ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

«До захисту допущено»
В.о. завідувача кафедри автоматики та телекомунікацій
_____ Валерій ПОЦЕПАЄВ
(підпис) (ім'я та прізвище)
«___» _____ 2022 р.

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему «Дослідження і модернізація телекомунікаційної мережі КП «Покровськтепломережа» із застосуванням SCADA-систем»

Виконав студент 2 курсу, групи ТКРм–21
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Садовніченко Максим Віталійович
(Прізвище, Ім'я та По-батькові) (підпис)

Керівник к.т.н. доцент _____ Вікторія ВОРОПАЄВА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент к.т.н. доцент _____ Наталія МАСЛОВА
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент к.т.н. доцент _____ Олександр КОЛЛАРОВ
(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:

Дар'я ЖУКОВСЬКА

16.12.2022 р.

Засвідчую, що у цій випускній кваліфікаційній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Луцьк – 2022 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

Захист відбувся _____

(дата)

з оцінкою_____

Секретар ЕК _____

(підпис)

Випускна кваліфікаційна робота

магістра

Тема: «Дослідження і модернізація телекомунікаційної мережі КП «Покровськтепломережа» із застосуванням SCADA-систем»

Виконавець, студент
гр. ТКРм–21 Максим САДОВНІЧЕНКО
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Керівник Вікторія ВОРОПАЄВА
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Консультанти: Олександр ІСАЄНКОВ
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Валерій ПОЦЕПАЄВ
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Гліб СТУПАК
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Луцьк – 2022

Державний вищий навчальний заклад
"Донецький національний технічний університет"

Інститут, факультет Комп'ютерно-інформаційних технологій та автоматизації
Кафедра Автоматика та телекомунікації
Освітньо-кваліфікаційний рівень магістр
Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри АТ
Валерій ПОЦЕПАЄВ
«____» _____2022 року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Садовніченко Максим Віталійович
(прізвище, ім'я, по батькові)
1. Тема проекту (роботи) «Дослідження і модернізація телекомунікаційної мережі КП «Покровськтепломережа» із застосуванням SCADA-систем»
керівник проекту (роботи) Воропаєва Вікторія Яківна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 28.09.2022 року № 446
2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи)_____
Технічна документація та матеріали з переддипломної практики

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Аналіз інфраструктури комунального підприємства
2) Аналіз технології
3) Модернізація мережі в центральному офісу
4) Модернізація мережі котельних

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
План будівлі центрального офісу
Інформаційна модель мережі
Структура мережі котельної

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Воропаєва В.Я. к.т.н., доцент		
2	Ісаєнков О.О. к.т.н., доцент		
3	Поцепаєв В.В. к.т.н, доцент		
Нормо-контроль	Жуковська Д.О., асистент	-	16.12.2022

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз мережі КП «Покровськтепломережа»	01.10.22 – 15.10.22	
2	Аналіз технології	16.10.22 – 30.10.22	
3	Розробка мережі центрального офісу	31.10.22 – 14.11.22	
4	Модернізація мережі котельних	15.11.22 – 02.12.22	
5	Додаток А – Охорона праці та безпека під час надзвичайних ситуаціях на підприємстві	03.12.22 – 09.12.22	
6	Представлення дипломної роботи науковому керівнику	12.12.22	
7	Захист дипломної роботи	22.12.22	

Студент _____ **Максим САДОВНІЧЕНКО**
(підпис) (прізвище та ініціали)

Керівник роботи _____ **Вікторія ВОРОПАЄВА**
(підпис) (прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

Посада, Ім’я та ПРІЗВИЩЕ	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Садовніченко Максим Віталійович. Дослідження і модернізація телекомунікаційної мережі КП «Покровськтепломережа» із застосуванням SCADA-систем / Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Луцьк, 2022.

Пояснювальна записка: 94 стор., 61 рис., 13 табл., 14 посилання.

У дипломній роботі проводився модернізація телекомунікаційної мережі на об’єктах КП «Покровськтемломережа» і запровадження SCADA-систем для котельних. Перед цим була проведена робота з аналізу мережі, під час якої були виявлені недоліки і підготовлений план подальшої роботи. Під час модернізації були запроваджені наступні рішення: VPN шлюз між об’єктами, система відеоспостереження, запровадження параметрів мережевої безпеки, сегментація мережі.

Ключові слова: МЕРЕЖА, SCADA, VPN, КОТЕЛЬНЯ, ВІДЕОСПОСТЕРЕЖЕНЯ, МЕРЕЖЕВА БЕЗПЕКА, UNIFI, БРАНДМАУЕР.

