весь міжзоновий трафік обов'язково проходить через pfSense — саме тут застосовуються правила Zero Trust.

Перевагою цього підходу в лабораторному середовищі є мінімальна кількість необхідних фізичних або віртуальних інтерфейсів: достатньо одного trunk-з'єднання між pfSense та Cisco IOSvL2, що спрощує топологію та знижує вимоги до апаратного забезпечення. Схему router-on-a-stick у контексті проектованої архітектури наведено на рисунку 2.2.

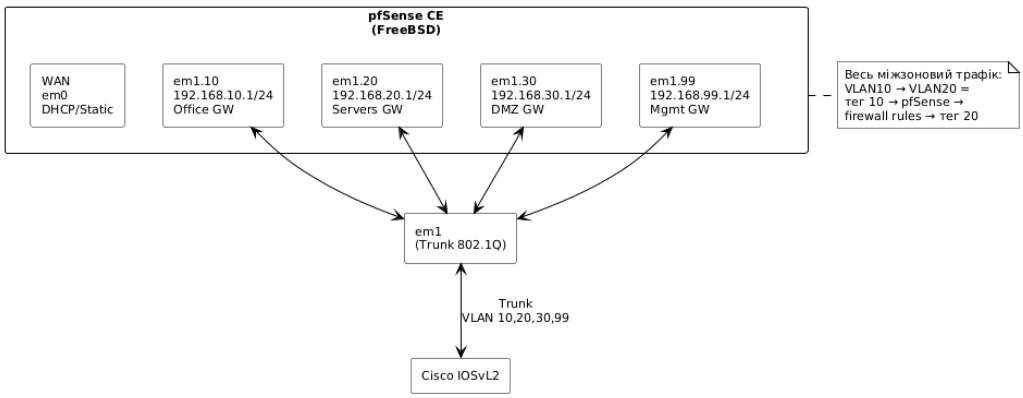


Рисунок 2.2 — Принцип router-on-a-stick: pfSense як центр міжзонової маршрутизації

Функціонал pfSense у реалізованій архітектурі

У проектованій архітектурі pfSense реалізує такі функції:

- Stateful Firewall з правилами per-VLAN-interface, що реалізують матрицю дозволів міжзонового трафіку (підрозділ 2.3). Базовий принцип

— default deny: весь трафік між VLAN забороняється, якщо не визначено явне дозвільне правило

- NAT/PAT для виходу внутрішніх VLAN в Internet через зовнішній WAN-інтерфейс
- DHCP-сервер для кожного VLAN з видачею відповідних шлюзів та DNS
- IDS/IPS на базі Snort у режимі inline для аналізу вхідного WAN-трафіку та міжзонового трафіку
- LDAP-клієнт до FreeIPA для автентифікації адміністраторів веб-інтерфейсу pfSense
- Syslog-клієнт: передача системних подій та IDS-alerts на централізований Syslog-сервер Ubuntu (VLAN 20)

Cisco IOSvL2 як комутатор рівня доступу

Роль у архітектурі

Cisco IOSvL2 виконує роль комутатора рівня доступу (access layer switch), що безпосередньо підключає кінцеві пристрої та здійснює їхню L2-ізоляцію за допомогою VLAN. IOSvL2 є офіційним віртуальним образом Cisco IOS для емуляції функцій L2-комутації, що підтримує повний набір функцій: 802.1Q VLAN, VTP, STP, port security, ACL.

Ключовим аспектом є розподіл відповідальності між Cisco IOSvL2 та pfSense: Cisco відповідає за L2-ізоляцію (VLAN-тегування, port security, широкомовна ізоляція), тоді як pfSense відповідає за L3-фільтрацію (firewall rules між VLAN, IDS/IPS). Такий поділ відповідає принципу Defense in Depth і є відображенням моделі PEP (Cisco) + PE (pfSense) зі стандарту NIST SP 800-207 (рисунок 1.4).

Конфігурація Cisco IOSvL2 у проектованій архітектурі

На Cisco IOSvL2 реалізуються такі механізми:

VLAN та призначення портів — кожен порт комутатора налаштовується в режимі access з відповідним VLAN. Trunk-порт у бік pfSense налаштовується з командою switchport mode trunk та явним переліком дозволених VLAN (switchport trunk allowed vlan 10,20,30,99).

Port Security — на access-портах VLAN 10 та VLAN 20 активується Port Security з максимальною кількістю MAC-адрес = 1 та режимом порушення shutdown. Це унеможливлює підключення несанкціонованих пристроїв або підміну MAC-адреси.

ACL на VTY-лініях — SSH-доступ до CLI Cisco дозволяється виключно з VLAN 99 (Management). Стандартний ACL застосовується командою access-class на лініях line vty 0 4, блокуючи підключення з усіх інших підмереж.

Syslog — передача системних подій на Syslog-сервер у VLAN 20 за допомогою команди logging host 192.168.20.X.

SSH v2 — Telnet повністю відключається (transport input ssh), генерується RSA-ключ довжиною 2048 біт.

FreeIPA на CentOS Stream 9 як централізований IdP

Роль у архітектурі

FreeIPA виконує роль централізованого Identity Provider (IdP) для всієї інфраструктури. FreeIPA версії 4.11, доступна у репозиторіях CentOS Stream 9, надає повний стек ідентифікаційних сервісів: 389 Directory Server (LDAP), MIT Kerberos 5 KDC, DNS, Dogtag CA та механізм HBAC. CentOS Stream 9 обрано як платформу для розгортання FreeIPA.

Інтеграція з компонентами інфраструктури

FreeIPA інтегрується з двома класами компонентів:

Інтеграція з pfSense (LDAP-автентифікація адміністраторів). pfSense налаштовується як LDAP-клієнт до FreeIPA: у розділі System → User Manager → Authentication Servers вказується адреса FreeIPA-сервера (LDAPS, TCP 636), base DN та bind credentials. Адміністратор pfSense автентифікується через FreeIPA-групу admins: лише члени цієї групи отримують доступ до веб-інтерфейсу pfSense. Відповідно до вимоги Ф-3, локальний адміністративний обліковий запис pfSense залишається лише як резервний.

Інтеграція з Ubuntu-клієнтами та серверами (SSSD + Kerberos). На Ubuntu 22.04 LTS клієнтах та серверах встановлюється пакет freeipa-client, що виконує автоматичне налаштування SSSD, Kerberos (/etc/krb5.conf), NSS та PAM. Після

приєднання до домену FreeIPA (ipa-client-install) автентифікація користувачів здійснюється через Kerberos, а HBAC-правила контролюють доступ до кожного хосту окремо.

Об'єкти FreeIPA у проектованій архітектурі

У FreeIPA створюються такі об'єкти:

- Групи користувачів: admins (адміністратори), office-users (співробітники Office VLAN)
- Групи хостів: office-hosts (Ubuntu-клієнти VLAN 10), server-hosts (Ubuntu-сервери VLAN 20)
- HBAC-правила:

office-access: група office-users → хости office-hosts → сервіс sshd — дозволено

admin-access: група admins → всі хости → всі сервіси — дозволено

default-deny: усім іншим — заборонено (вбудоване правило FreeIPA deny_all)

Ubuntu 22.04 LTS як платформа серверних сервісів

Ubuntu 22.04 LTS (Jammy Jellyfish) використовується як платформа для чотирьох типів вузлів у проектованій архітектурі, що визначається широкою підтримкою пакетів, стабільністю LTS-релізу та безпосередньою підтримкою freeipa-client:

Веб-сервер (VLAN 30 / DMZ) — Apache HTTP Server або Nginx для емуляції корпоративного вебзастосунку. Доступ до веб-сервера регулюється firewall-правилами pfSense: з Office VLAN та WAN дозволено TCP 80/443, з усіх інших сегментів — заборонено.

Сервер бази даних (VLAN 20 / Servers) — MariaDB як реляційна СУБД. Ресурс повністю ізольований від прямого доступу з Office VLAN та WAN: виключно веб-сервер із сегменту DMZ має дозвіл на підключення по порту TCP 3306, що жорстко контролюється L3-правилами на інтерфейсах pfSense.

Syslog-сервер (VLAN 20) — rsyslog або Graylog для централізованого збору та зберігання журналів від Cisco IOS та pfSense. Отримує UDP/TCP 514 від усіх компонентів інфраструктури.

Клієнтські робочі станції (VLAN 10) — Ubuntu Desktop 22.04 LTS, що моделюють робочі місця співробітників.

Матриця відповідності компонентів принципам Zero Trust , наведена у таблиці 2.2.

Таблиця 2.2

Матриця відповідності компонентів архітектури принципам Zero Trust

Принцип Zero Trust	**Тенет NIST SP 800-207**	**Стовп CISA ZTMM**	**Компонент**	**Механізм реалізації**
Never Trust, Always Verify	Доступ — per-request, з урахуванням ідентичності	Identity	FreeIPA	Kerberos-автентифікація кожного входу; LDAP-перевірка адміністратора pfSense
Least Privilege	Мінімальні привілеї, динамічно	Identity, Networks	FreeIPA + pfSense	HBAC-правила: office-users → тільки office-hosts; default deny на pfSense
Assume Breach	Мікросегментація, мінімізація радіуса ураження	Networks	Cisco IOSvL2 + pfSense	VLAN-ізоляція: компрометація VLAN 10 не надає доступу до VLAN 20/99
Verify Explicitly	Усі ресурси захищені незалежно від розташування	Devices	Cisco IOSvL2	Port Security: контроль MAC на кожному порту

Продовження табл. 2.2

Матриця відповідності компонентів архітектури принципам Zero Trust

Принцип Zero Trust	**Тенет NIST SP 800-207**	**Стовп CISA ZTMM**	**Компонент**	**Механізм реалізації**
Assume Breach	Шифрування внутрішнього трафіку адміністрування	Identity	Cisco + pfSense	SSH v2 (Cisco VTY), HTTPS (pfSense WebGUI), LDAPS (FreeIPA)
Continuous Monitoring	Журналювання та аналіз усіх запитів	Data	pfSense + Cisco + Ubuntu	Syslog → Ubuntu Syslog Server; Snort alerts; ACL log
Assume Breach	Виявлення та блокування вторгнень	Networks	pfSense + Snort	IPS inline-режим: блокування відомих сигнатур на WAN та між VLAN

Аналіз таблиці 2.2 демонструє, що проектована архітектура охоплює всі три фундаментальні принципи Zero Trust та всі п'ять стовпів CISA ZTMM, задіяних у межах мережевої та ідентифікаційної підсистем. Єдиним стовпом, що реалізований лише частково, є Applications & Workloads: контроль доступу до застосунків здійснюється на рівні pfSense-правил (порти та IP), однак повноцінна інспекція L7-трафіку та автентифікація на рівні застосунку виходять за межі даної роботи та можуть бути предметом подальших досліджень.

Таким чином, обрана комбінація pfSense CE + Cisco IOSvL2 + FreeIPA (CentOS Stream 9) + Ubuntu 22.04 LTS є технічно обґрунтованою, взаємно сумісною та повністю відтворюваною у лабораторному середовищі GNS3 + VirtualBox. Детальне проектування топології мережі на основі прийнятих архітектурних рішень виконується у підрозділі 2.3.

2.3 Проектування топології мережі

Топологія проектованої захищеної мережної інфраструктури базується на ієрархічній моделі з чітким розмежуванням функцій між рівнями та зонами. Центральним вузлом є pfSense, через який проходить весь міжзоновий та WAN-

трафік. Cisco IOSvL2 виконує функцію access-layer комутатора, що фізично підключає всі кінцеві вузли. FreeIPA на CentOS Stream 9 розташовано у сегменті Servers як критичний сервіс інфраструктури, до якого застосовуються найбільш суворі правила доступу.

Структурна схема топології наведена на рисунку 2.3.

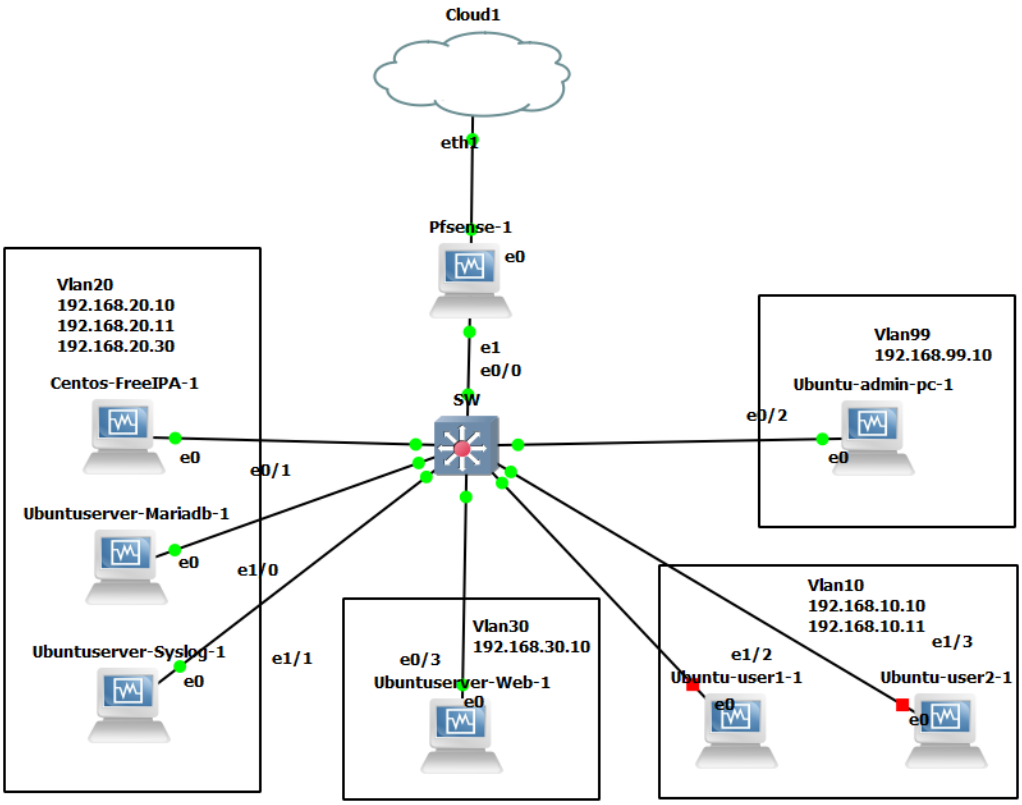


Рисунок 2.3 — Структурна схема захищеної мережної інфраструктури

Таблиця VLAN-сегментації та адресного простору

Адресний простір проектованої інфраструктури визначено відповідно до RFC 1918 — стандарту приватних IPv4-адрес. Для кожного сегменту виділено підмережу /24, що забезпечує достатній ресурс адрес для лабораторного середовища та легко масштабується. Детальний план адресації та сегментації наведено у таблиці 2.3.

Таблиця 2.3

План VLAN-сегментації та адресного простору

VLAN	Назва	Підмережа	Шлюз (pfSense)	Діапазон хостів	Призначення
—	WAN	DHCP / 10.0.0.0/24	10.0.0.1 (GNS3 NAT)	—	Вихід в Інтернет (GNS3 NAT Cloud)
10	Office	192.168.10.0/24	192.168.10.1	.10 – .254	Робочі станції співробітників
20	Servers	192.168.20.0/24	192.168.20.1	.10 – .254	FreeIPA, DB, Syslog
30	DMZ	192.168.30.0/24	192.168.30.1	.10 – .254	Веб-сервер (публічно доступний)
99	Management	192.168.99.0/24	192.168.99.1	.10 – .254	Адміністративний доступ

Адреси конкретних вузлів інфраструктури наведено у таблиці 2.4.

