НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	Комп'ютерних систем і мереж
_____/ Болбот І.М., д.т.н, проф. /	_____/ Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2025 р.	«___»_____2025 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему: «Дослідження та розробка мережевої інфраструктури факультету»

Спеціальність: 123 «Комп’ютерна інженерія»

Освітня програма: Комп’ютерні системи та мережі

Керівник дипломного проєкту: _____ / Коваленко О.Є. /
підпис ПІБ

Виконав: _____ / Шкурат В.І. /
підпис ПІБ

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 2025 р.

ЗАВДАННЯ

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Шкурату Владиславу Ігоровичу
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): 123 «Комп'ютерна інженерія».
Освітня програма: Комп'ютерні системи та мережі

Тема магістерської роботи: «Дослідження та розробка мережевої інфраструктури факультету»
затверджена наказом проректора з науково-педагогічної роботи та цифрової трансформації НУБІП України від "29 " жовтня 2024 р. № 1941 "С"
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи: мережева інфраструктура факультету, середовище віртуалізації EVE-NG Pro, Міжмережевий екран Fortigate-VM, комутатор FortiSwitch-108D-VM, система моніторингу FortiAnalyzer-VM.
Перелік питань, що підлягають дослідженню:

1. Аналіз предметної області для дослідження мережевої інфраструктури факультету
2. Проєктування мережі факультету з використаням сучасних вимог та технологій
3. Побудова моделі захищеної мережі навчального закладу

Дата видачі завдання " 29 " жовтня 2024 р.

Керівник магістерської роботи _____ / Коваленко О.Є. д.т.н., професор /
(підпис) (ПІБ, вчене звання і ступінь)

Завдання прийняв до виконання _____ / Шкурат В.І. /
(підпис) (ПІБ)

РЕФЕРАТ

Пояснювальна записка: 91с., 67 рис., 4 додатка, 20 використаних джерел.

МЕРЕЖА. НАВЧАЛЬНИЙ ЗАКЛАД, БЕЗПЕКА, МОНІТОРИНГ, FORTINET SECURITY FABRIC, ACTIVE DIRECTORY, EVE-NG, REMOTE ACCESS VPN

Мета роботи – дослідити поточну мережеву інфраструктуру факультету та розробити оновлену мережу, з урахуванням сучасних вимог.

Об’єкт – комп’ютерна мережа навчального закладу.

Предмет – принципи та методи реалізації мережевої інфраструктури факультету.

Робота складається з трьох розділів.

У першому розділі проведений аналіз поточної мережі факультету, розглянуто базові технології та виявлено її основні недоліки.

У другому розділі розглянуто сучасні архітектурні рішення, виконано їх порівняльний аналіз, та обґрунтовано вибір для моделювання.

У третьому розділі детально описаний процес практичного моделювання обраної архітектури в середовищі EVE-NG, та проведено налаштування її компонентів.

В результаті виконання магістерської роботи проведено аналіз поточної мережевої інфраструктури факультету та виявлено її основні недоліки: відсутність резервування, низький рівень безпеки, обмежені можливості адміністрування, застаріле обладнання, високий рівень навантаження. На основі сучасних підходів і технологій було обґрунтовано вибір оптимальної архітектури для її модернізації. Розроблена мережа забезпечує підвищений рівень безпеки, масштабованості, надійності, централізованого керування та моніторингу.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IP	–	Internet Protocol
DDoS	–	Distributed Denial-of-Service атака
STP	–	Spanning Tree Protocol
RSTP	–	Rapid Spanning Tree Protocol
MSTP	–	Multiple Spanning Tree Protocol
OSPF	–	Open Shortest Path First
BGP	–	Border Gateway Protocol
SPF	–	Shortest Path First
LSDB	–	Link-State Database
VLAN	–	Virtual Local Area Network
SD-Access	–	Software-Defined Access
ARP	–	Address Resolution Protocol
DAI	–	Dynamic ARP Inspection
DHCP	–	Dynamic Host Configuration Protocol
CDP	–	Cisco Discovery Protocol
LLDP	–	Link Layer Discovery Protocol
ACL	–	Access Control List
QoS	–	Quality of Service
LASP	–	Link Aggregation Control Protocol
PAgP	–	Port Aggregation Protocol
HSRP	–	Hot Standby Router Protocol
VRRP	–	Virtual Router Redundancy Protocol
GLBP	–	Gateway Load Balancing Protocol
IoT	–	Internet of Things
ISE	–	Identity Services Engine
LISP	–	Locator/ID Separation Protocol
VXLAN	–	Virtual Extensible LAN

ВСТУП

Сучасні ІТ-технології кардинально змінили наше життя, і освіта - не виняток. Сьогодні більшість навчальних процесів, наукових досліджень і адміністративних функцій тісно пов’язані з використанням комп’ютерних мереж. Вони забезпечують швидкий обмін даними, доступ до електронних ресурсів, комунікацію між підрозділами та користувачами. Без надійної, стабільної та захищеної мережевої інфраструктури ефективне функціонування навчального закладу практично неможливе.

Мережева інфраструктура факультету є основою для роботи серверів, навчальних лабораторій, систем електронного навчання, внутрішніх порталів, хмарних сервісів і засобів віддаленого доступу. Вона поєднує в єдину систему викладачів, студентів та адміністрацію, забезпечуючи безперервний обмін інформацією. З часом мережа зазнає змін, збільшується кількість підключених пристроїв, зростає обсяг передаваних даних, впроваджуються нові сервіси. Це призводить до підвищення навантаження на наявне обладнання, появи конфліктів конфігурацій, зниження продуктивності та складнощі у підтриманні безпеки.

Проблеми, що виникають у таких умовах, часто пов’язані з відсутністю чіткої структури, неефективним розподілом трафіку, недостатнім рівнем сегментації мережі та відсутністю централізованого контролю. Тому виникає необхідність у детальному дослідженні існуючої інфраструктури факультету, виявленні її слабких сторін і пошуку шляхів удосконалення з урахуванням сучасних стандартів побудови мереж.

Метою цієї роботи є дослідження мережі факультету, аналіз її поточного стану та визначення напрямів модернізації з метою підвищення ефективності, безпеки й керованості. Щоб це зробити, потрібно вирішити наступні завдання: провести аналіз логічної структури мережі, оцінити взаємодію між основними компонентами, визначити недоліки фізичному, канальному та мережевому рівнях,

розглянути можливі архітектурні підходи для модернізації та створити симуляційну модель із використанням сучасних засобів віртуалізації.

Важливими є і технології, що забезпечують централізоване управління, динамічний розподіл політик доступу та високий рівень захисту інформації. У цьому сенсі розглядаються підходи, реалізовані в таких рішеннях, як Cisco SD-Access і Fortinet Security Fabric, які дозволяють будувати масштабовані, гнучкі та безпечні мережі.

Практична частина роботи виконана в середовищі EVE-NG, що дало змогу створити повноцінну модель мережі факультету без використання фізичного обладнання. На основі цієї моделі проведено налаштування комутаторів, маршрутизаторів, міжмережевого екрану FortiGate, служби Active Directory та системи аналітики FortiAnalyzer. Це дозволило перевірити взаємодію компонентів, протестувати різні сценарії роботи мережі й оцінити ефективність запропонованих удосконалень.

Результатом дослідження є побудована модель мережі факультету враховуючи сучасні тенденції побудови, архітектурні рішення, а також рекомендації щодо покращення існуючої інфраструктури. Запропоновані рішення спрямовані на побудову правильної топології, підвищення рівня безпеки, спрощення адміністрування та створення умов для подальшого розвитку мережі відповідно до сучасних стандартів у сфері комп’ютерних систем і телекомунікацій.

1 ОГЛЯД ПРОБЛЕМ ТА МЕТОДІВ ЇХ ВИРІШЕННЯ ПРИ ПОБУДОВІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1 Що таке мережева інфраструктура

У сучасному швидко змінному цифровому просторі, міцна мережева інфраструктура є незамінною для бізнесів будь-якого роду. Вона є основою, яка забезпечує ефективну комунікацію, просте спільне використання даних та доступ до важливих ресурсів. З ростом технологій, розуміння цієї складної мережі, створеної між апаратними компонентами, стає все більш критичним для організацій.

Маршрутизатори, комутатори та брандмауери - три основні пристрої, які утворюють більшість мереж. Маршрутизатор - це мережевий пристрій, який приймає вхідні пакети даних з різних мереж і пересилає їх найкращим шляхом. Іншими словами, вони виступають у ролі дверей, забезпечуючи те, щоб дані з локальних мереж могли потрапити туди, куди необхідно, за межами мережі.

Комутатори роблять це можливим, пересилаючи пакети даних між пристроями в одній мережі. На відміну від хабів, комутатори можуть надсилати дані напряму отримувачеві, що призводить до більшої ефективності та меншої завантаженості мережі.

У той самий час, брандмауери виступають у ролі уважних охоронців мережевої безпеки, які контролюють та регулюють рух даних на підставі певних політик безпеки, перш ніж вони вийдуть за межі або потраплять до домашньої мережі. Їх головна функція полягає у забезпеченні мережі від несанкціонованого доступу та будь-яких можливих кібератак.

Вибір відповідної мережевої інфраструктури є важливим рішенням, яке залежить від багатьох факторів, включаючи розмір бізнесу, вимоги та навіть обмеження бюджету, а також потреби масштабування. Менші підприємства можуть використовувати всі-в-одному пристрої, які виконують функції маршрутизатора,

комутатора та брандмауера в одному пристрої, тоді як більші корпорації та урядові організації можуть мати конфігурації з спеціалізованими безпечними пристосуваннями для окремих одиниць. Прогнозування потреб у ширинах каналу, планування зростання кількості послуг та вибір між керованими чи некерованими послугами є важливими моментами.

Протокол Інтернету (IP) є основою передачі даних у комп'ютерних мережах по всьому світу та присвоює унікальну IP-адресу кожному підключеному пристрою, яку можна використовувати для ідентифікації та визначення місцезнаходження. Збільшення поступового росту кількості пристроїв, підключених до інтернету, є необхідним умовним фактором для переходу на IPv6 з метою заміни поточного обмеженого діапазону адрес.

Ось тут й приходить на допомогу розмежування мереж, яке фактично допомагає нам розбити велику мережу на менші підмережі для більш ефективного, безпечного та кращого управління трафіком. Логічне розділення пристроїв на окремі підмережі дає адміністраторам кращий контроль над доступом, одночасно зменшуючи трансляційний трафік і дозволяючи оптимальні рішення щодо маршрутизації.

Зростання кількості та масштабу кібернетичних загроз, зокрема шкідливого програмного забезпечення (malware), фішингу та DDoS-атак, визначає кібербезпеку як один із обов’язкових аспектів функціонування комп’ютерних мереж. Ефективна стратегія безпеки включає більше, ніж просто сильні фаєрволи - вона також має на увазі системи виявлення/запобігання вторгненням, антивірусне програмне забезпечення, своєчасну установку нових патчів та версій, а також навчання користувачів кібербезпеці.

Модель безпеки Zero-Trust може бути налаштована для уникнення доступу до мережевих ресурсів, окрім необхідності. Це забезпечує додаткову охорону під час пересилання даних та у стані спокою на вашому сервері бази даних. Збереження захисних механізмів, таких як найкращі практики безпеки, наприклад, шифрування чутливих даних під час передачі та у стані спокою, регулярні резервні копії та плани

відновлення після аварій, можуть допомогти вам тримати бізнес у русі, не втрачаючи значну частину операційної ефективності через кібератаки. [1]

1.2 Основні поняття локальної інфраструктури факультету

При створенні локальної мережевої інфраструктури факультету необхідно враховувати низку ключових аспектів, які забезпечують стабільну роботу системи та відповідають потребам освітнього процесу.

Одним із найважливіших етапів є вибір обладнання. Для різних типів мереж використовуються різні пристрої відповідно до їх функціоналу. Так, комутатори дозволяють об’єднати комп’ютери, сервери чи інші мережеві пристрої в єдиний сегмент, маршрутизатори забезпечують обмін даними між окремими мережами, а сервери виконують роль сховищ та центрів обробки інформації. Якість та продуктивність обраного обладнання безпосередньо впливають на швидкодію мережі, що особливо важливо в умовах постійного збільшення обсягів цифрових ресурсів у навчальному середовищі.

Ще одним важливим параметром є можливість масштабування. Мережева інфраструктура повинна бути гнучкою та легко адаптуватися до зростання кількості користувачів і впровадження нових технологій.

Окремі види обладнання працюють на різних рівнях моделі TCP/IP. Наприклад, комутатори функціонують на канальному рівні та є основними пристроями при побудові локальних мереж, оскільки здатні забезпечувати високу пропускну здатність. На відміну від них, концентратори є більш бюджетним рішенням, однак вони передають дані на всі підключені порти без можливості сегментації, що призводить до перевантаження та зниження продуктивності. Через це їхнє використання доцільне лише у невеликих або ізольованих сегментах, де критичність швидкості передачі даних є низькою, наприклад, для підключення камер спостереження.

Комутатори та маршрутизатори відіграють ключову роль у передачі даних у мережі. Перші організовують ефективний обмін інформацією всередині сегмента,

використовуючи Ethernet-кадри, тоді як другі визначають оптимальні маршрути для взаємодії між різними мережами.

1.2.1 Робота комутатора

Принцип роботи комутатора базується на формуванні таблиці MAC-адрес. На початковому етапі вона є порожньою, і пристрій працює у режимі вивчення мережі, передаючи всі отримані кадри на всі порти, окрім порту джерела. Поступово комутатор накопичує інформацію про MAC-адреси пристроїв та порти, через які вони доступні. Коли таблиця заповнюється, обмін даними відбувається цілеспрямовано, без широкомовних розсилок, що значно підвищує ефективність роботи локальної мережі.

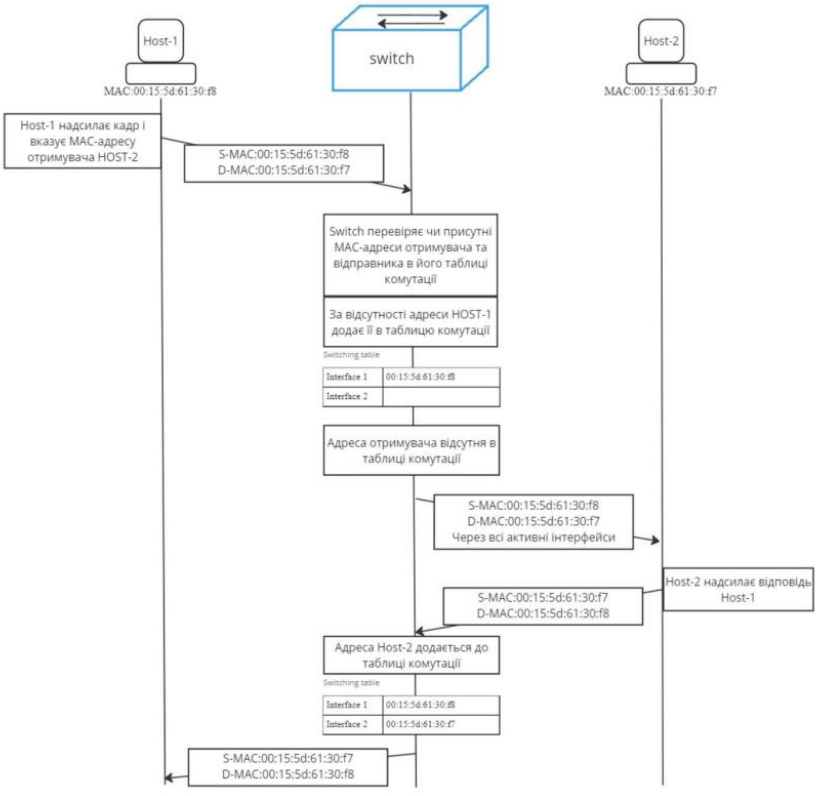


Рисунок 1.1 – Діаграма вивчення мережі комутатором

Якщо комутатор отримує кадр із MAC-адресою, яка вже присутня у таблиці комутації, але надходить він через інший порт, запис у таблиці оновлюється та прив’язується до нового інтерфейсу. При проєктуванні мережевої інфраструктури слід враховувати обсяг цієї таблиці, оскільки її переповнення може негативно позначитися на роботі обладнання.

На функціонування комутаторів впливають різні мережеві протоколи, одні з них STP та 802.1Q. У топологіях, що містять петлі, виникає ризик широкомовних штормів, коли широкомовні кадри нескінченно циркулюють між пристроями. Це пов’язано з тим, що кадри канального рівня не мають механізму контролю надмірної ретрансляції. Для усунення цієї проблеми застосовується протокол Spanning Tree Protocol (STP), який трансформує топологію в деревоподібну структуру, блокуючи надлишкові шляхи. Виявлення петель здійснюється на основі аналізу таблиці MAC-адрес: якщо одна й та сама адреса доступна через кілька інтерфейсів, протокол автоматично блокує один із них.

Протокол 802.1Q додає до кадру ідентифікатор VLAN, що дозволяє обмежувати передачу даних через конкретні інтерфейси. У цьому випадку інтерфейси комутатора можуть функціонувати в одному з трьох режимів:

- Access – призначений для роботи з одним VLAN; усі кадри, що надходять, маркуються певним тегом.

- Trunk – дозволяє передавати кадри з різними VLAN-ідентифікаторами через один порт.

- Hybrid – поєднує властивості попередніх режимів, підтримуючи як один нетегований VLAN, так і множину тегованих.[2]

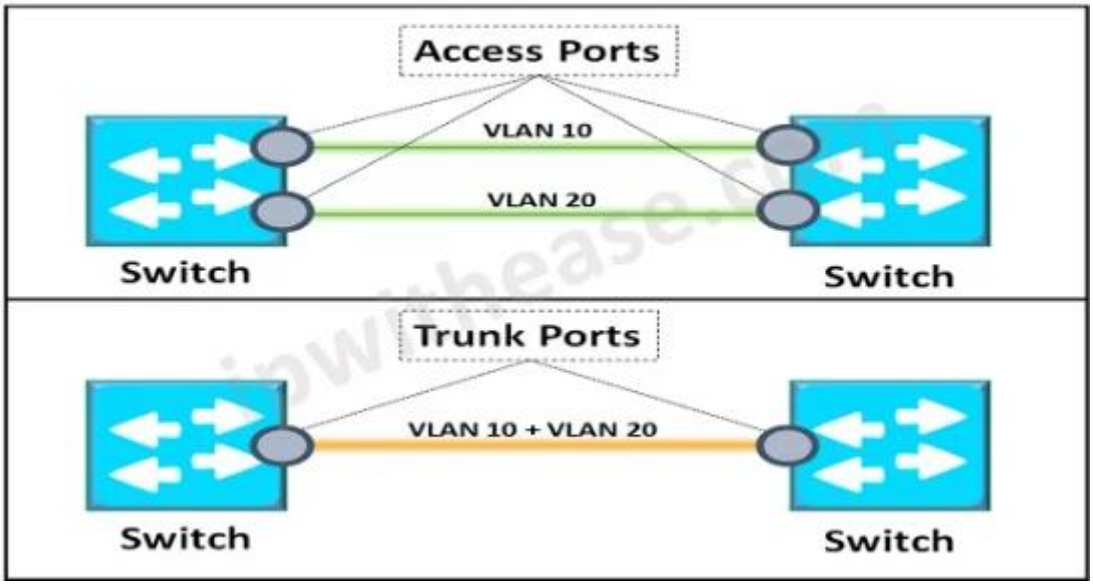


Рисунок 1.2 – Зображення режимів роботи інтерфейсів комутатора

1.2.2 Робота маршрутизатора

Маршрутизатори виконують поєднання різних мереж із відмінними архітектурами, забезпечуючи їхню взаємодію. Прийняття рішень щодо пересилання пакетів відбувається на основі інформації про мережеву топологію та правил, визначених адміністратором. Це дозволяє оптимізувати маршрутизацію та підвищувати ефективність обміну даними.

В моделі OSI маршрутизатор працює на мережевому рівні, адже забезпечує логічне з’єднання між сегментами мережі та організовує маршрутизацію пакетів. Сучасні маршрутизатори також мають розширений функціонал: виконують фільтрацію трафіку, підтримують політики безпеки та сприяють нормалізованому використанню ресурсів.

Основою прийняття рішень щодо маршрутизації є таблиці маршрутизації. Вони складаються з набору записів, де для кожного маршруту зазначені ключові параметри:

- Мережева адреса призначення – кінцева IP-адреса, куди потрібно доставити пакет.

- Маска підмережі – вказує, які біти IP-адреси належать мережі, а які ідентифікують хост.

- Шлюз за замовчуванням – маршрутизатор, через який передається трафік за відсутності прямого маршруту.

- Інтерфейс – фізичний чи логічний порт, через який відправляється пакет.

Прийняття рішення про пересилання пакета починається з аналізу його заголовка. Маршрутизатор порівнює адресу призначення з даними у таблиці маршрутизації. Якщо знайдено точний збіг, пакет пересилається за визначеним маршрутом. У випадку відсутності відповідного запису використовується маршрут за замовчуванням або застосовується механізм пошуку на основі найкращого часткового збігу.

Обмін інформацією про маршрути між маршрутизаторами здійснюється за допомогою протоколів маршрутизації, найрозповсюдженіші це OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol). Так, OSPF використовує алгоритм SPF (Shortest Path First), який дозволяє обчислювати оптимальні шляхи передачі даних на основі вартості з’єднань та топології мережі.

1.2.3 OSPF

Робота протоколу OSPF включає наступні етапи:

1 Формування бази стану каналів (LSDB) – кожен маршрутизатор збирає інформацію про сусідні пристрої та формує базу даних, що відображає стан усіх з’єднань у межах мережі.

2 Виконання алгоритму SPF – після формування LSDB маршрутизатор застосовує алгоритм SPF для визначення найкоротших шляхів до кожного вузла мережі з урахуванням вартості з’єднань.

3 Розповсюдження інформації – результати обчислень поширюються між маршрутизаторами, що дозволяє оновлювати таблиці маршрутизації в реальному часі.

4 Активація оптимальних маршрутів – після отримання актуальної інформації про найкоротші шляхи маршрутизатор оновлює власну таблицю та починає використовувати оптимальні маршрути для пересилання трафіку.

В результаті, OSPF забезпечує динамічне оновлення таблиць маршрутизації та готовність мережі до змін в топології, що дозволяє підтримувати ефективний і стабільний обмін даними.

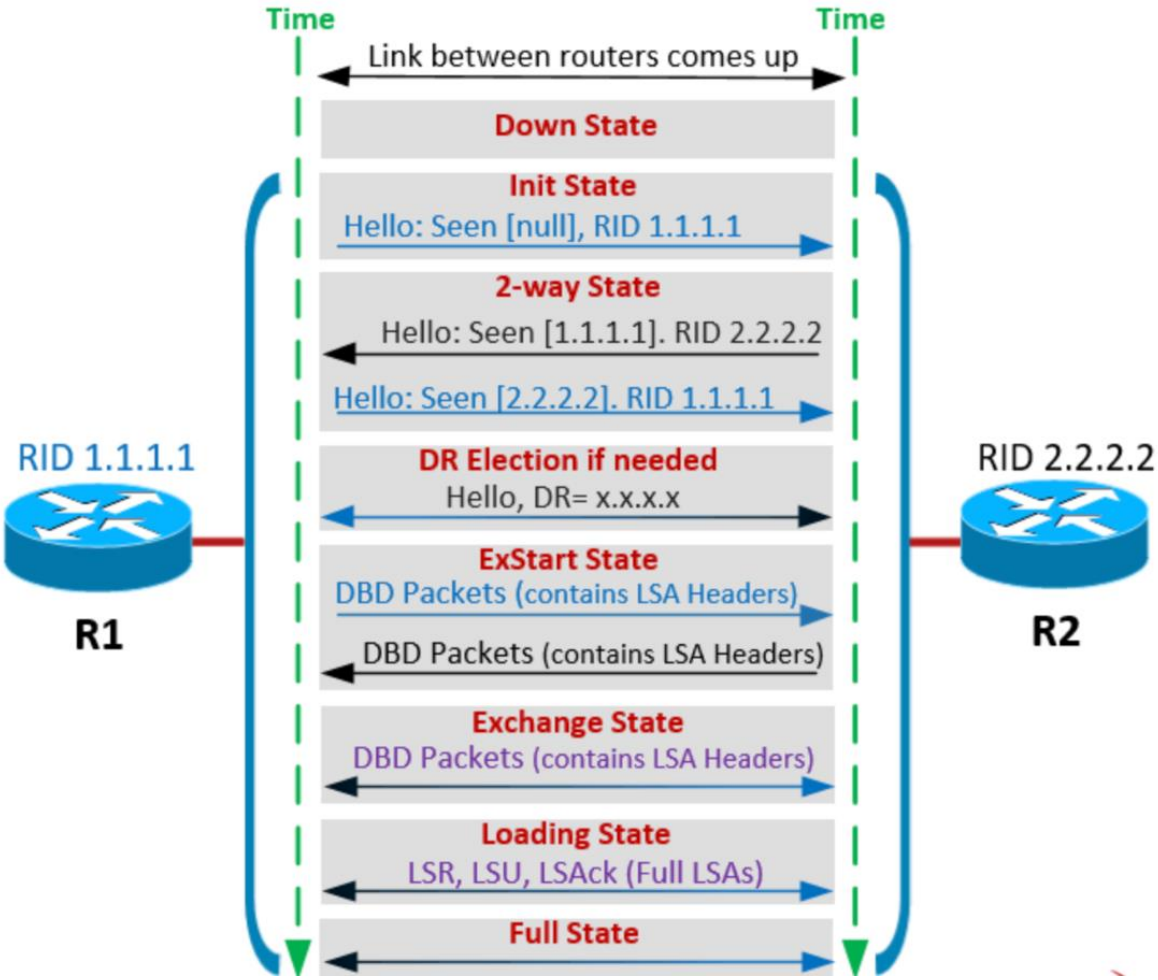


Рисунок 1.3 – Стани протоколу OSPF під час встановлення сусідства

У невеликих мережах, де всі пристрої розташовані в одному сегменті, достатньо статичної маршрутизації. Зі зростанням масштабів мережі та необхідністю розділення трафіку між різними групами користувачів виникає потреба у маршрутизації між VLAN.

1.2.4 Router-on-a-Stick

Одним із поширених рішень є метод Router-on-a-Stick. У цьому випадку використовується один фізичний інтерфейс маршрутизатора, налаштований у режимі транку, що підтримує теговані кадри (802.1Q). Для кожного VLAN на ньому створюється логічний підінтерфейс з унікальним VLAN ID. Надходження тегованих кадрів від комутатора дозволяє маршрутизатору ідентифікувати належність трафіку до конкретного VLAN та здійснювати його маршрутизацію відповідно до заданих правил.

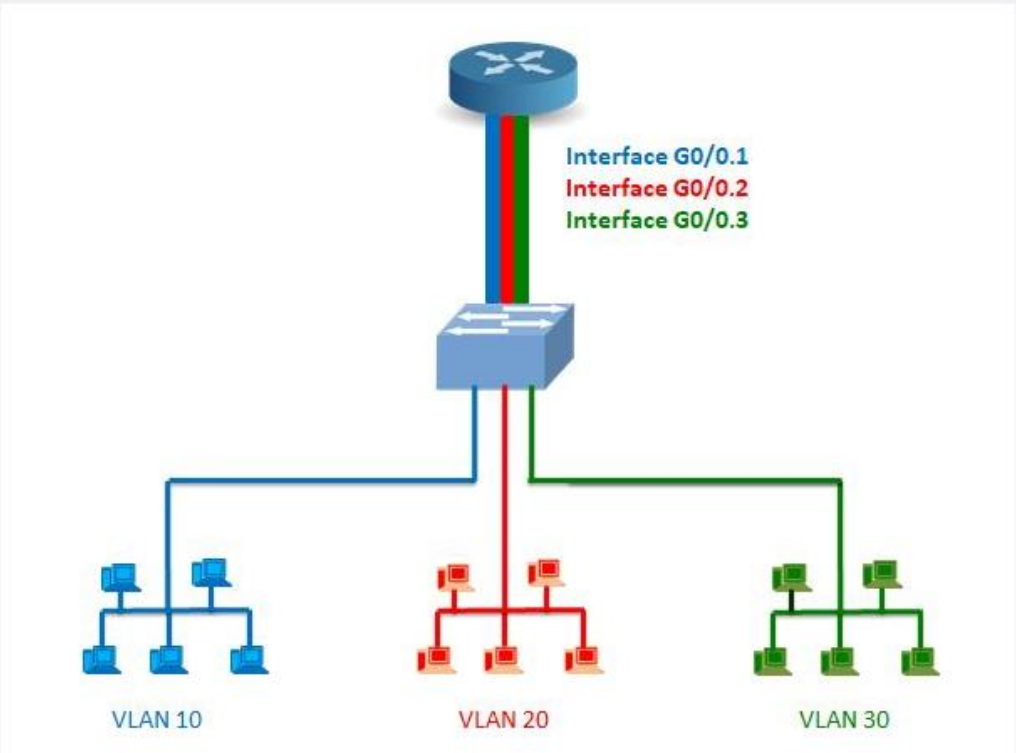


Рисунок 1.4 – Зображення методу Router-on-a-Stick

1.2.5 Сервіси, які може надавати маршрутизатор

Маршрутизатор у мережевій інфраструктурі виступає як центральний елемент, що забезпечує не лише пересилання пакетів, а й виконує певні додаткові сервісні функції. Однією з таких функцій є робота у ролі DHCP-сервера, який автоматично розподіляє IP-адреси між клієнтами мережі. Завдяки цьому пристрої

отримують усі необхідні параметри – власну адресу, шлюз за замовчуванням та DNS-сервер, що набагато спрощує процес підключення.

Ще одним важливим завданням є обробка доменних імен. Виконуючи функції DNS-сервера, маршрутизатор здійснює перетворення доменних імен у відповідні IP-адреси, що забезпечує зручність доступу до внутрішніх і зовнішніх ресурсів. Механізм NAT дозволяє використовувати єдину публічну адресу для виходу в Інтернет усіх клієнтів локальної мережі. Такий підхід не лише економить адресний простір, а й підвищує рівень захищеності мережевої взаємодії.

З точки зору безпеки ефективну роль відіграють вбудовані засоби фільтрації трафіку. Інтегрований міжмережевий екран аналізує пакети та блокує небажані з’єднання, а механізми контролю доступу визначають правила взаємодії між пристроями та ресурсами. Додатковий рівень захисту забезпечується підтримкою VPN-технологій, які дозволяють організувати захищені канали зв’язку для віддалених користувачів.

Також необхідний моніторинг та логування. Системи збору статистики дають змогу відстежувати навантаження на інтерфейси, виявляти проблеми та аналізувати роботу мережі в цілому. Журнали подій зберігають детальну інформацію про активність, що спрощує процес діагностики та пошуку несправностей. Крім того, маршрутизатор може регулювати пріоритети передачі даних за допомогою механізмів QoS, завдяки чому критично важливі сервіси отримують гарантовану пропускну здатність навіть за умов високого навантаження.

Разом з тим у процесі налаштування можливі певні труднощі. Найпоширенішими з них є помилки в адресації, які проявляються у вигляді конфліктів IP-адрес або некоректного визначення підмереж. Неправильна конфігурація DHCP часто призводить до збоїв у розподілі адресного простору, а недоліки у сфері безпеки до підвищеної вразливості мережі. Тому під час проєктування та адміністрування особливу увагу необхідно приділяти контролю конфігурацій та своєчасному оновленню захисних механізмів.

Ще одним важливим моментом є організація управління інфраструктурою. Систематичний моніторинг дозволяє своєчасно реагувати на інциденти, тоді як контроль змін конфігурації гарантує стабільність і передбачуваність у роботі обладнання. Наявність документованих налаштувань і можливість повернення до попереднього стану знижують ризик критичних помилок під час внесення змін.

Роль мережевої топології, яка визначає взаємозв'язки між пристроями та структуру локальної мережі є надзвичайно важливою. Від правильного вибору топології залежить ефективність використання ресурсів, зручність адміністрування та загальна стійкість до відмов. Для освітніх закладів це особливо важливо, оскільки забезпечення стабільного доступу до сервісів напряму впливає на якість навчального процесу.[3]

1.3 Проблеми та складнощі при проектуванні локальної мережевої інфраструктури

У факультетах мережева інфраструктура відіграє важливу роль у забезпеченні необхідних технічних умов для навчання та адміністративної роботи. Під час створення мережі виникає перелік задач, які потребують ретельного аналізу й вирішення. Розгортання та подальше управління інфраструктурою потребує зваженого підходу та врахування багатьох чинників для забезпечення стабільності й надійності її функціонування.