Список публікації здобувача:

1. Садовніченко М.В. Методи використання механізмів пошуку зворотнього шляху для захисту мережі від атаки спуфінга / Всеукраїнська науково-практична конференція «Телекомунікації, автоматизація, комп’ютерно-інтегровані технології-2021» (ТАК-2021), 01.12.2021р. Покровськ ДВНЗ «ДонНТУ», 2021р.
2. Садовніченко М.В., Воропаєва В.Я. Порівняльний аналіз VPN рішень для зв’язку між об’єктами критичної інфраструктури / Всеукраїнська науково-практична конференція «Телекомунікації, автоматизація, комп’ютерно-інтегровані технології-2022» (ТАК-2022), 01.12.2022р. Луцьк ДВНЗ «ДонНТУ», 2022р.

ABSTRACT

Sadovnichenko Maksym. Research and modernization of the telecommunications network of KP "Pokrovsktemlomerezh" using SCADA systems / Graduation qualifying work for obtaining an educational degree "Master" in specialty 172 "Telecommunications and Radio Engineering" - SHEE DonNTU Lutsk, 2022.

The work contains 94 pages, consists of an introduction, 4 sections, conclusions, a list of sources used with 14 titles, 61 figures, 13 tables, 4 appendices.

In the diploma work, the modernization of the telecommunications network at the facilities of KP "Pokrovsktemlomerezh" and the introduction of SCADA systems for boiler rooms were carried out. Prior to that, network analysis work was carried out, during which shortcomings were identified and a plan for further work was prepared. During modernization, the following solutions were implemented: VPN gateway between objects, video surveillance system, introduction of network security parameters, network segmentation.

Keywords: NETWORK, SCADA, VPN, BOILER ROOM, VIDEO SURVEILLANCE, NETWORK SECURITY, UNIFI, FIREWALL.

Publisher publication list:

1. Sadovnichenko M.V. Methods of using reverse path search mechanisms to protect the network from spoofing attacks / All-Ukrainian scientific and practical conference "Telecommunications, automation, computer-integrated technologies-2021" (TAK-2021), 01.12.2021. Pokrovsk State Educational Institution "DonNTU", 2021

2. Sadovnichenko M.V., Voropayeva V.Ya. Comparative analysis of VPN solutions for communication between critical infrastructure objects / All-Ukrainian scientific and practical conference "Telecommunications, automation, computer-integrated technologies-2022" (TAK-2022), 01.12.2022. Lutsk State Higher Secondary School "DonNTU", 2022.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACL - Access Control List

ARP - Address Resolution Protocol

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

IP - Internet Protocol

LAN - Local area network

MAC - Media Access Control

NAS - Network Attached Storage

OSI - Open Systems Interconnection

PoE - Power over Ethernet

RADIUS - Remote Authentication Dial-In User Service

SCADA - Supervisory Control And Data Acquisition

TCP - Transmission Control Protocol

VLAN - Virtual Local Area Network

VPN - Virtual Private Network

WAN - Wide Area Network

ПЛК - Програмований логічний контролер

ВСТУП

Актуальність роботи. Теплопостачання є частиною об’єктів критичної інфраструктури України. І тому на даних об’єктах є потрібним використання сучасних інформаційних технології, від телекомунікації і до автоматизації процесів. Також вони мають високі вимоги до структури і характеристики мереж.

Тому дуже важливо проводити модернізацію телекомунікаційної архітектури і систем автоматизації і управління робочими процесами для мінімізації аварійних ситуації.

Також важливо запроваджувати високі стандарти безпеки на підприємстві, як мережеві так і загальні. Запровадження безпечного зв’язку між віддаленими об’єктами також відіграє важливу роль при організації систем автоматизації та побудові телекомунікаційних мереж промислових підприємств та об’єктів критичної інфраструктури..

Метою кваліфікаційної роботи є підвищення параметрів безпеки функціонування телекомунікаційної мережі КП «Покровськтемломережа» та якості обслуговування абонентів підприємства шляхом модернізації телекомунікаційної інфраструктури КП «Покровськтепломережа» та запровадження технології SCADA в системи автоматизації управління котлами.

Об’єктом дослідження в даній роботі являється структурні підрозділи КП «Покровськтепломережа»

Предмет роботи – використання сучасних телекомунікаційних рішень і систем автоматизації.