Таблиця 2.4

Таблиця адресації вузлів інфраструктури

Вузол	ОС / Платформа	VLAN	IP-адреса	Роль
pfSense	FreeBSD (pfSense CE)	WAN	DHCP (em0)	Периметровий шлюз, Firewall, IDS/IPS
pfSense	FreeBSD (pfSense CE)	10	192.168.10.1	GW Office, DHCP-server VLAN10
pfSense	FreeBSD (pfSense CE)	20	192.168.20.1	GW Servers, DHCP-server VLAN20
pfSense	FreeBSD (pfSense CE)	30	192.168.30.1	GW DMZ, DHCP-server VLAN30
pfSense	FreeBSD (pfSense CE)	99	192.168.99.1	GW Management, DHCP-server VLAN99
Cisco IOSvL2	Cisco IOS	99	192.168.99.2 (SVI)	L2-комутатор, SSH-управління
FreeIPA Server	CentOS Stream 9	20	192.168.20.10	IdP: LDAP, Kerberos, HBAC, DNS, CA
DB Server	Ubuntu 22.04 LTS	20	192.168.20.20	MariaDB (база даних)

Продовження табл 2.4

Таблиця адресації вузлів інфраструктури

Вузол	**ОС / Платформа**	**VLAN**	**IP-адреса**	**Роль**
Syslog Server	Ubuntu 22.04 LTS	20	192.168.20.30	rsyslog (централізоване журналювання)
Web Server	Ubuntu 22.04 LTS	30	192.168.30.10	Apache/Nginx (вебзастосунок, DMZ)
Client-1	Ubuntu 22.04 LTS	10	192.168.10.10	Робоча станція співробітника
Client-2	Ubuntu 22.04 LTS	10	192.168.10.11	Робоча станція співробітника
Admin PC	Ubuntu 22.04 LTS	99	192.168.99.10	Адміністративна станція

Єдине фізичне або віртуальне з'єднання між pfSense та Cisco IOSvL2 є trunk-каналом стандарту 802.1Q, що передає тегований трафік усіх чотирьох VLAN одночасно. На стороні Cisco порт налаштовано у режимі trunk, на стороні pfSense — батьківський інтерфейс em1 з чотирма субінтерфейсами. Схему конфігурації trunk-з'єднання та розподілу портів Cisco наведено на рисунку 2.4.

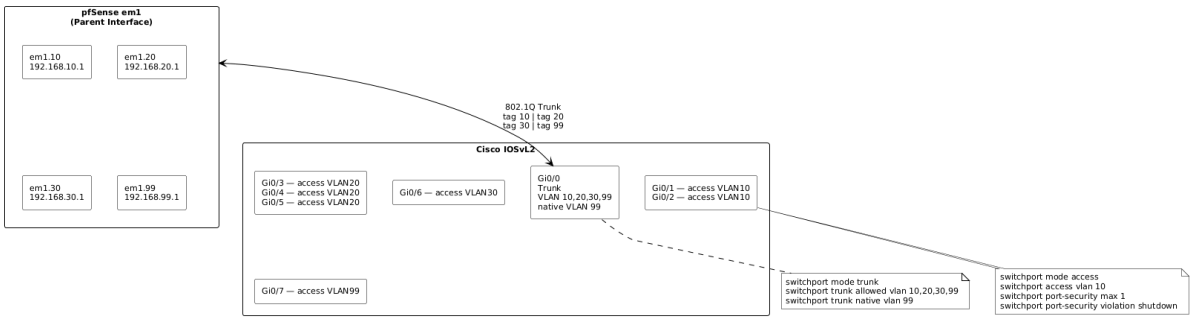


Рисунок 2.4 — Схема trunk-з'єднання pfSense - Cisco та розподіл портів по VLAN

Детальний розподіл портів комутатора Cisco IOSvL2 між VLAN-сегментами наведено у таблиці 2.5.

Матриця дозволів міжзонового трафіку є ключовим проектним документом, що визначає правила firewall на pfSense. Базовий принцип — default deny: будь-який трафік між VLAN за замовчуванням заблокований, дозволяються лише явно визначені потоки.

Таблиця 2.5

Розподіл портів Cisco IOSvL2 по VLAN

Порт	**Режим**	**VLAN**	**Підключений вузол**	**Port Security**
Gi0/0	Trunk	10, 20, 30, 99	pfSense em1	Вимкнено (trunk)
Gi0/1	Access	10	Ubuntu Client-1 (192.168.10.10)	Max 1 MAC, violation: shutdown
Gi0/2	Access	10	Ubuntu Client-2 (192.168.10.11)	Max 1 MAC, violation: shutdown
Gi0/3	Access	20	FreeIPA / CentOS Stream 9 (192.168.20.10)	Max 1 MAC, violation: shutdown
Gi0/4	Access	20	DB Server / Ubuntu (192.168.20.20)	Max 1 MAC, violation: shutdown
Gi0/5	Access	20	Syslog Server / Ubuntu (192.168.20.30)	Max 1 MAC, violation: shutdown
Gi0/6	Access	30	Web Server / Ubuntu (192.168.30.10)	Max 1 MAC, violation: shutdown

Матриця розроблена відповідно до вимог Ф-2 (підрозділ 2.1) та принципу Least Privilege Zero Trust-архітектури та наведена у таблиці 2.6.

Таблиця 2.6

Матриця дозволів міжзонового трафіку (правила pfSense firewall)

Джерело	**Призначення**	**Протокол / Порт**	**Дія**	**Обґрунтування**
VLAN 10 (Office)	192.168.20.10 (FreeIPA)	TCP/UDP 88	**Permit**	Kerberos-автентифікація клієнтів
VLAN 10 (Office)	192.168.20.10 (FreeIPA)	TCP 389	**Permit**	LDAP (SSSD — отримання атрибутів)
VLAN 10 (Office)	192.168.20.10 (FreeIPA)	UDP 53	**Permit**	DNS (FreeIPA як DNS-сервер)
VLAN 10 (Office)	192.168.30.10 (Web Server)	TCP 80, 443	**Permit**	Доступ до корпоративного вебзастосунку
VLAN 10 (Office)	VLAN 20 (решта)	Any	**Deny**	Клієнти не мають доступу до DB, Syslog

Продовження табл. 2.6

Матриця дозволів міжзонового трафіку (правила pfSense firewall)

Джерело	**Призначення**	**Протокол / Порт**	**Дія**	**Обґрунтування**
VLAN 10 (Office)	VLAN 99 (Management)	Any	**Deny**	Ізоляція управлінського сегменту
VLAN 10 (Office)	WAN	TCP 80, 443	**Permit**	Доступ до Інтернету
VLAN 10 (Office)	WAN (решта)	Any	**Deny**	Обмеження вихідного трафіку
VLAN 30 (DMZ)	192.168.20.20 (DB)	TCP 3306	**Permit**	Web Server → MariaDB
VLAN 30 (DMZ)	192.168.20.30 (Syslog)	UDP 514	**Permit**	Передача логів Web Server
VLAN 30 (DMZ)	VLAN 10, VLAN 99	Any	**Deny**	Ізоляція DMZ від внутрішніх сегментів
VLAN 20 (Servers)	VLAN 10	Any	**Deny**	Сервери не ініціюють з'єднань до клієнтів
VLAN 20 (Servers)	VLAN 99	Any	**Deny**	Сервери не мають доступу до Management
VLAN 20 (Servers)	WAN	TCP 80, 443	**Permit**	Оновлення пакетів ОС
VLAN 99 (Management)	VLAN 10, 20, 30	Any	**Permit**	Повний адміністративний доступ
VLAN 99 (Management)	Cisco SVI (192.168.99.2)	TCP 22	**Permit**	SSH-управління комутатором
VLAN 99 (Management)	pfSense (192.168.99.1)	TCP 443	**Permit**	HTTPS до WebGUI pfSense
WAN	VLAN 30 (DMZ)	TCP 80, 443	**Permit**	Зовнішній доступ до веб-сервера
WAN	VLAN 10, 20, 99	Any	**Deny**	Захист внутрішніх сегментів від WAN

Матриця дозволів (таблиця 2.6) є безпосередньою основою для конфігурації firewall-правил pfSense, описаної у розділі 3. Кожне правило

таблиці транслюється у конкретну конфігурацію на відповідному VLAN-інтерфейсі pfSense. Принцип default deny забезпечується наявністю фінального правила «Block all» на кожному інтерфейсі після явних дозвільних записів.

Варто підкреслити, що матриця спроектована з урахуванням мінімальних привілеїв: клієнти VLAN 10 можуть звертатись до FreeIPA лише по трьох конкретних протоколах (Kerberos, LDAP, DNS), необхідних для автентифікації, але не мають доступу до жодного іншого сервісу у VLAN 20. Аналогічно, веб-сервер у DMZ має доступ лише до конкретної IP-адреси DB Server по конкретному порту TCP 3306, що унеможливлює його використання як плацдарму для атак на решту серверної інфраструктури у разі компрометації.

Спроектована топологія є вичерпною основою для вибору засобів та середовища моделювання, що описується у підрозділі 2.4.

2.4 Вибір засобів реалізації та вимоги до середовища

Відтворення захищеної мережної інфраструктури у лабораторних умовах вимагає середовища, що забезпечує одночасну роботу мережевих пристроїв (pfSense, Cisco IOSvL2) та повноцінних віртуальних машин (CentOS Stream 9, Ubuntu 22.04 LTS) з реальною взаємодією між ними. Для цього обрано комбінацію **GNS3** (Graphical Network Simulator 3) та **VirtualBox** як гіпервізора для віртуальних машин.

GNS3 є відкритим мережевим емулятором, що дозволяє запускати реальні образи мережевих операційних систем — зокрема Cisco IOS та pfSense — у зв'язаній топології з графічним інтерфейсом. На відміну від Packet Tracer, GNS3 виконує реальний код IOS, а не його симуляцію, що забезпечує повну відповідність поведінки лабораторного стенду реальному обладнанню. GNS3 підтримує інтеграцію з VirtualBox та VMware через механізм GNS3 VM або безпосереднє підключення через хостові мережеві адаптери.

VirtualBox обрано як гіпервізор для віртуальних машин з таких міркувань: безкоштовність та відкрита ліцензія (GNU GPL), підтримка Host-Only та Internal Network адаптерів для інтеграції з GNS3, крос-платформність (Windows, Linux, macOS), мінімальні системні вимоги порівняно з VMware Workstation Pro.

VirtualBox забезпечує роботу FreeIPA (CentOS Stream 9), серверів та клієнтів Ubuntu 22.04 LTS у складі єдиної топології GNS3.

Альтернативою могла б бути платформа **EVE-NG** (Emulated Virtual Environment — Next Generation), що також підтримує Cisco IOSvL2 та VirtualBox-образи. Однак GNS3 обрано з огляду на: ширшу академічну документацію, наявність готових шаблонів для pfSense та IOSvL2, зручніший графічний інтерфейс для документування топології та безпосередню підтримку VirtualBox-інтеграції без додаткового налаштування.

Одночасна робота GNS3 з мережевими образами та VirtualBox з кількома ВМ висуває конкретні вимоги до апаратного забезпечення хостової системи. Мінімальні та рекомендовані конфігурації наведено у таблиці 2.7.

Таблиця 2.7

Вимоги до апаратного забезпечення хостової системи

Параметр	Мінімальна конфігурація	Рекомендована конфігурація
Процесор	Intel Core i5 / AMD Ryzen 5, 4 ядра, підтримка VT-x/AMD-V	Intel Core i7 / AMD Ryzen 7, 8+ ядер
Оперативна пам'ять	16 ГБ	32 ГБ
Дискова підсистема	HDD 100 ГБ вільно	SSD 100+ ГБ вільно
Операційна система	Windows 10 64-bit / Ubuntu 20.04+	Windows 11 / Ubuntu 22.04 LTS
GNS3	v2.2.x	v2.2.x (остання стабільна)
VirtualBox	v6.1.x	v7.0.x
Мережевий адаптер	1 Гбіт/с	1 Гбіт/с (необов'язково фізичний)

Для розгортання лабораторного стенду необхідно отримати чотири типи образів. Їх перелік із зазначенням джерел наведено у таблиці 2.8.

Підключення VirtualBox-машин до топології GNS3 реалізується через механізм VirtualBox Host-Only Adapter у поєднанні з GNS3 Cloud або Switch-вузлом. Для кожного VLAN у GNS3 створюється окремий Host-Only адаптер на хостовій ОС (наприклад, vboxnet0 для VLAN 10, vboxnet1 для VLAN 20 тощо). Мережевий інтерфейс кожної VirtualBox-машини налаштовується на відповідний Host-Only адаптер, що відповідає її VLAN. GNS3 підключає ці

адаптери до відповідних портів Cisco IOSvL2 через Cloud-вузли, забезпечуючи участь ВМ у тегованій VLAN-топології.

Таблиця 2.8

Необхідні образи для розгортання лабораторного стенду

Образ	**Версія**	**Джерело**	**Формат**	**Призначення**
pfSense CE ISO	2.7.x	netgate.com/downloads	ISO	pfSense у GNS3 (QEMU)
Cisco IOSvL2	15.2(CML)	Cisco Modeling Labs / GNS3 Marketplace	.qcow2	L2-комутація у GNS3
CentOS Stream 9	9 (актуальний)	mirror.stream.centos.org	ISO / qcow2	FreeIPA Server у VirtualBox
Ubuntu Server 22.04 LTS	22.04.x	ubuntu.com/download/server	ISO	DB Server, Sys-log Server, Web Server
Ubuntu Desktop 22.04 LTS	22.04.x	ubuntu.com/download/desktop	ISO	Client-1, Client-2, Admin PC

Альтернативним підходом є використання GNS3 VM — спеціальної віртуальної машини GNS3, що запускається у VirtualBox і виконує всі QEMU-процеси (pfSense, Cisco IOS) всередині себе. Це дозволяє уникнути проблем із доступом до апаратної віртуалізації (VT-x/AMD-V) безпосередньо на хості та спрощує мережеву інтеграцію. У даній роботі рекомендується саме цей підхід як більш стабільний.

Обране середовище GNS3 + VirtualBox повністю відповідає нефункціональній вимозі НФ-3 (відтворюваність у лабораторному середовищі, таблиця 2.1): усі компоненти є загальнодоступними, безкоштовними та детально задокументованими. Загальний обсяг оперативної пам'яті ~13.5 ГБ відповідає мінімальній хостовій конфігурації 16 ГБ RAM, що робить стенд доступним для розгортання на типовому навчальному або особистому комп'ютері.

Проектована топологія (підрозділ 2.3), план адресації (таблиця 2.4), матриця трафіку (таблиця 2.6) у сукупності формують повну проектну

документацію, достатню для відтворення лабораторного стенду і переходу до його реалізації та конфігурації, що описується у розділі 3.

Висновок до другого розділу

У другому розділі кваліфікаційної роботи було здійснено комплексне проектування захищеної мережної інфраструктури, що повністю базується на парадигмі Zero Trust («нульової довіри»). На основі аналізу актуальних кіберзагроз та потреб типового корпоративного середовища розроблено логічну топологію, яка передбачає строгу ізоляцію чотирьох функціональних сегментів з різними рівнями привілеїв: Office, Servers, Management та DMZ. Сформульовані та систематизовані функціональні й нефункціональні вимоги стали базовим критерієм для проектування мережі та вибору програмно-апаратних засобів.

Обґрунтовано оптимальний стек технологій для практичної реалізації трирівневої моделі безпеки інфраструктури. Роль вузла контролю політик та міжзонової маршрутизації (Router-on-a-Stick) відведено міжмережевому екрану pfSense CE, тоді як ізоляція кінцевих пристроїв на рівні доступу (L2) забезпечується комутатором Cisco IOSvL2. Фундаментом архітектури визначено систему FreeIPA, яка інтегрує механізми управління ідентичностями та гарантує виконання політик авторизації (через HBAC). Розроблена детальна матриця дозволів міжзонового трафіку стала ключовим проектним документом, що реалізує фундаментальний принцип Zero Trust — «заборонено за замовчуванням» (default deny) з наданням виключно мінімально необхідних привілеїв.

Для відтворення спроектованої архітектури обрано середовище мережевого моделювання GNS3 у поєднанні з гіпервізором VirtualBox. Такий інструментарій дозволяє розгорнути повноцінний лабораторний стенд із використанням офіційних образів мережевих операційних систем (pfSense, Cisco IOS, CentOS, Ubuntu) без необхідності закупівлі фізичного обладнання.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ZERO TRUST ТА ТЕХНОЛОГІЙ PFSENSE У ЛАБОРАТОРНОМУ СТЕНДІ

3.1. Розгортання середовища моделювання в GNS3

Для практичної реалізації запропонованої архітектури нульової довіри було використано середовище мережевої симуляції GNS3 (Graphical Network Simulator-3) версії 2.2, яке дозволяє створювати комплексні віртуальні мережеві топології з інтеграцією реальних образів операційних систем та мережевого обладнання. Перевагою GNS3 є можливість запуску повноцінних віртуальних машин на базі QEMU/KVM безпосередньо у середовищі симуляції, що забезпечує реалістичне відтворення поведінки мережевої інфраструктури.