Проблема обмеженої пропускної здатності мережі виникає тоді, коли кількість користувачів або обсяг трафіку перевищують можливості наявного обладнання та каналів зв'язку. Перевірка роботи з одного вузла може показувати задовільні результати, але справжні труднощі з'являються у випадках, коли одночасно працюють десятки чи сотні користувачів. Це може призводити до падіння швидкості, затримок у відповіді сервісів та загальної нестабільності. У варіанті факультету подібні перевантаження ускладнюють доступ до освітніх ресурсів, знижують ефективність роботи навчальних платформ і створюють

обмеження для організації занять. Тому ще на етапі проєктування слід враховувати не лише актуальні потреби, але й передбачати можливі зростання навантаження.

Проблема нестабільності мережі є ще одною проблемою. Вона може бути наслідком апаратних несправностей, аварій чи навіть природних факторів. Навіть кількахвилинні перебої в роботі інфраструктури можуть зупинити навчальний процес, адміністративні процедури та створити ризик втрати даних.

Недостатня масштабованість також часто стає проблемою. Якщо на початковому етапі впроваджуються рішення, що не враховують майбутнє зростання кількості користувачів і пристроїв, то з часом мережа перестає відповідати вимогам. Наприклад, використання обладнання з обмеженими можливостями може призвести до перевантаження, особливо у великих аудиторіях, де одночасно підключається значна кількість студентів.

Відсутність ефективних систем відновлення після збоїв створює додаткові ризики. У випадку інцидентів адміністратори змушені витрачати багато часу на відновлення роботи мережі, що призводить до простоїв навчального та адміністративного процесу. Це негативно впливає на якість освітньої діяльності факультету.

Недостатня увага до безпеки є ще однією проблемою. Якщо захист налаштований неправильно або реалізований частково, це відкриває можливості для несанкціонованого доступу, витоку персональних даних чи атак на інформаційні ресурси факультету. Кіберзагрози, такі як фішинг чи розповсюдження шкідливого ПЗ, можуть серйозно зашкодити роботі факультету.

Розробка та підтримка локальної мережевої інфраструктури факультету передбачає врахування значної кількості факторів, що впливають на її ефективність. Обсяг і різноманіття користувачів, таких як студенти, викладачі та адміністративний персонал, потребує налаштування різних рівнів прав доступу й постійного контролю. Потреба у високошвидкісному доступі до Інтернету зростає через використання відеоуроків, онлайн-курсів і платформ дистанційного навчання, що потребує стабільного та рівномірного розподілу навантаження між сегментами мережі. Безпека даних факультету також має велике значення через обіг

персональної інформації, тому застосовуються сучасні методи захисту: шифрування, контроль доступу та антивірусні рішення. Крім того, баланс між витратами та якістю мережевої інфраструктури залишається критичним, оскільки обмежений бюджет може змушувати використовувати застаріле обладнання, що обмежує функціональність та подальший розвиток мережі. Проєктування масштабованої та надійної мережі факультету вимагає продуманого підходу до топології, вибору обладнання та готовності до розширень у майбутньому.[4]

1.4 Аналіз поточного стану локальної мережі факультету

Освітня та наукова діяльність неможлива без надійної інформаційно-транспортної інфраструктури, важливим елементом якої є локальна комп’ютерна мережа. Вона забезпечує обмін даними між підрозділами факультету, доступ до освітніх ресурсів, інформаційних систем та зовнішніх сервісів. Ефективність її функціонування безпосередньо впливає на якість навчального процесу та рівень інформаційної безпеки. У зв’язку з цим актуальним є проведення аналізу поточного стану локальної мережі факультету, що дозволить виявити сильні та слабкі сторони її побудови, визначити можливі вразливі місця та сформувати рекомендації щодо подальшої оптимізації та модернізації.

1.4.1 Аналіз L2 рівня мережі

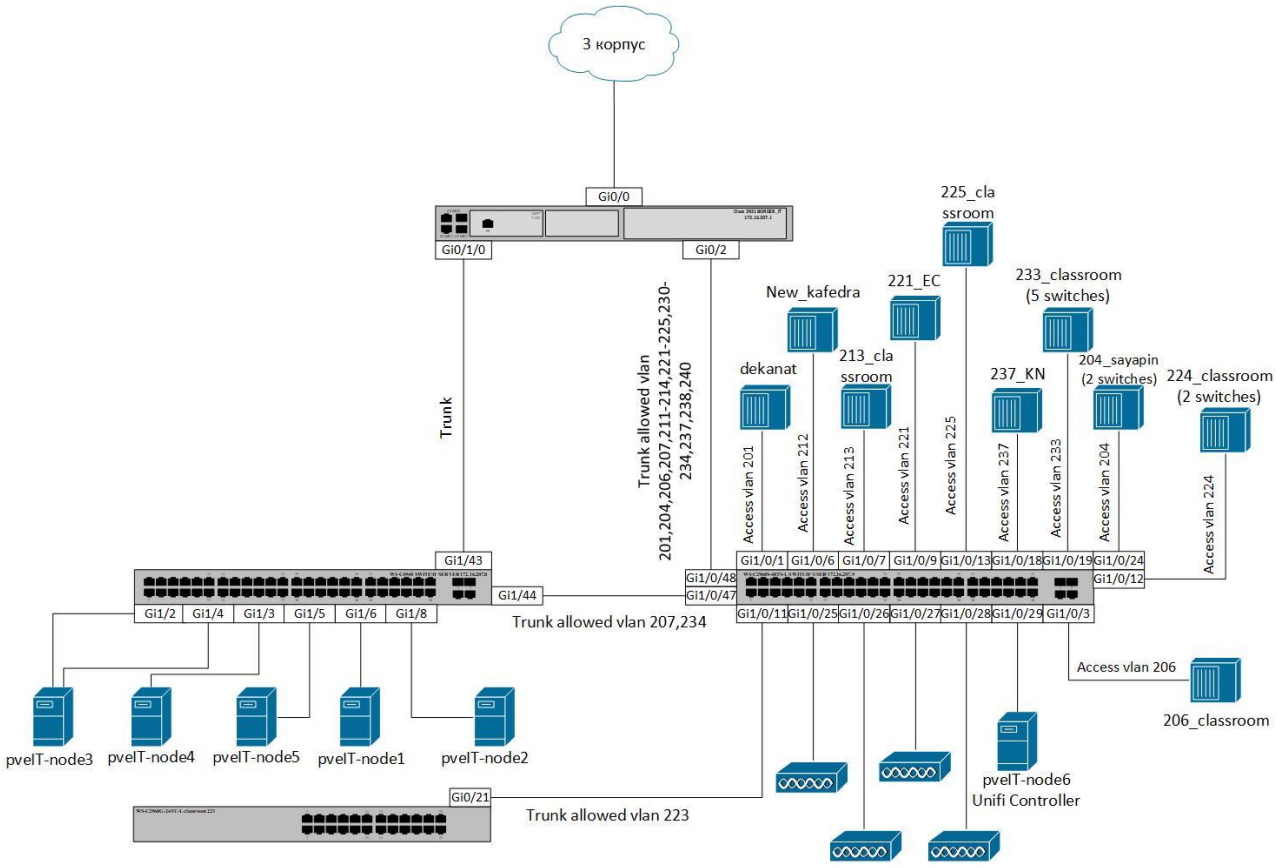


Рисунок 1.5 – L2 схема мережі факультету інформаційних технологій

На поданій L2-схемі зображено локальну мережу факультету, побудовану за ієрархічним принципом із чіткою сегментацією трафіку через VLAN. Головним елементом є роутер, який виконує роль ядра мережі за допомогою технології Router-on-a-Stick. Саме він об’єднує інші комутатори через trunk-з’єднання, забезпечуючи передачу кількох VLAN одночасно та доступ до зовнішніх ресурсів через підключення до іншого корпусу. На цьому рівні формується основна логіка маршрутизації та відбувається розмежування між сегментами мережі.

Важливим є комутатор другого рівня, до якого через trunk інтерфейси підключено серверну інфраструктуру. У мережі використовується шість вузлів pveIT-node, які є частиною віртуалізованого середовища Proxmox VE. Це вказує на те, що факультет активно застосовує віртуалізацію для навчальних або адміністративних завдань. Окремо виділений Unifi Controller, який управляє

точками доступу Wi-Fi, забезпечуючи бездротову інфраструктуру. Така побудова дозволяє централізовано керувати мережевими пристроями та зменшувати адміністративні витрати.

Від комутатора до різних аудиторій і лабораторій йдуть access-порти, кожен з яких прив’язаний до певного VLAN. Наприклад, VLAN 201 відповідає за деканат, VLAN 212 – за кафедру, VLAN 225 – за аудиторію 225, VLAN 233 – за групу некерованих комутаторів у 233-й аудиторії, VLAN 204 і 224 охоплюють аудиторії з кількома комутаторами. Такий підхід забезпечує логічну ізоляцію різних груп користувачів і дозволяє впроваджувати політику доступу залежно від потреб. Водночас видно, що деякі аудиторії мають по кілька комутаторів (наприклад, 233, 204, 224), що може свідчити про велику кількість робочих місць або підвищене навантаження.

Trunk-з’єднання між комутаторами налаштовані з дозволом лише необхідних VLAN, що є добре з точки зору безпеки та оптимізації пропускної здатності. Наприклад, один із trunk-лінків пропускає тільки VLAN 227 і 234, інший – лише VLAN 223. Це дозволяє зменшити широкомовний трафік і підвищує керованість мережі.

1.4.2 Недоліки L2 рівня мережі

Аналізуючи схему локальної мережі факультету, слід відзначити наявність недоліків, що знижують ефективність та надійність її функціонування. Однією з найбільш критичних проблем є використання у структурі сегментів не лише керованих комутаторів, а й концентраторів (хабів). Хаби працюють на фізичному рівні моделі OSI та не здійснюють селекцію трафіку, а лише ретранслюють усі кадри на всі порти. Це призводить до формування єдиного колізійного домену, збільшення ймовірності колізій, зростання затримок та значного зниження продуктивності мережі. Використання хабів в локальних мережах є застарілим підходом і негативно впливає як на швидкодію, так і на інформаційну безпеку.

В окремих аудиторіях за одним інтерфейсом access-порту комутатора підключено декілька хабів, до яких вже під’єднуються кінцеві користувачі. Така топологія створює багаторівневі каскадні колізійні домени, що погіршує якість передавання даних. У разі підвищеного навантаження можливе різке зниження пропускної здатності та поява затримок, або ж повна відмова сервісу, та поява Broadcast шторму, що робить роботу користувачів некомфортною, та іноді неможливою.

Ще одним недоліком є відсутність резервування каналів між комутаторами. На схемі присутнє лише одноканальне з’єднання trunk між роутером та комутаторами другого рівня. Це означає, що у випадку відмови одного з ключових інтерфейсів або кабелю, підключені до нього сегменти залишаться повністю ізольованими від мережі. Такий підхід знижує відмовостійкість інфраструктури.

Проблеми також спостерігаються у плані сегментації. Хоча VLAN і застосовуються, однак за відсутності сучасних комутаторів на рівні доступу (де замість них використані хаби) фактична ізоляція користувацького трафіку не досягається. Трафік, що проходить всередині сегменту з хабами, залишається неконтрольованим і вразливим до атак типу sniffing, оскільки будь-який клієнт у межах такого сегменту може перехоплювати дані інших користувачів. Це створює серйозні ризики для інформаційної безпеки навчального процесу.

Каскадне підключення декількох хабів до одного access-порту унеможливлює якісний моніторинг та управління мережею. Адміністратор бачить лише один логічний інтерфейс комутатора, але фактично за ним приховані численні користувачі, що ускладнює ідентифікацію проблемних вузлів, аналіз завантаженості та контроль доступу.

Поточний стан локальної мережі факультету характеризується рядом суттєвих технічних недоліків: використання застарілого обладнання (хабів) у сегментах доступу, відсутність резервування магістральних з’єднань, низький рівень інформаційної безпеки в окремих VLAN, а також обмежені можливості адміністрування. У сукупності ці фактори призводять до зниження продуктивності, підвищення ризиків відмов та уразливостей, що вимагає проведення оновлення

мережевої інфраструктури з переходом на комутатори рівня доступу та впровадженням сучасних механізмів відмовостійкості.

1.4.3 Аналіз L3 рівня мережі

Рисунок 1.6 – L3 схема мережі факультету інформаційних технологій

Подана схема на третьому рівні моделі OSI демонструє реалізацію маршрутизації між численними VLAN сегментами та вихід у зовнішню мережу через прикордонний маршрутизатор. У мережі використовується велика кількість підмереж, кожна з яких закріплена за відповідним VLAN. Як правило, для підмереж виділено адресний простір класу C (маска /24), що відповідає приблизно 254 доступним IP-адресам у кожному сегменті.

До маршрутизатора підключено понад двадцять VLAN. Усі вони мають окремі інтерфейси SVI (Switch Virtual Interface), які є «точками входу» користувацьких підмереж у мережеву інфраструктуру. Це означає, що використовується централізована маршрутизація.

Зовнішнє підключення реалізовано через інтерфейс з адресою з публічного діапазону /27, що надає доступ у зовнішню мережу. Саме через цей шлюз забезпечується вихід в інтернет та міжкорпусна взаємодія. Однак відсутність дублювання підключень маршрутизатора до інших зовнішніх ліній свідчить про наявність єдиної точки відмови: у разі виходу з ладу даного інтерфейсу або зовнішнього каналу факультет залишиться ізольованим від публічної мережі.

На роутері використовується зонова модель безпеки на основі Zone-Based Firewall (ZBFW), реалізована на прикордонному маршрутизаторі. Брандмауер здійснює базову фільтрацію трафіку між зонами outside, lan та dmz. Такий підхід дозволяє розмежувати критично важливі підмережі й забезпечити контроль обміну даними між ними на рівні політик доступу.

Функціонування ZBFW забезпечує базовий рівень сегментації та захисту, оскільки трафік, що прямує між зазначеними зонами, підлягає перевірці відповідно до правил. Це дозволяє зменшити ризик несанкціонованого доступу ззовні до внутрішніх ресурсів та частково ізолювати служби, розташовані в DMZ, від решти корпоративної мережі.

1.4.4 Недоліки L3 рівня мережі

Аналіз схеми маршрутизації показує, що мережа факультету має низку недоліків, які впливають як на її надійність, так і на ефективність роботи користувачів.

Для початку необхідно відзначити відсутність резервування зовнішнього підключення. Уся міжкорпусна взаємодія та доступ до інтернету здійснюється через єдиний канал, що створює критичну залежність від одного маршрутизатора та однієї фізичної лінії. У випадку технічного збою чи аварії цей вузол стане точкою відмови для всієї мережевої інфраструктури факультету.

Ще однією проблемою є підхід до організації адресного простору. Майже всі VLAN реалізовані на основі підмереж /24, хоча фактична кількість користувачів у більшості сегментів є значно меншою. Це призводить до нераціонального використання IP-адрес і створює надмірні широкомовні домени. В умовах одночасної роботи великої кількості таких підмереж формується додаткове навантаження на мережеве обладнання, що негативно позначається на швидкодії.

Політики ZBFW виявляються надто загальними; замість детальної сегментації застосовуються широкі правила, які фактично дозволяють значну частину трафіку між внутрішніми зонами або масивно «пропускають» запити до зовнішньої мережі. У таких умовах можливості ZBFW щодо обмеження та контролю доступу між підмережами істотно знижуються.

Конфігурація не включає сучасних функцій забезпечення безпеки. Немає ознак тонкої фільтрації на рівні додатків, інтеграції з системами запобігання вторгненням (IPS), URL-контент-фільтрації або антивірусного аналізу. Також відсутня продвинута система логування й оповіщення, що ускладнює оперативне виявлення та розслідування інцидентів. Як наслідок, навіть при наявності зонового механізму мережа лишається вразливою до складніших атак і має обмежену можливість коректного реагування на події безпеки.

Додатковим недоліком є складність адміністрування. Велика кількість VLAN при відсутності автоматизованих систем управління створює ризики помилок у конфігурації та ускладнює моніторинг. Адміністратору доводиться підтримувати значний обсяг статичних налаштувань, що підвищує ймовірність людського фактору при експлуатації мережі.

Аналізуючи навантаження CPU маршрутизатора за останні 30 днів, можна побачити, що завантаженість CPU сягала пікових значень досить часто, що також негативно впливає на роботу мережі.

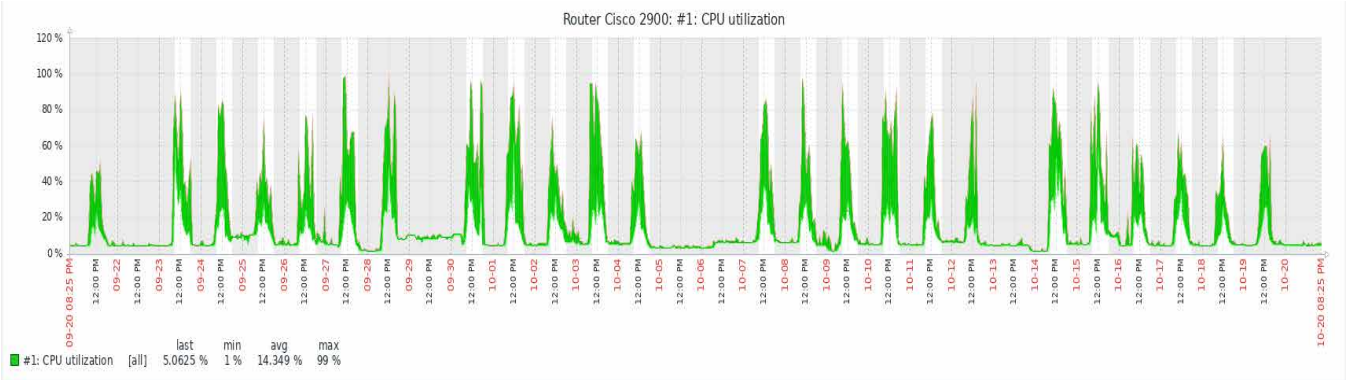


Рисунок 1.7 – Графік завантаження CPU на маршрутизаторі

Висновок до першого розділу

Наявна мережева інфраструктура факультету має змішану архітектуру, у якій поєднуються елементи різних рівнів розвитку мережевих технологій. Вона забезпечує базове функціонування та покриває основні потреби користувачів у доступі до інформаційних ресурсів, але характеризується низкою технічних недоліків. Використання хабів у ролі вузлів комутації знижує ефективність роботи, спричиняючи надлишковий трафік, колізії та зниження загальної пропускної здатності. Об’єднання кількох сегментів за одним інтерфейсом створює додаткові точки відмови та ускладнює подальший розвиток.

Маршрутизація реалізована без достатнього резервування та із застарілими механізмами розподілу трафіку. Відсутність розвиненої системи динамічних протоколів маршрутизації й слабка гнучкість у побудові логічних сегментів обмежують масштабованість і стійкість мережі. Хоча на прикордонному маршрутизаторі застосовується Zone-Based Firewall, його конфігурація зведена до мінімального набору правил між зонами outside, lan та dmz, що забезпечує лише базовий рівень захисту.

Стан мережі можна охарактеризувати як функціонально придатний, але технічно застарілий і такий, що вимагає значної модернізації. Виявлені недоліки не лише знижують якість обслуговування користувачів, але й створюють суттєві ризики для подальшої експлуатації та розвитку інфраструктури факультету.

2 ОБҐРУНТУВАННЯ АРХІТЕКТУРНИХ РІШЕНЬ ДЛЯ МОДЕРНІЗАЦІЇ ЛОКАЛЬНОЇ МЕРЕЖІ ФАКУЛЬТЕТУ

2.1 Огляд можливих архітектурних рішень

Огляд можливих архітектурних рішень є важливим етапом у процесі проєктування мережевої інфраструктури факультету, оскільки саме на цьому етапі визначається спектр технологій та підходів, які здатні забезпечити реалізацію сформованих вимог. Вибір архітектури мережі впливає на її подальшу масштабованість, рівень захисту даних, надійність функціонування та зручність адміністрування. У сучасній практиці найбільш поширеними підходами є класична ієрархічна модель побудови мережі Three-Tier Architecture, концепція програмно-визначеного доступу Cisco SD-Access, а також інтегрована архітектура Fortinet Security Fabric.

Кожен із цих варіантів має свої переваги та недоліки, що проявляються залежно від умов експлуатації, розміру організації та її специфічних потреб. Тому необхідно детально розглянути кожне з рішень для подальшого проведення порівняльного аналізу й визначення найбільш оптимального варіанту саме для факультету.

2.1.1 Топологія Three-Tier

Оскільки мережі можуть бути надзвичайно складними, з численними протоколами та різноманітними технологіями, Cisco розробила багаторівневу ієрархічну модель для проєктування надійної мережевої інфраструктури.

Трирівнева ієрархічна мережева топологія Cisco – це широко прийнята модель проєктування для великих кампусних та корпоративних мереж. Вона поділяє мережу на три окремі рівні: основний, розподільчий та доступний, кожен з яких має певні функції для підвищення масштабованості, надійності, продуктивності та керованості.

Дана топологія включає в себе три шари:

- Access Layer (Рівень доступу)
- Distribution Layer (Рівень розподілу)
- Core Layer (Основний рівень)

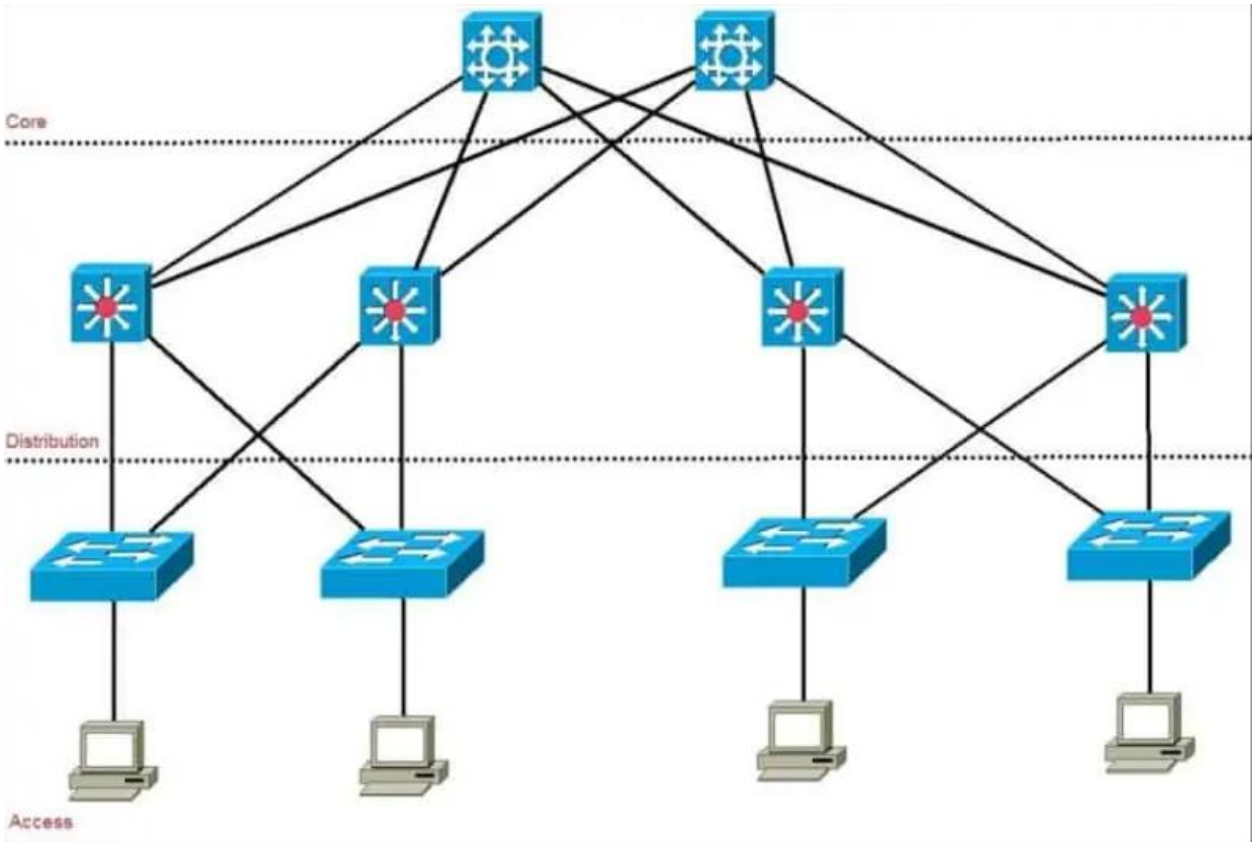


Рисунок 2.1 – Приклад Three-Tier топології

Рівень доступу є найнижчим рівнем трирівневої моделі та знаходиться найближче до кінцевих користувачів та їхніх пристроїв.

Підключення користувачів та пристроїв забезпечує мережевий доступ до кінцевих пристроїв, таких як ПК, ноутбуки, IP-телефони, принтери, бездротові точки доступу (AP) та сервери.

В основному працює на рівні 2 моделі OSI, пересилаючи кадри на основі MAC-адрес. Створює віртуальні локальні мережі (VLAN) для сегментації мережі на менші широкомовні домени, покращуючи безпеку та продуктивність. Впроваджує заходи безпеки, такі як безпека портів, щоб запобігти підключенню

неавторизованих пристроїв до мережі. Часто забезпечує живлення таких пристроїв, як IP-телефони та бездротові точки доступу, через кабель Ethernet за допомогою технології PoE. Можна застосовувати базові політики QoS для визначення пріоритетів певних типів трафіку (наприклад, голосового або відео).

На цьому рівні використовуються такі протоколи як Spanning Tree (STP/RSTP/MST), який необхідний для запобігання петель другого рівня в надлишкових мережевих шляхах, VLAN (802.1Q) для сегментації мережі на VLAN та дозволу кільком VLAN проходити через одне магістральне з'єднання, DHCP Snooping для запобігання несанкціонованим DHCP-серверам, динамічна перевірка ARP (DAI): для захисту від атак підміни ARP, CDP (Cisco Discovery Protocol) та LLDP (Link Layer Discovery Protocol) для виявлення пристроїв та обміну інформацією.

Рівень розподілу діє як посередник між рівнями доступу та основним рівнем. Він агрегує трафік від кількох комутаторів рівня доступу та забезпечує інтелектуальну маршрутизацію, фільтрацію та реалізацію політик.

Виконує маршрутизацію між різними віртуальними локальними мережами у межах блоку локальної мережі. Впроваджує списки контролю доступу (ACL), політики безпеки та політики QoS для контролю потоку трафіку та визначення пріоритетів даних. Забезпечує межі для доменів широкомовлення, запобігаючи впливу штормів широкомовлення на всю мережу. Забезпечує високу доступність завдяки резервним каналам зв'язку та протоколам, що забезпечують балансування навантаження. Об'єднує кілька фізичних каналів в один логічний канал для збільшення пропускної здатності та резервування за допомогою протоколів LASP та PAgP.

На цьому рівні використовуються такі протоколи як OSPF, EIGRP, RIP, BGP, використовуються для маршрутизації трафіку між різними VLAN та до рівня ядра. OSPF та EIGRP є поширеним вибором для підприємства. HSRP, VRRP або GLBP використовуються для забезпечення резервування шлюзу для кінцевих пристроїв. LACP або PAgP для об'єднання каналів між рівнями розподілу та доступу або між

рівнями розподілу та основними рівнями. Більш просунуті політики QoS, ніж на рівні доступу, включаючи регулювання, формування та черги.

Основний рівень – це основа мережі, призначена для високошвидкісної передачі даних з високою пропускною здатністю між різними пристроями розподільчого рівня. Він відповідає за швидке та надійне транспортування великих обсягів трафіку.

Її основна роль полягає в забезпеченні дуже швидкої комутації пакетів, переміщуючи дані якомога швидше. Будується з максимальним резервуванням для забезпечення безперебійної роботи мережі, оскільки будь-який збій на цьому рівні може вплинути на всю мережу. Розроблено для роботи з майбутнім зростанням та збільшенням потреб у трафіку.

На цьому рівні використовуються такі протоколи як OSPF, EIGRP, BGP. Зазвичай використовують швидкозбіжні протоколи маршрутизації. BGP може використовуватися, якщо ядро підключається до кількох постачальників послуг або інших автономних систем. MPLS може використовуватися у великих корпоративних основних мережах для управління трафіком та VPN-сервісів. Резервне обладнання та агрегація каналів є найголовнішим. FHRP зазвичай не потрібні в ядрі мережі, оскільки самі основні пристрої є маршрутизаторами.

В ідеалі, основний рівень не повинен впроваджувати жодних складних політик чи фільтрації, таких як ACL або QoS. Його основна увага зосереджена виключно на швидкості та ефективності пересилання. Застосування політик здійснюється на рівні розподілу.

Трирівнева ієрархічна модель Cisco забезпечує структурований та ефективний спосіб проєктування та управління складними мережами, забезпечуючи кращу продуктивність, масштабованість та надійність.[5]

2.1.2 Cisco SD-Access

Традиційна архітектура кампусної мережі не може повністю задовольнити поточні потреби мережі. Програмно-визначений доступ Cisco (SDA) – це відносно нова технологія, яка розширює віртуалізацію на рівень доступу мережі. Cisco SDA покращує кампусні мережі, використовуючи такі функції:

- Автоматизація мережі – SDA забезпечує централізоване керування мережевими пристроями за допомогою центру цифрової мережевої архітектури Cisco (DNA), що спрощує проєктування, налаштування та розгортання мережі.

- Аналіз мережі – SDA використовує телеметрію для проактивного прогнозування мережевих та безпекових ризиків.

- Служби ідентифікації – Cisco ISE (Identity Services Engine) ідентифікує підключені пристрої та користувачів. Він також надає контекстну інформацію, необхідну для впровадження політик безпеки сегментації мережі та контролю доступу.

- Застосування політик – Політики програм і доступу створюються на основі групових політик за допомогою списків контролю доступу груп безпеки (SGACL) – простішої та масштабованішої форми застосування політик на основі ідентифікації.

- Безпечна сегментація – Сегментація мережі спрощується завдяки рішенню SD-Access. Воно підтримує сегментацію для гостей, корпоративних мереж, об'єктів та інфраструктури з підтримкою IoT.

- Віртуалізація мережі – Одна фізична інфраструктура може підтримувати кілька віртуальних мереж (VN) з різними політиками доступу.

Архітектура Cisco SD-Access має чотири рівні: фізичний рівень, мережевий рівень, рівень контролера та рівень управління.

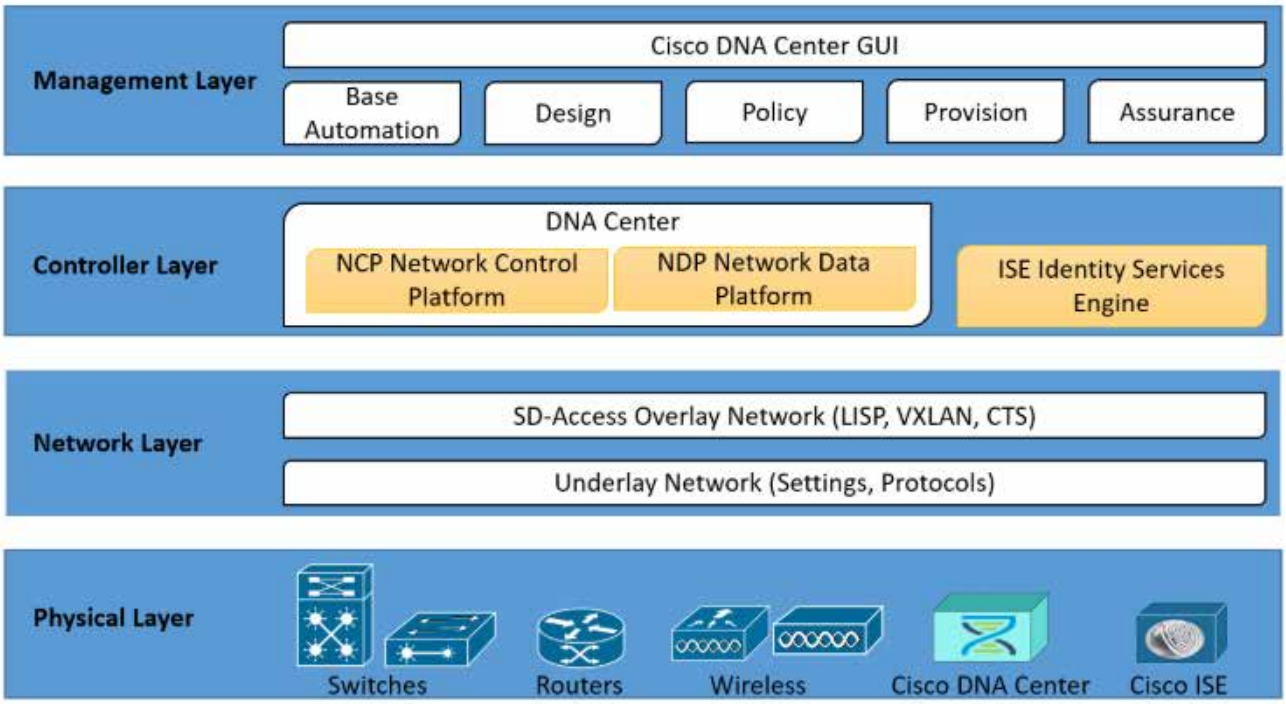


Рисунок 2.2 – Архітектура Cisco SD-Access

Архітектура Cisco SD-Access побудована за багаторівневим принципом і базується на ідеї відокремлення фізичної інфраструктури від логічного управління, що дозволяє централізовано контролювати мережеві ресурси, гнучко змінювати політики доступу та підвищувати безпеку.