Методи дослідження. При виконані цієї роботи виконувалися теоретичні та експериментальні дослідження із використання методів комп’ютерного моделювання і проектування.

Практична цінність роботи визначається можливістю впровадження проекту рішення для подальшого використання в телекомунікаційної мережі

об’єктів підприємства і автоматизації процесів.

Структура та обсяг роботи. Робота містить 94 сторінки, складається з вступу та 4 розділів, висновків до розділів, 61 рисунків, 13 таблиць, 4 додатків, списку використаних джерел, які містять 14 найменувань.

1 АНАЛІЗ ІСНУЮЧОЇ МЕРЕЖІ КП «ПОКРОВСЬКТЕПЛОМЕРЕЖА»

1.1 Загальна характеристика об’єктів комунального підприємства

В якості об’єкту аналізу дипломного проекту виступає 20 будівель КП «Покровськтепломережа». Це підприємство, яке займається послугами центрального теплопостачання в містах Покровськ і Родинське, а також селища Шевченко. Підприємство має в своєму складі: центральний офіс в якому розміщені співробітники підприємства і 19 котелень, з яких 15 находиться в м. Покровськ, 4 - в м. Родинське і 1 в селище Шевченко. На рис. 1.1 і 1.2 наведена карта об’єктів КП в місті Покровськ і Родинське відповідно. Загальна кількість працівників нараховує близько 250 осіб.

Задачею дослідження є модернізація корпоративної мережі, для збільшення параметрів якості обслуговування, збільшення мережевої безпеки і налаштування безпечного зв’язку між об’єктами.

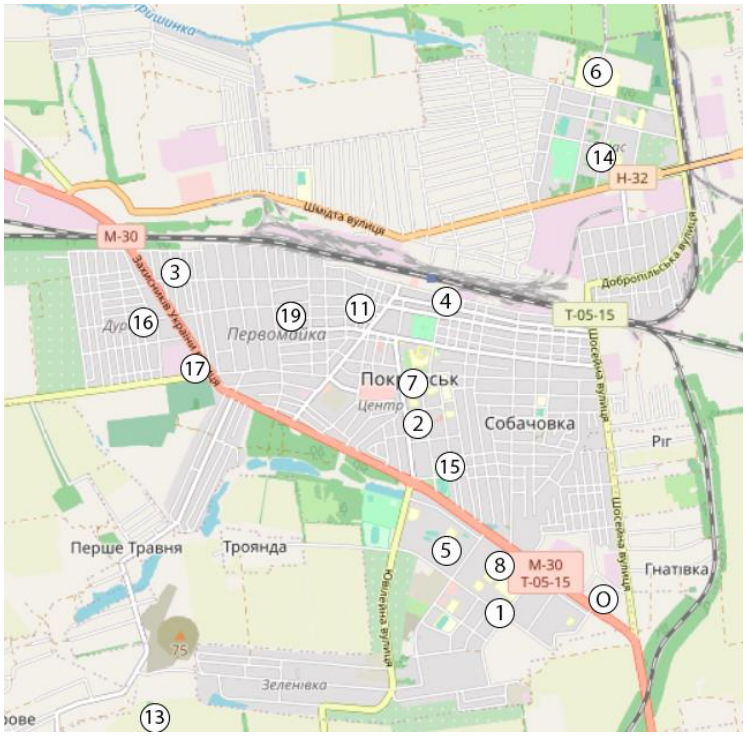


Рисунок 1.1 – Карта об’єктів в місті Покровськ і селище Шевченко(котельна №13)

Рисунок 1.2 – Карта об’єктів в місті Родинське

Наразі підприємство має локальну мережу центрального офісу, і локальні мережі кожної котельні які підключені до постачальника мережевих послуг.

1.2 Аналіз центрального офісу

Центральний офіс - це трьох поверхова будівля, в якій находяться 48 співробітників. Має наступні відділи: виробничий, плановий, бухгалтерія, юридичний, абонентський, кадрів, охорони праці, енергетиків і забезпечення.

Основні функції які виконуються в центральному офісі це: робота по оформлення звітів по виконаній роботі, бухгалтерський облік, нарахування і формування квитанції для споживачів, контроль і облік роботи котельних. Для виконання свої функції використовуються наступні рішення: програми Microsoft Office, онлайн сервісом Prozzoro, бухгалтерський облік, база даних абонентів і формування квитанції. Також під час опалювального сезону присутній диспетчер, який цілодобово знаходиться на зв’язку з котельними,

контролює їх роботу і також проводить облік споживання ресурсів кожного об’єкту.