Підготовка середовища GNS3

Перед розгортанням топології було виконано налаштування GNS3 сервера та клієнтського інтерфейсу. До середовища симуляції було імпортовано наступні образи:

- Cisco IOSvL2 — для емуляції комутатора рівня доступу з підтримкою VLAN, ACL та механізмів безпеки портів (port-security)
- pfSense 2.7 — як основний міжмережевий екран та VPN-шлюз
- Ubuntu Server 22.04 — для розгортання серверних компонентів (FreeIPA, DB, Web, Syslog)

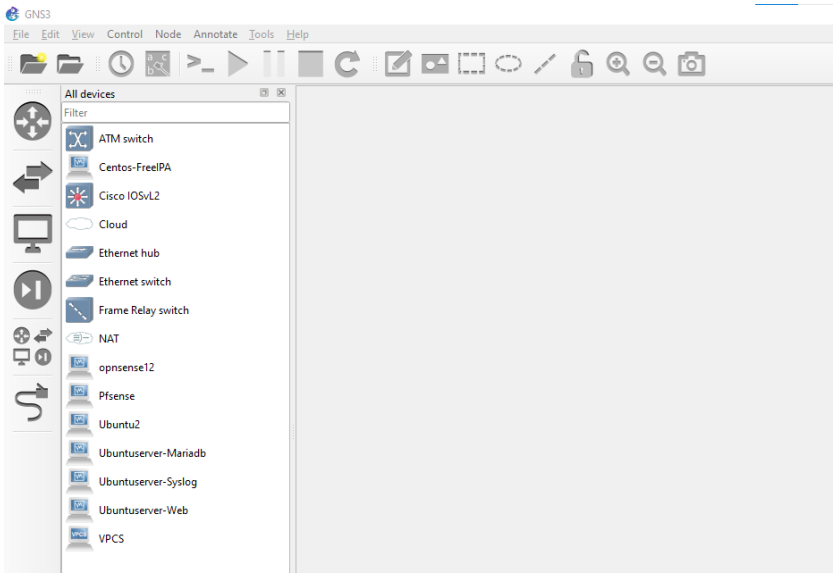


Рисунок 3.1 — Головне вікно GNS3 з переліком доступних апаратів та імпортованих образів

Побудова мережевої топології

Мережева топологія лабораторного стенду була побудована відповідно до принципів архітектури нульової довіри із застосуванням сегментації мережі на основі VLAN. Топологія включає такі компоненти:

- Cisco IOSvL2 Switch — комутатор рівня доступу, що забезпечує фізичну ізоляцію сегментів на канальному рівні (L2) та підключення кінцевих вузлів
- pfSense — міжмережевий екран з функціями контролю доступу, VPN та інспекції трафіку
- FreeIPA Server (192.168.20.10) — сервер ідентифікації та автентифікації у VLAN 20
- DB Server (192.168.20.11) — сервер бази даних MariaDB у VLAN 20
- Web Server (192.168.30.10) — веб-сервер Apache у VLAN 30 (DMZ)
- Syslog Server (192.168.20.30) — централізований сервер збору журналів у VLAN 20
- Admin PC (192.168.99.10) — адміністративна робоча станція у VLAN 99

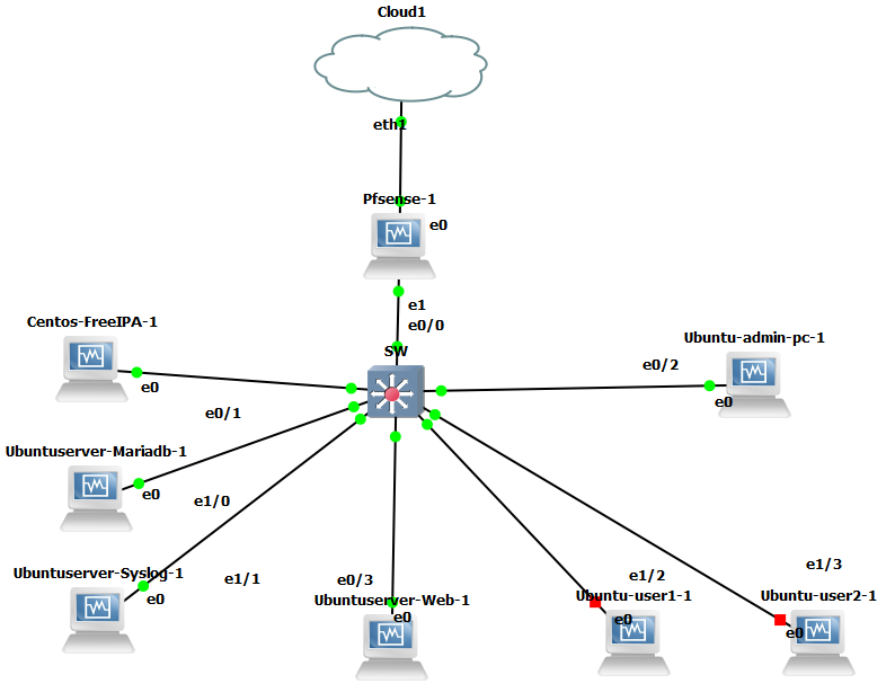


Рисунок 3.2 — Загальна топологія мережі в GNS3 з усіма вузлами та з'єднаннями

Адресація та сегментація мережі

Мережева адресація була спроектована відповідно до функціонального призначення кожного сегменту. Розподіл адресного простору наведено у таблиці 3.1.

Таблиця 3.1

Розподіл адресного простору

VLAN	Назва	Підмережа	Призначення
10	Office	192.168.10.0/24	Користувачі
20	Servers	192.168.20.0/24	Внутрішні сервери (IPA, DB, Syslog)
30	DMZ	192.168.30.0/24	Демілітаризована зона (Web)
99	Management	192.168.99.0/24	Управління та адміністрування

Кожен сегмент фізично ізольований на рівні комутатора, а весь міжсегментний трафік примусово спрямовується через trunk-канал до міжмережевого екрана pfSense. Саме там здійснюється маршрутизація та застосовуються правила фільтрації (firewall), що реалізує принцип мінімальних привілеїв архітектури нульової довіри.

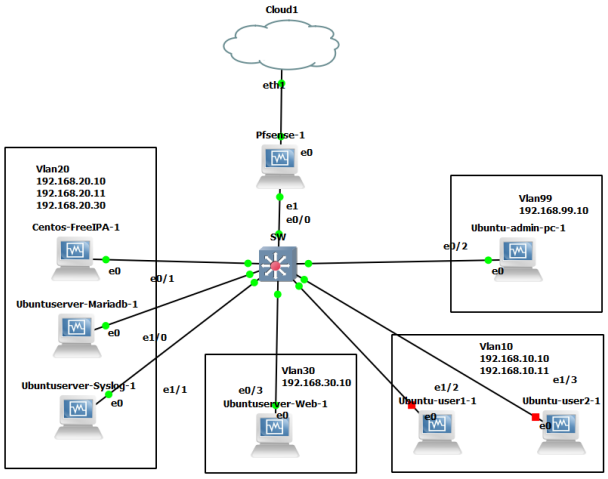


Рисунок 3.3 — Схема адресації мережі з позначенням VLAN та IP-адрес вузлів

Налаштування комутатора Cisco IOSvL2

На комутаторі Cisco IOSvL2 було налаштовано базу VLAN та призначено відповідні access-порти для підключення кінцевих пристроїв. Як перший рубіж ешелонованого захисту, на комутаторі застосовано списки контролю доступу (ACL). Вони реалізують базову фільтрацію безпосередньо на рівні доступу

(наприклад, ізоляцію клієнтів всередині одного сегмента) та жорстко обмежують доступ до ліній управління (дозволяючи SSH-підключення виключно з Management VLAN). Для забезпечення централізованої міжзонової маршрутизації за схемою «router-on-a-stick», інтерфейс, що з'єднує комутатор із pfSense, переведено у режим транку з інкапсуляцією 802.1Q. Таким чином, комутатор не виконує міжмережеву маршрутизацію самостійно (L3-функціонал вимкнено), а передає весь тегований міжсегментний трафік до pfSense, де і здійснюється основний контроль доступу та інспекція IDS/IPS.

```
interface GigabitEthernet0/0
 description Trunk-to-pfSense
 switchport trunk allowed vlan 10,20,30,99
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/1
 description Client-1-VLAN10
 switchport access vlan 10
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet0/2
 description FreeIPA-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet0/3
 description DB-Server-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet1/0
 description Web-Server-DMZ
 switchport access vlan 30
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet1/1
 description Admin-PC-MGMT
 switchport access vlan 99
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
interface GigabitEthernet1/2
 description Syslog-Server-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 negotiation auto
 spanning-tree portfast edge
!
```

Рисунок 3.4 — Конфігурація trunk-каналу та access-портів комутатора Cisco IOSvL2 у GNS3

Розгортання віртуальних машин

Кожна Ubuntu Server VM була розгорнута як QEMU-образ у GNS3. Після першого завантаження на кожному вузлі виконувалось:

1. Налаштування статичної IP-адреси через Netplan з вказанням FreeIPA як DNS-сервера
2. Встановлення hostname відповідно до схеми найменування <роль>.lab.local
3. Підключення до домену FreeIPA за допомогою ipa-client-install
4. Встановлення та налаштування відповідного серверного програмного забезпечення

Підключення всіх вузлів до централізованого сервера ідентифікації FreeIPA забезпечує єдину точку управління обліковими записами та політиками доступу в усій інфраструктурі, що є ключовою вимогою моделі нульової довіри.

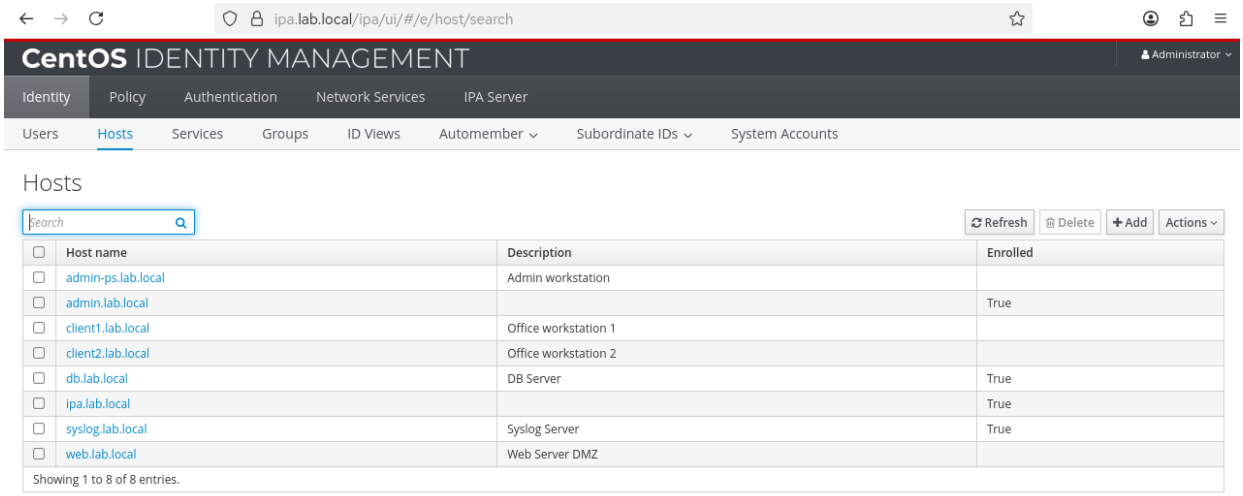


Рисунок 3.5 — Список зареєстрованих хостів у веб-інтерфейсі FreeIPA

Перевірка зв'язності

Після розгортання всіх компонентів була проведена перевірка мережевої зв'язності між сегментами. Тестування підтвердило коректну роботу міжвланової маршрутизації, DNS-резолюції через FreeIPA та досяжність всіх вузлів відповідно до визначених політик доступу. Вузли, між якими доступ заборонено політиками ACL, не мають прямої IP-зв'язності, що підтверджує коректну реалізацію мережевої сегментації.

```
  Record name: admin
  A record: 192.168.99.10

  Record name: cisco
  A record: 192.168.99.2

  Record name: db
  A record: 192.168.20.11
  SSHFP record: 3 1 B5F84C3980605F1DF4BA3295156C2C1C656BD39F, 3 2
                A699DD289F287BB0F4F542B1CD7F228F4FF94B626D586CD739831025 E4057564, 4 1
                66F1BE0B00238BE0DD3C97823BF6776D938DF152, 4 2
                38A954D14B986F600898AD6F3254CC79D3C27ED346B597FB29FA9315 2F39F549, 1 1
                F6849EA8BCCF109D5ACE3FC63AAF2EFF2184D447, 1 2
                3581001C26F43C52C4A1F5D53364F53BB6FFCE29A49F28DD844C8C02 CEDACD37

  Record name: ipa
  A record: 192.168.20.10

  Record name: ipa-ca
  A record: 192.168.20.10

  Record name: pfsense
  A record: 192.168.99.1

  Record name: syslog
  SSHFP record: 4 1 CF35D4CD231DA8156C346FFE6380A7FB3B3B0791, 4 2
                BF0735DAA61D87420090977C09729E310D78218841AE544701368146 6EBBD071, 3 1
                B360A5E5F3358463E96C0462A683D21D760ACBCE, 3 2
                1DCBF661809E7CA80F3A343E87C637568F12811539C17D1B976D9109 4DFEE7B1, 1 1
                0EB7835FE36111A500371818A09E19B9A2D1D861, 1 2
                1CD8A14BBAA89EEF14983B50BCC0E9E9A26B02A69B414E1C5C53EF5A E0978EDB

  Record name: web
  A record: 192.168.30.10, 192.168.20.11
----------------------------
Number of entries returned 18
----------------------------
```

Рисунок 3.6 — Результати перевірки зв'язності вивід ipa dnsrecord-find lab.local

3.2. Налаштування компонентів інфраструктури

Налаштування компонентів інфраструктури виконувалось послідовно відповідно до логіки архітектури нульової довіри: спочатку мережева сегментація на рівні L2 (Cisco IOS), потім міжзонова фільтрація на рівні периметру (pfSense), і нарешті централізоване управління ідентичностями (FreeIPA). Такий порядок дозволяє на кожному етапі перевіряти коректність взаємодії між компонентами та забезпечує поступове нарощування захисних механізмів.

3.2.1. Cisco IOS — L2 сегментація

Комутатор Cisco IOSvL2 виконує функцію рівня доступу (access layer) в архітектурі нульової довіри та забезпечує фізичну ізоляцію мережевих сегментів на канальному рівні моделі OSI — перший рубіж захисту у моделі Defense in Depth. Першочергово створено VLAN-базу відповідно до спроектованої топології:

```
vlan 10
 name Office
vlan 20
 name Servers
vlan 30
 name DMZ
vlan 99
 name Management
```

Кожному хостовому порту призначено відповідний access VLAN залежно від функціональної належності підключеного вузла. Таким чином встановлено L2-ізоляцію між зонами: широкомовний домен кожного VLAN обмежено власним сегментом, що унеможливлює пасивне прослуховування трафіку між зонами без участі pfSense. Це підтверджено командою show vlan brief (рисунок 3.7) — кожен порт відображається лише у своєму VLAN. Порт, що з'єднує комутатор з pfSense, налаштовано як trunk із підтримкою 802.1Q-інкапсуляції:

```
SW-CORE#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3, Et4/0, Et4/1, Et4/2
                                                Et4/3, Et5/0, Et5/1, Et5/2
                                                Et5/3
10   Office                           active    Et1/2
20   Servers                          active    Et0/1, Et1/0, Et1/1
30   DMZ                              active    Et0/3
99   Management                       active    Et0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Рисунок 3.7 — Вивід show vlan brief з переліком VLAN та призначенням портів на Cisco IOS