На найнижчому рівні, фізичному, розташовані комутатори, маршрутизатори, точки бездротового доступу, а також контролери Cisco DNA Center і Cisco ISE. Саме ці компоненти забезпечують базову комунікацію та створюють основу для роботи вищих рівнів.

Cisco Identity Services Engine (ISE) – це безпечна платформа доступу до мережі, яка забезпечує підвищену обізнаність, контроль та узгодженість для користувачів і пристроїв, які отримують доступ до мережі організації. ISE є невід'ємним компонентом SD-Access для впровадження політики контролю доступу до мережі. ISE виконує впровадження політик, забезпечуючи динамічне

зіставлення користувачів і пристроїв з масштабованими групами та спрощуючи комплексне забезпечення дотримання політик безпеки. В ISE користувачі та пристрої відображаються в простому та гнучкому інтерфейсі. ISE інтегрується з Cisco Catalyst Center за допомогою API Cisco Platform Exchange Grid (pxGrid) та Representational State Transfer (REST) для сповіщень про події кінцевих точок та автоматизації конфігурації політик в ISE.

Мережевий рівень складається з двох складових: underlay-мережі, яка відповідає за традиційні налаштування та протоколи маршрутизації, і overlay-мережі, побудованої на базі технологій LISP, VXLAN. Overlay забезпечує створення віртуальних сегментів, завдяки чому трафік користувачів і сервісів можна логічно розділяти незалежно від фізичного розташування пристроїв. Це дозволяє ізолювати групи користувачів, реалізувати контроль доступу та швидко розгортати нові сервіси.

Рівень контролера представлений платформою Cisco DNA Center, яка об’єднує два основні модулі: NCP (Network Control Platform) та NDP (Network Data Platform). Перший відповідає за управління мережевими ресурсами та координацію роботи пристроїв, тоді як другий здійснює збір і аналіз телеметрії, забезпечуючи видимість стану мережі. Важливу роль відіграє Cisco ISE, яка реалізує механізми ідентифікації та автентифікації користувачів, а також контроль дотримання політик доступу.

На верхньому рівні знаходиться Management Layer, у центрі якого розташований графічний інтерфейс Cisco DNA Center GUI. Він надає адміністраторам інструменти для автоматизації базових операцій, розробки та впровадження політик, централізованого розгортання конфігурацій і постійного моніторингу якості обслуговування. Завдяки цьому управління мережею зводиться до роботи з політиками та сервісами, а не з окремими пристроями, що значно зменшує складність адміністрування.

У результаті така архітектура забезпечує повну сегментацію трафіку, централізований контроль безпеки, спрощене масштабування та гнучке управління ресурсами, що робить SD-Access одним із найбільш сучасних підходів до побудови корпоративних мереж.

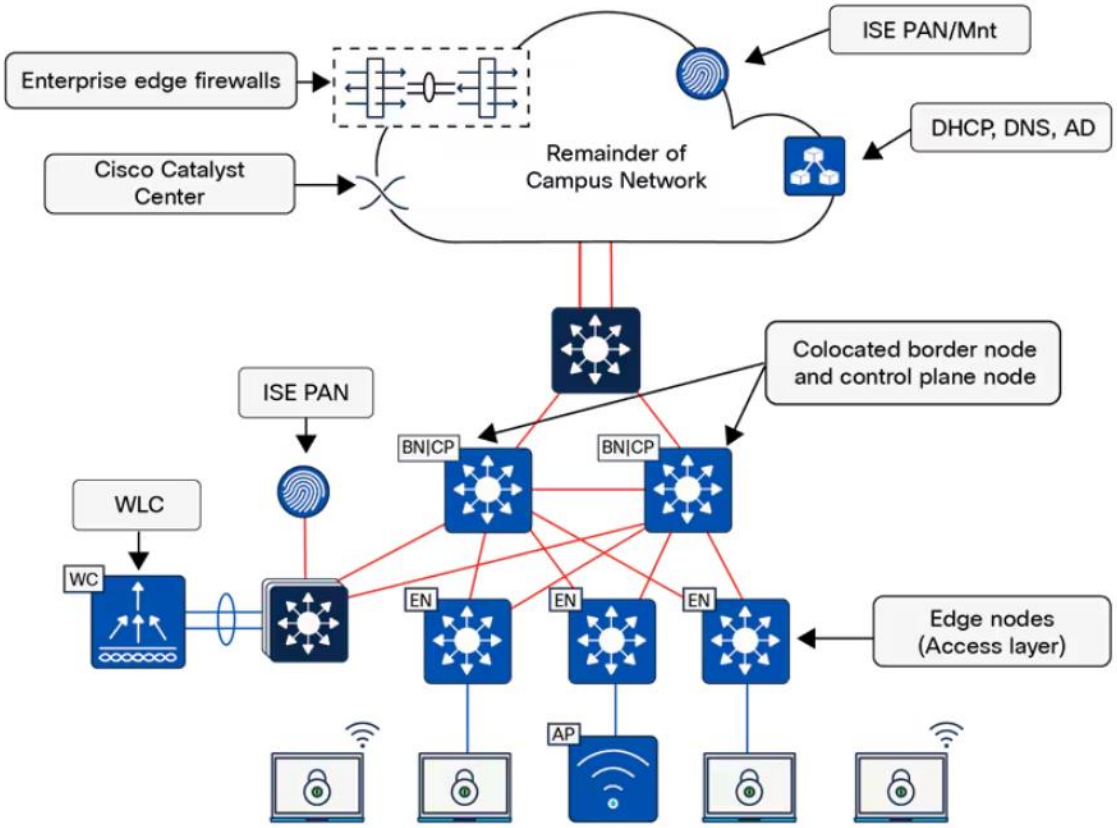


Рисунок 2.3 – Приклад топології SD-Access (мале підприємство)

Таблиця 2.1 – Обмеження для невеликих об’єктів

Endpoints	<10 000
Fabric nodes	<100
Control plane nodes	2
External border nodes	2
Access points	<500

Для менших розгортань сайт SD-Access fabric часто реалізується з використанням дворівневої конструкції. На невеликому сайті висока доступність забезпечується завдяки поєднанню пограничного вузла та вузла контролю. Для забезпечення стійкості та альтернативних шляхів переадресації в оверлеї та підлеглих мережах, ці комутатори повинні бути з'єднані безпосередньо один з одним.[6]

2.1.3 Fortinet Security Fabric

Fortinet Security Fabric – це інтегрована мережева архітектура, спрямована на побудову єдиного середовища безпеки, яке охоплює усі ключові елементи мережевої інфраструктури. На відміну від традиційних підходів, де кожен засіб захисту функціонує ізольовано, Security Fabric забезпечує взаємодію між різними рішеннями Fortinet, такими як міжмережеві екрани, комутатори, точки доступу, системи захисту кінцевих пристроїв та хмарні сервіси. Така модель дозволяє централізовано збирати та аналізувати дані, відслідковувати реакцію на інциденти, автоматизувати політики безпеки та зменшувати час реагування на загрози.

Завдяки цьому підходу навчальний заклад чи організація отримує не набір окремих рішень, а цілісну екосистему, здатну масштабуватися, швидко адаптуватися до нових викликів та забезпечувати однаковий рівень захисту як у локальних сегментах мережі, так і у віддалених чи хмарних мережах. Це робить Security Fabric чудовим варіантом для побудови сучасної інфраструктури, де критично важливо поєднати продуктивність, простоту управління та високий рівень безпеки.

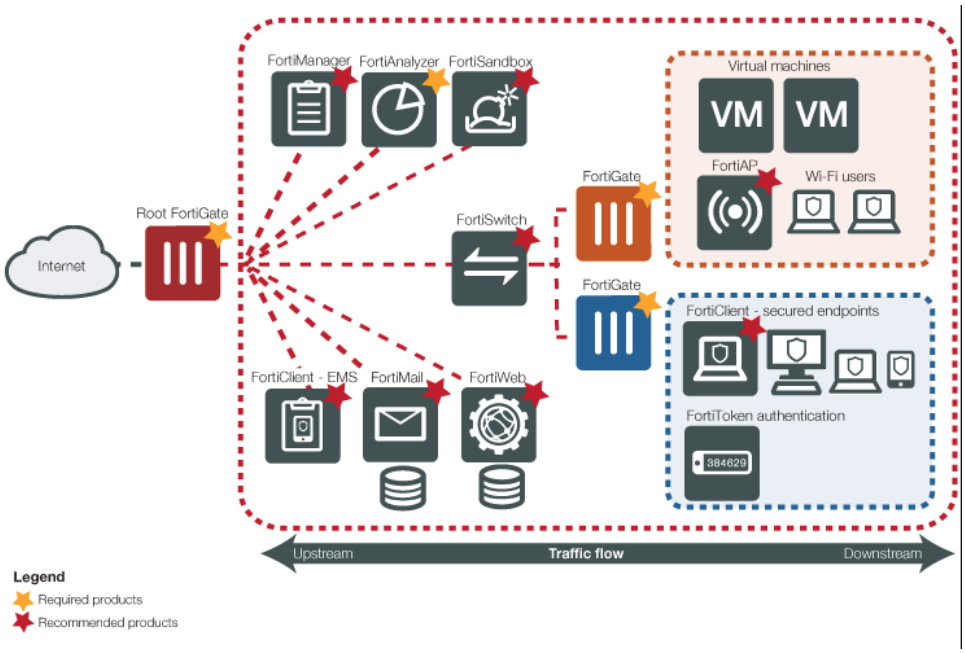


Рисунок 2.4 – Структурна схема Fortinet Security Fabric

FortiGate - міжмережевий екран нового покоління (NGFW), що дозволяє захищати периметр мережі (або різні сегменти) від різних загроз. Ядро фабрики безпеки. Флагманський продукт компанії Fortinet.

FortiAnalyzer - пристрій для збирання та аналізу логів з різних пристроїв Fortinet. Він відповідає за централізоване збирання, збереження та аналіз журналів подій від різних пристроїв екосистеми. Його основна функція полягає у перетворенні великого обсягу розрізненої інформації з міжмережевих екранів, комутаторів, точок доступу та інших компонентів у структуровані дані, які можна використовувати для моніторингу, звітності та розслідування інцидентів безпеки.

Завдяки можливостям FortiAnalyzer адміністратор отримує не лише огляд поточного стану мережі, але й інструменти для виявлення аномалій, визначення тенденцій у трафіку та побудови аналітичних моделей поведінки користувачів. Варто відзначити підтримку автоматизованої генерації звітів, що спрощує аудит та доведення відповідності нормативним вимогам. У комплексі це підвищує рівень прозорості всієї інфраструктури та дозволяє швидше реагувати на потенційні загрози.

FortiGate та FortiAnalyzer вже утворюють своєрідну фабрику безпеки: FortiGate захищає мережу від загроз, генерує логи та відправляє їх на FortiAnalyzer. FortiAnalyzer у свою чергу аналізує ці логи та дозволяє будувати за ними звіти, а також автоматизувати різні процеси, що залежать від надходження тих чи інших логів.

FortiClient EMS - рішення для централізованого керування та захисту кінцевих точок. Дозволяє збирати з пристроїв різну телеметрію і на її основі керувати доступом пристроїв у різні мережі. Ця телеметрія також дозволяє розширити видимість мережі. Як і стандартні клієнти, володіє функціоналом антивірусу, веб-фільтрації, контролю додатків, сканера вразливостей, контролю USB підключень і т.д. Поряд з FortiGate і FortiAnalyzer дозволяє автоматизувати поведінку при виявленні загроз.

FortiSwitch – комутатори від Fortinet. Можуть працювати як окремі пристрої, так і керуватися самим FortiGate за допомогою пропрієтарного протоколу FortiLink.

У такому разі вони є розширеннями портів FortiGate. Це також розширює видимість мережі, а також дозволяє автоматизувати поведінку при виявленні загрози - наприклад, помістити окремий пристрій у карантинний VLAN. У такому випадку пристрій отримає мінімально необхідний доступ (це можна налаштувати), а всі можливі комунікації з іншими пристроями в мережі будуть припинені, щоб запобігти поширенню загрози.

FortiAP – бездротова точка доступу від Fortinet. Дозволяє забезпечити безпеку користувачів, що підключаються до мережі WiFi. Через точку доступу також розширюється видимість мережі та з'являються можливості автоматизації, аналогічно до FortiSwitch. [7]

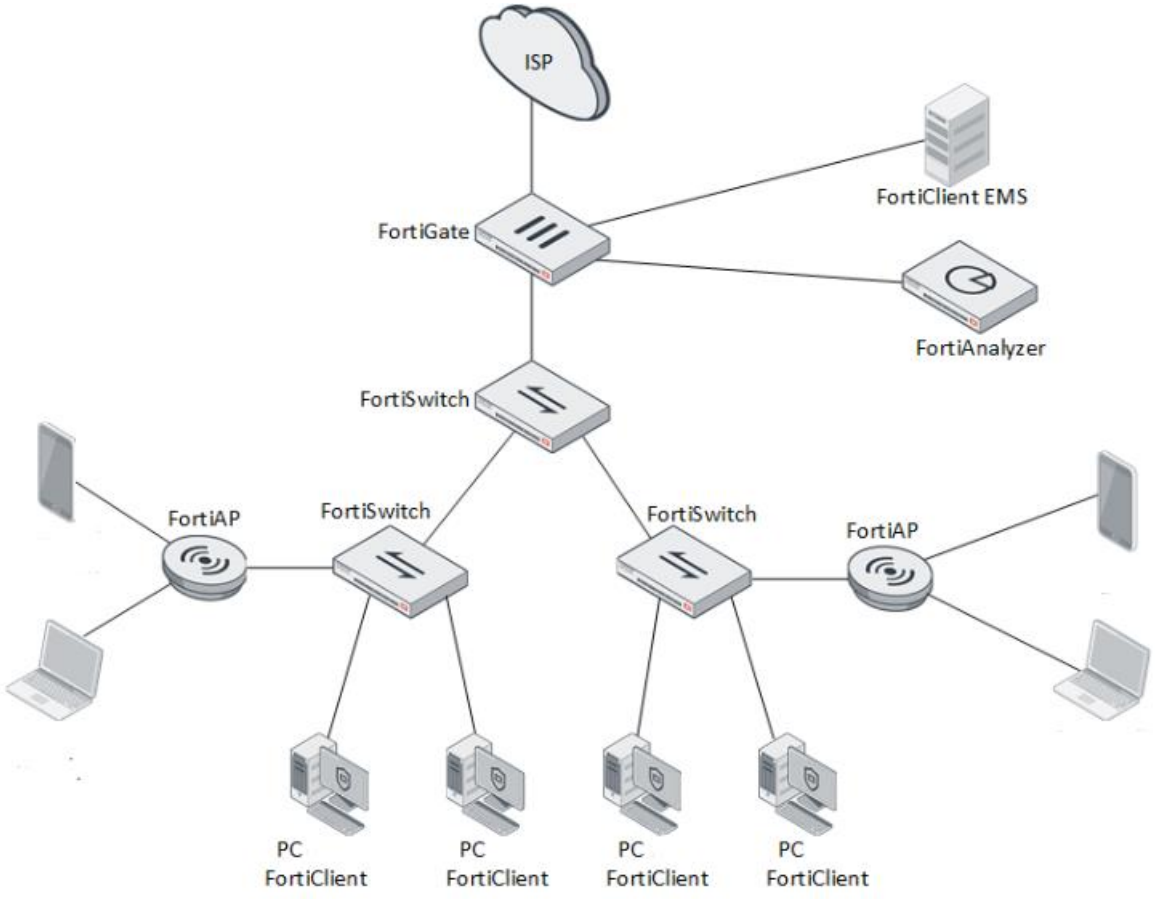


Рисунок 2.5 – Приклад топології Fortinet Security Fabric

В архітектурі Fortinet Security Fabric усі компоненти інтегровані в єдину систему, де кожен елемент виконує свою функцію, але при цьому тісно взаємодіє з іншими для забезпечення цілісності захисту та керованості інфраструктури. Центральним вузлом виступає FortiGate, який виконує роль міжмережевого екрану нового покоління, забезпечує маршрутизацію, контроль доступу та інтеграцію з іншими пристроями. Саме через нього проходить увесь трафік, що робить його логічним центром мережевої безпеки.

FortiSwitch підключаються безпосередньо до FortiGate та працюють у режимі керованих пристроїв. Завдяки цьому адміністратор отримує можливість централізованого управління комутацією, застосування політик безпеки до портів та сегментації трафіку без потреби у використанні окремих консолей. Подібний підхід дозволяє створювати захищені віртуальні сегменти, а також забезпечує контроль за підключенням кінцевих пристроїв.

FortiAP реалізують бездротовий доступ, але їхня ключова особливість полягає в тому, що вони теж контролюються з боку FortiGate. Це дозволяє застосовувати однакові політики безпеки для користувачів незалежно від того, чи вони підключаються через кабель, чи через Wi-Fi. У результаті зникає традиційна проблема різниці у рівнях захисту між дротовими та бездротовими сегментами.

FortiAnalyzer забезпечує централізоване збирання логів і статистики з усіх перелічених пристроїв. На його основі здійснюється моніторинг подій безпеки, формування звітів і виявлення потенційних інцидентів. Це дозволяє не лише мати повну картину подій у мережі, а й оперативно реагувати на загрози.

FortiClient EMS використовується для керування кінцевими пристроями ПК та ноутбуками з встановленим FortiClient. Він дозволяє впроваджувати політики безпеки безпосередньо на рівні користувацьких пристроїв, контролювати оновлення та забезпечувати додатковий захист під час підключення до мережі факультету.

Взаємодія між компонентами побудована за принципом повної інтеграції: FortiGate виступає як центральний контролер, FortiSwitch та FortiAP забезпечують доступ і сегментацію, FortiAnalyzer відповідає за аналіз і моніторинг, а FortiClient

EMS гарантує контроль за кінцевими вузлами. Такий підхід створює єдине захисне середовище, де всі елементи працюють узгоджено, що особливо важливо для інфраструктури навчального закладу з різнорідними пристроями та користувачами. [8]

2.2 Порівняльний аналіз архітектурних рішень

У процесі модернізації локальної мережі факультету необхідно обрати архітектурний підход, який найкраще відповідатиме потребам освітньої інфраструктури. Традиційні та сучасні рішення у сфері побудови мереж значно відрізняються як за принципами організації, так і за рівнем функцій безпеки, автоматизації та управління. Тому для прийняття рішення потрібно провести порівняльний аналіз варіантів, а саме класичної трирівневої архітектури, програмно-орієнтованої мережі Cisco Software-Defined Access та інтегрованої концепції Fortinet Security Fabric. Порівняння цих архітектурних рішень за низкою критеріїв дозволить оцінити їхні переваги та обмеження й визначити найбільш оптимальний варіант для умов функціонування навчального закладу.

2.2.1 Критерії порівняння

Для проведення порівняльного аналізу архітектурних рішень необхідно визначити ключові параметри, за якими можна оцінити їхню придатність для використання в умовах навчального закладу.

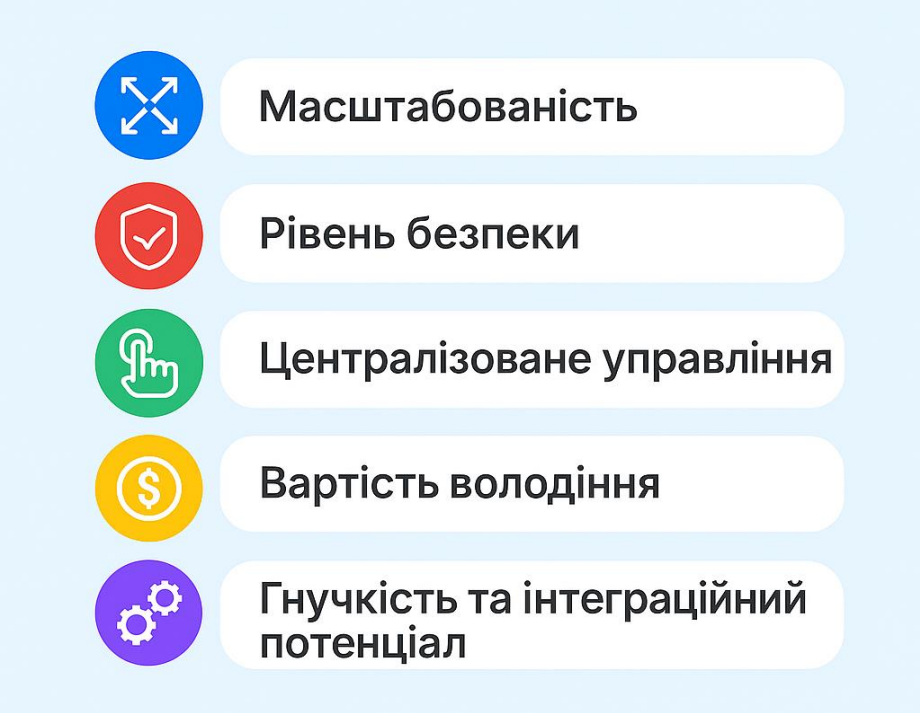


Рисунок 2.6 – Критерії порівняння

Одним із важливих параметрів виступає масштабованість, адже мережа факультету повинна мати запас для розвитку та підтримувати можливість підключення нових користувачів і пристроїв без кардинальної перебудови всієї інфраструктури.

Важливою характеристикою є рівень інформаційної безпеки. Сюди відносяться вбудовані механізми автентифікації та авторизації, можливості сегментації мережі, захист від зовнішніх і внутрішніх загроз, а також інтеграція з системами контролю та моніторингу. Саме безпека у навчальному середовищі має особливе значення, оскільки поряд із навчальними ресурсами передбачається робота з персональними даними студентів і співробітників.

Сучасні архітектури повинні забезпечувати централізований контроль, спрощену конфігурацію та автоматизацію рутинних процесів. Це дозволяє значно зменшити навантаження на адміністратора та мінімізувати ймовірність людських помилок.

При виборі архітектури також необхідно враховувати економічну складову. Вартість обладнання та програмних рішень, а також витрати на їхню подальшу підтримку і розвиток часто визначають реальні можливості впровадження того чи іншого підходу.

Гнучкість інтеграції - це здатність архітектури працювати разом з іншими технологіями, підтримку сучасних стандартів і сумісність з існуючими сервісами. Для навчального закладу це особливо важливо, оскільки інфраструктура розвивається поступово і повинна залишатися відкритою до модернізацій.

Сформований набір критеріїв: масштабованість, безпека, зручність управління, економічна доцільність та інтеграційний потенціал, дає змогу провести комплексне порівняння архітектурних рішень і визначити найбільш ефективний підхід для умов факультету.[9]

2.2.2 Опис та оцінка варіантів

Класична трирівнева архітектура застосовується у корпоративних мережах, де існує потреба у чіткому розмежуванні функціональних рівнів. Вона складається з рівня доступу, рівня агрегації та ядра. Кожен із цих рівнів виконує власні завдання: доступ забезпечує підключення кінцевих пристроїв, агрегація відповідає за маршрутизацію між підмережами та політиками, ядро за високошвидкісну комутацію та зв’язок із центром обробки даних чи зовнішніми мережами. Якщо говорити про продуктивність, то така архітектура здатна обробляти значні обсяги трафіку, але створює додаткові затримки через велику кількість рівнів. Масштабованість реалізується добре, але розширення вимагає значних капіталовкладень та правильного планування топології. У плані безпеки вона залежить від окремих засобів захисту на різних рівнях, міжмережевих екранів, ACL, VLAN-сегментації, що може ускладнювати адміністрування. Для навчального закладу триступенева модель може виявитись надто громіздкою та дорогою, особливо якщо мережа не є дуже великою. Водночас вона є перевіреним часом рішенням і може бути привабливою завдяки зрозумілій структурі.

Архітектура Cisco Software-Defined Access належить до нового покоління мережевих рішень, де керування виноситься на програмний рівень. Центральним елементом виступає контролер Cisco DNA Center, який відповідає за автоматизацію, аналітику та моніторинг. Фізична інфраструктура стає лише транспортним середовищем, а логіка роботи визначається політиками, які легко змінювати. Ключовою перевагою є висока гнучкість: наприклад, у навчальному закладі можна швидко створити сегменти мережі для викладачів, студентів та адміністративного персоналу, не змінюючи фізичну топологію. Масштабованість значно вища порівняно з класичними моделями, адже додавання нових пристроїв або користувачів може бути автоматизоване. Безпека забезпечується мікросегментацією, ідентифікацією користувачів та централізованим контролем доступу. Однак такі рішення є дорогими, а для їх підтримки потрібні висококваліфіковані спеціалісти. Для університетів це може бути проблемою через обмежений бюджет та кадрові ресурси.

Fortinet Security Fabric пропонує інтегровану екосистему, у якій усі компоненти, від міжмережевого екрану FortiGate до комутаторів FortiSwitch, точок доступу FortiAP, аналітичних систем FortiAnalyzer та клієнтських агентів FortiClient працюють як єдиний організм. Завдяки цьому адміністратор отримує централізовану систему управління, де безпека, моніторинг та керування об’єднані в одному середовищі.

Масштабованість цього рішення є достатньою для середніх та великих навчальних закладів. До фабрики можна підключати нові пристрої без складної конфігурації, використовуючи FortiLink та автоматичне виявлення обладнання. Продуктивність залежить від конкретних моделей, але завдяки інтеграції всі компоненти оптимізовані для спільної роботи. Безпека є сильним боком фабрики, застосовується багаторівневий захист, централізований моніторинг загроз та автоматизовані реакції на інциденти. Вартість загалом нижча, ніж у SDA, але вища за традиційні рішення через потребу у фірмових пристроях. Для навчального закладу Fortinet є збалансованим варіантом, тому що поєднує високу безпеку, простоту керування та оптимальну вартість.

Недоліком може бути залежність від одного вендора, що у майбутньому звужує можливості інтеграції зі сторонніми рішеннями. Проте, якщо ставити пріоритет на простоту адміністрування і комплексний захист, то цей підхід виглядає найбільш доцільним.[20]

Таблиця 2.2 – Порівняльна таблиця архітектурних рішень

Критерій	Three-Tier Architecture	Cisco SDA	Fortinet Security Fabric
Масштабованість	Забезпечується завдяки ієрархії рівнів, але вимагає значних інвестицій при розширенні.	Висока завдяки централізованому контролеру та автоматизації, легко підтримує великі мережі.	Добра для середніх і великих мереж, додавання пристроїв спрощується завдяки FortiLink.
Безпека	Базується на VLAN, ACL і зовнішніх міжмережевих екранах, контроль розподілений і складний.	Високий рівень: вбудована мікросегментація, ідентифікація користувачів, політики на основі ролей.	Комплексна: інтегровані засоби захисту, централізований моніторинг та автоматична реакція на загрози.
Керованість	Управління розподілене між пристроями, складне адміністрування у великих мережах.	Централізоване керування через DNA Center, автоматизація конфігурацій і моніторинг у реальному часі.	Єдиний центр управління за допомогою FortiGate або FortiManager, просте адміністрування навіть при обмежених ресурсах.

Продовження таблиці 2.2

Вартість	Високі капітальні витрати, додаткові інвестиції у засоби безпеки та обслуговування.	Дуже високі витрати на впровадження та підтримку, вимагає кваліфікованого персоналу.	Середня вартість: дешевше за SDA, дорожче за класичні рішення, але оптимальне співвідношення ціна/можливості.
Інтеграційний потенціал	Висока сумісність зі стандартними рішеннями, але складність інтеграції нових технологій.	Добре інтегрується з екосистемою Cisco, але обмежена сумісність із рішеннями інших вендорів.	Тісно інтегроване середовище Fortinet, обмеження через залежність від одного виробника.

Як видно з порівняння, трирівнева архітектура є перевіреним підходом, який добре працює в класичних мережах, але сьогодні вона вже виглядає менш гнучкою та потребує значних ресурсів при масштабуванні чи підвищенні вимог до безпеки.

Архітектура Cisco SDA вирізняється сучасними можливостями, такими як автоматизація й мікросегментація, але разом з тим потребує великих інвестицій і спеціальних знань для підтримки. Це робить її не завжди виправданою для середніх інфраструктур.

Fortinet Security Fabric виглядає більш збалансованим рішенням: воно забезпечує централізоване управління, інтегровану безпеку та відносно просте впровадження. Завдяки цьому можна отримати сучасний рівень захисту й зручності без великих витрат, що робить цей варіант найбільш привабливим у нашому випадку.

Для забезпечення наочності порівняння введемо систему кількісної оцінки. Кожен критерій для кожної архітектури буде оцінено за 10-бальною шкалою.

Таблиця 2.3 – Кількісна оцінка архітектурних рішень

Критерій	Three-Tier Architecture	Cisco SDA	Fortinet Security Fabric
Масштабованість	4	9	8
Безпека	4	10	9
Керованість	3	8	9
Вартість	3	1	7
Інтеграційний потенціал	6	5	5
Підсумковий бал	20	33	38

Класична трирівнева архітектура отримала найнижчий підсумковий бал. Це зумовлено через суттєві недоліки у критеріях керованості та вартості, а також низькими показниками безпеки та масштабованості в сучасних умовах.

Рішення Cisco SDA продемонструвало найвищі показники у категоріях безпеки та масштабованості. Проте його загальний бал 33 виявився нижчим за лідера через надзвичайно високу вартість впровадження та обмежений інтеграційний потенціал поза власною екосистемою.

Архітектура Fortinet Security Fabric набрала найвищий підсумковий бал. Дане рішення показує найкращу збалансованість за всіма ключовими критеріями. Воно поєднує високі оцінки за безпеку та керованість з оптимальним співвідношенням вартості. Згідно з проведеним аналізом, саме цей варіант є найбільш обґрунтованим для реалізації.

Висновок до другого розділу

Проведений аналіз дозволив розглянути три різні підходи до побудови мережевої інфраструктури: класичну трирівневу архітектуру, Cisco SD-Access та Fortinet Security Fabric. Кожне рішення має свої переваги й обмеження: традиційна модель вирізняється зрозумілою структурою, але важко масштабується й не відповідає сучасним вимогам безпеки; Cisco SDA пропонує гнучкість, автоматизацію та розширені механізми контролю, але вимагає значних інвестицій; Fortinet Security Fabric поєднує ключові функції безпеки, централізоване управління та відносну простоту впровадження.

Порівняння за вибраними критеріями показало, що для навчального закладу найкращим виглядає використання підходу Fortinet. Це рішення дозволяє одночасно забезпечити захищеність, зручність адміністрування та прийнятний рівень витрат, що робить його оптимальним для подальшої побудови мережевої інфраструктури факультету.

3 ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ФАКУЛЬТЕТУ

EVE-NG (Emulated Virtual Environment – Next Generation) – це середовище, яке дозволяє будувати й тестувати складні мережеві топології без використання реального обладнання, та дає можливість розгорнути віртуальні маршрутизатори, комутатори та міжмережеві екрани різних виробників і перевірити їхню роботу в єдиній лабораторії. Завдяки цьому можна відтворити роботу майже будь-якої мережі, від невеликих стендів до великих корпоративних сценаріїв.