Прилади які використовуються в офісі є офісні комп’ютери і також МФУ і принтери що пов’язано з великою кількістю паперової роботи. В офісі відсутні сервери, чи інші важливі кінцеві прилади. На рис. 1.3. наведений мережевий план офісу.

Центральний офіс має наступний план мережі:

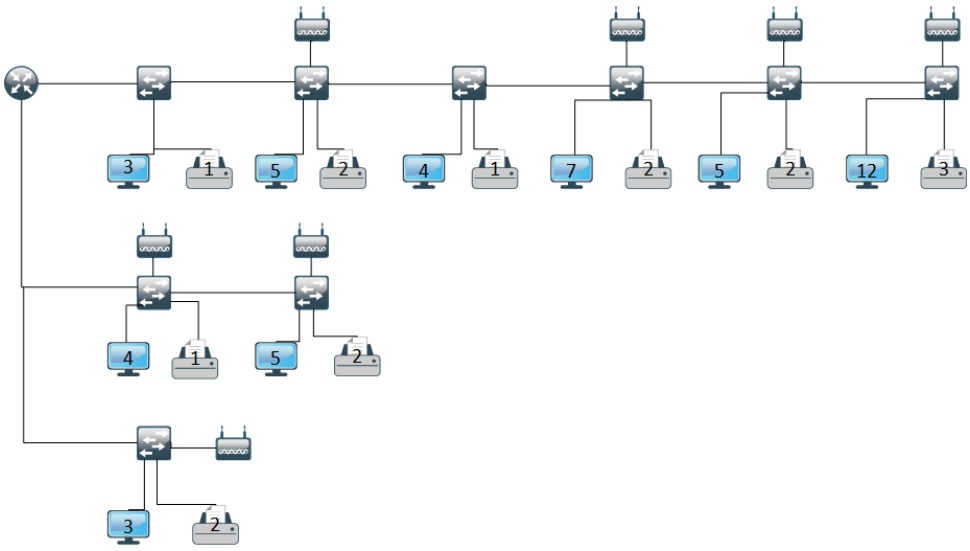


Рисунок 1.3 – Мережевий план офісу з кінцевими пристроями

Наявна мережа має наступний план, загальна кількість кінцевих пристроїв 64 які підключені до комутаторів і вони з’єднані по топології шина. Такий тип з’єднання є ненадійним у випадку виходу одного мережевого пристрою, велика кількість пристроїв втрачають доступ до мережі. Також в мережі відсутній централізований сервер для зберігання даних, і деякі комп’ютери виступають в якості сервера для бухгалтерій і абонентського відділу. Мережа має низький рівень безпеки так як відсутні наступні реалізації: брандмауер, керуванням доступу для користувачів, системи аутентифікації.

1.3 Аналіз мережі котельних

1.3.1 Опис роботи котельні

Зазвичай котельна може мати від одного газового котлу до декількох, в залежності від потужності котельної. Які відповідають за нагрів води яка циркулює в робочому контурі і подається в теплосистему до кінцевих користувачів. На рис. 1.4 наведена схема котельної.