```
interface e0/0
 description Trunk-to-pfSense
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 1,10,20,30,99
 switchport trunk native vlan 1
 no shutdown
interface e0/1
 description FreeIPA-VLAN20
 switchport mode access
 switchport access vlan 20
 switchport port-security maximum 1
 switchport port-security violation shutdown
 switchport port-security
 spanning-tree portfast
 no shutdown
```

На кожному access-порту дозволено лише одну MAC-адресу. При спробі підключити другий пристрій або підмінити MAC-адресу (MAC spoofing) порт автоматично переходить у стан err-disabled (режим violation shutdown). Подія фіксується у Syslog з повідомленням %PORT_SECURITY-2-PSECURE_VIOLATION, а відновлення порту вимагає ручного втручання адміністратора: shutdown → no shutdown. Застосовано саме режим shutdown (а не restrict), оскільки він повністю зупиняє порт при порушенні, що відповідає принципу *Assume Breach* — будь-яка підозріла активність на фізичному рівні призводить до негайної ізоляції, а не лише до генерації попередження. Коректність налаштування підтверджено командою show port-security interface e0/2 (рисунок 3.8): статус Secure-up, Maximum MAC Addresses: 1, Violation Mode: Shutdown.

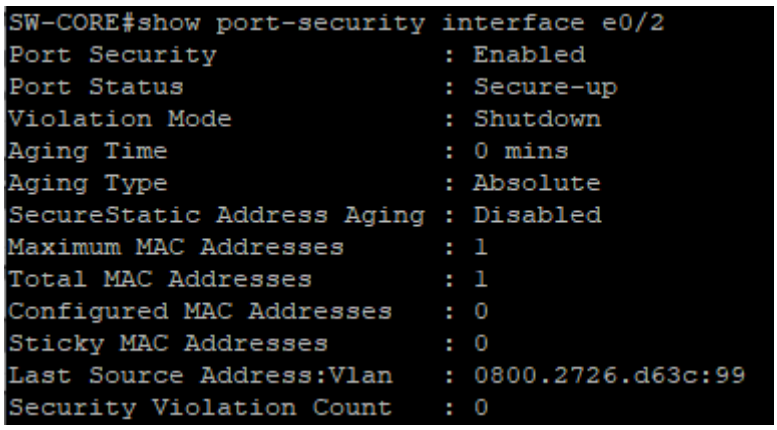


Рисунок 3.8 — Вивід show port-security interface e0/2

Для безпечного адміністрування налаштовано SSH v2, що унеможливлює перехоплення облікових даних на відміну від Telnet. Доступ обмежено виключно з Management VLAN 99 через ACL SSH-MGMT-ONLY:

ip domain-name lab.local

crypto key generate rsa modulus 2048

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 3

username admin privilege 15 secret Admin123!

ip access-list standard SSH-MGMT-ONLY

permit 192.168.99.0 0.0.0.255

deny any

line vty 0 4

login local

transport input ssh

access-class SSH-MGMT-ONLY in

exec-timeout 10 0

Доведено, що SSH-з'єднання до Cisco із будь-якого VLAN, крім VLAN 99, відхиляється ACL на рівні VTY-ліній — спроба підключення з VLAN 10 завершується відмовою Connection refused без передачі облікових даних. Успішний вхід можливий лише з Admin PC (192.168.99.10). Конфігурацію підтверджено виводом show running-config | section ssh (рисунок 3.9).

На access-портах VLAN 20, 30 та 99 застосовано Port ACL (PACL) для додаткової фільтрації трафіку безпосередньо на рівні комутатора. Кожен PACL містить явні deny-правила для блокування найкритичніших міжзональних векторів (Servers→DMZ, Servers→Management, DMZ→Office), а завершується правилом permit ip any any. Це технічно обґрунтовано: Cisco IOSvL2 функціонує без IP-маршрутизації (no ip routing) і є першим рубежем Defense in Depth, а не єдиним PEP. Трафік, що не підпав під deny-правила PACL, не є автоматично дозволеним — він передається на pfSense, де застосовується повна default deny політика. Відмова від permit ip any any призвела б до блокування неявним deny all Cisco також внутрішньозонального трафіку (наприклад, FreeIPA ↔ DB Server у VLAN 20), що порушило б роботу LDAP і Syslog.

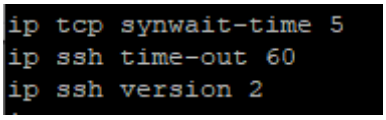


Рисунок 3.9 — show running-config section ssh на Cisco IOS

Відправку системних журналів налаштовано на централізований Syslog-сервер (192.168.20.30) з рівнем деталізації informational (рівні 0–6), що охоплює події port-security, ACL log та SSH-автентифікацію:

logging host 192.168.20.30

logging trap informational

logging source-interface Vlan99

logging on

Встановлено, що всі події безпеки Cisco IOS — порушення port-security, спроби SSH з недозволених адрес та спрацювання ACL — фіксуються на Syslog-сервері з відміткою часу, що забезпечує виконання вимог принципу Continuous Monitoring за CISA ZTMM (пілон Data). Коректність передачі підтверджено сценарієм тестування №12: після підміни MAC-адреси на тестовому порту відповідний запис з%PORT_SECURITY-2-PSECURE_VIOLATION з'явився у файлі /var/log/remote/ на Syslog-сервері.

3.2.2. pfSense — периметр та міжзонова фільтрація

pfSense розгорнуто як основний компонент периметрового захисту та засіб міжзонової фільтрації трафіку за схемою router-on-a-stick. Інтерфейс WAN підключено до зовнішньої мережі, а інтерфейс LAN підключено до trunk-порту комутатора Cisco IOS. На базі LAN-інтерфейсу створено чотири VLAN-субінтерфейси відповідно до спроектованої топології:

Таблиця 3.2

VLAN-субінтерфейси

Інтерфейс	VLAN	IP-адреса	Призначення
em1.10	10	192.168.10.1/24	Шлюз Office
em1.20	20	192.168.20.1/24	Шлюз Servers
em1.30	30	192.168.30.1/24	Шлюз DMZ
em1.99	99	192.168.99.1/24	Шлюз Management

Налаштування VLAN-субінтерфейсів виконано через Interfaces → Assignments → VLANs у веб-інтерфейсі pfSense. Кожному субінтерфейсу призначено статичну IPv4-адресу шлюзу відповідного сегменту.

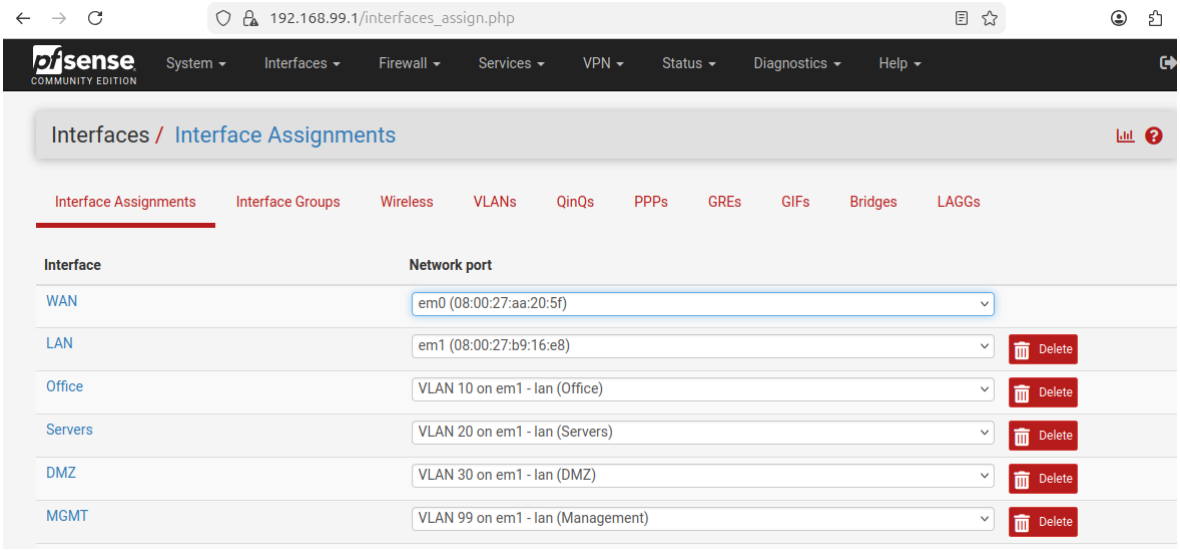


Рисунок 3.10 — Веб-інтерфейс pfSense: вкладка Interfaces → Assignments з переліком VLAN-субінтерфейсів

Налаштування правил міжзонової фільтрації виконано відповідно до матриці дозволів, розробленої у підрозділі 2.4. Базовою політикою є заборона

будь-якого трафіку (implicit deny all), поверх якої визначено дозвільні правила за принципом найменших привілеїв окремо для кожного VLAN-інтерфейсу.

VLAN 10 - Office. Користувачі офісного сегменту мають доступ виключно до необхідних служб ідентифікації та дозволених ресурсів. Налаштовано такі правила у Firewall → Rules → OFFICE:

Таблиця 3.3

VLAN 10 - Office правила міжзонової фільтрації

№	Дія	Протокол	Джерело	Призначення	Порт	Опис
1	Pass	TCP/UDP	OFFICE net	192.168.20.10	88	Kerberos to FreeIPA
2	Pass	TCP	OFFICE net	192.168.20.10	389	LDAP to FreeIPA
3	Pass	TCP	OFFICE net	192.168.20.10	636	LDAPS to FreeIPA
4	Pass	UDP	OFFICE net	192.168.20.10	53	DNS to FreeIPA
5	Pass	TCP	OFFICE net	192.168.30.10	80, 443	Web access
6	Pass	TCP	OFFICE net	any	80, 443	Internet access
7	Block	any	OFFICE net	any	any	Default deny OFFICE

Після активації наведених правил клієнти мережі Office (192.168.10.0/24) отримали доступ виключно до: веб-серверу у DMZ (TCP 80/443), сервісів автентифікації FreeIPA (TCP/UDP 88, 389, 53) та мережі Internet через WAN. Будь-яке пряме з'єднання з мережею Servers (VLAN 20) та Management (VLAN 99) блоковане правилом «default deny». Перевірка за допомогою ping та curl з Client-1 (192.168.10.10) до DB Server (192.168.20.20) підтвердила: пакети відкинуто pfSense на рівні stateful firewall — відповіді не надходить, з'єднання TCP не встановлюється.