На відміну від більш простих рішень, таких як Cisco Packet Tracer, який підходить здебільшого для базового відпрацювання команд, EVE-NG дозволяє працювати з реальними образами пристроїв різних виробників. Це дає можливість тестувати мережеві сценарії, максимально наближені до реальних. У порівнянні з GNS3, який також використовується для моделювання, EVE-NG є більш гнучким у масштабуванні та зручнішим у колективній роботі, оскільки надає повноцінний веб-інтерфейс і можливість одночасного доступу для кількох користувачів. Така функціональність робить його оптимальним варіантом для моделювання мережі факультету, де потрібно протестувати взаємодію багатьох компонентів та оцінити їхню роботу у комплексі.[10]

Зручність EVE-NG полягає в тому, що створені лабораторії можна запускати й змінювати у кілька кліків. Це робить інструмент зручним як для навчання, так і для проєктування. Під час дослідження, EVE-NG використовується для моделювання мережевої інфраструктури факультету, на його базі буде перевірено логіку побудови, роботу сегментації, політики безпеки та загальну стабільність архітектури перед тим, як її можна буде реалізувати на практиці.

3.1 Розгортання EVE-NG

Для встановлення eve-ng потрібно підключитися по SSH до віртуальної машини. Після війти як привілейований користувач за допомогою команди sudo –i та виконати команду wget -O - https://www.eve-ng.net/repo/install-eve.sh | bash -i

Рисунок 3.1 – Встановлення EVE-NG Community

Командами apt update та upgrade оновлюємо віртуальну машину та перезавантажуємо сервер командною reboot. Після перезавантаженя необхідно підключитися до машини по SSH і налаштувати root пароль (перед налаштуванням потрібно натиснути Ctrl+C і ввести команду sudo –i щоб стати root користувачем)

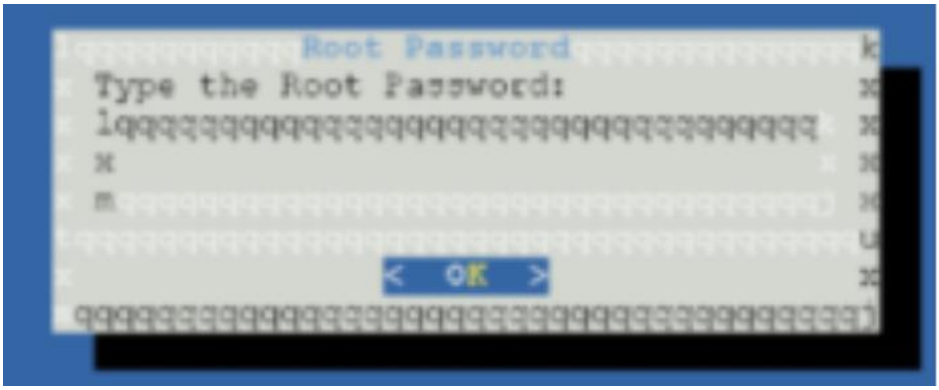


Рисунок 3.2 – Налаштування паролю root

При налаштуванні імені хоста та DNS домену приймаємо налаштування за замовчуванням. При появі запиту про використання DHCP або статичної IP адреси обираємо DHCP.

При появі запиту про використання DHCP або статичної IP адреси ообираємо DHCP і натискаємо «ENTER».

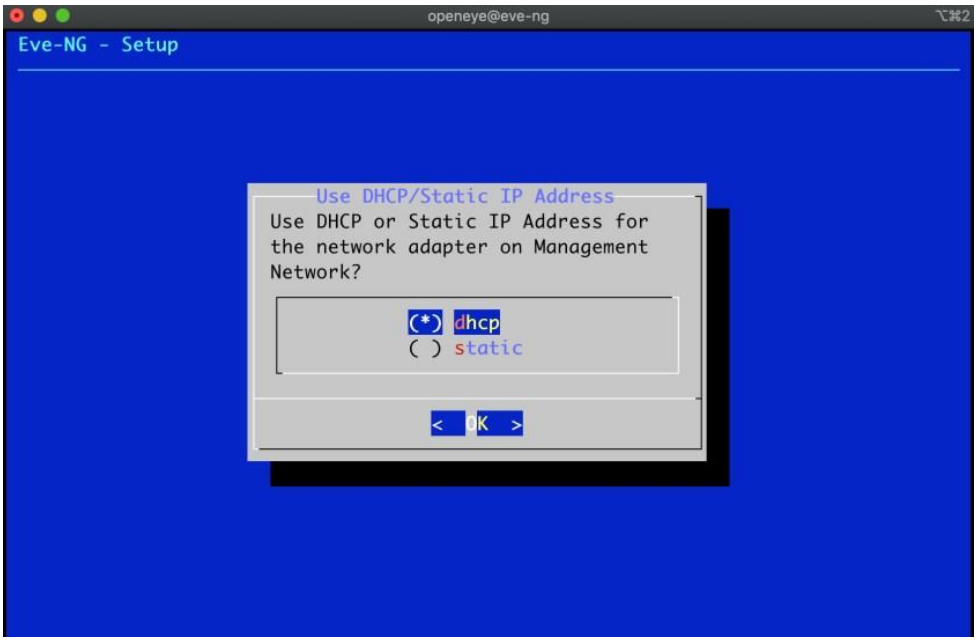


Рисунок 3.3 – Вибір налаштувань IP-адреси

На настопному кроці залишаємо поле для IP-адреси NTP сервера порожнім і натискаємо «Enter». В останньому пункті обираємо спосіб підключення віртуальної машини до Інтернету - direct connection.

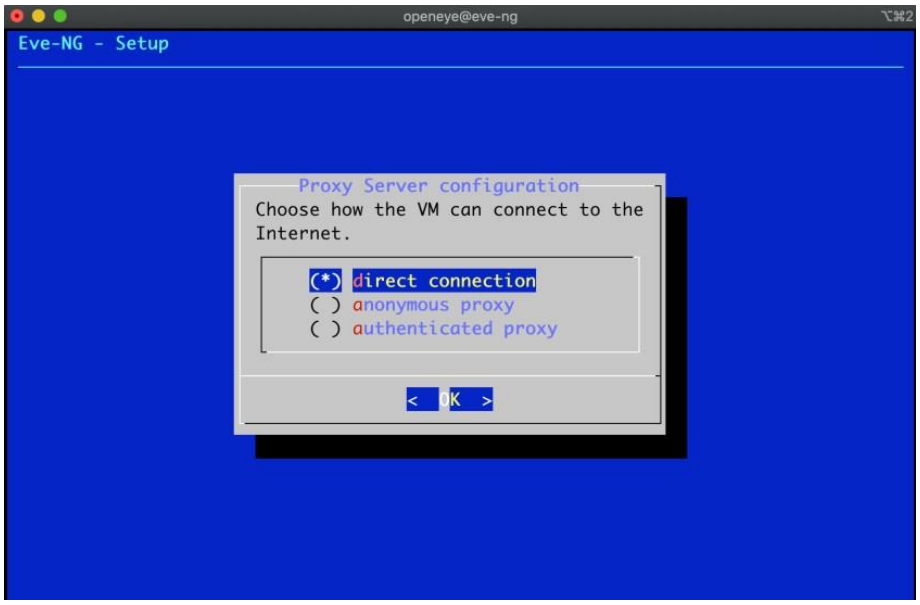


Рисунок 3.4 – Вибір способу підключення ВМ до Інтернету

Після останнього пунтку майстер налаштувань виходить із системи і віртуальна машина перезавантажується. Після перезавантаження системи підключаємося до EVE за допомогою публічної адреси.

3.1.1 Завантаження образів

Для завантаження образів на сервер використовується FTP клієнт FileZilla. Для того щоб мати можливість підключится до сервера, необхідно задати пароль для root користувача, який буде використовуватися при підключенні до серверу по протоколу SFTP. Задати пароль в Ubuntu можно за допомогою команди passwd вказавши ім’я користувача, для якого задається пароль.

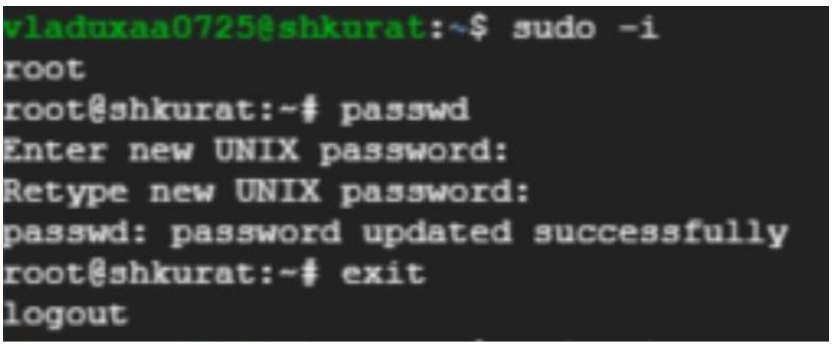


Рисунок 3.5 – Встановлення паролю root

Після встановлення паролю можна підключитись до серверу по протоколу SFTP вказавши IP-адресу сервера – 172.19.170.5, ім’я користувача та пароль.

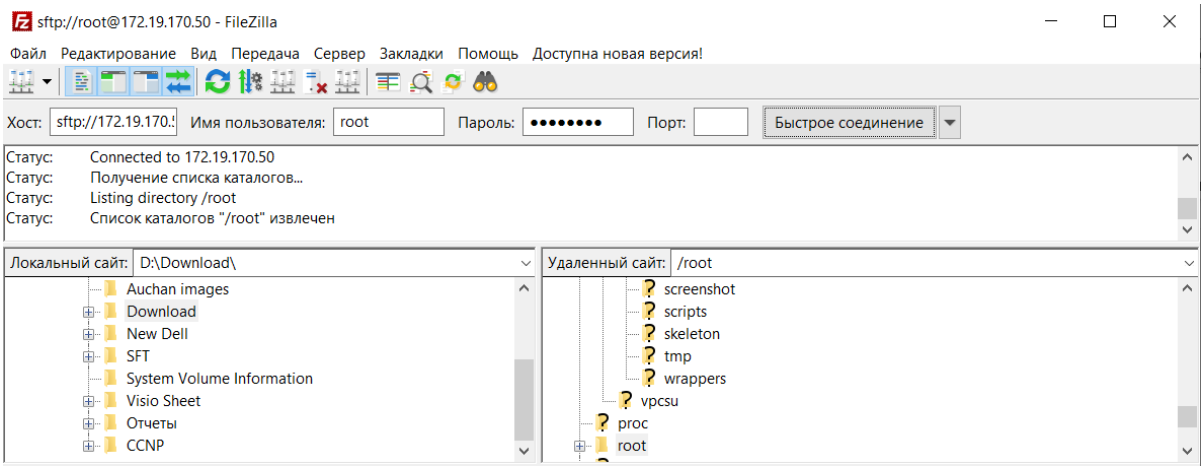


Рисунок 3.6 – Підключення до сервера за допомогою FileZilla

Образи для EVE-NG повинні завантажуватися в директорію /opt/unetlab/addons/qemu. При цьому для кожного образу створюється окремий спеціально названий каталог оскільки eve-ng дуже чутливий до імен каталогів, використовуваних для образів Qemu. Завантажити образи можна простим Drag-and-drop з будь-якої директорії локального ком'ютера на віддалений сервер.

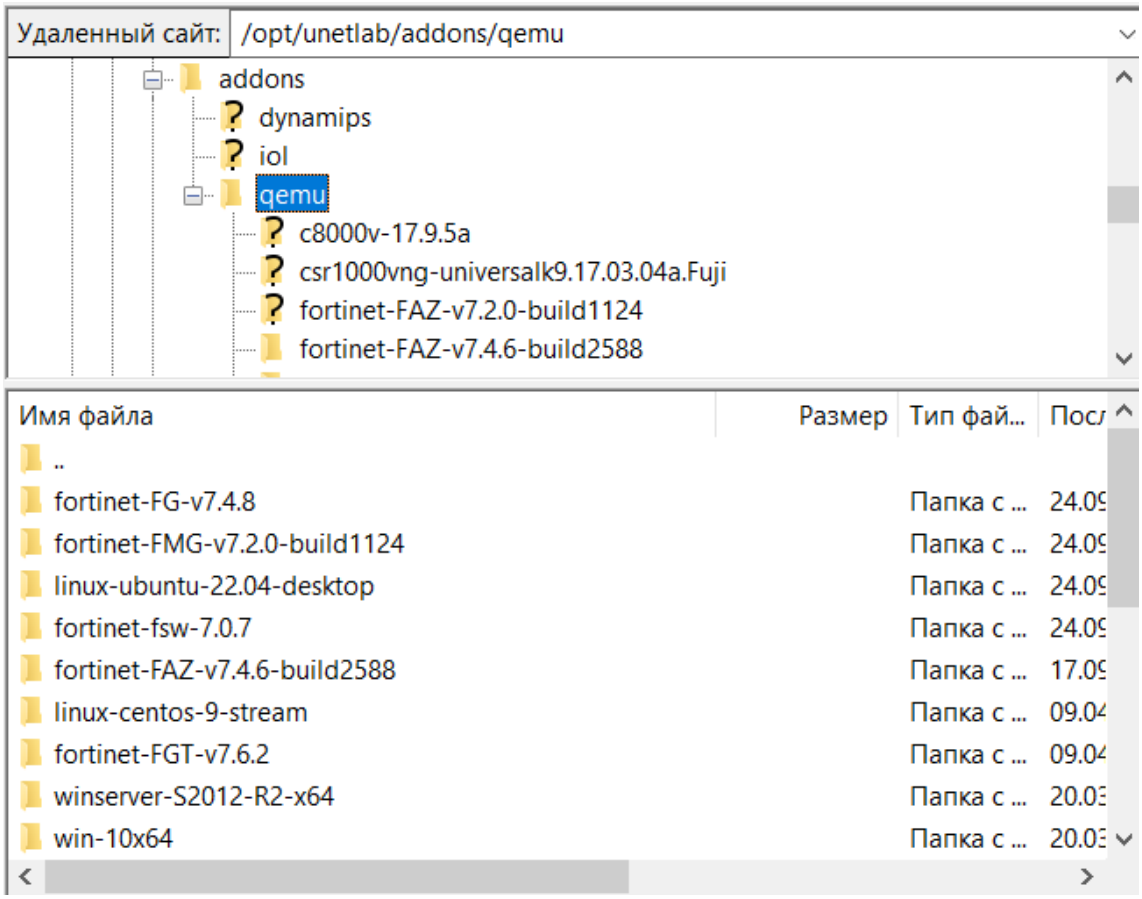


Рисунок 3.7 – Завантаження Qemu образів на сервер

На останньому кроці, для виправлення прав доступу необхідно виконати команду /opt/unetlab/wrappers/unl_wrapper -a fixpermissions, яка змінить права для доданих образів. [11]

3.2 Побудова симуляційного середовища в EVE-NG

Побудова симуляційного середовища є головним етапом для перевірки працездатності розробленої архітектури та відпрацювання сценаріїв її функціонування без залучення фізичного обладнання. Для цього використовується платформа EVE-NG, яка дає можливість розгортати повноцінні віртуальні копії мережевих пристроїв та моделювати їхню взаємодію.

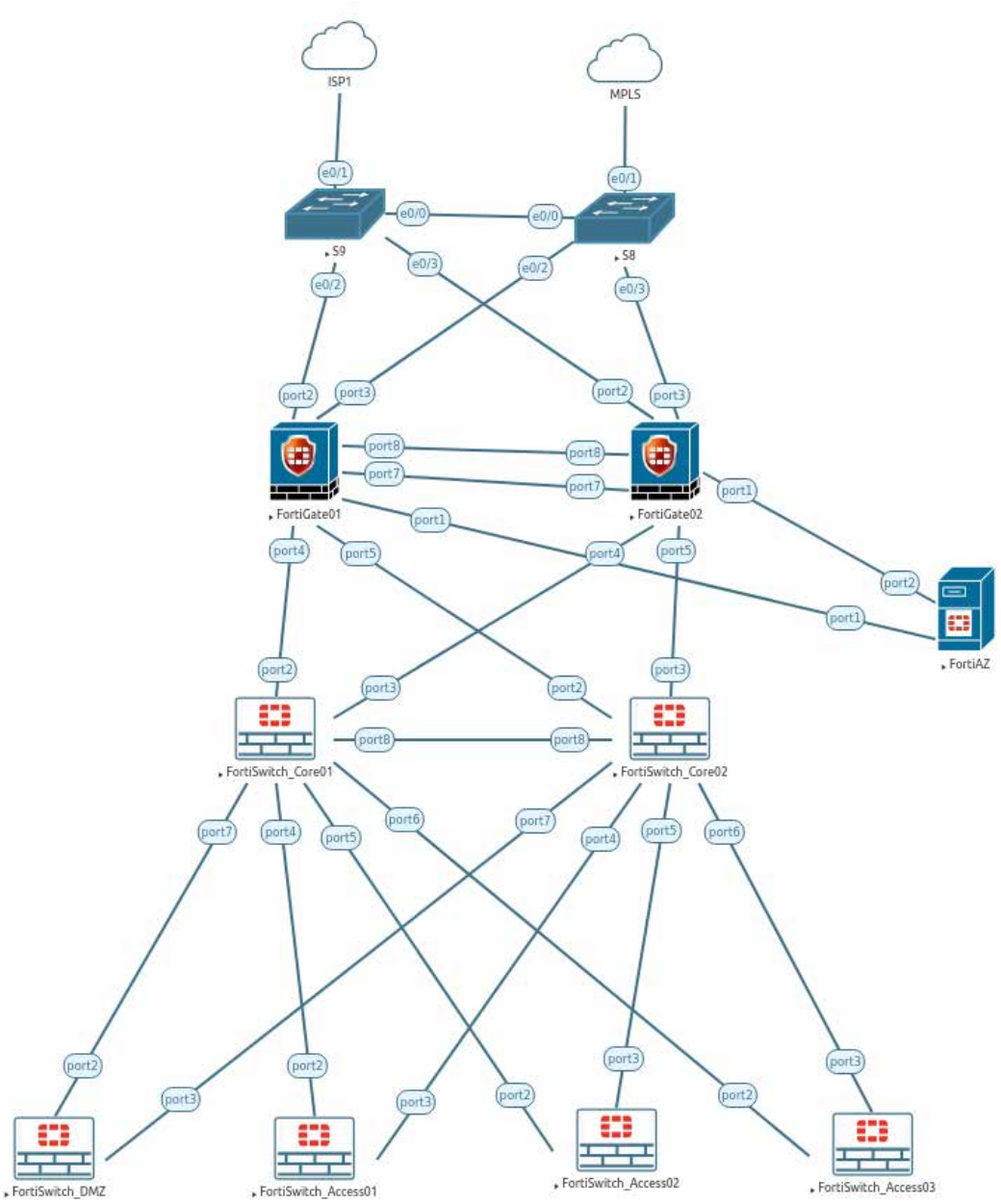


Рисунок 3.8 – Логічна топологія мережі в EVE-NG

На схемі представлено логічну структуру мережі, відтворену у симуляційному середовищі. Вона включає два маршрутизованих підключення до провайдерів ISP та MPLS, відмовостійкий кластер між двома міжмережевими екранами FortiGate, ядро мережі на базі комутаторів FortiSwitch Core01 та Core02, а також рівень доступу, що реалізований через кілька комутаторів FortiSwitch Access. Для винесених сервісів створено окремий сегмент на FortiSwitch DMZ, а для централізованого моніторингу та аналізу інтегровано систему FortiAnalyzer.

Така побудова структури мережі дозволяє перевірити коректність взаємодії між усіма компонентами, налаштувати політики безпеки, протестувати резервування каналів та оцінити ефективність обраної архітектури у навчальному закладі.

3.3 Конфігурація мережі

3.3.1 Налаштування демаркаційних комутаторів

Демаркаційні комутатори – це комутатори, які встановлюються на стороні клієнта в точці підключення до мережі провайдера. Вони забезпечують розмежування мережевої інфраструктури клієнта та провайдера, спрощують обслуговування і підвищують надійність роботи мережі. При моделюванні демаркаційні комутатори використовуються переважно для забезпечення високої доступності (HA), резервування каналів зв’язку та безперервності роботи сервісів у разі відмови одного з вузлів або каналів зв’язку.

```
DSW01(config)#vlan 175
DSW01(config-vlan)#na
DSW01(config-vlan)#name MPLS
DSW01(config-vlan)#exit
DSW01(config)#vlan
DSW01(config)#vlan 176
DSW01(config-vlan)#nam
DSW01(config-vlan)#name ISP
DSW01(config-vlan)#exit
```

Рисунок 3.9 – Налаштування VLAN-ів на демаркаційному комутаторі

```
DSW01(config)#interface range e0/1-3
DSW01(config-if-range)#sw
DSW01(config-if-range)#switchport mode acc
DSW01(config-if-range)#switchport mode access
DSW01(config-if-range)#sw
DSW01(config-if-range)#switchport acc
DSW01(config-if-range)#switchport access vl
DSW01(config-if-range)#switchport access vlan 176
DSW01(config-if-range)#
```

Рисунок 3.10 – Переведення інтерфейсів в режим Access для VLAN 176

Аналогічну конфігуацію необхідно провести й для другого комутатора, тільки використовувати для цього VLAN 175, в результаті досягнута відмовостійкість на рівні провайдерів для фаєрволів FortiGate.

3.3.2 Налаштування FortiGate, FortiSwitch та Active Directory

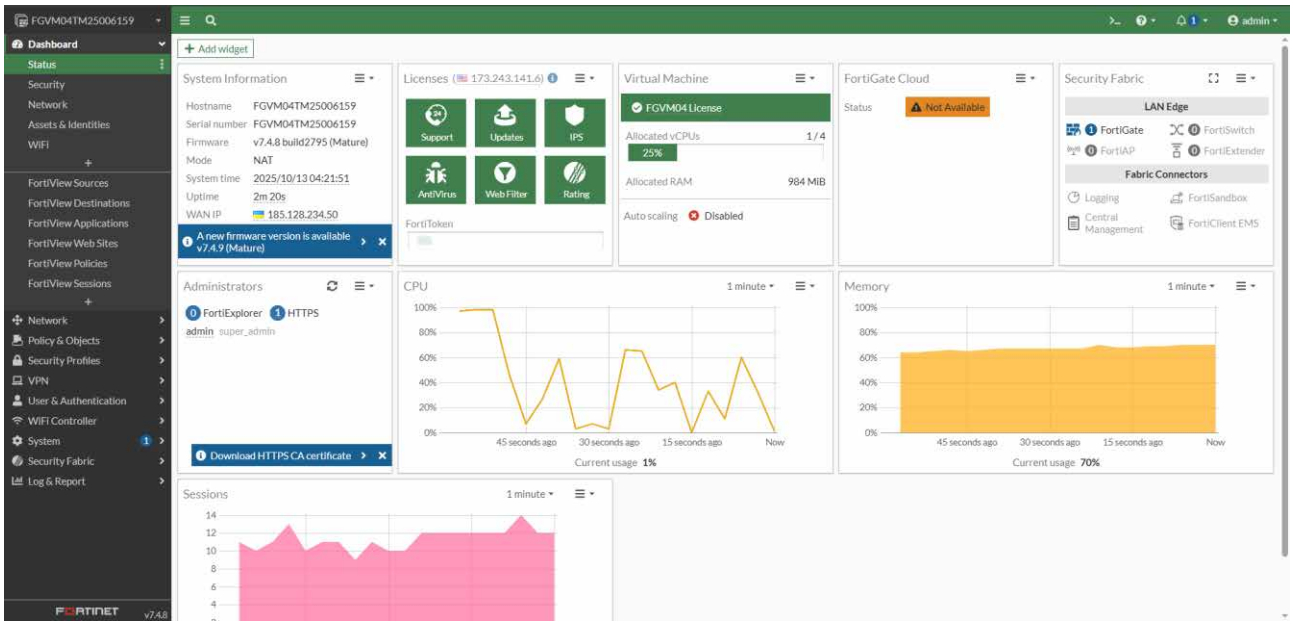


Рисунок 3.11 – Головна сторінка системи FortiGate

Перш ніж приступити до налаштування FortiGate, спочатку потрібно створити HA пару між двома пристроями.

Механізм високої доступності HA у міжмережевих екранах FortiGate забезпечує безперебійну роботу мережевих сервісів у разі відмови одного з пристроїв. Для цього декілька пристроїв об’єднуються у кластер, де один з них працює як основний, а всі інші як резервні. У випадку збою основного вузла управління трафіком автоматично переходить до резервного, що дозволяє зберегти активні з’єднання та уникнути переривання сервісів.

FortiGate підтримує два режими роботи HA: Active-Passive та Active-Active. У режимі Active-Passive трафік обробляється лише основним пристроєм, тоді як резервний залишається в режимі очікування та переходить у роботу лише у випадку відмови основного. У режимі Active-Active навантаження розподіляється між усіма пристроями кластера, що підвищує продуктивність системи.

Під час роботи кластера відбувається постійна синхронізація конфігурації та таблиць сеансів між вузлами, завдяки чому користувачі не помічають перемикання. Така архітектура підвищує надійність мережі, забезпечує безперервність бізнес-процесів та мінімізує вплив можливих збоїв або технічного обслуговування на роботу системи.[12]

Під час моделювання мережі буде використовуватись режим Active-Passive, оскільки навантаження трафіку незначне.

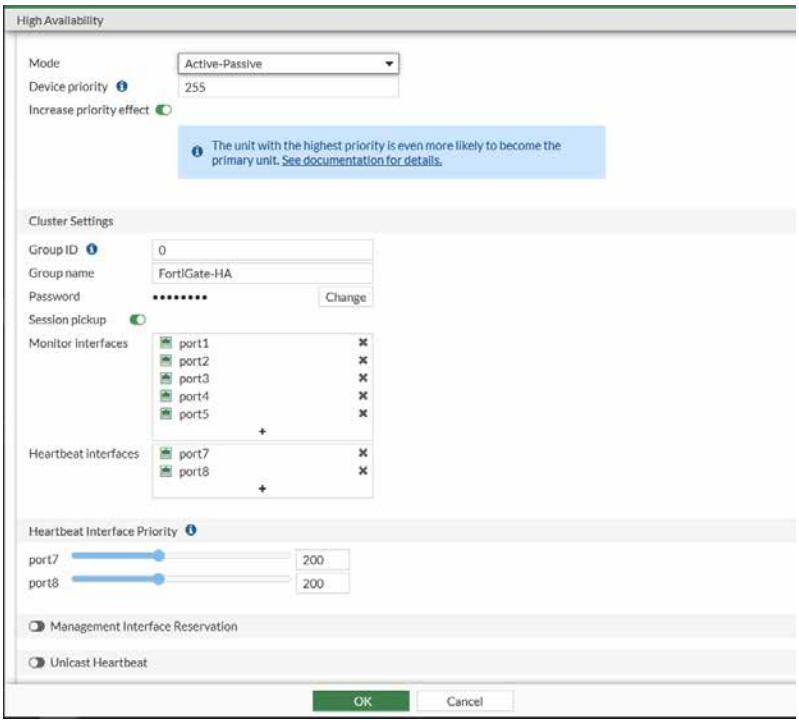


Рисунок 3.12 – Налаштування HA для основного FortiGate

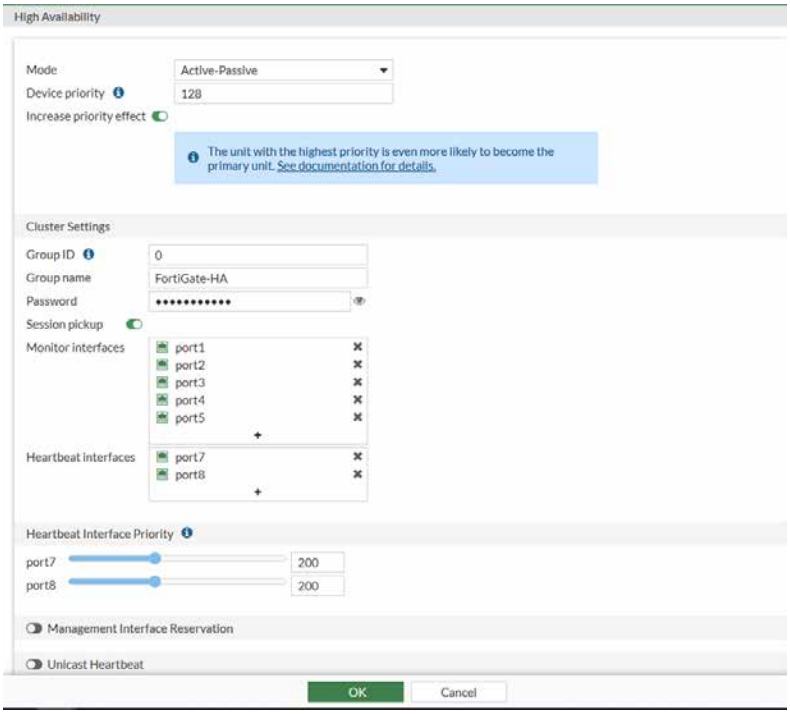


Рисунок 3.13 – Налаштування HA для запасного FortiGate

Як можна побачити, при налаштуванні HA пари, приорітетність визначає, Який з пристроїв буде активним в даній парі пристроїв

Після застосування конфігурації, пристрої починають комунікувати між собою та синхронізувати конфігурацію, бази даних, тощо.

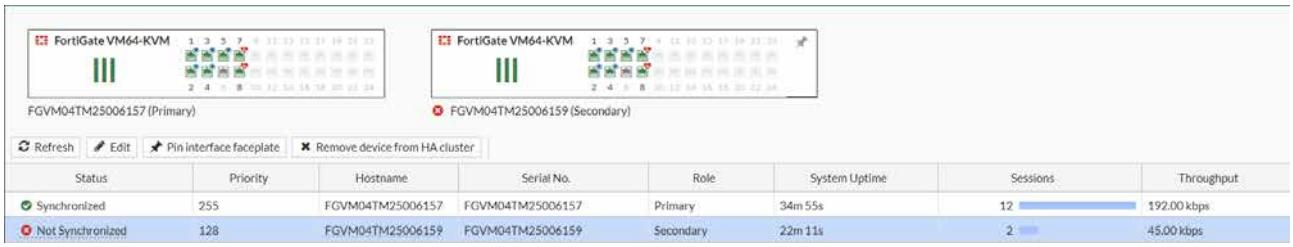


Рисунок 3.14 – Стан синхронізації між двома пристроями

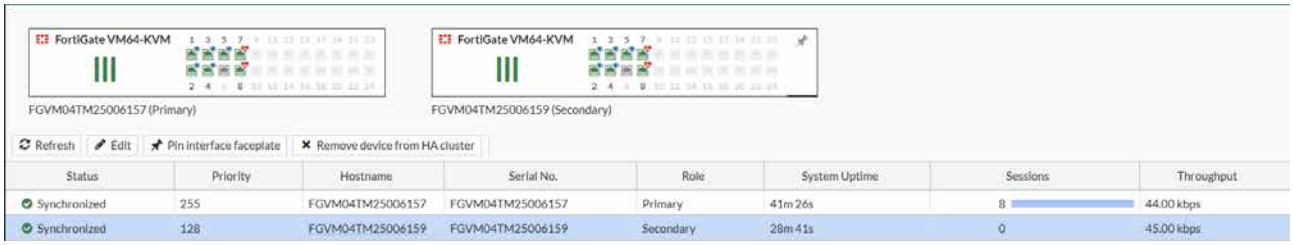


Рисунок 3.15 – Синхронізація проведена успішно

Успішна синхронізація між пристроями FortiGate забезпечує узгодженість усіх налаштувань у кластері, що є важливим фактором стабільної та надійної роботи системи. Завдяки цьому адміністрування спрощується, тому що зміни, внесені на одному пристрої, автоматично застосовуються до всіх інших. Під час перемикання між вузлами активні сесії зберігаються, тому користувачі не відчувають перерв у роботі сервісів. Крім того, така синхронізація підвищує відмовостійкість мережі. У разі виходу з ладу одного з пристроїв його функції миттєво перебирає резервний, зберігаючи поточний стан системи. Це також дозволяє проводити оновлення або технічне обслуговування без зупинки роботи всієї інфраструктури, що позитивно впливає на її загальну стабільність і надійність.