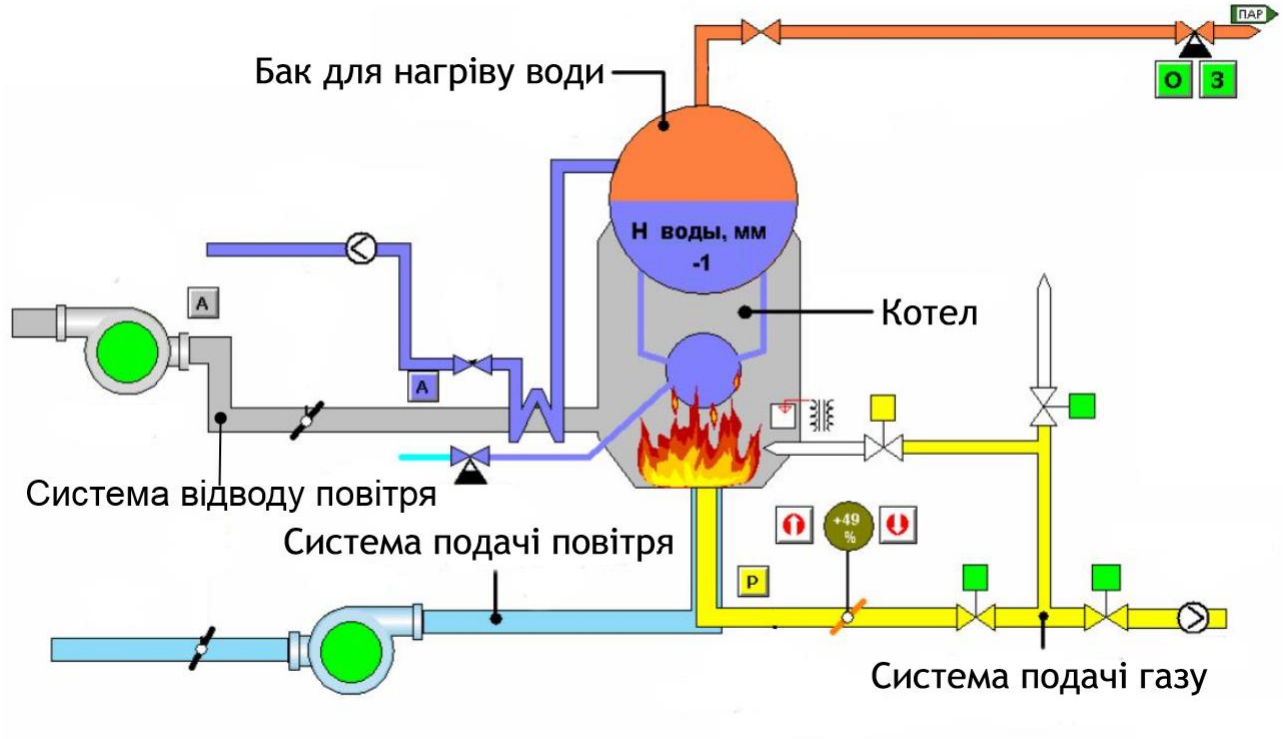


Рисунок 1.4 – Схема котельної

Схема котельні має наступний вигляд. Головний елемент який відповідає за нагрів теплообміннику є газовий пальник на який поступає газ з системи. По теплообміннику протікає вода із теплосистеми. Триходовий кран кран забезпечує регулювання температури води відповідно уставу який розраховується в залежності від температури зовнішнього котлу і системи відводу повітря який виконує функцію відводу продуктів згоряння. Такі котли називають турбованими.

Котли серій КВГ-4,5-150 має в своєму використані КП

«Покровськтепломережа» для подачі тепла споживачам, яка наведена на рис. 1.5. Вона має застарілу систему управління і контролю радянських часів, яка має низьку ефективність.

Рисунок 1.5 – Система контролю роботи котельні

1.3.2 Аналіз мережі і устаткування котельні

Мережа в котельних мають однакову структуру і функціональність. Вона має примітивний вигляд, це маршрутизатор який підключений до місцевого постачальника і декілька кінцевих пристроїв які підключені до мережі. До кінцевих пристроїв відносяться офісні комп’ютери і також принтери або МФУ.

Роботу яку виконується на котельних пов’язані відповідно зі самою роботою і обслуговування котлів. Але також виконуються функції з створення відповідних звітів роботи котельних, електронний документообіг.

Також всі котельні повинні мати цілодобовий зв’язок з диспетчером який

находиться в центральному офісі. Зв’язок відбувається з допомогою GSM-телефонів під час екстрених ситуації, і також за допомогою електронної пошти для відправки документів або звітів.

1.4 Проблематика наявної мережі

Для розвиту і вдосконалення компаніям завжди потрібно застосовувати сучасні комп’ютерні технологій, які дозволяють підтримувати степінь інформаційно-технічного забезпечення на високому рівні.

Необхідність модернізації полягає в тому, що існуюча мережа приладів вже застарілі, або взагалі відсутні деякі важливі телекомунікаційні рішення. Так як важливо проводити повний аналіз мережі і її модернізацію кожні 5-7 років.

Під час аналізу всієї наявної мережі КП «Покровськтепломережі» були виявлено проблеми в центральному офісі і також в мережі котельних.

Проблеми в центральному офісі:

- Відсутність центрального серверу для зберігання і обробки даних
- Низький рівень мережевої безпеки
- Відсутня система відеоспостереження

І також мережа котельних має наявні проблеми:

- Відсутність безпечного з’єднання з центральним офісом
- Відсутність систем охорони з використанням мережевих рішень
- Застаріла система обліку і автоматизації котельні

Після повного аналізу наявної мережі і всіх проблем які в неї є, будуть проведені наступні заходи для модернізації наявної мережі:

- Повна переробка архітектури мережі підприємства
- Встановлення і налаштування серверу
- Запровадження алгоритмів безпеки в мережі
- Впровадження сучасних телекомунікаційних рішень

- Впровадження SCADA систем на котельних
- Налаштування безпечного зв’язку між офісом і котельними

Висновки розділу 1

У першому розділі випускної кваліфікаційної роботі був проведений аналіз об’єктів комунально підприємства «Покровськтепломережа».