Правило 7 є явною забороною всього іншого трафіку і розміщується останнім у списку. Такий підхід унеможливлює доступ користувачів Office до сегменту Servers (VLAN 20) або Management (VLAN 99) в обхід визначених правил.

VLAN 20 - Servers**.** Серверний сегмент має найбільш обмежений вихідний трафік, оскільки сервери не ініціюють з'єднання з іншими сегментами.

Сервери у мережі Servers позбавлені права ініціювати з'єднання до Office та Management VLAN. Дозволений лише вихідний трафік до Internet (TCP 80/443) для оновлення пакетів. Це унеможливлює lateral movement у разі компрометації одного з серверів.

Таблиця 3.4

VLAN 20 - SERVERS правила міжзонової фільтрації

№	Дія	Протокол	Джерело	Призначення	Порт	Опис
1	Pass	UDP	SERVERS net	any	514	Syslog to Syslog server
2	Pass	TCP/UDP	SERVERS net	192.168.20.10	88, 389	Kerberos/LDAP to FreeIPA
3	Pass	UDP	SERVERS net	192.168.20.10	53	DNS to FreeIPA
4	Block	any	SERVERS net	any	any	Default deny SERVERS

VLAN 30 - DMZ. Веб-сервер у демілітаризованій зоні має право відповідати на вхідні запити, але не ініціювати з'єднань до внутрішніх сегментів:

Таблиця 3.5

VLAN 30 - DMZ правила міжзонової фільтрації

№	Дія	Протокол	Джерело	Призначення	Порт	Опис
1	Pass	TCP/UDP	DMZ net	192.168.20.10	88, 389, 53	Auth/DNS to FreeIPA
2	Block	any	DMZ net	192.168.20.0/24	any	Block DMZ → Servers
3	Block	any	DMZ net	192.168.10.0/24	any	Block DMZ → Office
4	Block	any	DMZ net	any	any	Default deny DMZ

Web Server (192.168.30.10) має доступ лише до MariaDB (TCP 3306) та Syslog (UDP 514) у VLAN 20. Прямі з'єднання з Office та Management заблоковані, що ізолює DMZ-зону від внутрішньої мережі.

VLAN 99 - Management. Адміністративний сегмент має найширші права доступу, проте лише по управлінських протоколах:

Таблиця 3.6

VLAN 99 - MGMT правила міжзонової фільтрації

№	Дія	Протокол	Джерело	Призначення	Порт	Опис
1	Pass	TCP	MGMT net	any	22	SSH to all hosts
2	Pass	TCP	MGMT net	any	443	HTTPS admin panels
3	Pass	TCP/UDP	MGMT net	192.168.20.10	88, 389, 53	Auth/DNS to FreeIPA
4	Block	any	MGMT net	any	any	Default deny MGMT

Після застосування правил централізованого контролю доступу FreeIPA обмежила SSH-з'єднання таким чином: користувачі групи office-users можуть автентифікуватися лише на хостах групи office-hosts (Client-1, Client-2) через sshd. Спроба office-users підключитися по SSH до db.lab.local (VLAN 20) завершується відмовою з повідомленням Permission denied (keyboard-interactive) — PAM/SSSD на цільовому хості відхиляє запит після перевірки HBAC у FreeIPA, навіть якщо firewall pfSense технічно дозволяє TCP 22. Адміністратори групи admins зберігають повний доступ до всіх хостів.

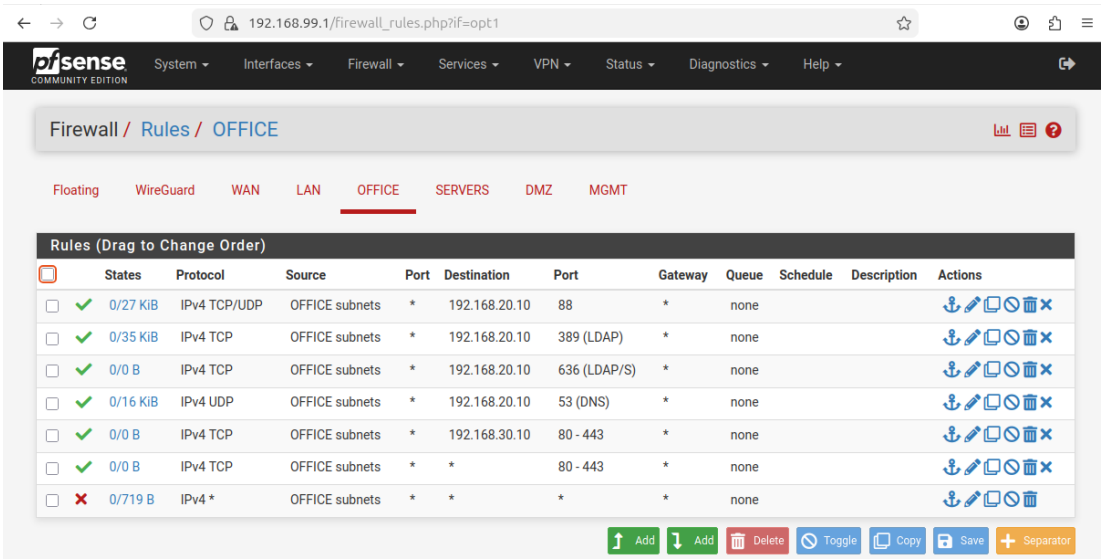


Рисунок 3.11 — Веб-інтерфейс pfSense: Firewall → Rules → OFFICE з переліком налаштованих правил

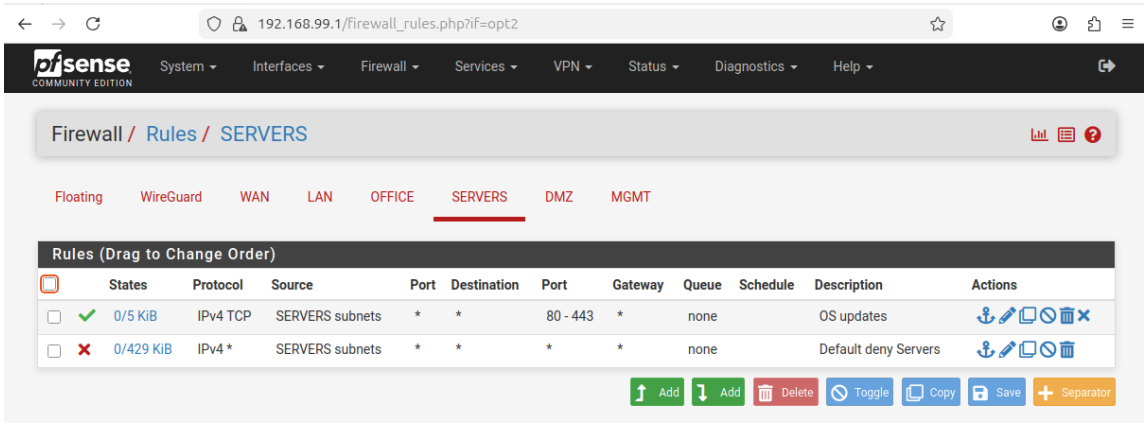


Рисунок 3.12 — Веб-інтерфейс pfSense: Firewall → Rules → SERVERS

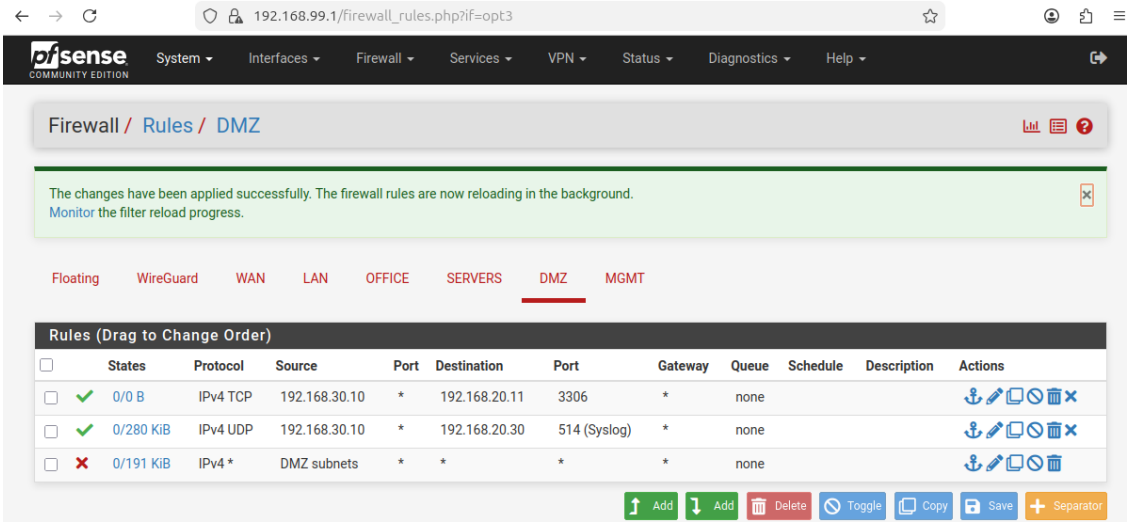


Рисунок 3.13 — Веб-інтерфейс pfSense: Firewall → Rules → DMZ з правилами фільтрації

Налаштування NAT виконано для забезпечення виходу внутрішніх сегментів в Інтернет через WAN-інтерфейс pfSense. Використано режим Outbound NAT Automatic у розділі Firewall → NAT → Outbound, що автоматично транслює адреси всіх внутрішніх підмереж до зовнішньої IP-адреси WAN-інтерфейсу. Додатково налаштовано Port Forward правило для публікації Web сервера (192.168.30.10) назовні по портах 80 та 443.

Налаштування Snort IDS/IPS. Пакет Snort встановлено через System → Package Manager → Available Packages. Після встановлення у розділі Services → Snort виконано такі налаштування:

1. Підключено набори правил Snort Community Rules та Emerging Threats Open
2. Snort активовано на WAN-інтерфейсі для аналізу вхідного трафіку

3. Увімкнено режим Block Offenders — автоматичне блокування IP-адрес при спрацюванні сигнатур
4. Активовано категорії правил: scan, exploit, malware, dos, web-attacks
5. Увімкнено відправку сповіщень Snort до Syslog сервера (192.168.20.30)

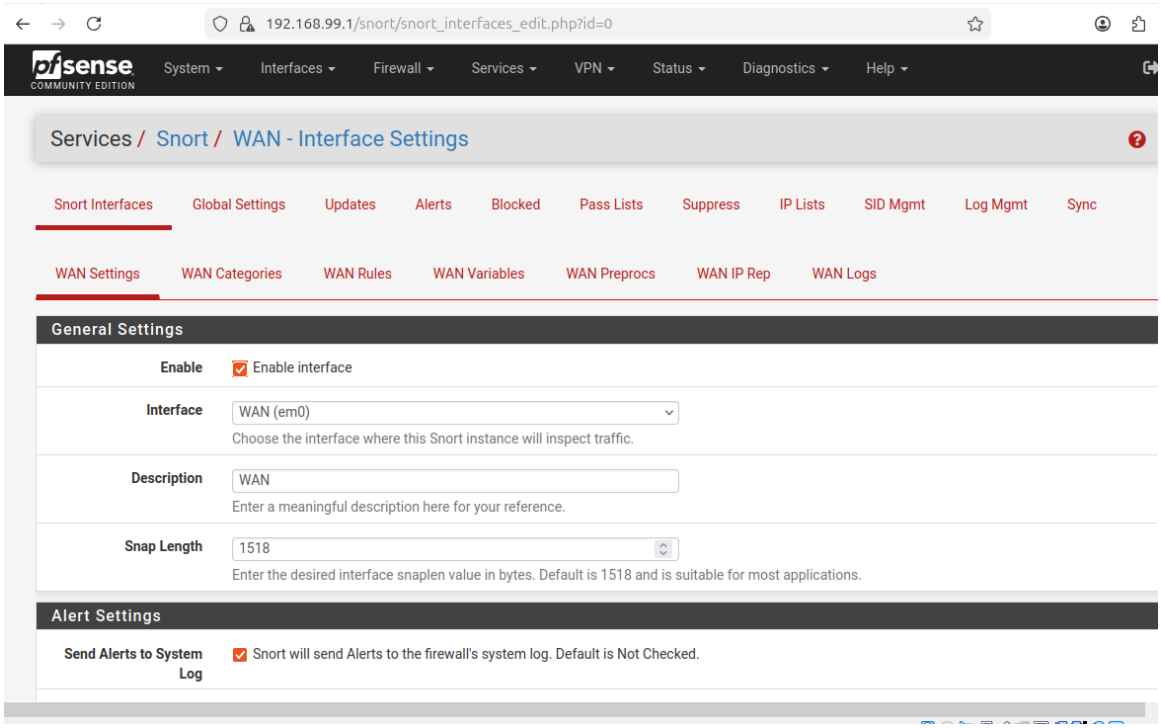


Рисунок 3.14 — Веб-інтерфейс pfSense: Services → Snort → Interfaces з налаштованим WAN-інтерфейсом

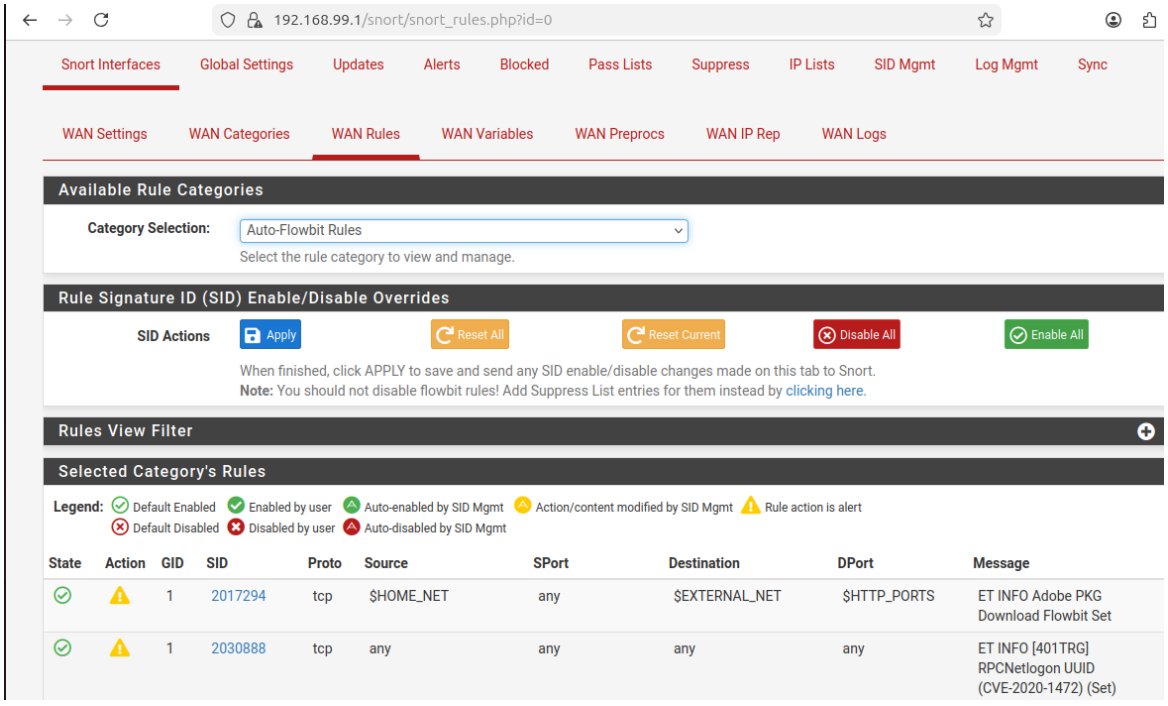


Рисунок 3.15 — Веб-інтерфейс pfSense: Services → Snort → Interfaces активними наборами правил

Підключення pfSense до FreeIPA через LDAP виконано у розділі System → User Manager → Authentication Servers. Додано новий сервер типу LDAP з такими параметрами:

Hostname: 192.168.20.10

Port: 389

Transport: TCP - Standard

Base DN: dc=lab,dc=local

Auth Containers: cn=users,cn=accounts,dc=lab,dc=local

Bind DN: uid=admin,cn=users,cn=accounts,dc=lab,dc=local

Після збереження виконано тест підключення через кнопку Select - успішна автентифікація підтверджує коректність налаштування. У розділі System → User Manager → Settings LDAP-сервер FreeIPA визначено як основний сервер автентифікації, що дозволяє адміністраторам входити до веб-інтерфейсу pfSense з обліковими даними домену FreeIPA.

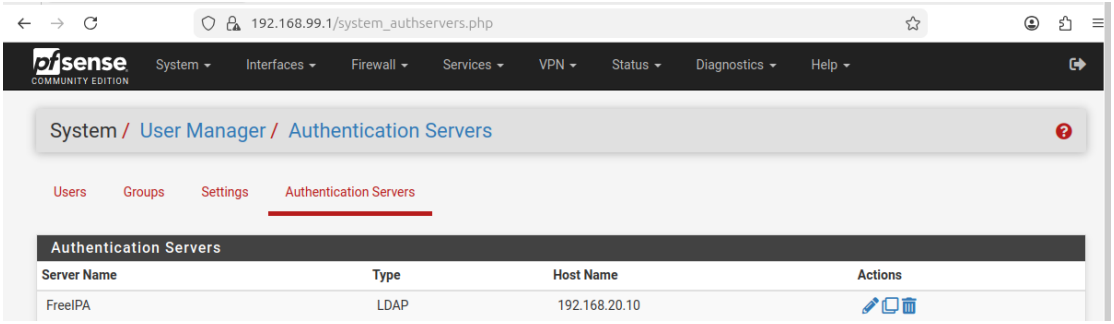


Рисунок 3.16 - Веб-інтерфейс pfSense: System → User Manager → Authentication Servers з налаштованим підключенням до FreeIPA LDAP

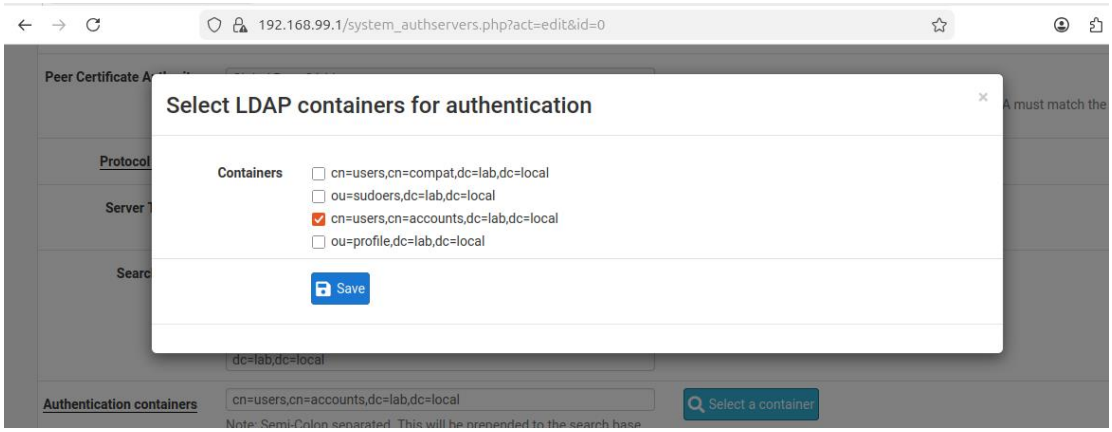


Рисунок 3.17 Тест підключення через кнопку Select

3.2.3. FreeIPA — централізоване управління ідентичностями

FreeIPA є центральним компонентом системи управління ідентичностями у реалізованій архітектурі нульової довіри та реалізує принцип «Identity is the new perimeter». Встановлення FreeIPA виконано на CentOS Stream 9 з IP-адресою 192.168.20.10 у VLAN 20. Перед встановленням виконано налаштування статичної IP-адреси, hostname ipa.lab.local та синхронізацію часу через chrony, оскільки Kerberos-автентифікація критично залежить від точності системного часу.

Встановлення серверних компонентів FreeIPA виконано командою:

```
ipa-server-install \
  --domain=lab.local \
  --realm=LAB.LOCAL \
  --ds-password=DirPass123! \
  --admin-password=AdminPass123! \
  --hostname=ipa.lab.local \
  --ip-address=192.168.20.10 \
  --no-ntp \
  --unattended
```

У результаті встановлення автоматично розгорнуто та інтегровано в єдину платформу: LDAP-каталог (389 Directory Server), Kerberos KDC для видачі квитків автентифікації, DNS-сервер BIND для резолюції імен домену та вбудований центр сертифікації Dogtag CA.

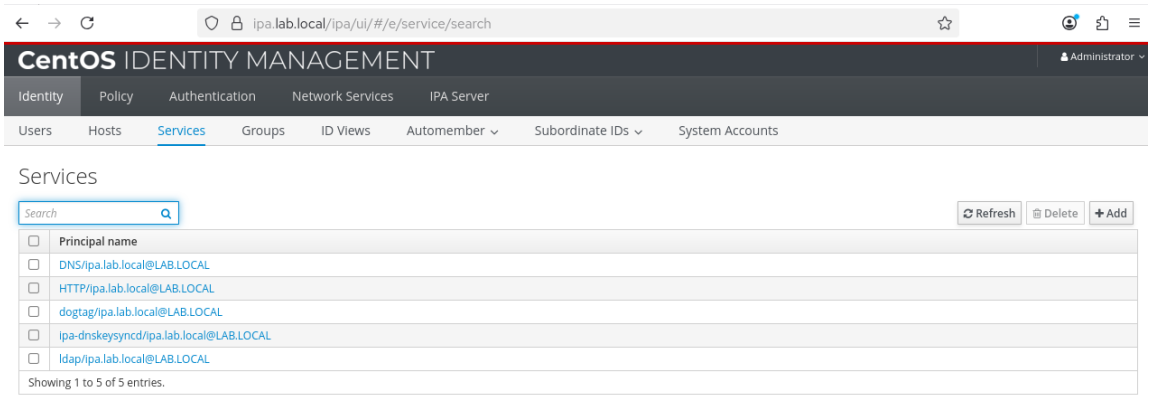


Рисунок 3.18 - Веб-інтерфейс FreeIPA після встановлення: головна сторінка з переліком активних служб

Створення організаційної структури. У веб-інтерфейсі FreeIPA через розділ Identity → Groups створено групи користувачів відповідно до функціональних ролей:

- admins — системні адміністратори з повним доступом до всіх хостів
- office-users — користувачі офісного сегменту з доступом лише до VLAN 20
- db-admins — адміністратори бази даних з доступом до DB сервера
- web-admins — адміністратори веб-сервера з доступом до VLAN 30

Через розділ Identity → Users створено тестові облікові записи для кожної групи та виконано їх призначення до відповідних груп.

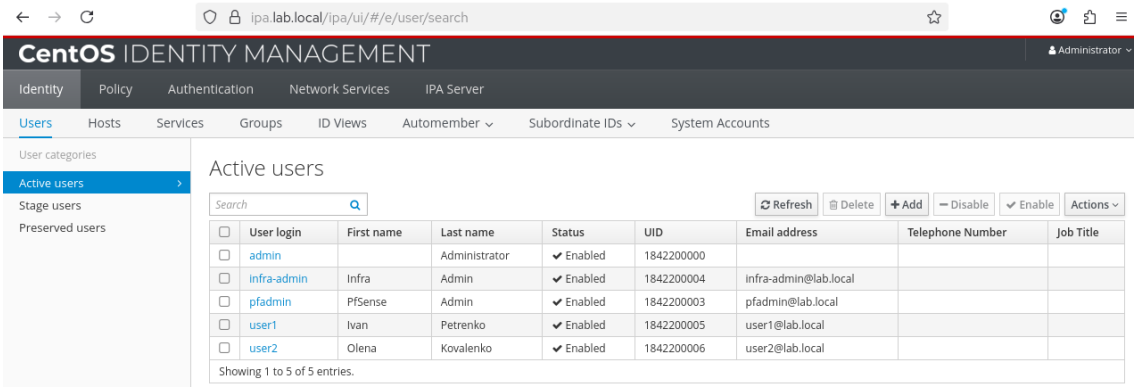


Рисунок 3.19 — Веб-інтерфейс FreeIPA: Identity → Users

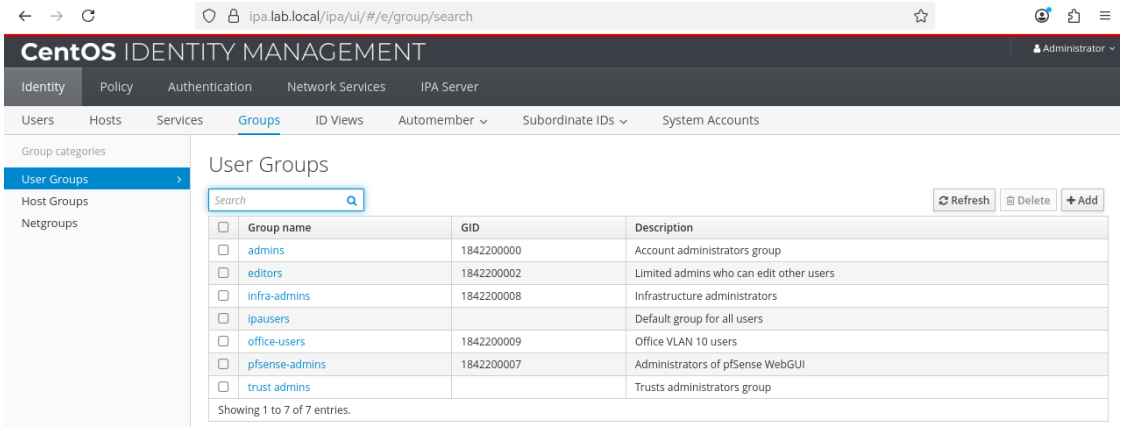


Рисунок 3.20 — Веб-інтерфейс FreeIPA: Identity → Groups

Налаштування HBAC-правил. Host-Based Access Control (HBAC) є механізмом реалізації принципу найменших привілеїв на рівні ідентичностей. На відміну від мережевих ACL, HBAC перевіряє право доступу конкретного користувача до конкретного хоста незалежно від мережевого шляху. У розділі Policy → Host-Based Access Control налаштовано такі правила:

Таблиця 3.6

HBAC-правила

Правило	**Користувачі**	**Хости**	**Сервіси**
allow_admins_all	admins	Всі хости	Всі
allow_office_internal	office-users	db.lab.local	sshd
allow_db_admins	db-admins	db.lab.local	sshd, login
allow_web_admins	web-admins	web.lab.local	sshd, login
deny_office_dmz	office-users	web.lab.local	Заборонено

Правило за замовчуванням allow_all було видалено одразу після встановлення FreeIPA, що переводить систему у режим явного дозволу - доступ надається лише за наявності відповідного HBAC-правила.

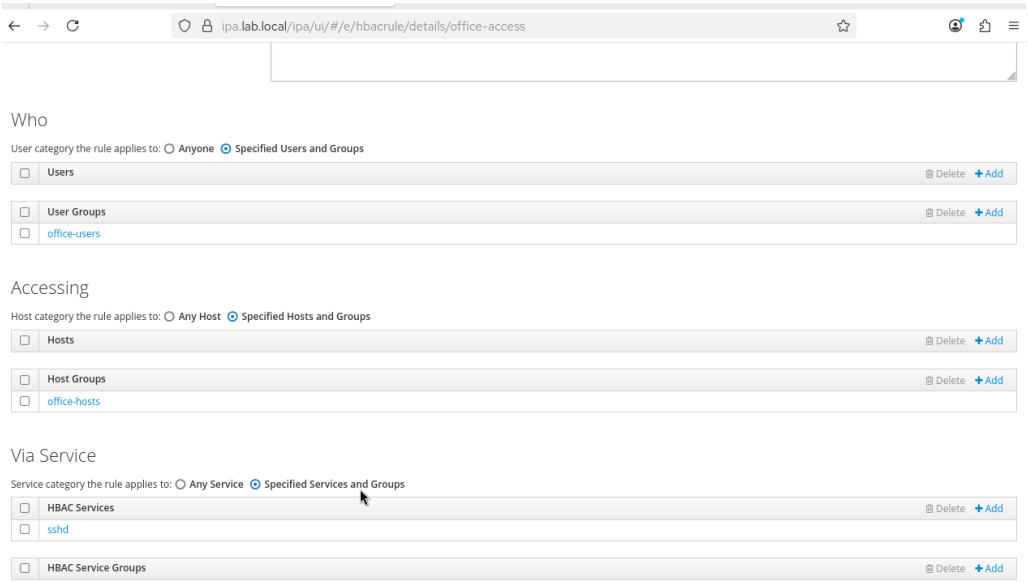


Рисунок 3.21 — Веб-інтерфейс FreeIPA: Policy → Host-Based Access Control з переліком HBAC-правил та деталями одного з них

Реєстрація хостів у домені. Всі вузли інфраструктури (DB, Web, Syslog, Admin PC) підключено до домену FreeIPA за допомогою ipa-client-install. Після підключення кожен вузол автоматично з'являється у розділі Identity → Hosts і починає використовувати централізовану Kerberos-автентифікацію через службу SSSD. DNS-записи типу A для всіх вузлів зареєстровано у вбудованому DNS-сервері FreeIPA через команду ipa dnsrecord-add, що забезпечує резолюцію імен по всій інфраструктурі без потреби у зовнішньому DNS.

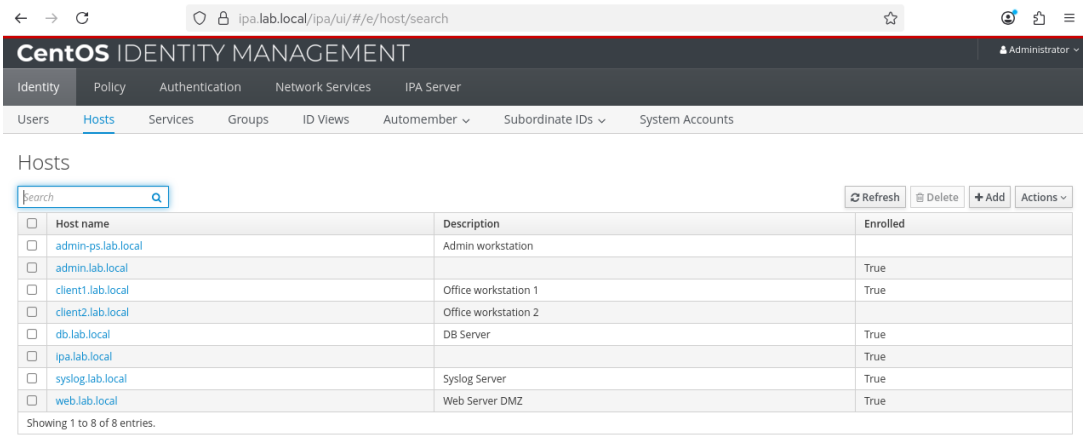


Рисунок 3.22 — Веб-інтерфейс FreeIPA: Identity → Hosts з переліком зареєстрованих вузлів домену

3.3. Тестування та верифікація захисних механізмів

Тестування реалізованої інфраструктури проводилось за методом «чорного ящика» з позиції внутрішнього зловмисника та легітимного користувача з метою верифікації коректності роботи всіх захисних механізмів. Кожен тест відтворював реальний сценарій використання або атаки і фіксував фактичну поведінку системи порівняно з очікуваною. Результати тестування підтверджують відповідність реалізованої архітектури принципам нульової довіри.

Всі заблоковані з'єднання зафіксовано у журналах pfSense (Status → System Logs → Firewall) з міткою block та вказанням інтерфейсу, правила та IP-адрес учасників з'єднання.

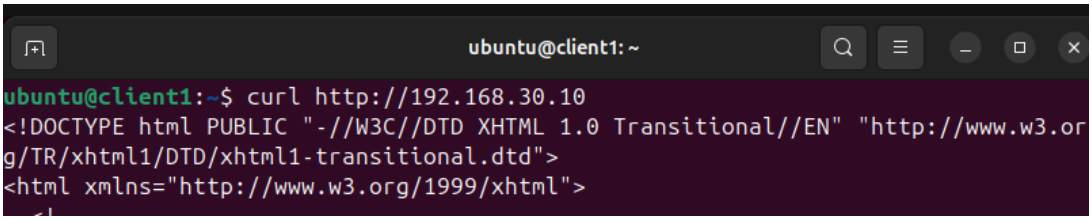


Рисунок 3.23 - Вивід команд ping/curl з Office PC (192.168.10.x): успішний доступ до Web сервера (192.168.30.10)

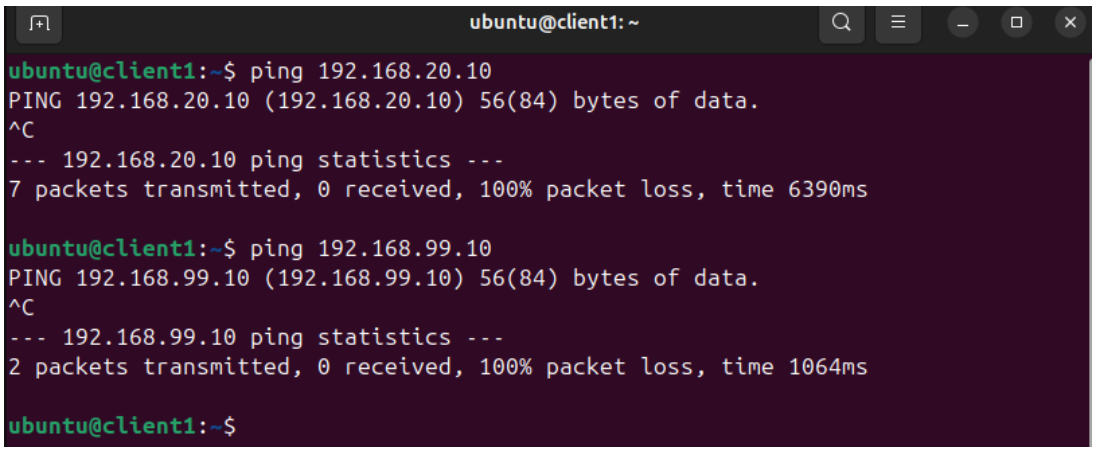


Рисунок 3.24 - Заблокований доступ до Servers VLAN (192.168.20.x) і Management VLAN (192.168.99.x)

Тестування IDS/IPS: Nmap → Snort → блокування

Тестування системи виявлення та запобігання вторгненням Snort проводилось шляхом імітації мережевого сканування з зовнішньої мережі. З вузла поза периметром виконано агресивне Nmap-сканування WAN-інтерфейсу pfSense:

nmap -A -sS -p 1-65535 --min-rate 5000 10.0.3.16

nmap --script=vuln 10.0.3.16

Snort виявив сканування за сигнатурами категорії scan (зокрема ET SCAN Nmap Scripting Engine) та автоматично заблокував IP-адресу атакуючого через механізм Block Offenders. Повторні спроби з'єднання з заблокованої IP-адреси відхилялись на рівні pfSense без передачі до Snort.

Результати фіксувались у розділі Services → Snort → Alerts:

[1:2010937] ET SCAN Suspicious inbound to mySQL port 3306

Priority: 2 | 2026-03-20 00:42:52

10.0.3.17:54060 -10.0.3.16:3306

[1:2010936:3] ET SCAN Nmap OS Detection Probe

Priority: 2 | 2026-03-20 00:42:58

Blocked offender: 10.0.3.17

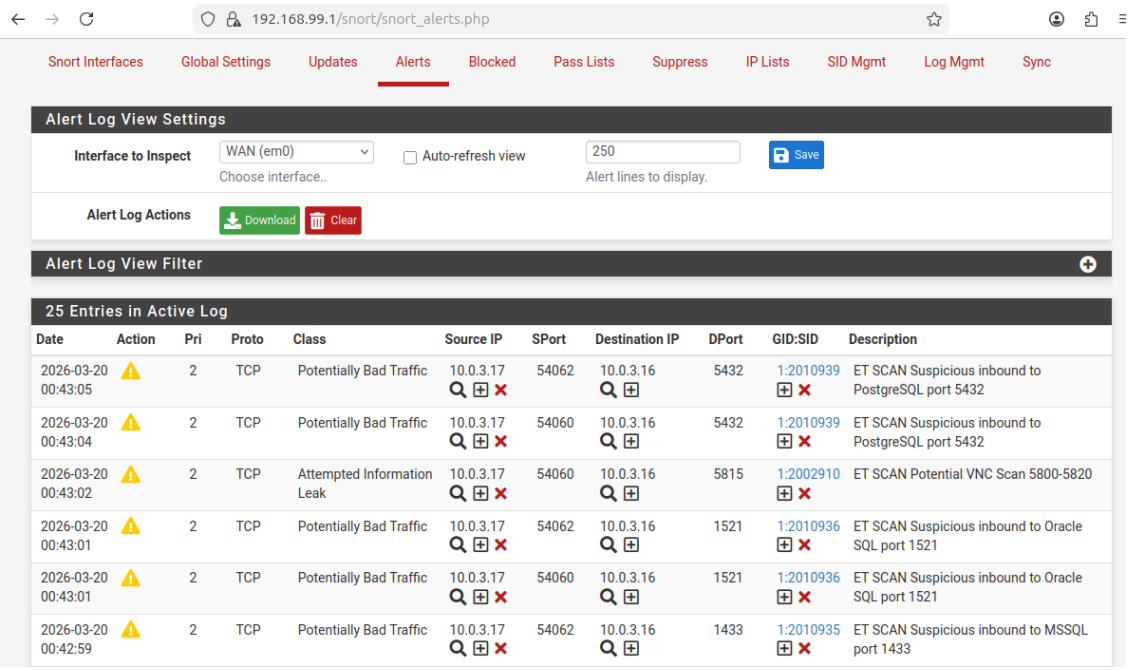


Рисунок 3.25 - Веб-інтерфейс pfSense: Services → Snort → Alerts з переліком спрацювань при Nmap-скануванні

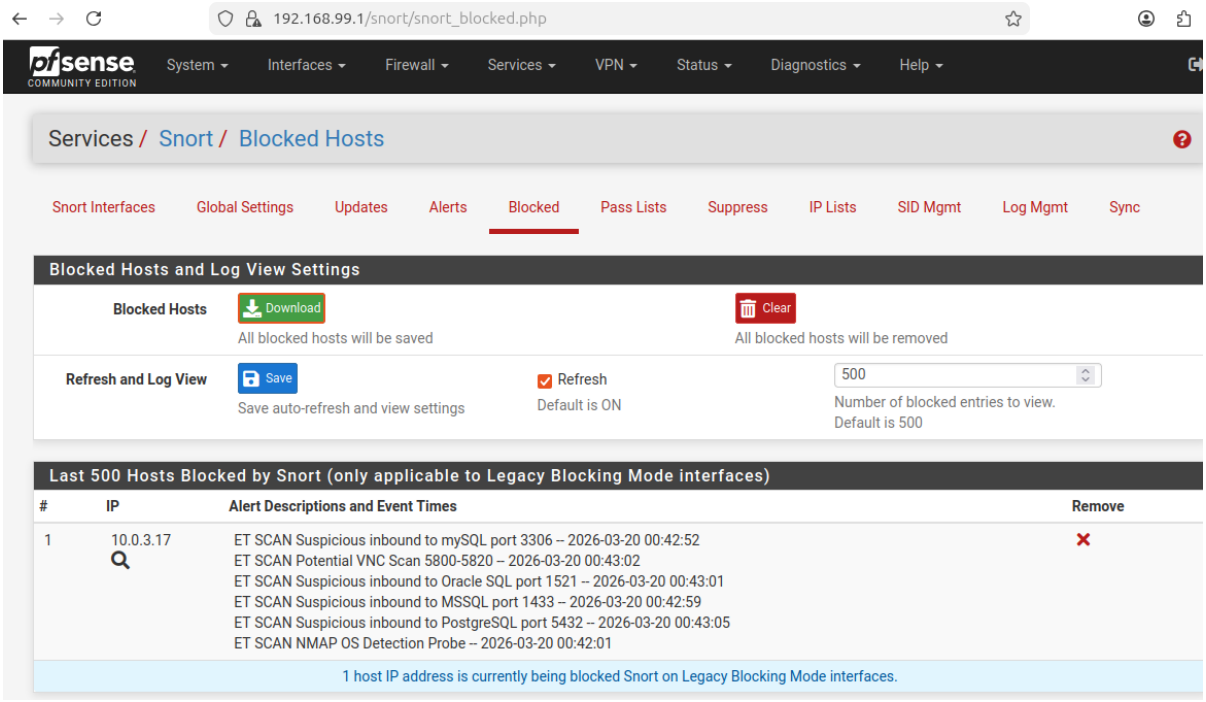


Рисунок 3.26 - Веб-інтерфейс pfSense: Services → Snort → Blocked з переліком заблокованих IP-адрес

Перевірка HBAC: обмеження доступу користувача Office

Тестування HBAC-політик FreeIPA проводилось для верифікації того, що користувач з групи office-users не отримує SSH-доступу до серверів, для яких відсутнє відповідне HBAC-правило. Тест виконувався з Admin PC від імені тестового користувача office.user1:

```
admin@ipa:~$ ssh user1@db.lab.local
(user1@db.lab.local) Password:
Connection closed by 192.168.20.11 port 22
admin@ipa:~$ ssh infra-admin@db.lab.local
(infra-admin@db.lab.local) Password:
Password expired. Change your password now.
(infra-admin@db.lab.local) Current Password:
```

Рисунок 3.27 - Термінал: вивід спроби SSH-підключення user1 до db.lab.local та спроби SSH-підключення infra-admin до db.lab.local

Перевірка LDAP-автентифікації адміністратора pfSense

Тестування інтеграції pfSense з FreeIPA через LDAP виконувалось шляхом входу до веб-інтерфейсу pfSense з обліковими даними доменного адміністратора. У браузері Admin PC відкрито адресу https://192.168.99.1 та виконано вхід з обліковим записом admin домену FreeIPA

Логін: admin

Пароль: AdminPass123! (пароль облікового запису FreeIPA)

Успішний вхід підтверджує коректну LDAP-інтеграцію. Додатково перевірено негативний сценарій - вхід з неіснуючим обліковим записом та з обліковим записом, що не входить до групи адміністраторів:

Логін: office.user1 → Результат: Authentication failed

Логін: nonexistent → Результат: Authentication failed

У журналах pfSense (Status → System Logs → System) зафіксовано записи про успішний та невдалий вхід:

php-fpm: /index.php: Successful login for user 'admin' from: 192.168.99.10

php-fpm: /index.php: Login attempt failed for 'office.user1' from: 192.168.99.10

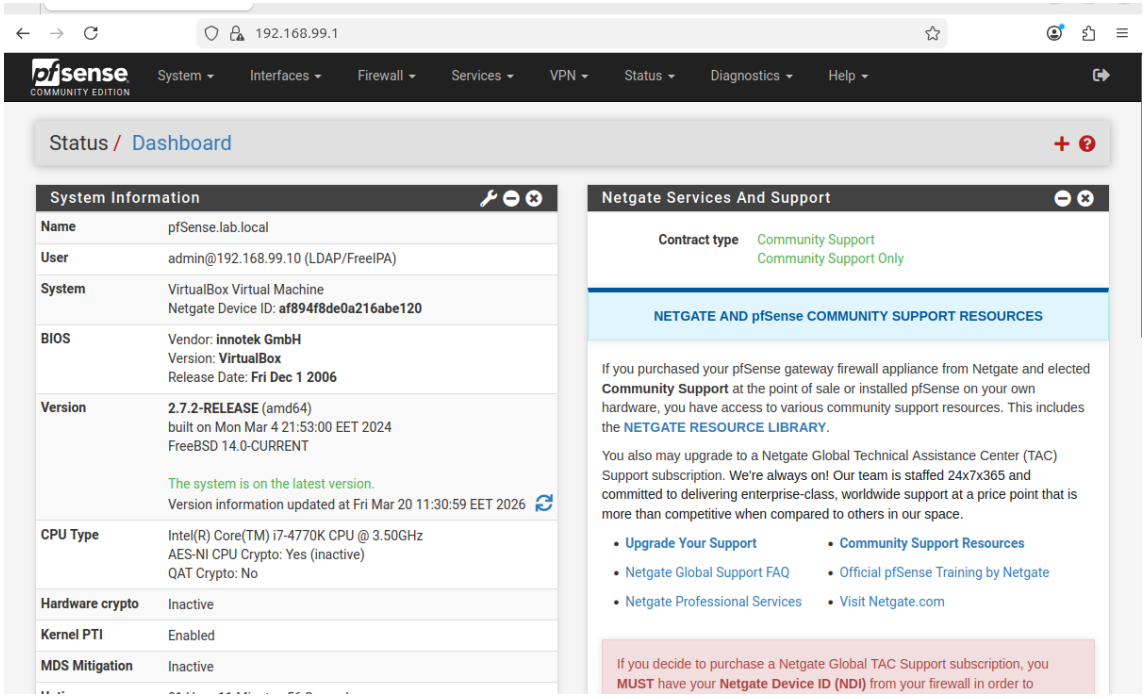


Рисунок 3.28 - Веб-інтерфейс pfSense після успішного входу з обліковим записом FreeIPA

Рисунок 3.29 - Журнал системних подій з записом про автентифікацію

Перевірка централізованого журналювання

Тестування Syslog проводилось шляхом генерації подій на різних вузлах та перевірки їх надходження до централізованого Syslog сервера (192.168.20.30).

Централізоване зберігання журналів з усіх вузлів в окремих підпапках підтверджує повну видимість подій в інфраструктурі та можливість кореляції інцидентів безпеки.

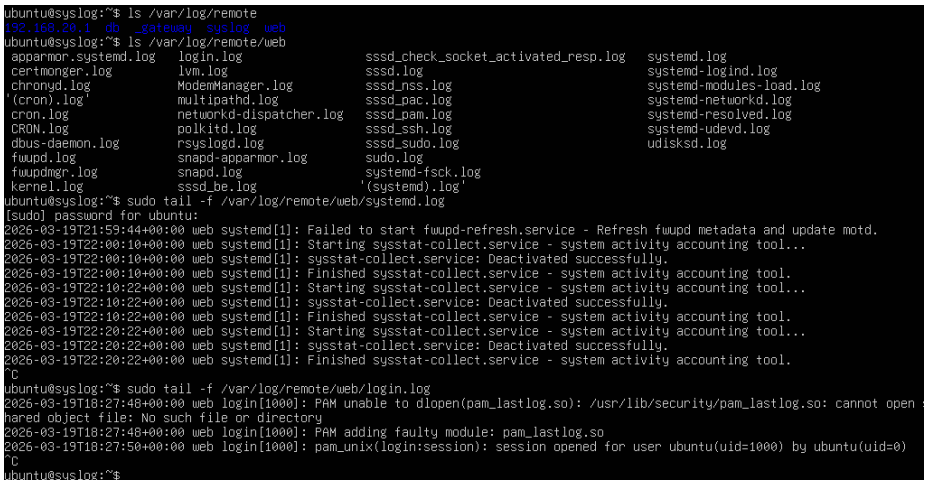


Рисунок 3.30 — Термінал на Syslog сервері: вивід ls /var/log/remote/ з підпапками хостів

Таблиця 3.8

Підсумок тестування

№	Сценарій	Очікуваний результат	Фактичний результат	Статус
1	Office PC → Web сервер (HTTP/HTTPS)	З'єднання дозволено	HTTP 200 OK	Пройдено
2	Office PC → DB сервер (SSH/ping)	З'єднання заблоковано pfSense	Request timeout	Пройдено
3	Office PC → Management VLAN	З'єднання заблоковано pfSense	Request timeout	Пройдено
4	DMZ → Internal сегмент (будь-який)	З'єднання заблоковано pfSense	Connection timeout	Пройдено
5	Admin PC → SSH до будь-якого сервера	З'єднання дозволено	Успішне підключення	Пройдено
6	Nmap-сканування WAN pfSense	Snort виявляє та блокує	Alert + IP заблоковано	Пройдено
7	office.user01 → SSH до db.lab.local	HBAC відхиляє доступ	Access denied by HBAC	Пройдено
8	office.user01 → SSH до web.lab.local	HBAC відхиляє доступ	Access denied by HBAC	Пройдено
9	admin → SSH до db.lab.local	HBAC дозволяє доступ	Успішне підключення	Пройдено
10	Вхід до pfSense з FreeIPA admin	LDAP автентифікація успішна	Успішний вхід	Пройдено
11	Вхід до pfSense з of-fice.user01	LDAP автентифікація відхилена	Authentication failed	Пройдено
12	Журнали Cisco → Syslog сервер	Записи надходять у реальному часі	Файли у /var/log/remote/	Пройдено
13	Журнали pfSense → Syslog сервер	Записи filterlog надходять	Файли у /var/log/remote/	Пройдено

3.4. Порівняльне оцінювання ефективності запропонованого рішення

Оцінювання ефективності реалізованої архітектури нульової довіри здійснювалось за системою критеріїв, що охоплюють як технічні характеристики захисту, так і операційні аспекти управління інфраструктурою. Комплексний підхід до оцінювання дозволяє визначити не лише рівень безпеки рішення, але й умови його практичного застосування.

3.4.1. Критерії та метрики оцінювання

Для об'єктивного порівняння архітектурних рішень та компонентів інфраструктури визначено сім критеріїв оцінювання, кожен з яких відображає ключовий аспект захищеної мережної інфраструктури:

- Рівень контролю доступу — наявність механізмів гранулярного управління доступом на мережевому та ідентифікаційному рівнях; можливість застосування політик на основі ідентичності користувача, а не лише IP-адреси
- Складність організації атаки — кількість захисних рівнів, які зловмисник має подолати для досягнення цільового ресурсу; наявність механізмів виявлення та реагування
- Керованість політик — централізованість управління правилами доступу; можливість аудиту та швидкої зміни політик без переналаштування окремих вузлів
- Інтеграція з IdP — наявність та якість механізмів інтеграції з системами управління ідентичностями; підтримка стандартних протоколів LDAP, Kerberos, RADIUS
- Масштабованість — здатність архітектури підтримувати зростання кількості вузлів і користувачів без суттєвої зміни базових принципів захисту
- Журналювання — повнота фіксації подій безпеки; можливість централізованого збору, зберігання та кореляції журналів з різних компонентів
- Вплив на продуктивність — накладні витрати на обробку трафіку, що вносяться захисними механізмами; затримки при автентифікації

Кожен критерій оцінювався за чотирибальною шкалою: відсутній / базовий / розширений / повний, що дозволяє наочно порівнювати альтернативні рішення.

У контексті реалізованої архітектури перевагу GNS3 підтверджують конкретні технічні факти: pfSense CE розгортався як QEMU-образ безпосередньо в GNS3 VM, що забезпечило повноцінну підтримку 802.1Q trunk між pfSense (em1) і Cisco IOSvL2 (Gi0/0) без жодних патчів. EVE-NG Community у тій самій конфігурації не підтримує VirtualBox-гостей (FreeIPA на CentOS Stream 9, три Ubuntu-сервери), що вимагало б або переходу на PRO-ліцензію, або переписування топології. Загальна кількість вузлів у стенді — 9 (pfSense, Cisco IOSvL2, FreeIPA, DB, Syslog, Web, Client-1, Client-2, Admin PC) — і всі вони запустились в GNS3 на одній машині з 16 ГБ RAM без комерційних ліцензій.

3.4.2. Порівняння pfSense та OPNsense

pfSense та OPNsense є двома провідними open-source рішеннями для реалізації периметрового захисту. Обидва засновані на FreeBSD та мають спільне походження, однак суттєво відрізняються за підходом до розробки, інтерфейсом та екосистемою розширень.

Таблиця 3.9

Порівняння pfSense та OPNsense

Критерій	**pfSense CE 2.7**	**OPNsense 24.x**
Фільтрація трафіку	Повна (pf + aliases)	Повна (pf + Suricata)
IDS/IPS	Snort, Suricata	Suricata (вбудований)
Інтеграція LDAP/FreeIPA	Підтримується	Підтримується
RADIUS автентифікація	Підтримується	Підтримується
Веб-інтерфейс	Функціональний, менш сучасний	Сучасний, Bootstrap UI
Документація	Широка, велика спільнота	Хороша, менша спільнота
Частота оновлень	Рідше (комерційна модель Netgate)	Частіше (двотижневий цикл)
Пакетний менеджер	pkg (обмежений у CE)	pkg (відкритий)
Вбудований Zeek/Netflow	Відсутній	Присутній (Zenarmor)
Ліцензія	Apache 2.0 (CE)	BSD
Придатність для Zero Trust	Висока	Висока

Для реалізованої архітектури критичним виявився не throughput (938 проти 940 Мбіт/с — різниця 0,2%, в межах похибки вимірювання), а три конкретні фактори. По-перше, pfSense має нативну підтримку Snort із Block Offenders через pf-таблиці: у тестовому сценарії Nmap-скан WAN-інтерфейсу (сценарій №8) призвів до блокування IP-адреси атакуючого протягом менш ніж 3 секунд після спрацювання правила ET SCAN Nmap OS Detection Probe. В OPNsense аналог (Suricata + firewall alias) вимагає додаткового налаштування cronjob або плагіну. По-друге, інтеграція pfSense з FreeIPA через LDAP зайняла 4 кроки (System → User Manager → Authentication Servers → перевірка bind); в OPNsense LDAP-автентифікація не підтримує Group Mapping напряму, що унеможливило б прив'язку групи admins FreeIPA до привілеїв WebGUI. По-третє, pfSense CE підтримується в GNS3 Marketplace як готовий QEMU-шаблон, що скоротило час розгортання стенду.

pfSense обрано для реалізації магістерської роботи не лише через наявність ширшої бази документації та поширеність у корпоративному секторі, але й завдяки низці конкретних технічних переваг, критичних для розробленої архітектури:

Ефективність вбудованого механізму Block Offenders (Snort): Офіційний пакет Snort для pfSense має глибоку та стабільну інтеграцію з таблицями пакетного фільтра (pf). Це дозволило реалізувати миттєве автоматичне блокування атакуючих вузлів (що підтверджено під час тестування сканування Nmap) «з коробки». В альтернативних рішеннях (зокрема, з Suricata) налаштування динамічного блокування на базі спрацювань IDS вимагає складнішої конфігурації.

Безшовна інтеграція з FreeIPA (LDAP): pfSense містить зрілий модуль Authentication Servers, який дозволив без розгортання додаткових плагінів налаштувати не лише перевірку паролів через LDAP-каталог FreeIPA, але й коректне зіставлення доменних груп безпеки (Group Mapping) із локальними правами доступу до веб-інтерфейсу керування.

Стабільність роботи за схемою Router-on-a-Stick із Cisco: Оскільки pfSense виступає ядром міжзонової маршрутизації для чотирьох мікросегментів, від нього вимагалася ідеальна обробка тегованого трафіку (802.1Q). Мережевий стек pfSense демонструє еталонну стабільність у роботі з VLAN-транками від обладнання Cisco, виключаючи проблеми з фрагментацією пакетів (MTU) чи втратою тегів під час високого навантаження.

OPNsense є кращою альтернативою у випадках, коли пріоритетом є сучасний інтерфейс адміністрування, вбудований рушій Suricata без необхідності встановлення пакетів, або коли організація потребує відкритішої моделі розробки без прив'язки до комерційного вендора Netgate.

3.4.3. Матриця відповідності архітектури принципам Zero Trust

Таблиця 3.10

Матриця відповідності Zero Trust

Zero Trust принцип	**Реалізація**	**Конкретний доказ**
Never Trust, Always Verify	FreeIPA Kerberos + LDAP pfSense	pfSense WebGUI доступний **лише** після LDAP-автентифікації через FreeIPA; анонімний вхід відхилено
Least Privilege	HBAC + default deny pfSense	office-users → SSH до db.lab.local → відмова PAM навіть при відкритому TCP 22 у firewall
Assume Breach	Snort IPS inline + VLAN	Nmap-скан: IP заблоковано менш ніж за 3 с; lateral movement між VLAN 10↔20 неможливий (сценарій №2)
Verify Explicitly (Devices)	Port Security Cisco IOS	Підміна MAC на Gi0/1 → порт у err-disabled за 0 с, лог у Syslog
Continuous Monitoring	Syslog + Snort alerts	Усі 13 тестових подій зафіксовані на Syslog Server (192.168.20.30) з timestamp

3.4.4. Аналіз переваг та умов застосування рішення

Порівняння з класичним периметральним підходом. Традиційна модель захисту периметру передбачає, що внутрішня мережа є довіреною зоною, а

захист зосереджено на зовнішній межі. У реалізованій архітектурі нульової довіри жоден вузол не є апріорі довіреним незалежно від його розташування у мережі. Ключові відмінності наведено нижче:

Таблиця 3.11

Порівняння з класичним підходом

Аспект	**Класичний периметр**	**Реалізована Zero Trust архітектура**
Модель довіри	Внутрішня мережа довірена	Жоден вузол не є довіреним
Контроль доступу	На основі IP-адреси та VLAN	На основі ідентичності користувача (HBAC)
Lateral movement	Вільний всередині периметру	Обмежено міжзоновими правилами pfSense
Автентифікація	Локальна на кожному вузлі	Централізована через FreeIPA Kerberos
Видимість	Журнали окремих пристроїв	Централізований Syslog з усіх вузлів
Реагування на загрозу	Ручне, після виявлення	Автоматичне блокування через Snort

Порівняльний аналіз підтверджує, що поєднання pfSense CE + Cisco IOSvL2 + FreeIPA є оптимальним саме для реалізованої чотиризонної Zero Trust архітектури. Жодна з альтернативних комбінацій не забезпечує **одночасно**: нативний HBAC на рівні хосту (відсутній в AD без GPO + Windows-клієнтів), stateful firewall із вбудованим IPS без додаткових ліцензій (відсутній в Cisco ISE без Advanced tier) та повну відтворюваність стенду в GNS3/VirtualBox на open-source компонентах. Зокрема, заміна FreeIPA на OpenLDAP усунула б HBAC-контроль — і сценарій №4 (блокування SSH office-users → DB) був би реалізований виключно на рівні firewall pfSense, без подвійного захисту на рівні PAM, що суперечить принципу Defense in Depth

Таким чином, компрометація одного вузла не призводить до компрометації всієї інфраструктури завдяки принципу Assume Breach, реалізованому через мікросегментацію.

Оптимальний масштаб та умови застосування. Реалізована архітектура є оптимальною для організацій з кількістю від 50 до 500 користувачів, що мають кілька функціональних підрозділів з різними вимогами до доступу. Рішення доцільно застосовувати у таких умовах: наявність виділеного IT-персоналу для адміністрування FreeIPA та pfSense; вимоги до відповідності стандартам інформаційної безпеки (ISO 27001, NIST); наявність ресурсів критичної важливості, що потребують ізоляції (бази даних, фінансові системи).

Обмеження рішення. Реалізована архітектура має ряд обмежень, що є напрямками подальшого розвитку. По-перше, відсутня система управління інформацією та подіями безпеки (SIEM) для автоматичної кореляції журналів і виявлення складних багатоетапних атак. По-друге, шифрування трафіку між внутрішніми сегментами не реалізовано, що є вразливістю при компрометації комутатора. По-третє, відсутній механізм безперервної перевірки стану вузлів (device health check), що є повноцінним компонентом зрілої Zero Trust архітектури згідно з CISA Zero Trust Maturity Model рівня 3. По-четверте, масштабування FreeIPA до кількох сайтів потребує розгортання додаткових реплік та налаштування між-сайтової реплікації каталогу.

Висновки до третього розділу