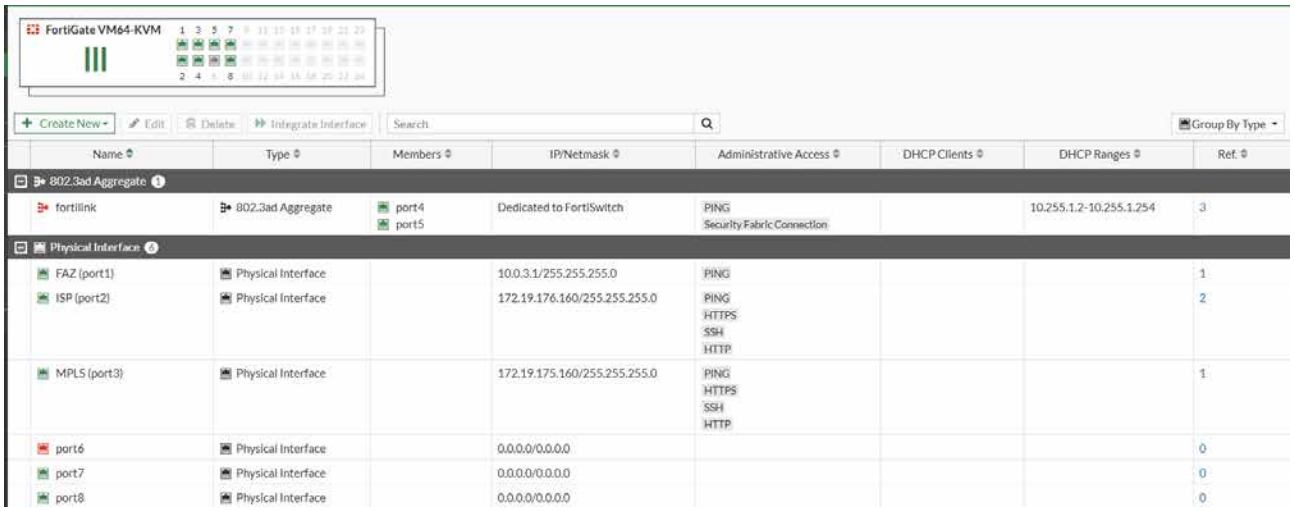


Рисунок 3.16 – Налаштування інтерфейсів FortiGate

Технологія FortiLink є найголовнішим елементом концепції Security Fabric від Fortinet, що спрямована на централізований контроль усіх елементів мережі. За її допомогою мережеві комутатори FortiSwitch можуть бути підключені до FortiGate як керовані пристрої через спеціальний тунель управління CAPWAP. Це дає змогу адміністратору здійснювати конфігурацію портів, VLAN, політик безпеки та моніторинг комутаторів без потреби у використанні окремої системи управління.

Використання FortiLink значно спрощує адміністрування, знижує ризик помилок при налаштуванні, підвищує рівень захисту мережевої інфраструктури та забезпечує узгоджену політику безпеки на всіх рівнях мережі факультету.[13]

Для сигментації мережі централізовано створюються необхідні VLAN, з подальшим розповсюдженням по необхідним комутаторам FortiSwitch.

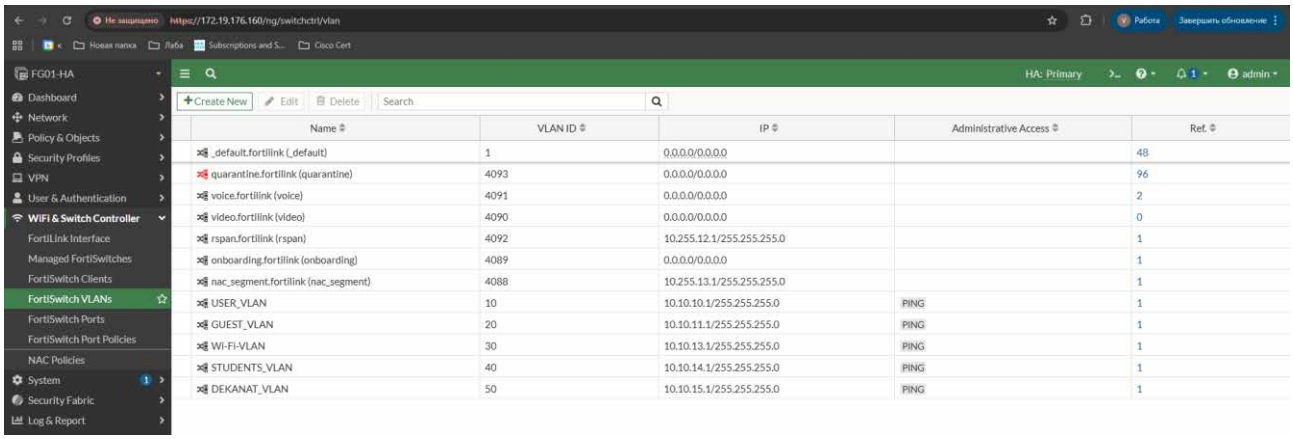


Рисунок 3.17 – Створенні VLAN для сигментації мережі

Для конжного інтерфейсу можна призначити один або декілька VLAN, в залежності від потреби

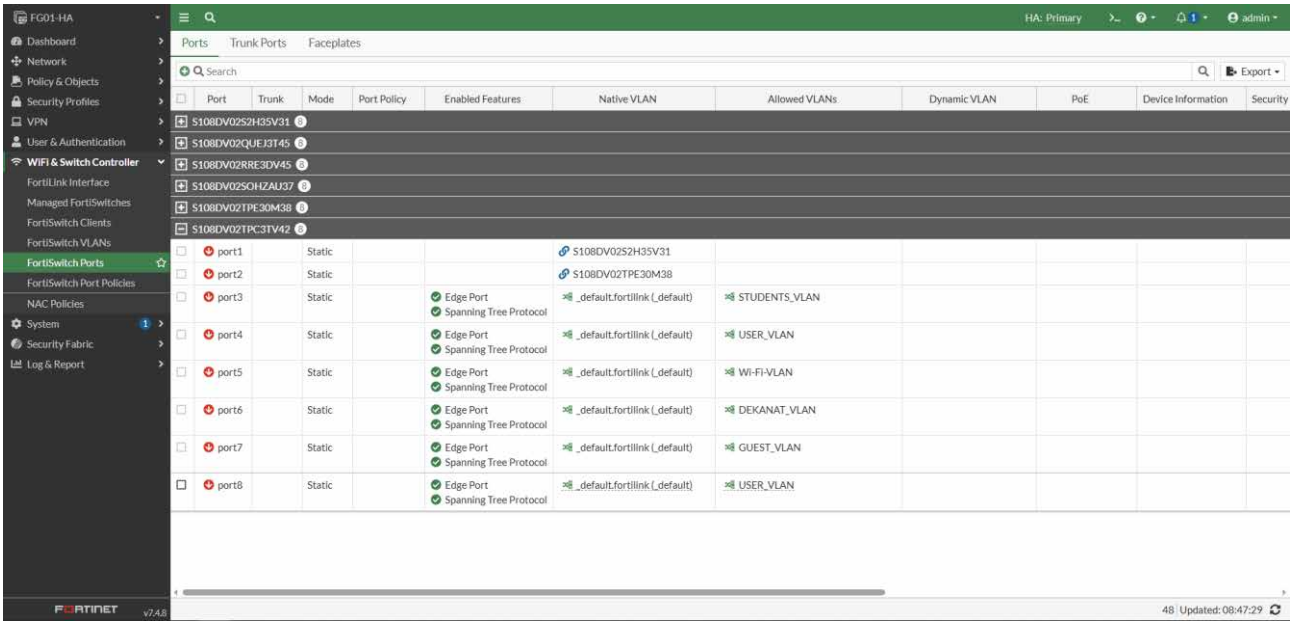


Рисунок 3.18 – Централізований менеджмент FortiSW. Призначення VLAN

Для контролю доступу між підмережами необхідно використовувати Firewall Policy - набір правил, які визначають порядок обробки мережевого трафіку. Ці політики регулюють доступ між різними сегментами мережі, визначаючи, який трафік дозволений або заборонений, а також які додаткові механізми безпеки застосовуються під час його проходження. За замовчуванням, правила працюють в режимі White Lists, тобто якщо трафік не дозволений правилом – він буде заблокований за допомогою Implicit Deny.

Рисунок 3.19 – Правило за замовчуванням Implicit Deny

Кожна політика містить набір параметрів, таких як: вихідна та цільова зона або інтерфейс, IP-адреси джерела і призначення, сервіси (протоколи та порти), дію (allow/deny), а також додаткові функції, такі як NAT, фільтрація вебтрафіку, антивірусна перевірка чи інспекція додатків.

Для прикладу, створено правило, яке дозволяє користувачам підмережі DEKANAT_VLAN звертатись до мережі інтернет за протоколами HTTP, HTTPS, при цьому використовуючи NAT, аби в публічний простір трафік виходив з публічним IP адресом інтерфейсу.

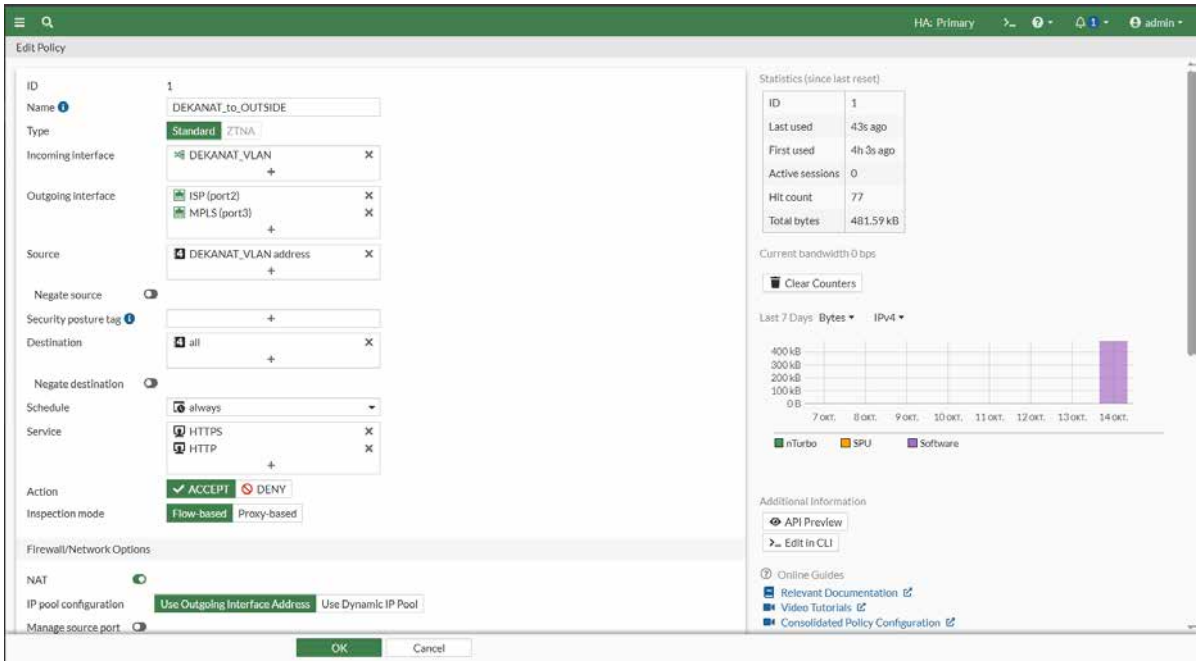


Рисунок 3.20 – Створення правила доступу DEKANAT_VLAN до мережі інтернет

Гостьовій підмережі, за правилами безпеки, заборонено звертатись куди завгодно окрім мережі Інтернет. Це можна реалізувати за допомогою Firewall Policy.

Також необхідно забезпечити доступ авторизованим користувачам до корпоративних ресурсів. В результаті базові налаштування політик контролю доступу будуть виглядати наступним чином.

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security
Uncategorized											
DEKANAT_to_OUTSIDE (1)	DEKANAT_VLAN	ISP (port2) MPLS (port3)	DEKANAT_VLAN address	all	always	HTTPS HTTP	ACCEPT		NAT	Standard	no-i
GUEST_Policy (2)	GUEST_VLAN	ISP (port2)	GUEST_VLAN address	all	always	ALL	ACCEPT		NAT	Standard	no-i
AuthUSERS_to_DMZ (3)	STUDENTS_VLAN USER_VLAN DEKANAT_VLAN	DMZ	DEKANAT_VLAN address STUDENTS_VLAN address USER_VLAN address	DMZ address	always	ALL	ACCEPT		Disabled	Standard	no-i
Implicit											
implicit_deny (0)	any	any	all	all	always	ALL	DENY				

Рисунок 3.21 – Базові налаштування політик контролю доступу

Необхідно зауважити, що для внутрішньої комунікації між підмережами неохідно вимикати NAT, аби уникнути заміни IP адреси джерела.

Для організації віддаленого доступу користувачів до мережевих ресурсів факультету можна використовувати технологію Remote Access VPN по протоколу SSL.

SSL VPN легкі в реалізації і не вимагають установки і обслуговування певного клієнтського програмного забезпечення - всього лише сучасний браузер. Ці типи VPN забезпечують більш високий рівень сумісності клієнтської платформи, а також конфігурації для брандмауерів і віддалених мереж.

Вони полегшують доступ до захищених мережевих ресурсів віддалено, використовуючи автентифікований шлях, який шифрує весь мережевий трафік від кінця до кінця. Це створює враження, що користувач знаходиться у внутрішній мережі, незалежно від його фактичного географічного розташування.

SSL VPN вимагає значно меншої технічної підтримки та адміністративних витрат, ніж традиційні VPN-клієнти, завдяки простоті їх використання і залежно від звичайно використовуваних веб-клієнтів.

SSL VPN можуть надати адміністраторам детальний контроль доступу, оскільки вони створюють тунелі для зазначених додатків замість всієї корпоративної мережі. Це означає, що можна обмежити користувачів в з'єднанні SSL VPN тільки тими додатками, до яких їм дозволено доступ, а не до всієї мережі.[14]

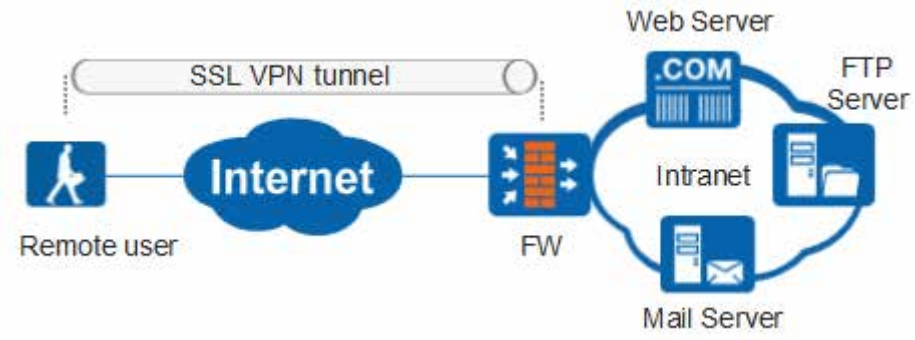


Рисунок 3.22 – Приклад SSL VPN з’єднання

В FortiGate доступ по SSL VPN реалізується за допомогою додатку FortiClient, який можна завантажити перейшовши за URL адресою фаєрволу.

Для ідентифікації користувачів, які зможуть підключатись до інфрастуктури буде використано Active Directory, групи користувачів передаються за допомогою протоколу LDAP – мережевий протокол прикладного рівня для надсилання запитів та модифікації даних служби каталогів через TCP/IP. LDAP є відкритим, комерційно-нейтральним, промисловим стандартним протоколом.

Будь-який запис у каталозі LDAP складається з одного або декількох атрибутів і володіє унікальним ім'ям. Відносне унікальне ім'я має вигляд ІмяАтрибута = значення. На одному рівні каталогу не може існувати двох записів з однаковими відносними унікальними іменами. В силу цієї структури унікального імені записи в каталозі LDAP можна легко уявити у вигляді дерева.

Запис може складатися тільки з тих атрибутів, які визначені в описі класу запису (object class), які, у свою чергу, об'єднані в схеми (schema). У схемі визначено, які атрибути є для даного класу обов'язковими, а які - необов'язковими. Також схема визначає тип і правила порівняння атрибутів. Кожен атрибут запису може зберігати кілька значень.[15]

Таблиця 3.1 – Типи атрибутів LDAP

Скорочена назва	Атрибут	Ідентифікатор об’єкта (OID)
CN	CommonName	2.5.4.3
L	LocalityName	2.5.4.7
ST	StateOrProvinceName	2.5.4.8
O	OrganizationName	2.5.4.10
OU	OrganizationalUntilName	2.5.4.11
C	CountryName	2.5.4.6
STREET	StreetAddress	2.5.4.9
DC	DomainComponent	0.9.2342.19200300.100.1.25
UID	Userid	0.9.2342.19200300.100.1.1

Для встановлення Active Directory Domain Service необхідно відкрити «Диспетчер серверів» і обрати пункт «Добавити ролі і компоненти».

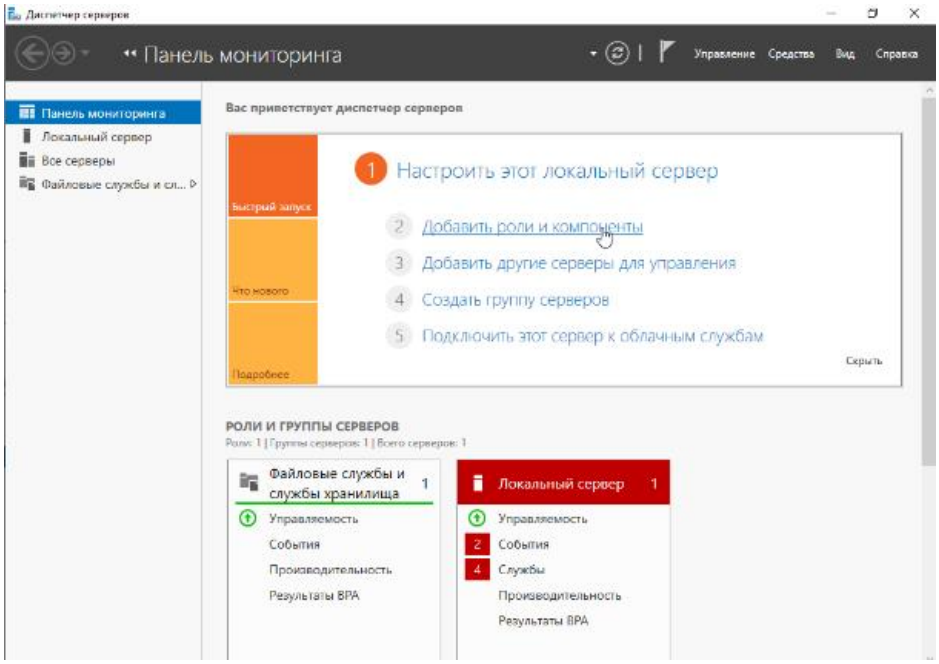


Рисунок 3.23 – Вибір підменю «Добавити ролі і компоненти»

Після чого відкриється вікно «Мастер додавання ролей та компонентів». Під час встановлення в підпункті «Тип встановлення» необхідно вибрати варіант «Встановлення ролей або компонентів».

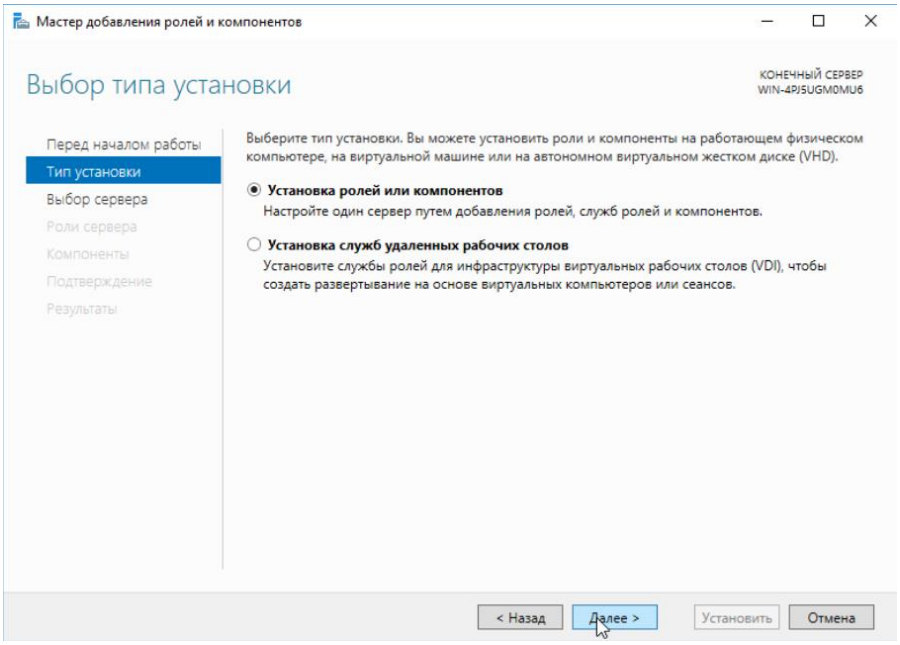


Рисунок 3.24 – Вибір типу встановлення «Встановлення ролей»

В наступному підменю «Вибір серверу» необхідно вибрати сервер або віртуальний жорсткий диск, на який будуть встановлені ролі і компоненти.

На цій сторінці вказані сервери під керуванням Windows Server 2012 або більш нового випуску Windows Server, які були додані з допомогою команди «Додати сервер» в диспетчері серверів.

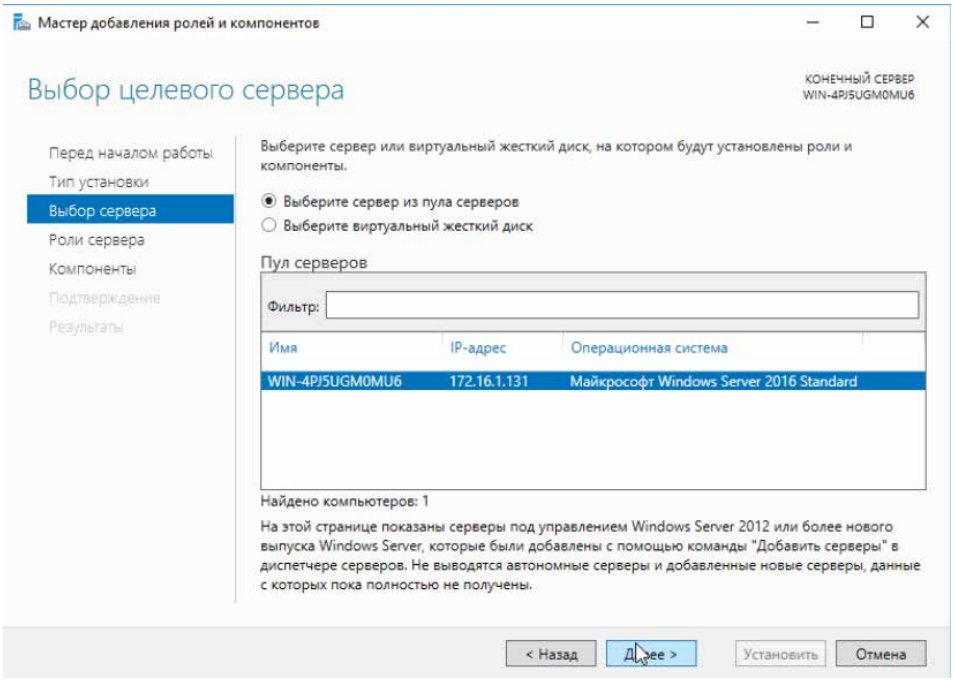


Рисунок 3.24 – Вибір об’єкту для встановлення компонентів

В наступному вікні «Ролі серверу» необхідно відзначити ролі для встановлення на сервер. В даному потрібно вибрати роль «Доменні служби Active Directory ».

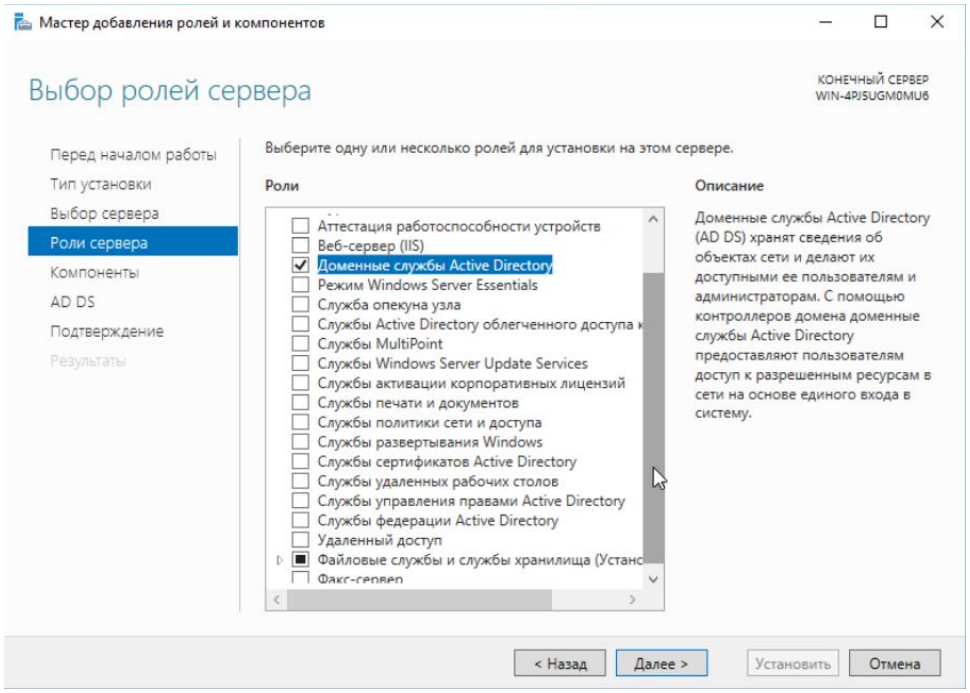


Рисунок 3.25 – Вибір ролі серверу

В вікні «Підтвердження встановлення компонентів» потрібно встановити галку напроти автоматичного перезапуску кінцевого серверу. Також в цьому вікні відображаються всі додаткові компоненти, які будуть встановлені. Після перевірки списку компонентів проводимо встановлення за допомогою кнопки «Встановити».

Після встановлення та перезавантаження серверу у вікні «Диспетчер серверів» в вертикальному меню з’явиться вкладка «AD DS». У горизонтальному меню потрібно натиснути на знак оклику і вибрати «Підвищити роль цього сервера до рівня контролера». Це потрібно для того, аби сервер став контролером домену, і все запити від клієнтів надходили до нього.[16]

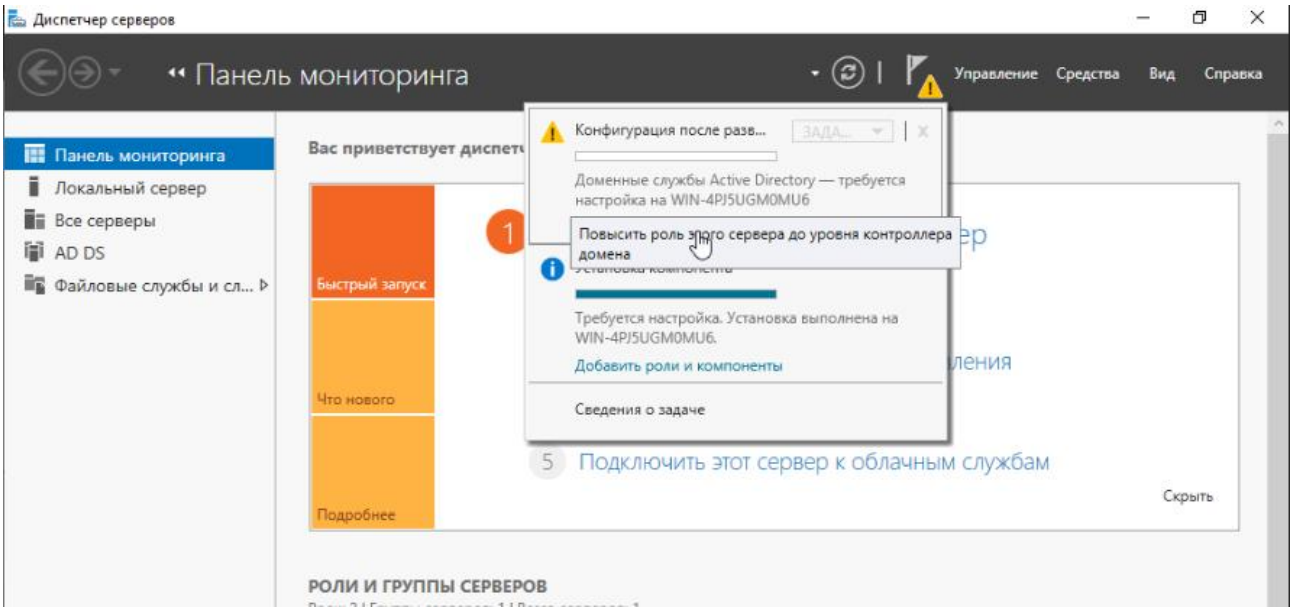


Рисунок 3.26 – Підвищення ролі серверу до «контролера домену»

Після встановлення компоненту необхідно провести його налаштування, тому у вікні налаштувань «AD DS» потрібно вибрати операцію розгортання «Додати новий ліс» і вказати назву кореневого домену. Назва не може бути однокомпонентною, наприклад, company.local замість company. Також, назва повинна бути унікальною.

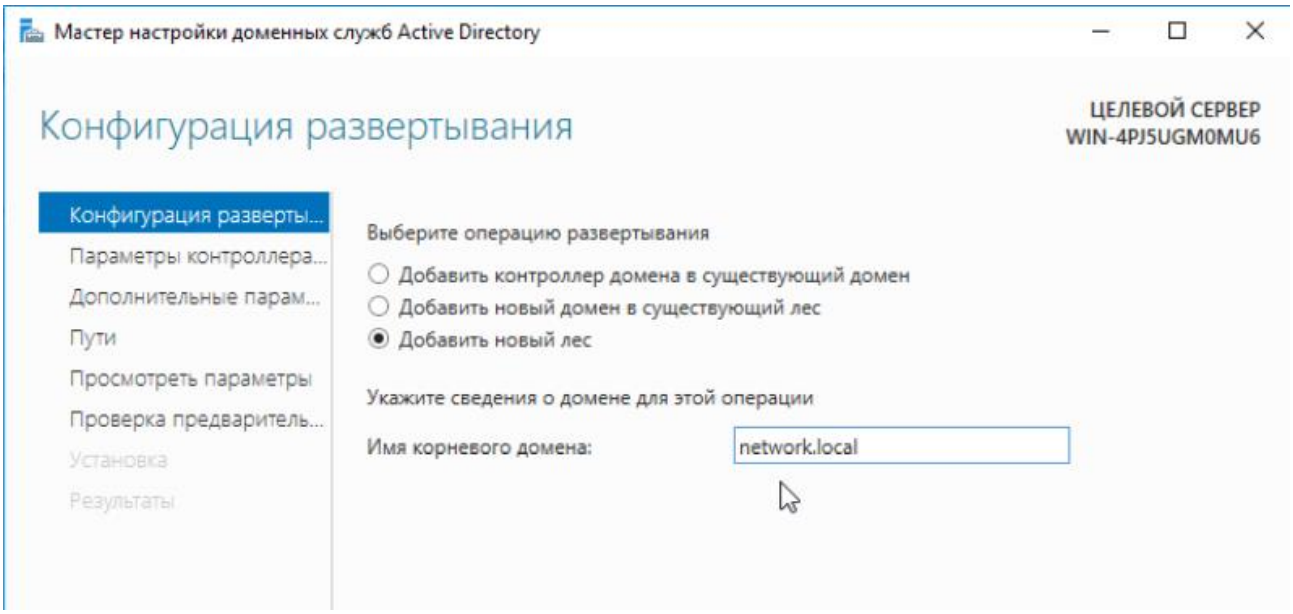


Рисунок 3.27 – Встановлення назви кореневого домену

На наступному кроці в підменю «Параметри контролера домена» потрібно ввести пароль для режиму відновлення служб каталогів

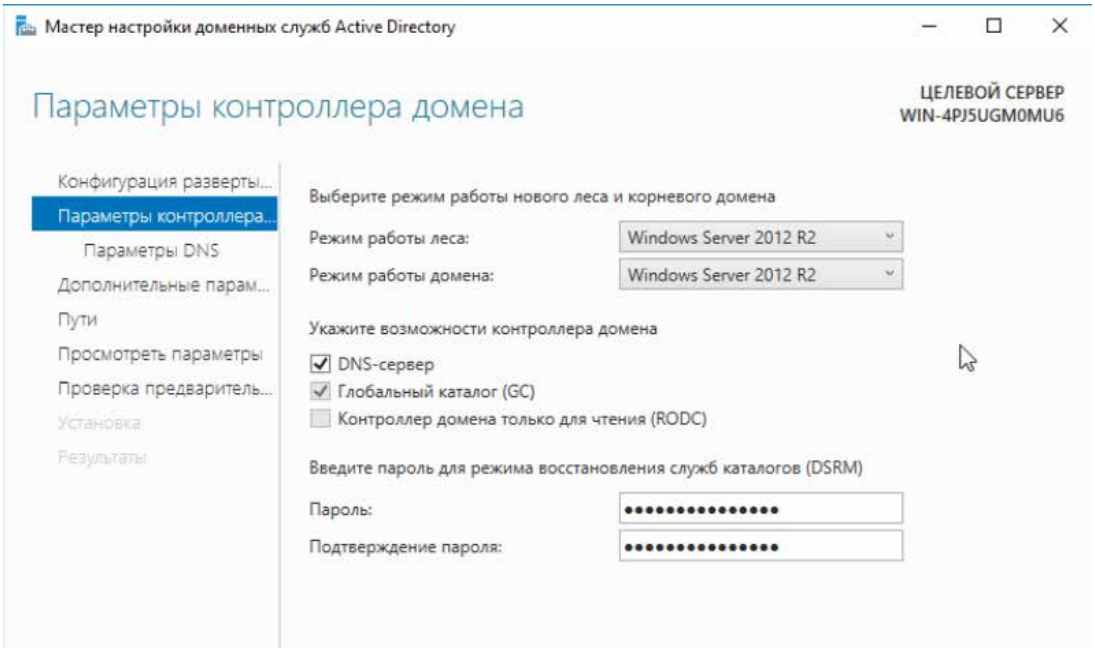


Рисунок 3.28 – Налаштування параметрів контролера домена

У всіх наступних підменю можна натискати «Далі» перевіривши запропоновані параметри. Після всіх налаштувань відбудеться перевірка попередніх вимог для коректної роботи контролера домена. Якщо перевірки виконані успішно і налаштування задовольняють вимогам, буде запропоновано запустити встановлення налаштувань з подальшим перезавантаженням серверу.

Після перезавантаження сервера можна переходити до створення облікових записів. Для створення нових облікових записів і адміністраторів потрібно відкрити оснащення «Active Directory Users and Computers», для цього відкрити «Диспетчер серверів» і перейти в розділ AD DS. У контекстному меню сервера вибрати відповідну оснастку.

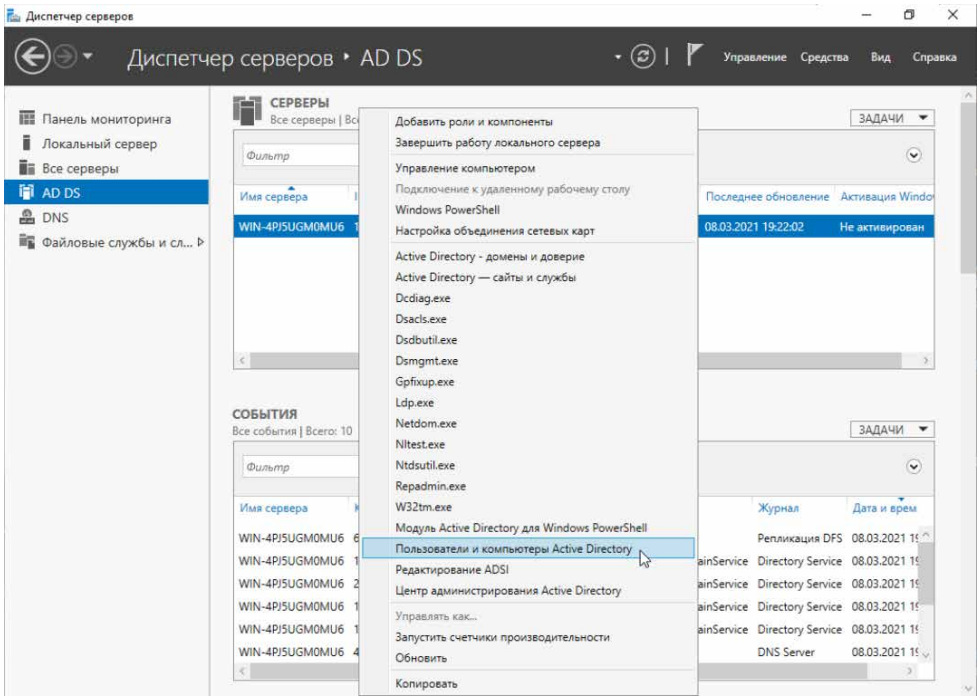


Рисунок 3.29 – Оснастка для створення облікових записів

У новому вікні потрібно розгорнути дерево домену і знайти каталог з користувачами Users. Правою кнопкою миші натиснути на каталог і вибрати «Створити -> Користувач». Для нового користувача потрібно задати особисті дані, далі ввести пароль, який повинен складатись від 14 символів і містити букви різного регістра і цифри, а також, як мінімум, один спец. символ.

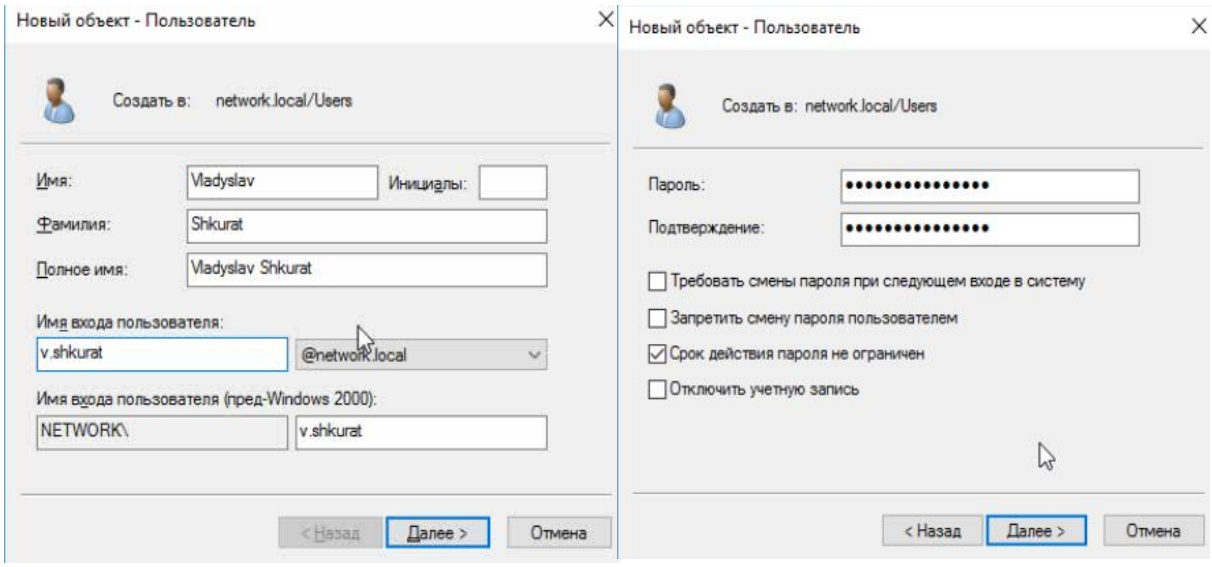


Рисунок 3.30 – Створення нового користувача

Щоб користувач міг керувати службами Active Directory, його необхідно додати в групу «Адміністратори домена». Для цього за допомогою правої кнопки миші потрібно відкрити властивості користувача і перейти у вкладку «Член груп». Натиснути кнопку «Додати» для додавання в групу.[16]

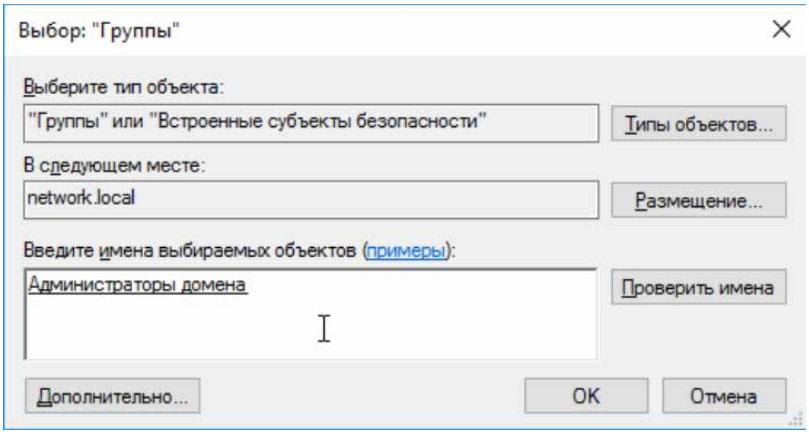


Рисунок 3.31 – Внесення користувача в групу «Адміністратори домена»

Після налаштування Active Directory можна перейти до конфігурації SSL VPN. Перш за все, необхідно підключити FortiGate до Active Directory за допомогою протоколу LDAP. Для цього, в меню Users&Authentication необхідно вибрати підменю LDAP Servers, та натиснути «Create New»

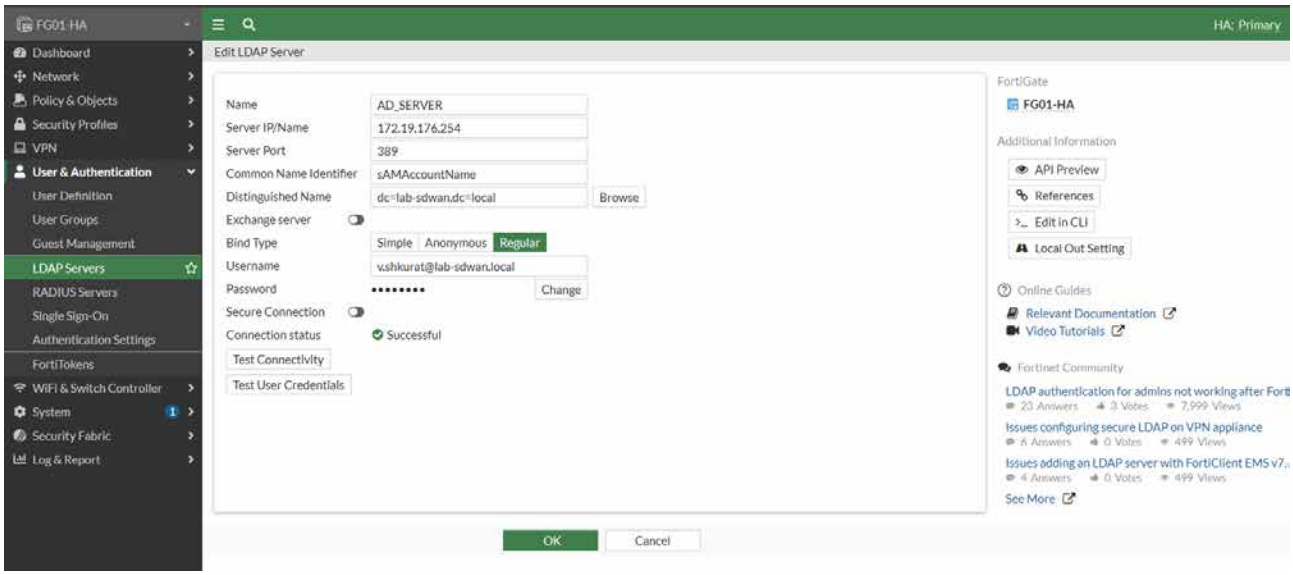


Рисунок 3.32 – Налаштування LDAP підключення

При успішному налаштуванні має бути можливість вивантаження LDAP каталогу з Active Directory.

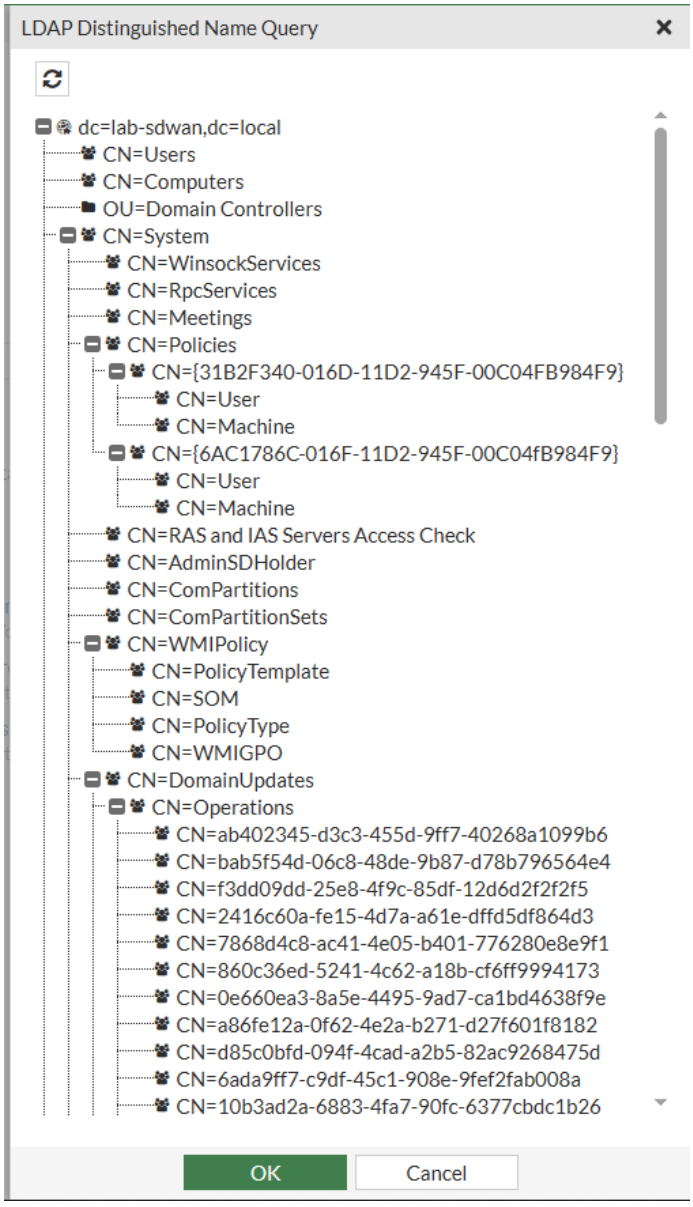


Рисунок 3.33 – Вивантажений LDAP каталог

Після потрібно створити необхідні групи, в разі необхідності розмежування доступу по групах. Ім'я групи на FortiGate має відповідати групі, яка передається в Vendor Specific Attribute. Це можна зробити перейшовши в підменю User Groups та натистути «Create New».

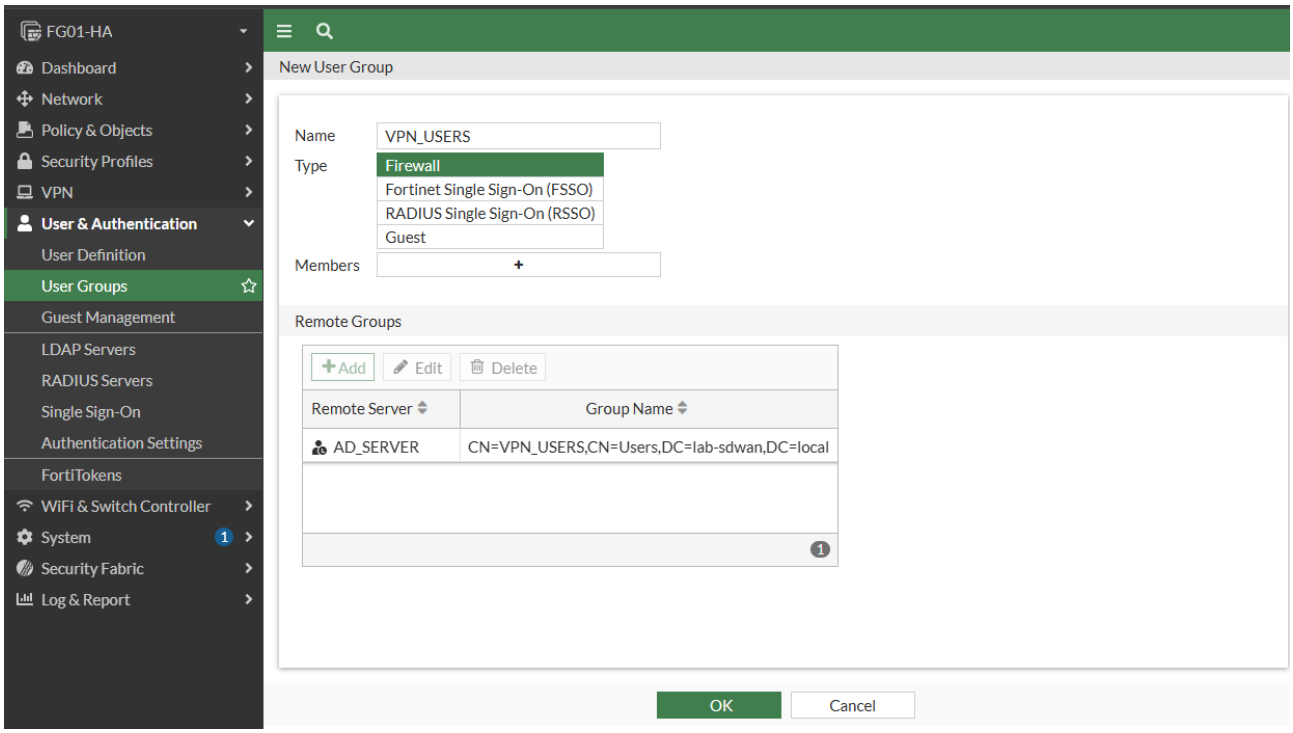


Рисунок 3.34 – Вказування необхідної групи Active Directory

Після цього можна редагувати необхідні SSL портали та виконати налаштування VPN. Коли віддалений клієнт підключається до Fortigate, він в свою чергу автентифікує користувача на основі імені користувача, пароля та домену автентифікації. Успішний вхід визначає права доступу віддалених користувачів відповідно до групи користувачів. Налаштування групи користувачів визначають, працюватиме з’єднання в режимі WEB-only або в режимі тунелю.

Режим WEB-only забезпечує віддаленим користувачам швидкий та ефективний спосіб доступу до серверних програм з будь-якого тонкого клієнтського комп'ютера, обладнаного веб-браузером.

У тунельному режимі віддалені клієнти підключаються до блоку FortiGate, який діє як захищений шлюз HTTP / HTTPS і автентифікує віддалених користувачів як членів групи користувачів.

Клієнт SSL VPN зашифровує весь трафік з віддаленого клієнтського комп'ютера та надсилає його до FortiGate через тунель SSL VPN

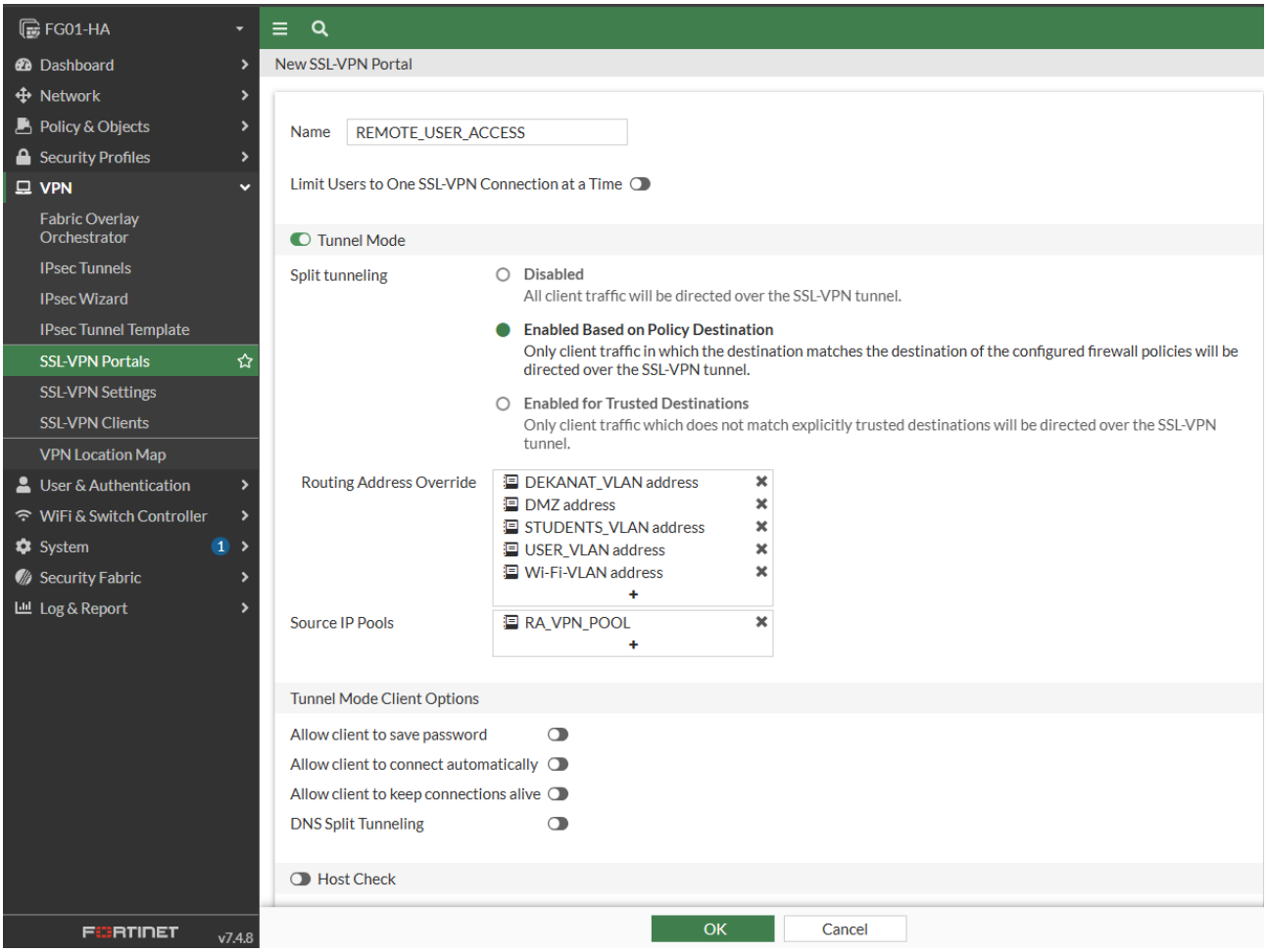


Рисунок 3.35 – Налаштування SSL-VPN порталу

Активовано Tunnel Mode, який забезпечує створення зашифрованого тунелю між клієнтом і шлюзом FortiGate. При цьому весь трафік або лише певна його частина може проходити через VPN. Параметр Split tunneling встановлено у режим Enabled Based on Policy Destination, що дозволяє передачу лише трафіку, який призначений для певних внутрішніх мереж, визначених політиками безпеки, та передаватись через тунель, тоді як інший трафік користувача (наприклад, доступ

до інтернету) проходитиме напряму. При моделюванні в тунель маршрутизуються лише локальні мережі факультету.

Поле Source IP Pools визначає пул адрес (RA_VPN_POOL), з якого користувачам видаватимуться IP-адреси при встановленні VPN-з'єднання. Даний інтерфейс реалізує безпечний простір віддаленого доступу, де чітко визначено, які ресурси факультету будуть доступні користувачам через VPN, а які залишатимуться поза тунелем.

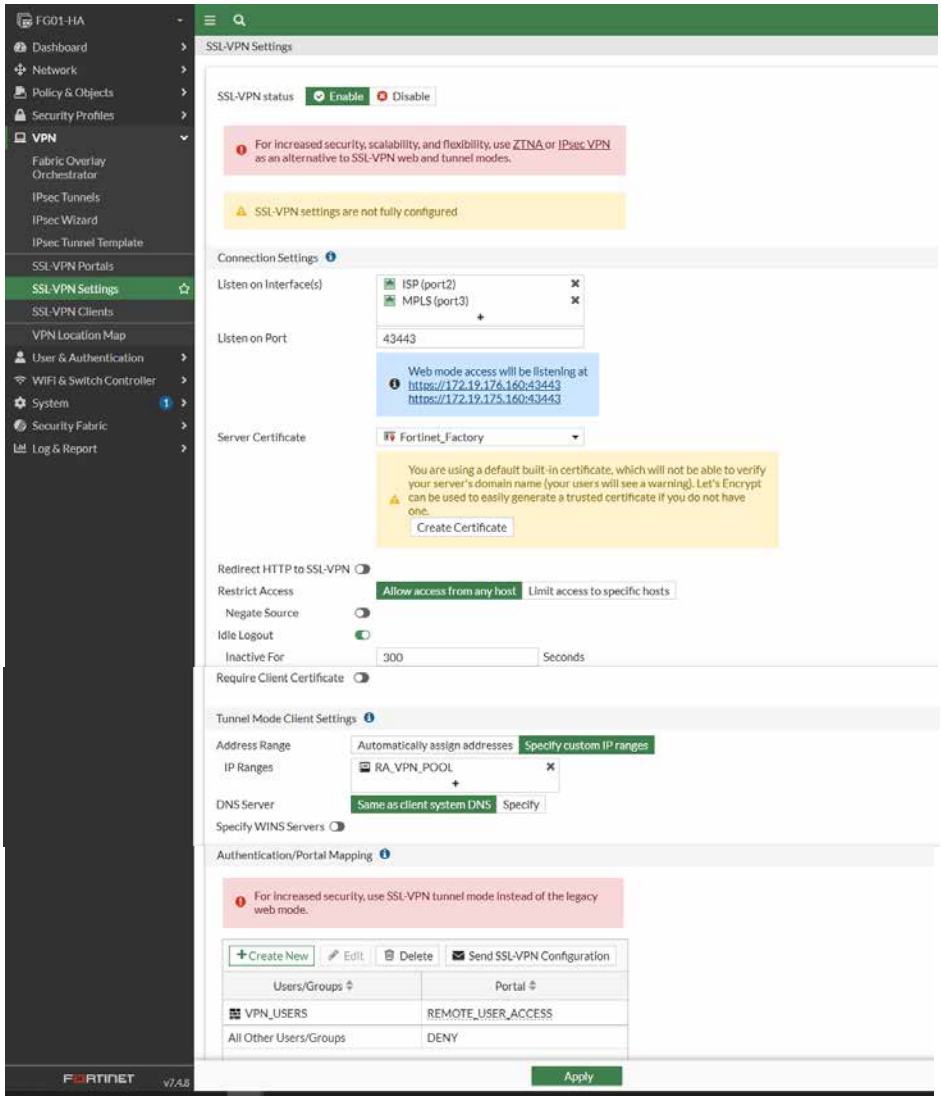


Рисунок 3.36 – Налаштування SSL-VPN

Після потрібно додати групи в політики IPv4, вона використовується для управління трафіком, що проходить через пристрій за допомогою протоколів IPv4. Для прикладу, нам потрібно, аби користувачі SSL-VPN змогли використовувати корпоративні ресурси факультету по протоколу RDP.

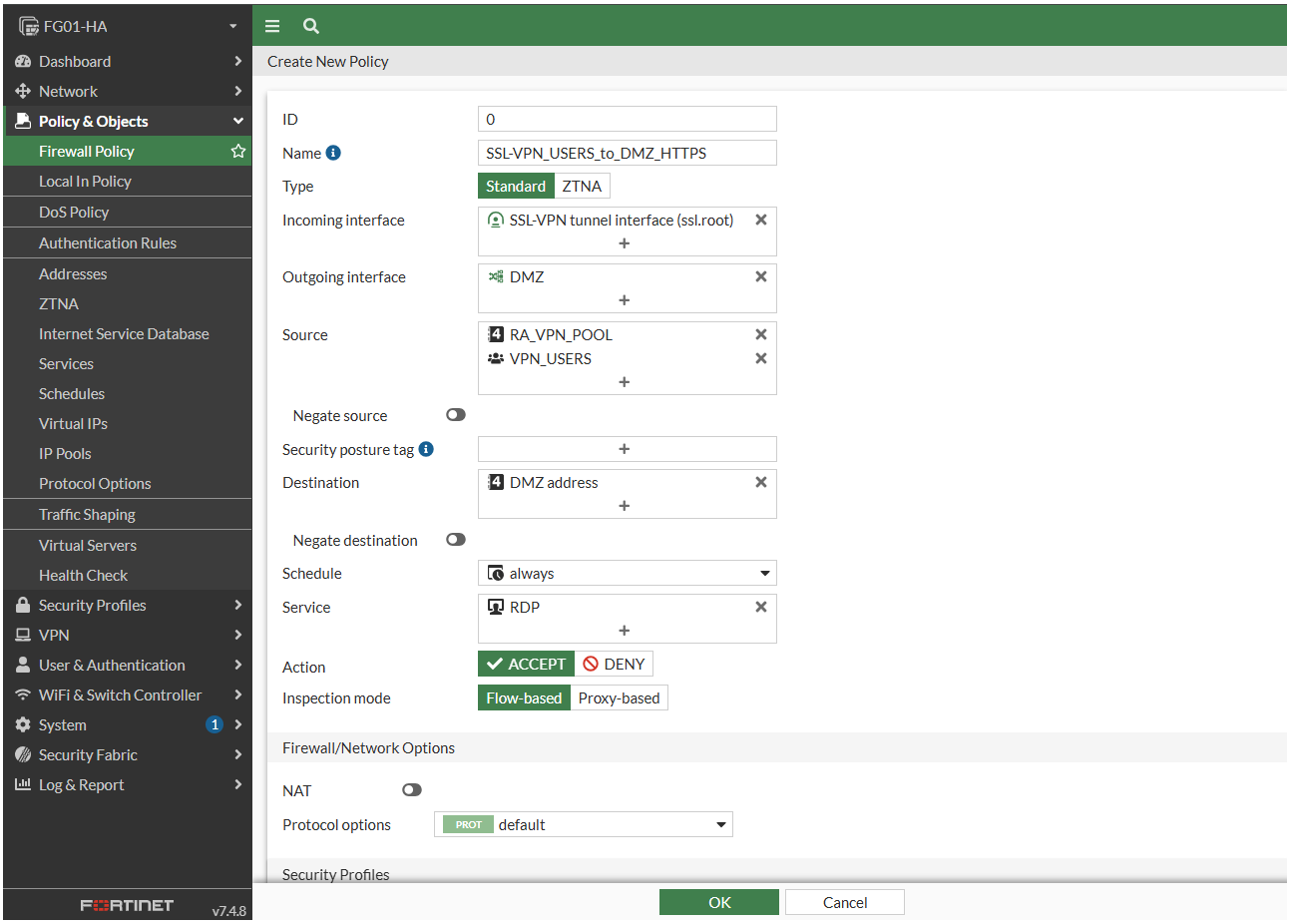


Рисунок 3.38 – Створенння політики IPv4 для трафіку SSL VPN

Для перевірки працездатності необхідно завантажити FortiClient, та спробувати підключитись до віддаленої локації. В налаштуваннях вказати публічні айпі адреси, за якими може виконуватись підключення, та номер порта.

При першій спробі підключення необхідно підтвердити, що сертифікат є довіреним, оскільки він не підписаний жодним публічним центром сертифікаціїї.