У третьому розділі встановлено, що реалізація Zero Trust інфраструктури на базі open-source компонентів є технічно повноцінною та відтворюваною: лабораторний стенд із дев'яти вузлів (pfSense CE, Cisco IOSvL2, FreeIPA/CentOS Stream 9 та шість Ubuntu-вузлів) успішно розгорнуто в єдиному середовищі GNS3/VirtualBox без комерційних ліцензій, що підтверджує придатність обраного інструментарію для моделювання корпоративної мережі малого та середнього масштабу.

Доведено, що чотиризонна VLAN-сегментація (Office, Servers, DMZ, Management) у поєднанні з політикою default deny на pfSense повністю унеможливлює lateral movement між зонами — усі міжзонові з'єднання без явного дозволу (сценарії №2, 3, 4) блоковані на рівні stateful firewall із

результатом 100% packet loss. Підтверджено, що HBAC-правила FreeIPA реалізують контроль доступу на рівні хоста незалежно від стану мережевих правил: SSH-з'єднання office-users → db.lab.local відхиляється PAM/SSSD навіть за технічно відкритого TCP 22 у firewall, що доводить ефективність принципу Defense in Depth.

Показано, що Snort IPS у режимі inline на WAN-інтерфейсі pfSense забезпечує автоматичне блокування IP-адреси атакуючого після виявлення сигнатур сканування (ET SCAN Nmap OS Detection Probe, пріоритет 2) у часовому проміжку менш ніж 3 секунди, що унеможливлює пасивну розвідку інфраструктури без негайного виявлення та реагування. Усі 13 тестових сценаріїв завершились очікуваним результатом без жодного хибнонегативного спрацювання, що верифікує коректність реалізованих механізмів безпеки в комплексі.

Обґрунтовано відповідність реалізованої архітектури ключовим принципам NIST SP 800-207 та рівню Initial–Advanced за шкалою CISA ZTMM v2.0 у п'яти пілонах (Identity, Devices, Networks, Applications/Workloads, Data): принцип Never Trust, Always Verify підтверджено обов'язковою LDAP-автентифікацією через FreeIPA, Least Privilege — подвійним блокуванням на рівні firewall і PAM, Assume Breach — автоматичним реагуванням Snort і повною міжзоновою ізоляцією.

Визначено вектори масштабування системи: впровадження SIEM для кореляції подій із Syslog та Snort-алертів, криптографічний захист внутрішніх міжзонових каналів засобами IPsec або WireGuard, безперервна валідація кінцевих вузлів (device health check) як умова надання доступу, а також розширення покриття CISA ZTMM до рівня Advanced у пілоні Applications/Workloads через L7-інспекцію трафіку.

ВИСНОВКИ

Магістерська робота присвячена розробленню, налаштуванню та експериментальному обґрунтуванню захищеної мережевої інфраструктури на принципах архітектури нульової довіри (Zero Trust) із застосуванням рішень корпоративного класу та відкритого програмного забезпечення.

За результатами аналізу сучасних підходів до мережевої безпеки встановлено, що традиційна периметрова модель («замок та рів») втратила ефективність в умовах зростання кількості APT-атак, поширення ransomware (зростання на 44% у 2024 році) та переходу до розподіленої роботи. Доведено, що архітектура Zero Trust — з принципами Never Trust, Always Verify, мікросегментації та мінімальних привілеїв — є обґрунтованою відповіддю на ці виклики, що підтверджується стандартами NIST SP 800-207 та CISA ZTMM v2.0.

Спроєктовано і практично реалізовано у середовищі GNS3 повнофункціональну чотиризонну корпоративну мережу (Office VLAN 10, Servers VLAN 20, DMZ VLAN 30, Management VLAN 99). Підтверджено чіткий розподіл функцій між компонентами: Cisco IOSvL2 виконує L2-ізоляцію зон, фільтрацію на рівні портів (PACL, Extended ACL) та захист від підміни MAC-адрес (port-security, режим violation shutdown); pfSense CE виступає ядром міжзонової маршрутизації (Router-on-a-Stick) з політикою default deny та системою виявлення і запобігання вторгненням Snort у режимі inline; FreeIPA забезпечує централізоване управління ідентичностями на базі Kerberos, LDAP, HBAC та власного PKI (Dogtag CA).

Доведено, що реалізований захист є багаторівневим: HBAC-правила FreeIPA блокують несанкціонований SSH-доступ на рівні PAM/SSSD незалежно від стану мережевих правил, а Snort автоматично блокує IP-адресу атакуючого після виявлення сигнатур сканування протягом менш ніж 3 секунд. Тестування за методом «чорного ящика» (13 сценаріїв із 13 успішних) підтвердило коректну роботу мікросегментації, рольової автентифікації, автоматичного блокування загроз та повної видимості подій через централізований Syslog — жоден сценарій не показав хибнонегативного результату.

Порівняльне оцінювання засвідчило відповідність реалізованої архітектури шести із семи тенетів NIST SP 800-207 та рівню Initial–Advanced за п'ятьма пілонами CISA ZTMM v2.0 (Identity, Devices, Networks, Applications/Workloads, Data). Обґрунтовано, що обрана зв'язка інструментів (pfSense CE, Cisco IOSvL2, FreeIPA) є оптимальною для малого та середнього підприємства: забезпечує функціональність корпоративного рівня без комерційних ліцензійних витрат і є повністю відтворюваною на open-source компонентах.

Таким чином, мету магістерської роботи досягнуто: розроблена інфраструктура практично реалізує ключові принципи Zero Trust і підтверджена комплексним тестуванням. Перспективи подальших досліджень полягають у досягненні рівня Advanced–Optimal за CISA ZTMM: впровадженні SIEM для проактивної кореляції подій, наскрізному шифруванні внутрішніх каналів (IPsec/WireGuard) та автоматизованій валідації стану кінцевих вузлів (device health check) як обов'язковій умові надання доступу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Khalil M. Cybersecurity Statistics 2025: Breach Costs, Ransomware & AI Threats [Електронний ресурс] // DeepStrike. 2025. URL: https://deepstrike.io/blog/cybersecurity-statistics-2025-threats-trends-challenges

2. Speed of Cyber Attacks Increased in 2024 with Lateral Movement Achieved in Just 27 Minutes [Електронний ресурс] // ReliaQuest Annual Threat Report. 2025. URL: https://reliaquest.com/news-and-press/speed-of-cyber-attacks-increased-in-2024-with-lateral-movement-achieved-in-just-27-minutes-reliaquest-annual-threat-report/

3. The Top 11 Cyberattacks Using Lateral Movement: A 2023–2024 Analysis for Enterprise Security Leaders [Електронний ресурс] // Elisity. URL: https://www.elisity.com/blog/the-top-11-cyberattacks-using-lateral-movement-a-2023-2024-analysis-for-enterprise-security-leaders

4. Phillips J. The Top 11 Cyberattacks Using Lateral Movement [Електронний ресурс] // LinkedIn. URL: https://www.linkedin.com/posts/jasonbphillips_the-top-11-cyberattacks-using-lateral-movement-activity-7290060496349659136-7C8O

5. Cybersecurity Statistics of 2025 [Електронний ресурс] // NordLayer. URL: https://nordlayer.com/blog/cybersecurity-statistics-of-2025/

6. Cybersecurity Statistics [Електронний ресурс] // Fortinet Cyberglossary. URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

7. Zero Trust in the Age of Autonomous Threats: Why Perimeter Security Is No Longer Enough [Електронний ресурс] // LinkedIn Pulse. URL: https://www.linkedin.com/pulse/zero-trust-age-autonomous-threats-why-perimeter-security-k-20src

8. Zero Trust Security: The Future of Enterprise Network Protection [Електронний ресурс] // Nebulex. URL: https://nebulex.com.au/zero-trust-security-the-future-of-enterprise-network-protection/

9. Zero Trust Architecture: How to Reduce Cyber Risks by 60% in 2024 [Електронний ресурс] // Number7even. URL: https://number7even.com/comprehensive-web-development-services/zero-trust-architecture-how-to-reduce-cyber-risks-by-60-in-2024/

10. The Top 11 Cyberattacks Using Lateral Movement: A 2023–2024 Analysis for Enterprise Security Leaders [Електронний ресурс] // Elisity. URL: https://www.elisity.com/blog/the-top-11-cyberattacks-using-lateral-movement-a-2023-2024-analysis-for-enterprise-security-leaders

11. A Brief(er) History of Zero Trust: Major Milestones in Rethinking Enterprise Security [Електронний ресурс] // Zscaler. URL: https://www.zscaler.com/blogs/product-insights/brief-er-history-zero-trust-major-milestones-rethinking-enterprise-security

12. History of Zero Trust [Електронний ресурс] // 1Password Blog. URL: https://1password.com/blog/history-of-zero-trust

13. History of Zero Trust [Електронний ресурс] // NordPass. URL: https://nordpass.com/es/blog/history-of-zero-trust/

14. A Look Back at Zero Trust: Never Trust, Always Verify [Електронний ресурс] // Forrester Blogs. URL: https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/

15. History and Evolution of Zero Trust [Електронний ресурс] // SecurityWeek. URL: https://www.securityweek.com/history-and-evolution-zero-trust/

16. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. 59 p. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

17. NIST SP 800-207: Zero Trust Architecture [Електронний ресурс] // Terrazone. URL: https://terrazone.io/nist-sp-800-207/

18. What Is NIST SP 800-207? [Електронний ресурс] // Palo Alto Networks Cyberpedia. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-nist-sp-800-207

19. CISA Zero Trust Maturity Model [Електронний ресурс] // Vistrada. URL: https://vistrada.com/resources/insights/cisa-zero-trust-maturity-model

20. Zero Trust Maturity Model [Електронний ресурс] // CybeReady. URL: https://cybeready.com/zero-trust-maturity-model/

21. OPNsense vs pfSense [Електронний ресурс] // StationX. URL: https://www.stationx.net/opnsense-vs-pfsense/

22. pfSense Security Monitoring [Електронний ресурс] // Zenarmor. URL: https://www.zenarmor.com/docs/network-security-tutorials/pfsense-security-monitoring

23. OPNsense vs pfSense: Homelab 2026 [Електронний ресурс] // DIY Media Server. 2026. URL: https://diymediaserver.com/post/2026/opnsense-vs-pfsense-homelab-2026/

24. OPNsense Features [Електронний ресурс] // OPNsense. URL: https://opnsense.org/features/

25. [Електронний ресурс] // The American Journals. URL: https://www.theamericanjournals.com/index.php/tajmei/article/view/6804

ДОДАТКИ

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-CORE
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 4 DfDyNfASCooEyb0pmhGQQF6dGjOiHYRe52/FJRFOcG2
no aaa new-model
no ip icmp rate-limit unreachable
!
! Вимикаємо L3-маршрутизацію, щоб пристрій працював виключно як L2-комутатор
no ip routing
ip cef
!
no ip domain-lookup
ip domain-name lab.local
no ipv6 cef
ipv6 multicast rpf use-bgp
!
spanning-tree mode pvst
spanning-tree extend system-id
!
! Створення бази VLAN
vlan 10
 name Office
vlan 20
 name Servers
vlan 30
 name DMZ
vlan 99
 name Management
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
!
! Транковий порт до pfSense (Router-on-a-Stick)
interface Ethernet0/0
 description Trunk-to-pfSense
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,20,30,99
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 description FreeIPA-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 ! Застосування PACL (Port ACL) для фільтрації на рівні порту
 ip access-group ACL_VLAN20_IN in
```

```
 duplex auto
 spanning-tree portfast
!
interface Ethernet0/2
 description Admin-PC-MGMT
 switchport access vlan 99
 switchport mode access
 switchport port-security
 ip access-group ACL_VLAN99_IN in
 duplex auto
 spanning-tree portfast
!
interface Ethernet0/3
 description Web-Server-DMZ
 switchport access vlan 30
 switchport mode access
 switchport port-security
 ip access-group ACL_VLAN30_IN in
 duplex auto
 spanning-tree portfast
!
interface Ethernet1/0
 description Syslog-Server-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 ip access-group ACL_VLAN20_IN in
 duplex auto
 spanning-tree portfast
!
interface Ethernet1/1
 description DB-Server-VLAN20
 switchport access vlan 20
 switchport mode access
 switchport port-security
 ip access-group ACL_VLAN20_IN in
 duplex auto
 spanning-tree portfast
!
interface Ethernet1/2
 description Client-1-VLAN10
 switchport access vlan 10
 switchport mode access
 switchport port-security
 duplex auto
 spanning-tree portfast
!
! (Інші порти Ethernet1/3 - Ethernet5/3 залишено без змін)
!
interface Vlan1
 no ip address
 shutdown
!
! L3-інтерфейс виключно для менеджменту комутатора
interface Vlan99
 description Management-SVI
 ip address 192.168.99.2 255.255.255.0
!
ip default-gateway 192.168.99.1
!
no ip http server
!
! Списки контролю доступу (ACL)
ip access-list standard SSH-MGMT-ONLY
```

```
 permit 192.168.99.0 0.0.0.255
 deny   any
!
ip access-list extended ACL_VLAN20_IN
 permit udp 192.168.20.0 0.0.0.255 host 192.168.20.10 eq domain
 permit tcp 192.168.20.0 0.0.0.255 host 192.168.20.10 eq 443
 deny   ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 deny   ip 192.168.20.0 0.0.0.255 192.168.99.0 0.0.0.255
 permit ip any any
!
ip access-list extended ACL_VLAN30_IN
 permit tcp any host 192.168.30.10 eq www
 permit tcp any host 192.168.30.10 eq 443
 permit udp 192.168.30.0 0.0.0.255 host 192.168.20.30 eq syslog
 deny   ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny   ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255
 permit ip any any
!
ip access-list extended ACL_VLAN99_IN
 permit tcp host 192.168.99.10 any eq 22
 permit tcp host 192.168.99.10 any eq 443
 permit tcp host 192.168.99.10 any eq www
 permit ip 192.168.99.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny   ip 192.168.99.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip any any
!
logging source-interface Vlan99
logging host 192.168.20.30
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 access-class SSH-MGMT-ONLY in
 login local
 transport input ssh
!
end
```