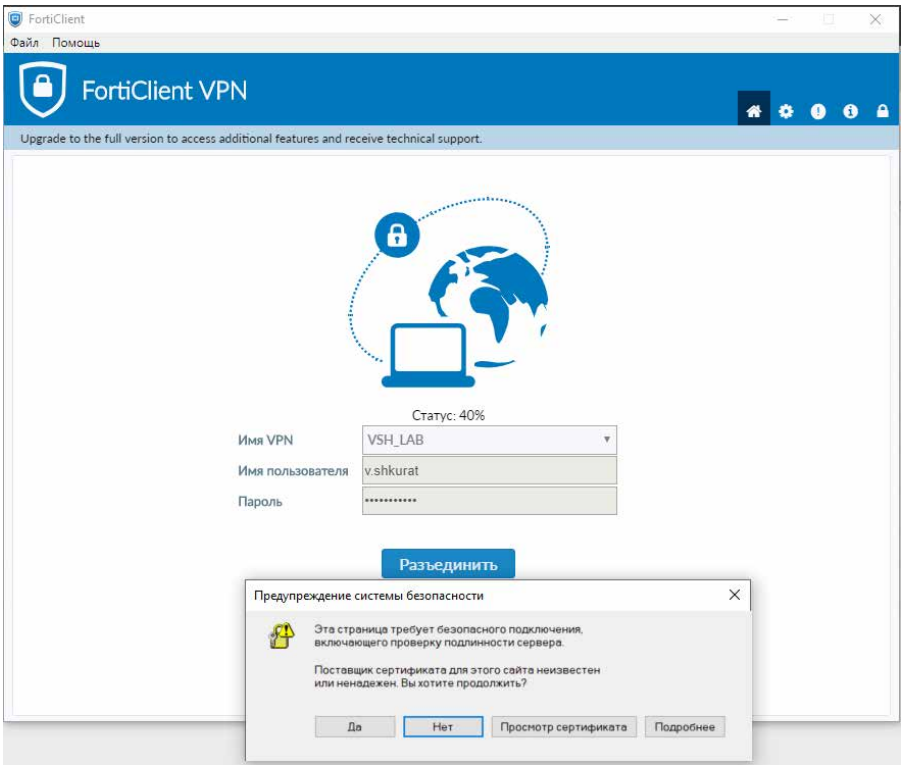


Рисунок 3.39 – Підтвердження недовіреного сертифікату

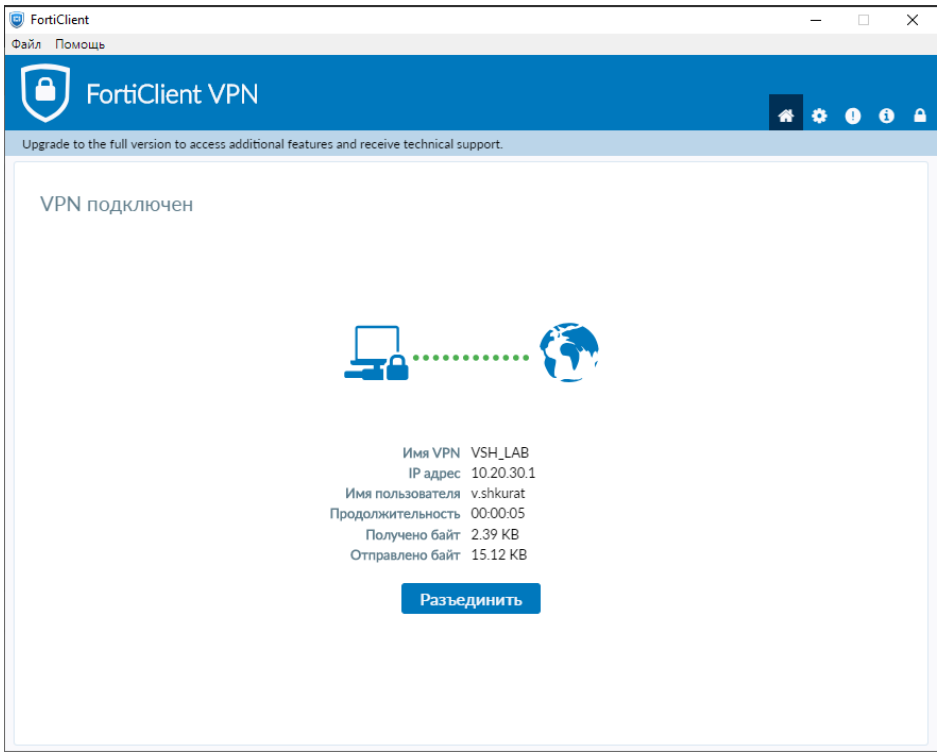


Рисунок 3.40 – Вдале підключення до віддаленої мережі

Під час підключення, у користувача має бути доступ до віддалених ресурсів відповідно до політик безпеки. Також пристрій, з якого підключений користувач, отримує маршрути, відповідно до конфігурації SSL VPN

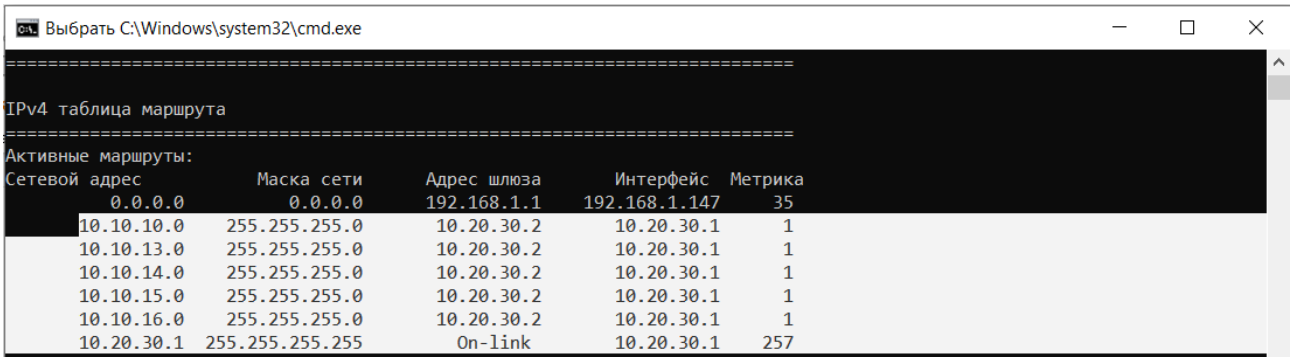


Рисунок 3.41 – Таблиця маршрутизації ПК під час підключення до SSL VPN

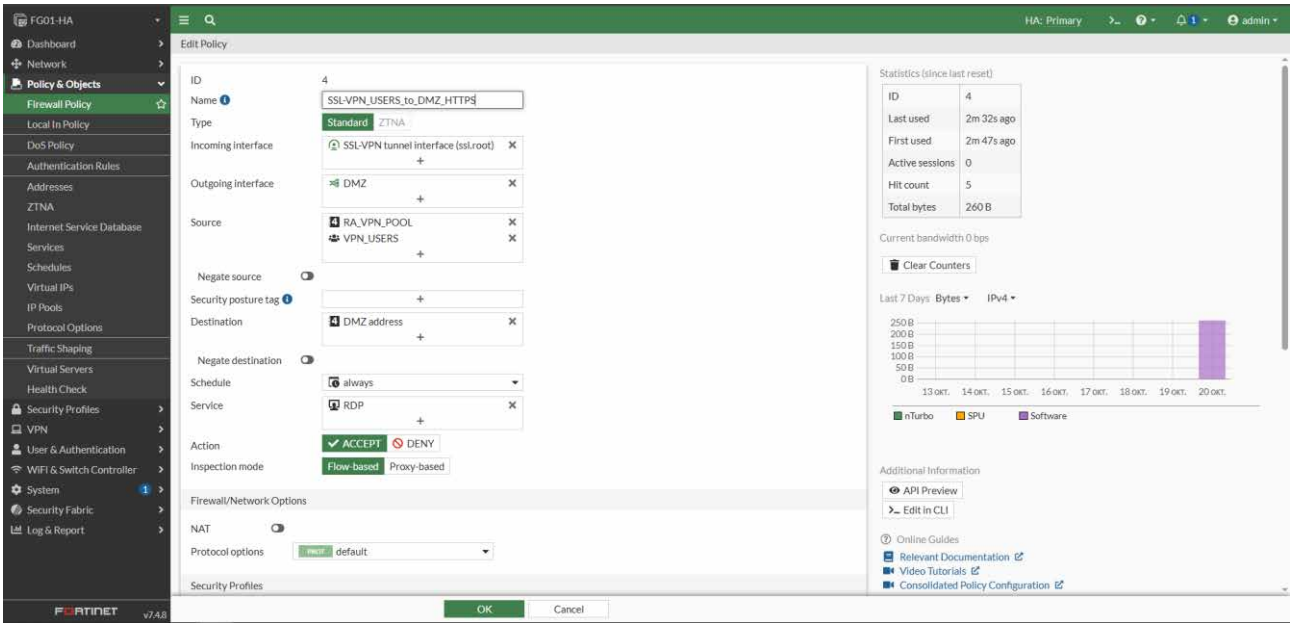


Рисунок 3.42 – Трафік, згенерований клієнтом SSL VPN

3.3.3 Налаштування FortiAnalyzer

FortiAnalyzer забезпечує централізований збір, зберігання та аналітику логів з усіх пристроїв мережі, наприклад міжмережевих екранів, комутаторів та інших елементів інфраструктури.

Основною метою впровадження FortiAnalyzer є моніторинг мережевих процесів, оперативне виявлення інцидентів безпеки та створення єдиної точки моніторингу. Завдяки інтеграції з FortiGate та іншими пристроями Fabric, адміністратор отримує зручний інтерфейс для контролю подій, аналізу трафіку та формування звітів, що спрощує управління безпекою мережі факультету.[17]

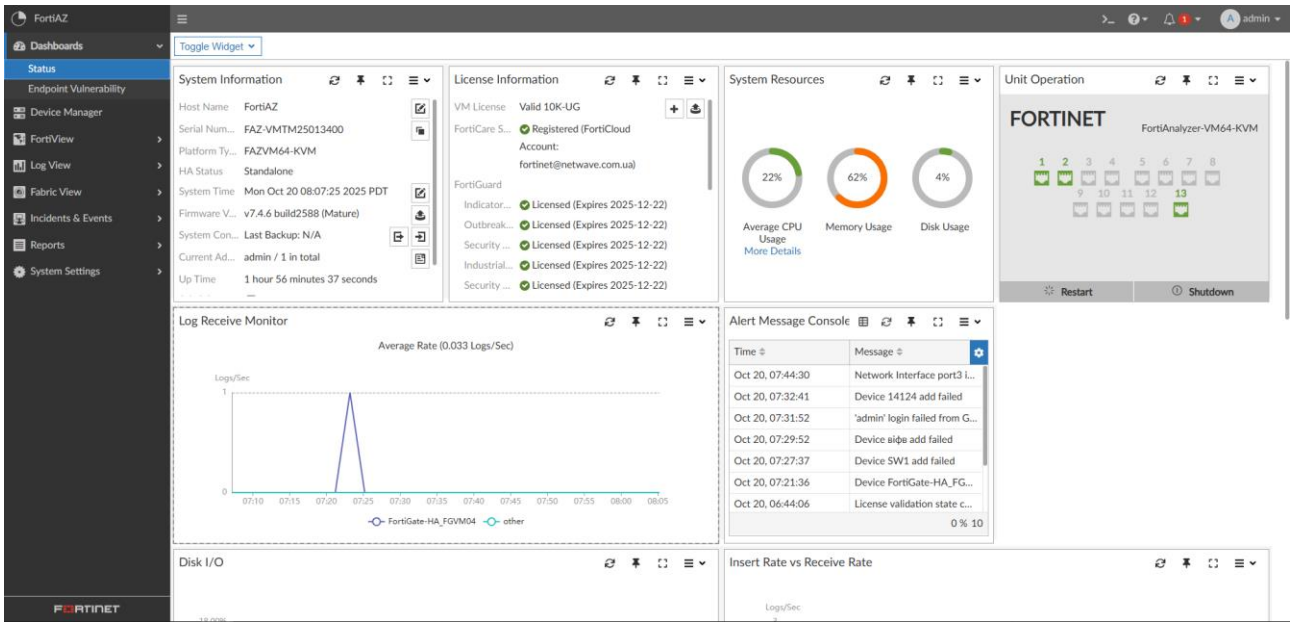


Рисунок 3.43 – Головна сторінка FortiAnalyzer

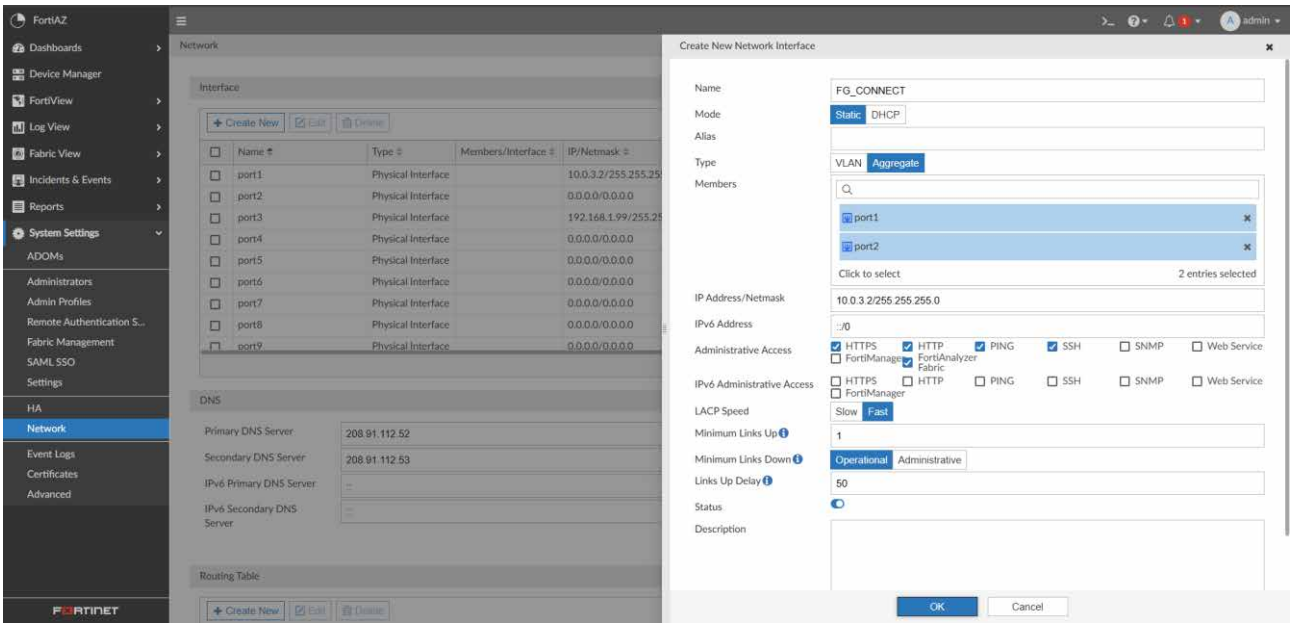


Рисунок 3.44 – Налаштування інтерфейсу для підключення до FortiGate

На FortiGate необхідно налаштувати підключення до FortiAnalyzer в підменю «Fabric Connectors»

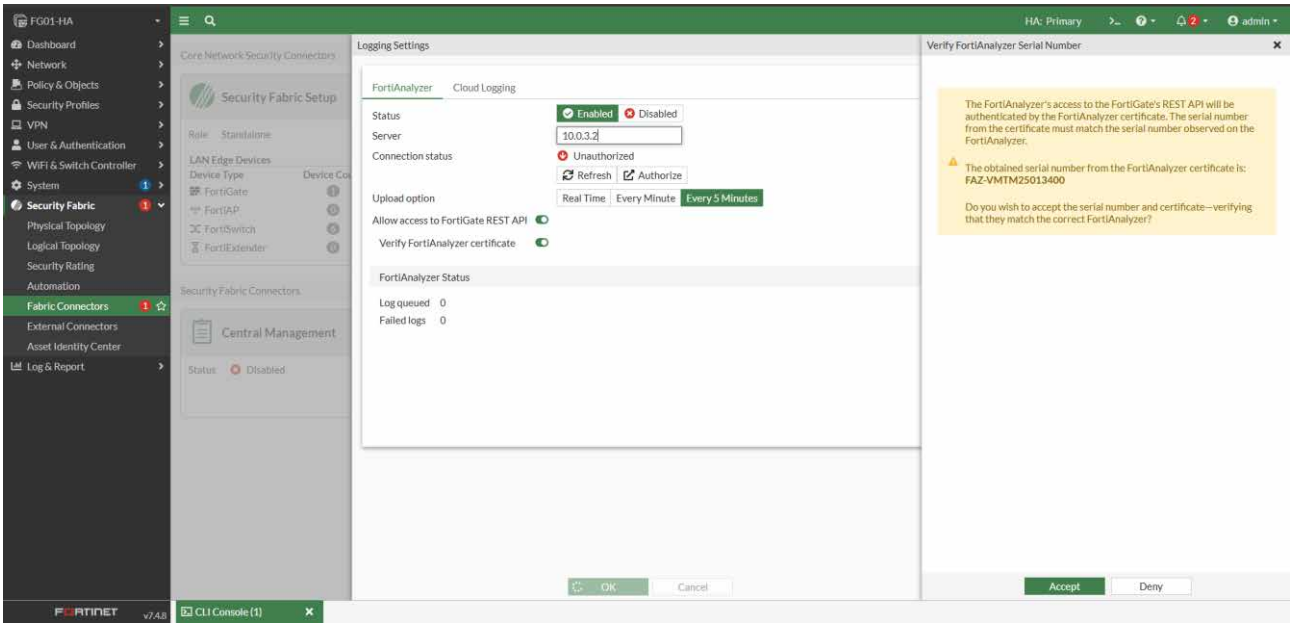


Рисунок 3.45 – Підключення FortiAnalyzer на FortiGate

Після підключення FortiAnalyzer, необхідно провести авторизацію FortiGate з боку FortiAnalyzer.

Рисунок 3.46 – Авторизація FortiGate на FortiAnalyzer

Після цього, підключення з боку FortiGate та FortiAnalyzer успішне, логи з системи успішно транслюються на FortiAnalyzer.

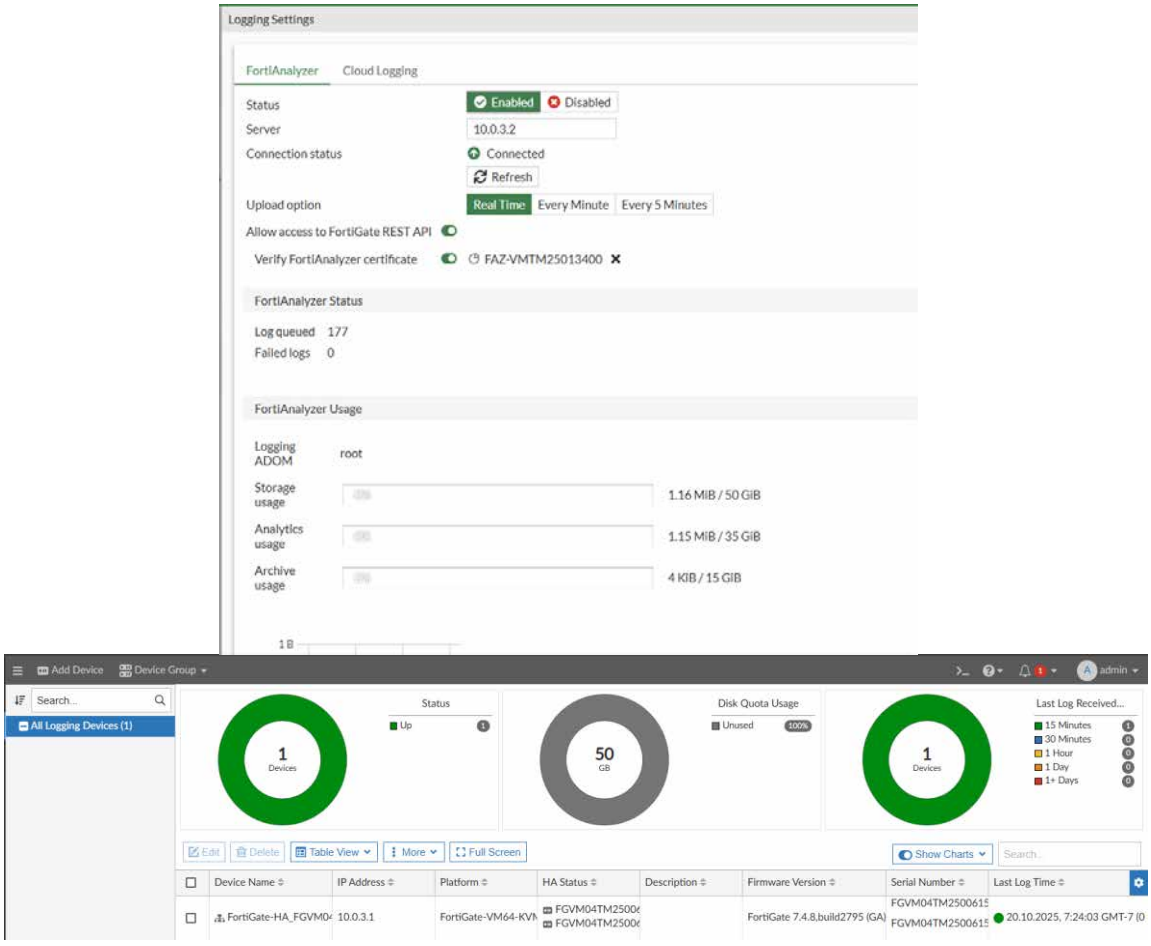


Рисунок 3.47 – Успішне підключення FortiGate та FortiAnalyzer

Подібним способом можна підключати всі пристрої сімейства Fortinet, та мати централізовану систему збереження інформації про пристрої. Нажаль, за обмежень лабораторних умов, vFortiSwitch неможливо додати до FortiAnalyzer.[18]

Після підключення пристрою FortiGate до FortiAnalyzer адміністратор отримує можливість централізовано збирати, зберігати та аналізувати журнали подій від усіх елементів мережевої інфраструктури. Такий підхід забезпечує повну видимість мережевих процесів, дозволяє швидко виявляти інциденти безпеки та аналізувати їхні причини. FortiAnalyzer автоматично класифікує події, створює статистичні звіти та надає інструменти для глибокого аудиту трафіку. Це значно підвищує ефективність адміністрування мережі, спрощує моніторинг і сприяє оперативному реагуванню на потенційні загрози.

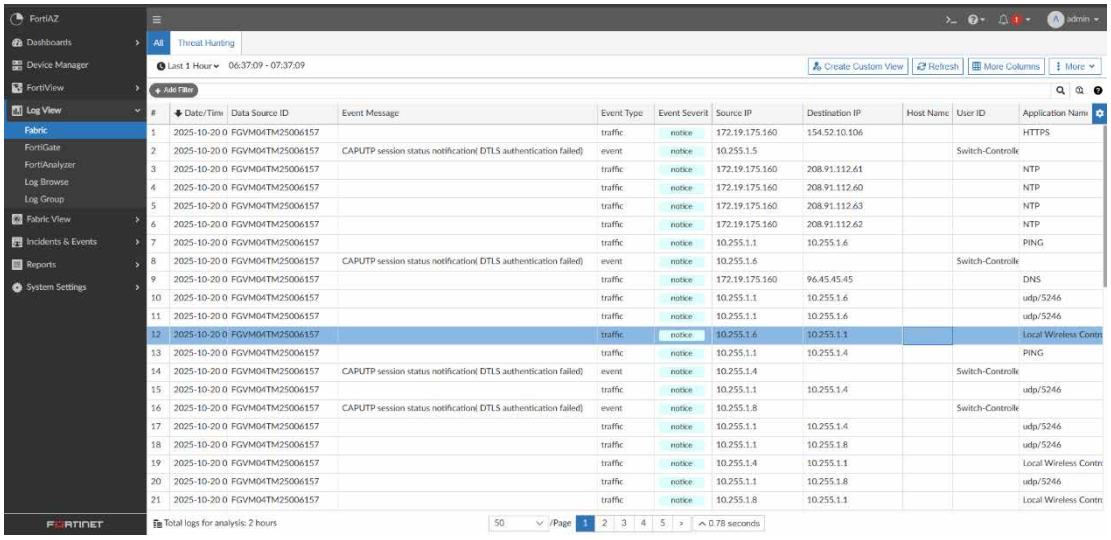


Рисунок 3.48 – Централізований збір логів з всіх пристроїв

Також надається можливість представлення Log View, де у режимі реального часу відображаються події, пов’язані з трафіком: інформація про джерело, призначення, тип сервісу, обсяг переданих даних і дії, виконані політиками безпеки. Такий підхід дозволяє швидко виявляти порушення, оцінювати ефективність політик безпеки та отримувати повну аналітику стану мережі.

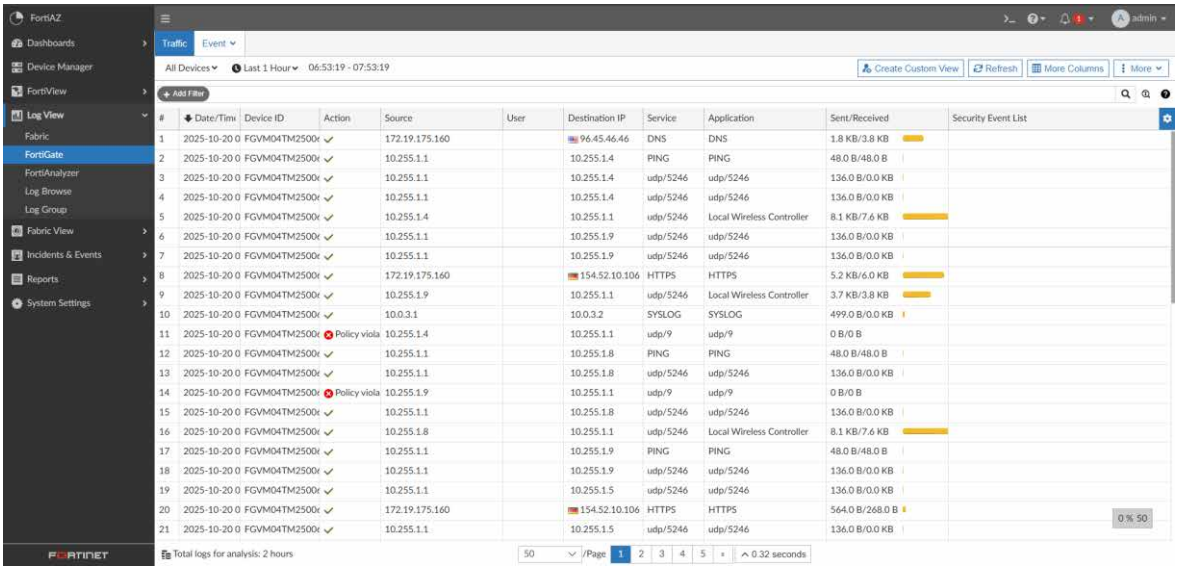


Рисунок 3.49 – Логи мережевої активності FortiGate

У вікні FortiView «Traffic» відображається зведена інформація про джерела трафіку, кількість сесій, обсяг переданих даних і рівень загроз. Інструмент дозволяє швидко оцінити активність у мережі, виявити потенційно небезпечні або надмірно активні вузли, а також провести глибший аналіз поведінки пристроїв і користувачів.

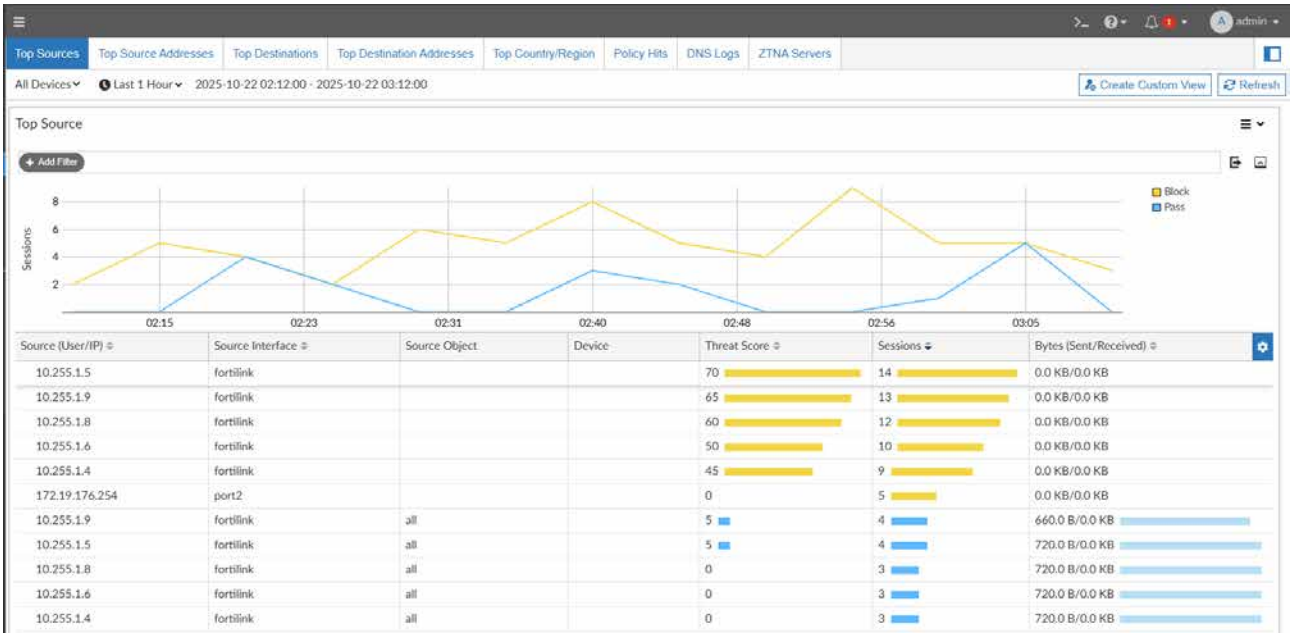


Рисунок 3.50 – Кількість трафіку в мережі

Вікно FortiView «VPN» використовується для перегляду активних VPN-підключень. Тут відображаються користувачі, тип тунелю, тривалість сеансу, обсяг переданих даних і місце підключення. Такий інтерфейс дозволяє швидко оцінити стан VPN-з'єднань, виявити проблеми з доступом або перевантаженням, а також відстежити підозрілу активність у мережі.

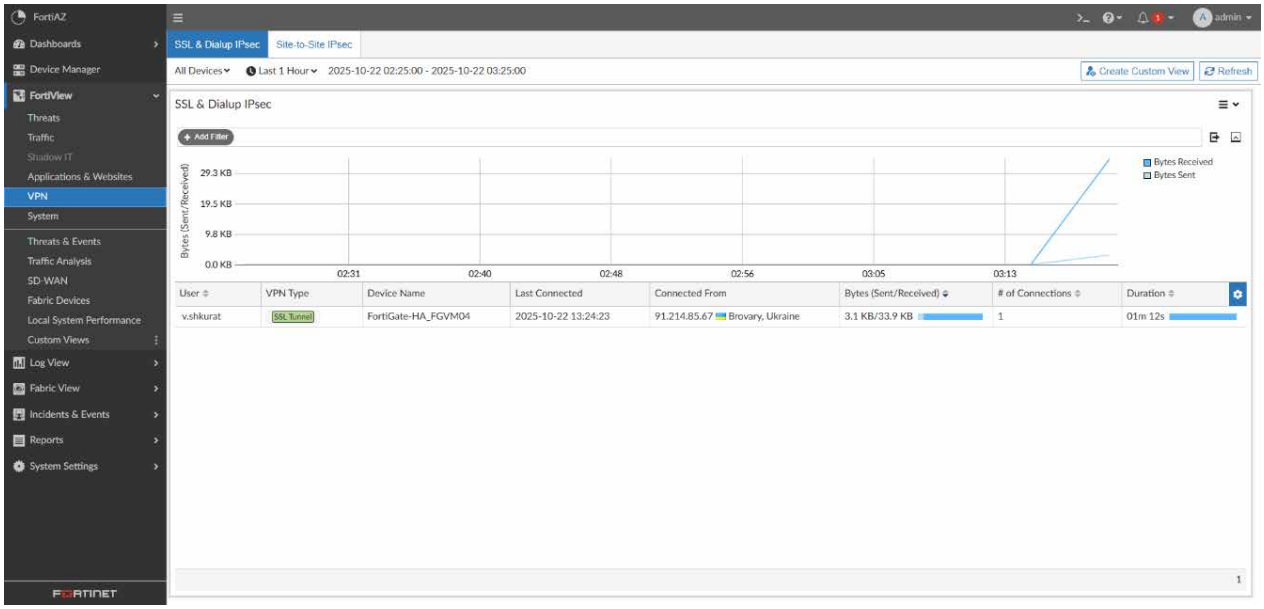


Рисунок 3.51 – Сесії VPN користувачів

Вікно FortiView «System» відображає загальну інформацію про використання ресурсів пристроїв FortiGate у системі FortiAnalyzer. У ньому можна побачити середні та пікові показники навантаження, наприклад, використання процесора, пам'яті, диску, трафік і кількість активних сесій. Це допомагає оцінити стан пристроїв і зрозуміти, чи є перевантаження або відхилення від норми.

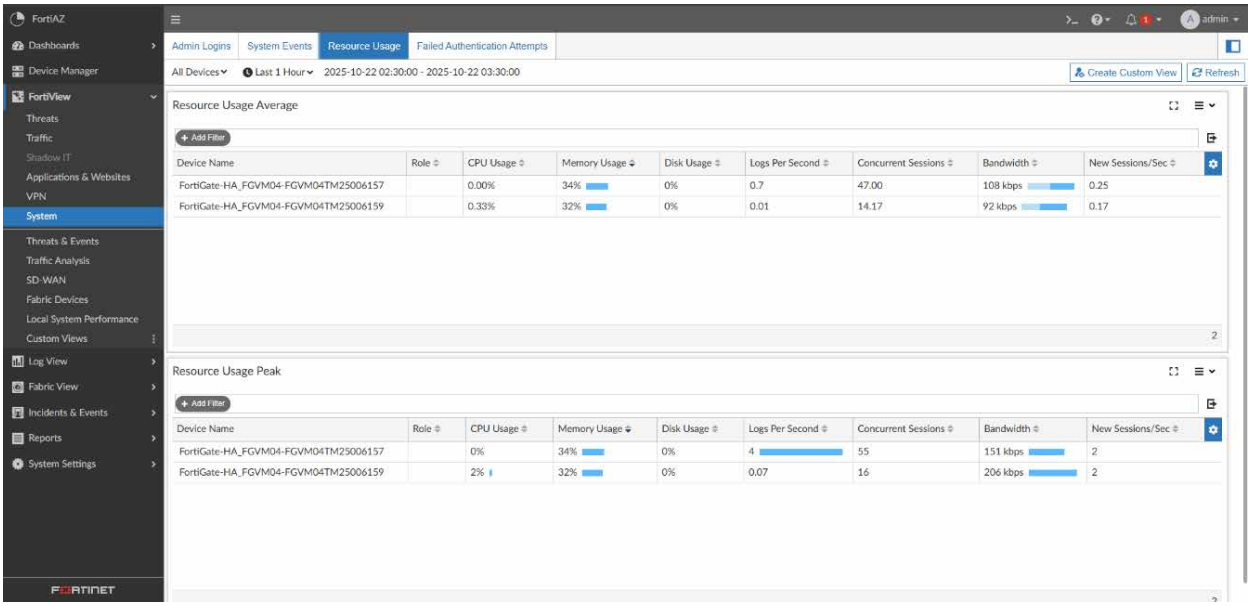


Рисунок 3.52 – Системні параметри підключених пристроїв

Вікно FortiView «Traffic Analysis» використовується для аналізу мережевого трафіку. Воно показує основні джерела, напрямки, країни походження з’єднань та політики, за якими проходив трафік. Такий огляд дозволяє швидко оцінити активність у мережі, виявити найактивніших користувачів або напрямки обміну даними.

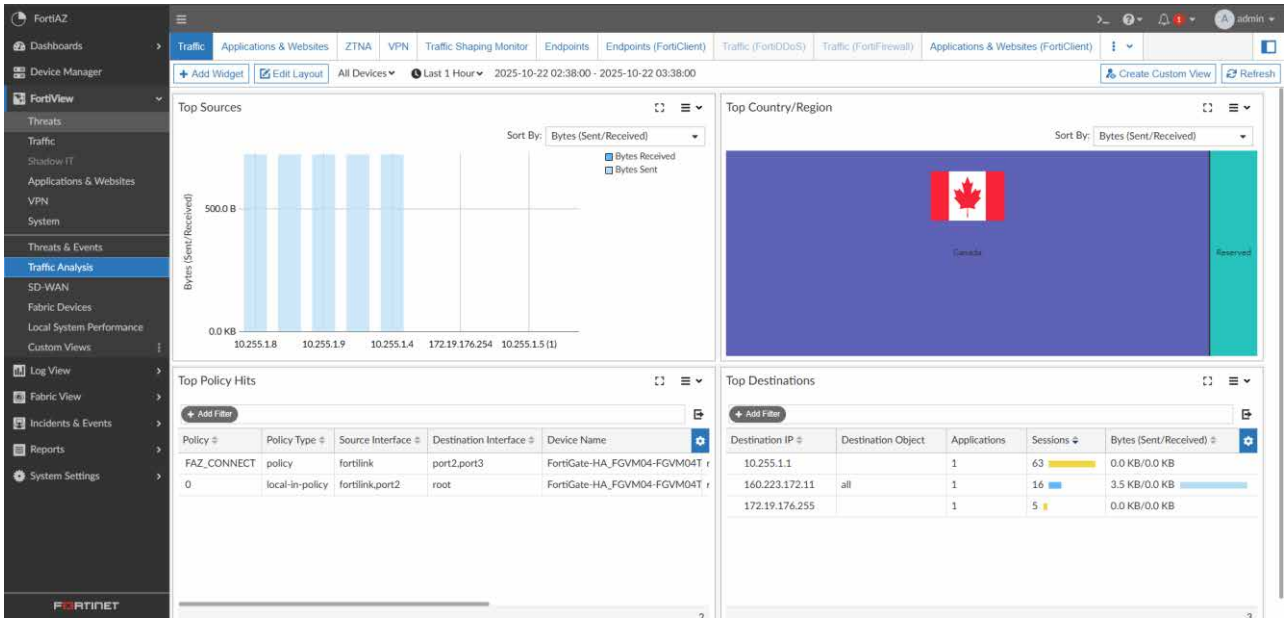


Рисунок 3.53 – Аналітика трафіку в мережі

Крім централізованого збору та аналізу логів, FortiAnalyzer надає широкі можливості для створення детальних звітів про стан мережевої безпеки. Система дозволяє формувати як стандартні, так і користувацькі звіти, що охоплюють інформацію про трафік, спрацювання політик, активність користувачів, виявлені загрози та продуктивність обладнання. Звіти можуть автоматично генеруватись за розкладом або створюватись вручну для конкретного періоду часу, що спрощує аудит і контроль роботи мережі. Завдяки цьому адміністратор отримує не лише поточну картину подій, а й історичний аналіз тенденцій безпеки, що сприяє підвищенню ефективності управління інфраструктурою.[19]

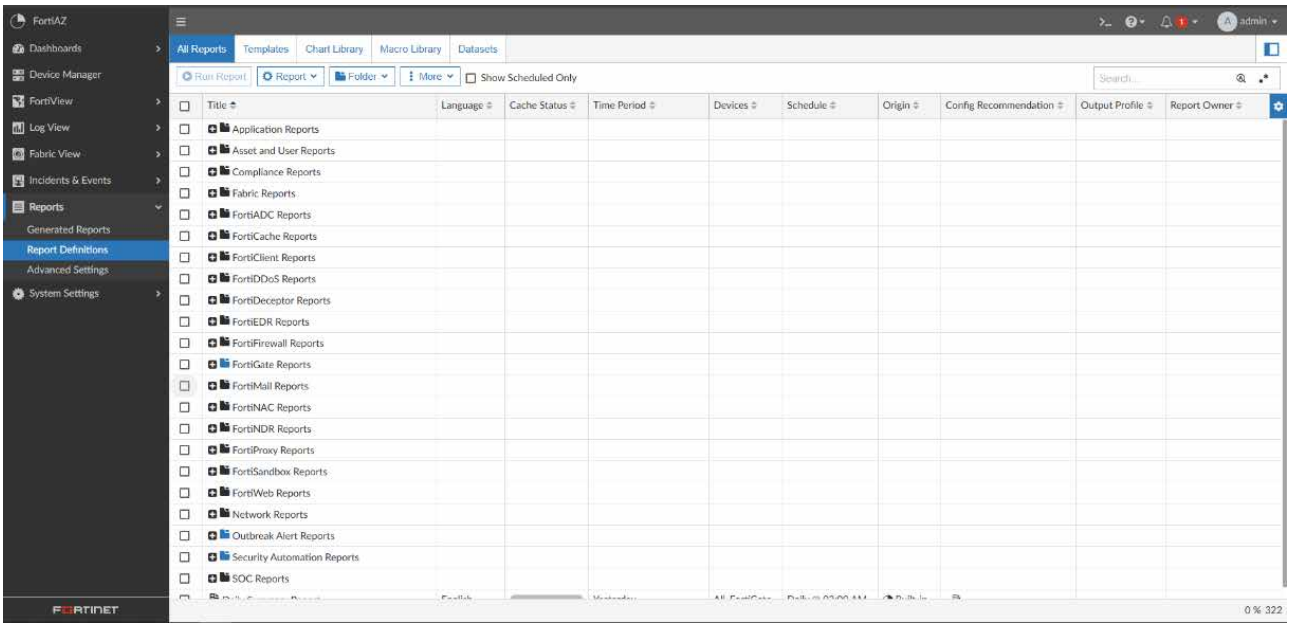


Рисунок 3.54 – Шаблони звітності FortiAnalyzer

Висновок до третього розділу

У цьому розділі було виконано повний цикл проєктування та моделювання мережевої інфраструктури факультету. На основі попереднього аналізу вимог було сформовано концепцію побудови мережі, що враховує потреби в безпеці, надійності, гнучкому управлінні ресурсами та можливості подальшого розширення.

Для реалізації поставлених завдань використано середовище EVE-NG, яке дозволило створити детальну симуляційну модель мережі. Було проведено розгортання необхідних образів мережевого обладнання та налаштовано ключові компоненти інфраструктури. Здійснено конфігурацію демаркаційних комутаторів, міжмережевого екрану FortiGate, керованих комутаторів FortiSwitch, служби каталогів Active Directory, а також системи централізованого моніторингу та аналізу FortiAnalyzer.

У процесі роботи перевірено взаємодію між пристроями, функціонування основних сервісів, обробку політик безпеки та збір статистики трафіку. Отримані результати підтвердили коректність налаштувань і відповідність моделі поставленим технічним вимогам.

Запропонована модель демонструє можливість побудови єдиної керованої мережевої системи з централізованим контролем трафіку, політик доступу та подій безпеки. Вона може бути використана для навчальних цілей, тестування нових рішень, а також як основа для впровадження сучасних підходів до автоматизації та віртуалізації мережевої інфраструктури факультету.

ВИСНОВКИ

У процесі виконання роботи було проведено всебічне дослідження мережевої інфраструктури факультету. На основі аналізу існуючої топології та принципів її функціонування визначено основні недоліки поточного стану мережі, серед яких відсутність чіткої сегментації трафіку, використання застарілого обладнання, недостатній рівень інформаційної безпеки та складність централізованого керування мережевими ресурсами. Такі проблеми знижують ефективність роботи локальної мережі, ускладнюють адміністрування та створюють потенційні ризики для стабільності функціонування сервісів факультету.

Пошук оптимального підходу до модернізації показав, що ефективність сучасних мереж визначається не лише швидкістю передавання даних, а й рівнем взаємодії між компонентами безпеки, автоматизацією керування та здатністю системи швидко реагувати на загрози. Саме тому було описано доцільність впровадження архітектури Fortinet Security Fabric, яка забезпечує інтеграцію всіх пристроїв у єдину керовану екосистему. Її перевагами виявилися глибока взаємодія між елементами захисту, централізоване адміністрування через FortiAnalyzer, автоматичне виявлення пристроїв і застосування політик безпеки, а також можливість подальшого масштабування без зміни базової структури мережі.

Побудована модель у середовищі EVE-NG підтвердила практичну ефективність цього підходу. Взаємодія між FortiGate, FortiSwitch та FortiAnalyzer продемонструвала стабільність роботи системи, зручність централізованого моніторингу та чітке розмежування трафіку. Внаслідок цього мережа стала більш захищеною, керованою та гнучкою до змін у майбутньому.

Модернізація інфраструктури факультету на основі Fortinet Security Fabric дозволяє створити сучасне, надійне та безпечне середовище, яке відповідає поточним вимогам до навчальних і адміністративних процесів. Впровадження такої архітектури не лише підвищує продуктивність і стабільність мережі, а й формує основу для подальшого розвитку цифрової інфраструктури факультету.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Розуміння основ мережевої інфраструктури [Електронний ресурс]. – 2024 – Режим доступу: https://www.qtiancom.com/uk/blog/understanding-the-basics-of-network-infrastructure9 – Дата звернення: 12.09.2025

2 Ed Harmoush. Virtual Local Area Networks (VLANs) [Електронний ресурс]. – Practical Networking. – Режим доступу: https://www.practicalnetworking.net/stand-alone/vlans/ – Дата звернення: 12.09.2025.

3 Ковальчук А. О. Розробка та дослідження методів маршрутизації в корпоративних мережах [Електронний ресурс]. – 2023. – Режим доступу: https://ela.kpi.ua/bitstreams/ec37c294-636e-4bd4-bbb7-280a8a899404/download – Дата звернення: 12.09.2025.

4 IMC. Рішення для корпоративних мереж: надійність, ефективність, безпека [Електронний ресурс]. – Режим доступу: https://imc.ua/services/corporate-network – Дата звернення: 13.09.2025.

5 GeeksforGeeks. Three-Layer Hierarchical Model in Cisco [Електронний ресурс]. – 2024. – Режим доступу: https://www.geeksforgeeks.org/three-layer-hierarchical-model-in-cisco/ – Дата звернення: 14.09.2025.

6 Cisco. Cisco SD-Access Solution Overview: Segmentation [Електронний ресурс]. – Solution Overview. – 2023. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/solution-overview-c22-739012.html – Дата звернення: 14.09.2025.

7 FORTISERVICE. Fortinet Security Fabric на практиці. Частина 1. Загальний огляд [Електронний ресурс]. – Стаття. – 2020. – Режим доступу: https://habr.com/ru/companies/fortiservice/articles/526604/ – Дата звернення: 21.09.2025.

8 Fortinet Inc. Fortinet Security Fabric Enables Digital Innovation [Електронний ресурс]. – White Paper. – 2019. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-security-fabric.pdf – Дата звернення: 21.09.2025.

9 LRQA. Network design and configuration - 6 key factors [Електронний ресурс]. – Стаття. – 2024. – Режим доступу: https://www.lrqa.com/en/insights/articles/network-design-and-configuration-6-key-factors/ – Дата звернення: 22.09.2025.

10 EVE-NG. EVE-NG [Електронний ресурс]. – Офіційний сайт. – 2025. – Режим доступу: https://www.eve-ng.net/ – Дата звернення: 22.09.2025

11 Network Hunt. How to add cisco IOU/IOL to EVE-NG [Електронний ресурс]. – Стаття. – 2022. – Режим доступу: https://networkhunt.com/how-to-add-cisco-iou-iol-to-eve-ng/ – Дата звернення: 22.09.2025

12 Fortinet. FortiOS Handbook - High Availability [Електронний ресурс]. – Handbook. – 2019. – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8e55781b-1a1c-11e9-9685-f8bc1258b856/FortiOS-5.6-High_Availability.pdf – Дата звернення: 22.09.2025.

13 Fortinet. FortiSwitch-FortiLink Guide [Електронний ресурс]. – 2024. – Режим доступу: https://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/173260/configuring-fortilink – Дата звернення: 23.09.2025.

14 VPN Wired. SSL VPN Explained: Working, Benefits, Types, and Security [Електронний ресурс]. – Стаття. – 2023. – Режим доступу: https://vpnwired.com/ssl-vpn/ – Дата звернення: 22.09.2025.

15 Вікіпедія. Lightweight Directory Access Protocol [Електронний ресурс]. – Енциклопедична стаття. – 2024. – Режим доступу: https://uk.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol – Дата звернення: 25.09.2025.

16 Microsoft. Install Active Directory Domain Services (Level 100) [Електронний ресурс]. – Документація. – 2023. – Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100- – Дата звернення: 26.09.2025.

17 Fortinet Inc. FortiAnalyzer [Електронний ресурс]. – Data Sheet. – 2024. – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf – Дата звернення: 10.10.2025.

18 Fortinet. FortiAnalyzer Administration Guide [Електронний ресурс]. – Administration Guide. – 2024. – Режим доступу: https://docs.fortinet.com/document/fortianalyzer/7.4.4/administration-guide/997210/authorizing-devices – Дата звернення: 10.10.2025.

19 Network Interview. FortiAnalyzer: The Complete Guide [Електронний ресурс]. – Технічний огляд. – 2024. – Режим доступу: https://networkinterview.com/fortianalyzer/ – Дата звернення: 15.10.2025.

20 Reddit. Your Pros/Cons with Fortinet [Електронний ресурс]. – Обговорення. – 2024. – Режим доступу: https://www.reddit.com/r/fortinet/comments/1bnjllk/your_proscons_with_fortinet/ – Дата звернення: 22.10.2025.

ДОДАТОК А – ПОСТЕР

Міністерство освіти і науки України
Національний університет біоресурсів та природокористування України

Дослідження мережевої інфраструктури факультету

Виконавець: Шкурат Владислав Ігорович, комп'ютерні системи і мережі, КСІМ-24006м
Науковий керівник: Коваленко Олексій Єпіфанович, доктор технічних наук, професор

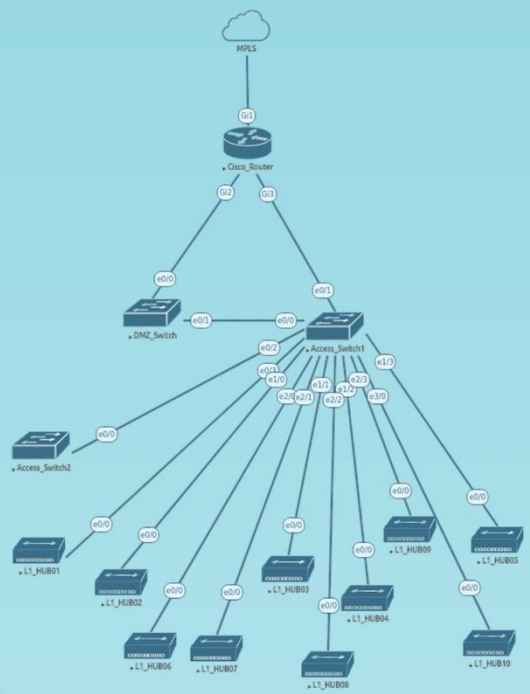
Анотація роботи

Мета – дослідити поточну мережеву інфраструктуру факультету та розробити оновлену мережу, з урахуванням сучасних вимог.
Об'єкт – комп'ютерна мережа навчального закладу.
Предмет – принципи та методи реалізації мережевої інфраструктури факультету

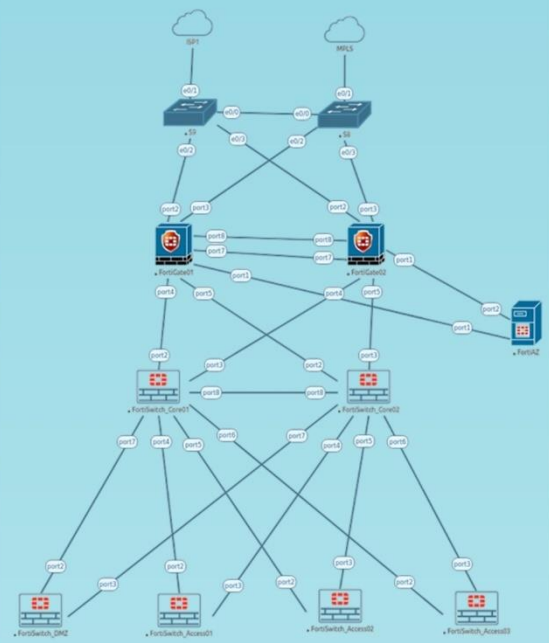
Характеристика роботи

В роботі проведено аналіз, модернізація та моделюванню мережевої інфраструктури факультету. Розглянуто теоретичні основи побудови локальних мереж, проведено аналіз існуючої інфраструктури та визначено її недоліки. На основі отриманих результатів обгрунтовано вибір архітектурного рішення й виконано моделювання оновленої мережі з використанням сучасних технологій та засобів віртуалізації.

Структурна схема мережі факультету



Мережа з урахуванням сучасних вимог на базі FortiGate Fabric

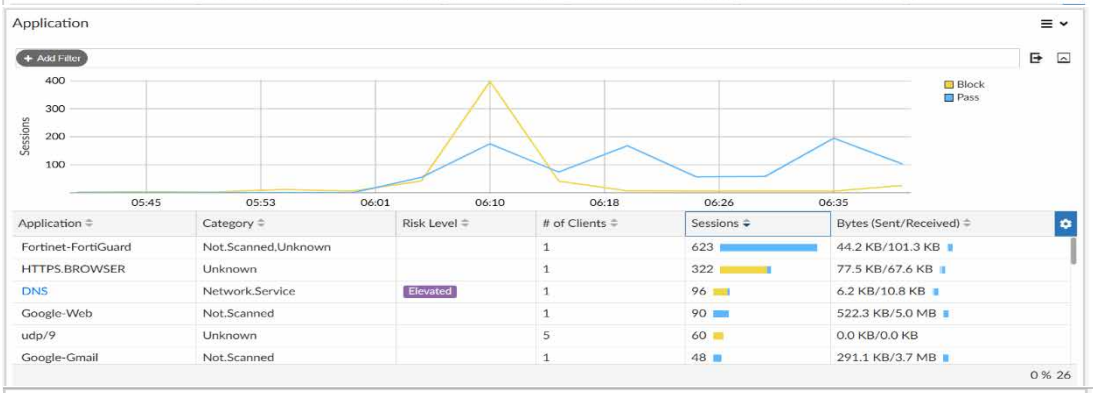


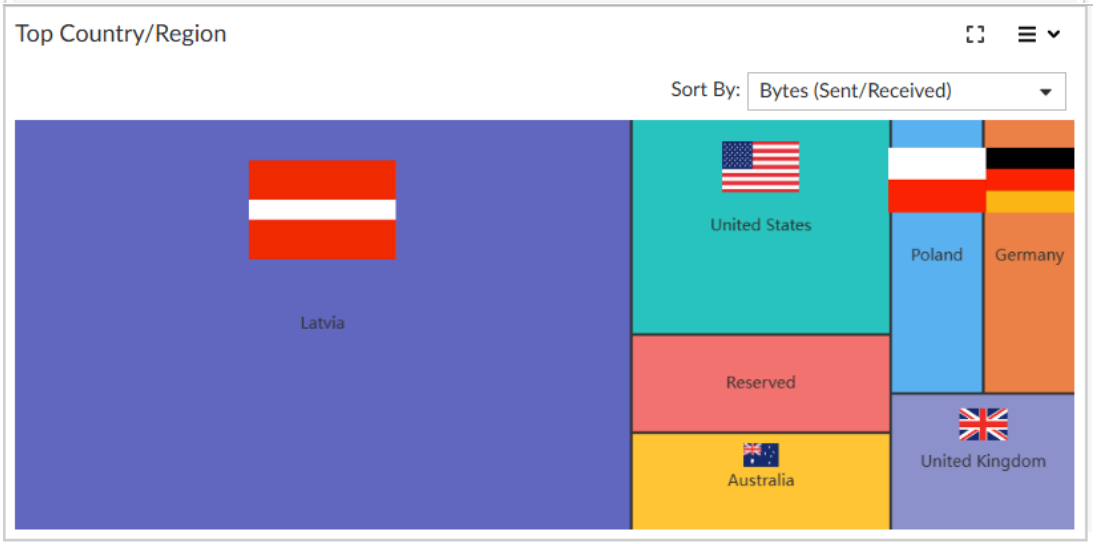
Висновки

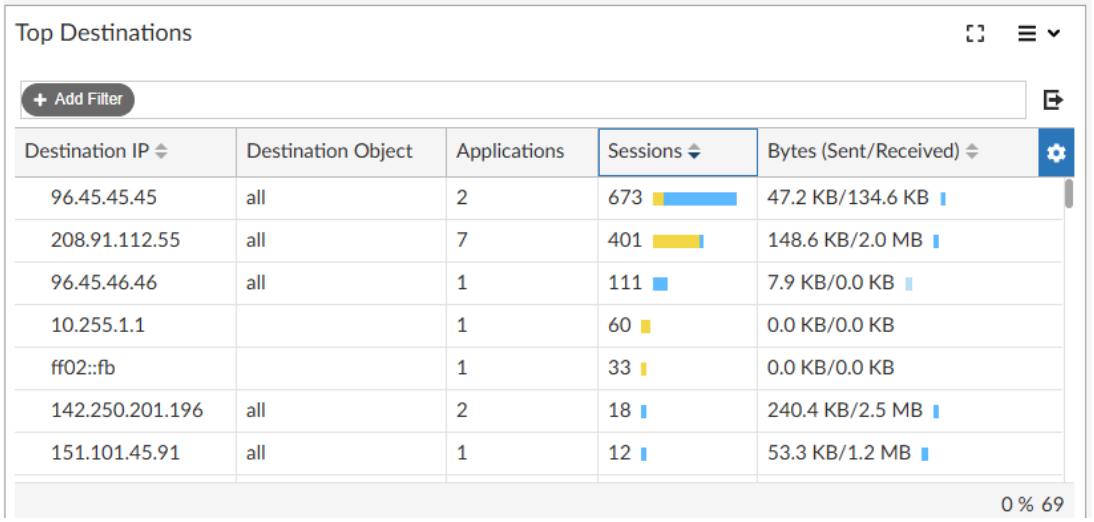
У ході роботи було проведено аналіз поточної мережевої інфраструктури факультету та виявлено її основні недоліки: відсутність резервування, низький рівень безпеки, обмежені можливості адміністрування, застаріле обладнання, високий рівень навантаження. На основі сучасних підходів і технологій було обгрунтовано вибір оптимальної архітектури для її модернізації. Розроблена мережа забезпечує підвищений рівень безпеки, масштабованості та надійності. Запропоновані рішення спрямовані на створення стабільного та ефективного мережевого середовища факультету.

ДОДАТОК Б – МАГІЧНИЙ КВАДРАТ РЕЙТИНГУ ENTERPRISE РІШЕНЬ

ДОДАТОК В – РЕЗУЛЬТАТ РОБОТИ МЕРЕЖІ. ФІЛЬТРОВАНИЙ ТРАФІК







ДОДАТОК Д – КОНФІГУРАЦІЙНИЙ ФАЙЛ МІЖМЕРЕЖЕВИХ ЕКРАНІВ FORTIGATE-VM

```
#config-version=FGVMK6-7.4.8-FW-build2795-250523:opmode=0:vdom=0:user=admin
#conf_file_ver=268173463054521
#buildno=2795
#global_vdom=1
config system global
    set admintimeout 480
    set alias "FGVM04TM25006157"
    set gui-auto-upgrade-setup-warning disable
    set gui-local-out enable
    set hostname "FG01-HA"
    set log-uuid-address enable
    set sslvpn-web-mode enable
    set switch-controller enable
    set timezone "Europe/Kyiv"
end
:
:
config system interface
    edit "port1"
        set vdom "root"
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 172.19.176.160 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "ISP"
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 172.19.175.160 255.255.255.0
        set allowaccess ping https ssh http
        set type physical
        set alias "MPLS"
        set snmp-index 3
    next
    :
    :
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set switch-controller-source-ip fixed
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "port4" "port5"
        set lldp-reception enable
        set lldp-transmission enable
        set snmp-index 12
        set auto-auth-extension-device enable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set switch-controller-iot-scanning enable
        set swc-first-create 255
    next
    :
    :
    edit "USER_VLAN"
        set vdom "root"
        set ip 10.10.10.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 20
        set ip-managed-by-fortiipam disable
```

```
        set interface "fortilink"
        set vlanid 10
    next
    edit "GUEST_VLAN"
        set vdom "root"
        set ip 10.10.11.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 21
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 20
    next
    edit "Wi-Fi-VLAN"
        set vdom "root"
        set ip 10.10.13.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 22
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 30
    next
    edit "STUDENTS_VLAN"
        set vdom "root"
        set ip 10.10.14.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 23
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 40
    next
    edit "DEKANAT_VLAN"
        set vdom "root"
        set ip 10.10.15.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 24
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 50
    next
    edit "DMZ"
        set vdom "root"
        set ip 10.10.16.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 25
        set ip-managed-by-fortiipam disable
        set interface "fortilink"
        set vlanid 60
    next
    edit "FAZ_CONNECT"
        set vdom "root"
        set ip 10.0.3.1 255.255.255.0
        set allowaccess ping https http
        set type redundant
        set member "port1"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 26
        set ip-managed-by-fortiipam disable
    next
end
config system ha
    set group-name "FortiGate-HA"
    set mode a-p
    set password ENC
oBA70PaiWOvgceXGm0cYcbn1rL5nAqRM2B1rB9JDg6R9JCwnepVaY4ep9BZ7KnKiA2aeRY62Nd22EPzu3NsXSvvYepQ
0xdDU/wDgfjBFzW/AUwhdkvLAOFljhA06SoZ9MljwOqZeB/cyJmjxDOXL6jlVOs1ny5pcKqxOUqEU3R5ZrpGm29GFu8
HHHGdaI5qheUsU1llmMjY3dkVA
```

```
    set hbdev "port7" 200 "port8" 200
    set session-pickup enable
    set override enable
    set priority 255
    set monitor "port2" "port3"
end
:
:
config user group
    edit "SSO_Guest_Users"
    next
    edit "Guest-group"
        set member "guest"
    next
    edit "VPN_USERS"
        set member "AD_SERVER"
        config match
            edit 1
                set server-name "AD_SERVER"
                set group-name "CN=VPN_USERS,CN=Users,DC=lab-sdwan,DC=local"
            next
        end
    next
end
config vpn ssl web portal
    edit "full-access"
        set tunnel-mode enable
        set ipv6-tunnel-mode enable
        set web-mode enable
        set ip-pools "SSLVPN_TUNNEL_ADDR1"
        set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    next
    edit "DENY"
        set forticlient-download disable
    next
    edit "tunnel-access"
        set tunnel-mode enable
        set ipv6-tunnel-mode enable
        set ip-pools "SSLVPN_TUNNEL_ADDR1"
        set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    next
    edit "REMOTE_USER_ACCESS"
        set tunnel-mode enable
        set ip-pools "RA_VPN_POOL"
        set split-tunneling-routing-address "DEKANAT_VLAN address" "DMZ address"
"STUDENTS_VLAN address" "USER_VLAN address" "Wi-Fi-VLAN address"
    next
end
config vpn ssl settings
    set banned-cipher SHA1 SHA256 SHA384
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "RA_VPN_POOL"
    set port 43443
    set source-interface "port2" "port3"
    set source-address "all"
    set source-address6 "all"
    set default-portal "DENY"
    config authentication-rule
        edit 1
            set groups "VPN_USERS"
            set portal "REMOTE_USER_ACCESS"
        next
    end
end
config firewall policy
    edit 1
        set name "DEKANAT_to_OUTSIDE"
        set uuid 188f1a44-a846-51f0-942b-b31c0fc33426
        set srcintf "DEKANAT_VLAN"
        set dstintf "port2" "port3"
        set action accept
        set srcaddr "DEKANAT_VLAN address"
        set dstaddr "all"
        set schedule "always"
        set service "HTTPS" "HTTP"
        set logtraffic all
        set nat enable
        set port-preserve disable
```

```
    next
    edit 2
        set name "GUEST_Policy"
        set uuid 695da6ca-a918-51f0-e2eb-4c4f09130259
        set srcintf "GUEST_VLAN"
        set dstintf "port2"
        set action accept
        set srcaddr "GUEST_VLAN address"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 3
        set name "AuthUSERS_to_DMZ"
        set uuid 46f7e7f2-a919-51f0-2ca5-ba007c0e28e5
        set srcintf "STUDENTS_VLAN" "USER_VLAN" "DEKANAT_VLAN"
        set dstintf "DMZ"
        set action accept
        set srcaddr "DEKANAT_VLAN address" "STUDENTS_VLAN address" "USER_VLAN address"
        set dstaddr "DMZ address"
        set schedule "always"
        set service "ALL"
    next
    edit 4
        set name "SSL-VPN_USERS_to_DMZ_HTTPS"
        set uuid 845a3aac-ada4-51f0-f89b-49f70361d4ec
        set srcintf "ssl.root"
        set dstintf "DMZ"
        set action accept
        set srcaddr "RA_VPN_POOL"
        set dstaddr "DMZ address"
        set schedule "always"
        set service "RDP"
        set groups "VPN_USERS"
    next
    edit 5
        set name "FAZ_to_OUTSIDE"
        set uuid 6d010780-adba-51f0-9573-5e4094b1302c
        set srcintf "FAZ_CONNECT"
        set dstintf "port2" "port3"
        set action accept
        set srcaddr "FAZ_CONNECT address"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set port-preserve disable
    next
    edit 6
        set name "MGMT_to_FAZ"
        set uuid 8db07132-adba-51f0-0900-b62c400bc338
        set srcintf "port2" "port3"
        set dstintf "FAZ_CONNECT"
        set action accept
        set srcaddr "all"
        set dstaddr "FAZ"
        set schedule "always"
        set service "HTTPS"
    next
    edit 7
        set name "FAZ_CONNECT"
        set uuid d829b0c4-adc0-51f0-0ef5-55dd214eb057
        set srcintf "any"
        set dstintf "any"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
config switch-controller managed-switch
    :
    :
    edit "S108DV02TPC3TV42"
        set sn "S108DV02TPC3TV42"
```

```
        set fsw-wan1-peer "fortilink"
        set fsw-wan1-admin enable
        set poe-detection-type 3
        set version 1
        set max-allowed-trunk-members 8
        set dynamic-capability 0x00000000000000001306ea751c55f9ff
        config ports
            edit "port1"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port2"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "quarantine"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port3"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "STUDENTS_VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port4"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "USER_VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port5"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "Wi-Fi-VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port6"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "DEKANAT_VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port7"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "GUEST_VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
            edit "port8"
                set speed-mask 207
                set vlan "_default"
                set allowed-vlans "USER_VLAN"
                set untagged-vlans "quarantine"
                set export-to "root"
            next
        end
    next
end
config router static
    edit 1
        set gateway 172.19.176.1
        set device "port2"
    next
    edit 2
        set gateway 172.19.175.1
        set device "port3"
    next
end
```