Була проведена аналітична робота всіх наявних об’єктів КП, а саме центральний офіс і 19 котелень які находяться в м. Покровськ, м. Родинське і с. Шевченко. Була проведена робота по виявлені недоліків проектування і роботи локальної мережі даних об’єктів.

Основі проблеми які були виявлені під часу аналізу наступний. Те що інтернет мережа підприємства побудована погано, і не має розділення користувачів по відділам. Також відсутня інфраструктура централізованих серверів, і за чого дані всі дані просто зберігаються на робочих комп’ютерах працівників. Відсутня інфраструктура захисту в локальної мережі, і за цього має високу загрозу кібератаки.

На котельних присутні наступні проблеми. Найголовніша відсутність безпечного зв’язку котельних з центральним офісом. Також застаріла система автоматизації котельні. І відсутня система охорони на об’єктах.

Були виділені основні сфери в яких будуть проводитися модернізація, а саме: мережева інфраструктура, кібербезпека і система автоматизації. І в наступних розділах роботи будуть розглянуті технології які будуть запроваджуватися під час модернізації мережі.

2 АНАЛІЗ ТЕХНОЛОГІЇ

2.1 Ethernet

2.1.1 Склад Ethernet

Комп’ютерні мережі сьогодні стали невід’ємною частиною. Її використовують для таких можливостей як: електрона пошта, доступ до віддалених баз даних, спілкування і обмін даними між користувачами, пошук інформації, використання потужності віддалених машин тощо.

Ethernet – це технологія яка основана на витої парі, що складається з хостів які об’єднанні за допомогою комутаторів. За технічним визначенням відноситься до сімейства протоколів стандарту IEEE 802.3.

Мережа – це будь-яка сукупність незалежних пристроїв, які обмінюються інформацією один з одним через спільне середовище зв’язку. Локальні мережі (LAN) зазвичай обмежуються географічною територією, такою як одна будівля або корпус університету. Глобальна же мережа об’єднує кілька локальних мереж між собою, які географічно розподілені.

Кожен вузол у сегменті Ethernet має апаратні або програмні можливості для надсилання та отримання кадрів Ethernet. Склад кадру представлений на рис. 2.1.

Рисунок 2.1 – Склад кадру Ethernet

Кадр починається з восьми октетної преамбули яка складається з нулів і одиниць, що забезпечує синхронізацію для приймаючого хоста. За нею

безпосередньо йде шість байтів адреса призначення, а потім 6 байтів адреса відправника. Вони мають формат фізичної адреси мережевого обладнання відомою як MAC-адреса. Адреси є локально унікальними. Після адрес іде двох байтове поле яке описує довжину або тип корисного навантаження. Далі слідує корисне навантаження, як правило кадр вищого рівня(наприклад IP-пакет) разом з інформаційною складовою. [1]

2.1.2 Комутатор

Комутатор це пристрій який дозволяє з’єднати пристрої і ділянки мережі між собою. Він працює на канальному рівні OSI, тобто пересилає пакети на основі їх MAC-адреси.

На початку комутатор не знає MAC-адресу кожного вузла. Коли вузол надсилає кадр, комутатор дізнається з якого порту надійшов цей кадр і додає MAC-адресу відправника та номер порту до таблиці. Далі комутатор шукає адресу одержувача у своїй пам’яті, і якщо вона не знайдена, кадр повторно надсилається на всі інші порти(заповнення). Заповнення фреймів працює, оскільки кінцеві вузли ігнорують фрейми, у яких адреса одержувача не збігається з їх власною, і лише правильний одержувач приймає фрейм до вищих рівнів для обробки.

Коли в мережу надсилаються додаткові кадри, комутатор швидко створює таблицю пар портів і MAC-адрес. Оскільки для ідентифікації кожного хоста потрібен лише один кадр, швидко створюється таблиця, яка відображає часткове уявлення комутатора про топологію мережі, і одно адресні кадри надсилаються лише на один порт, що відповідає адресі одержувача. На рис. 2.2 наведено приклад розподілу MAC-адрес до портів комутатору.

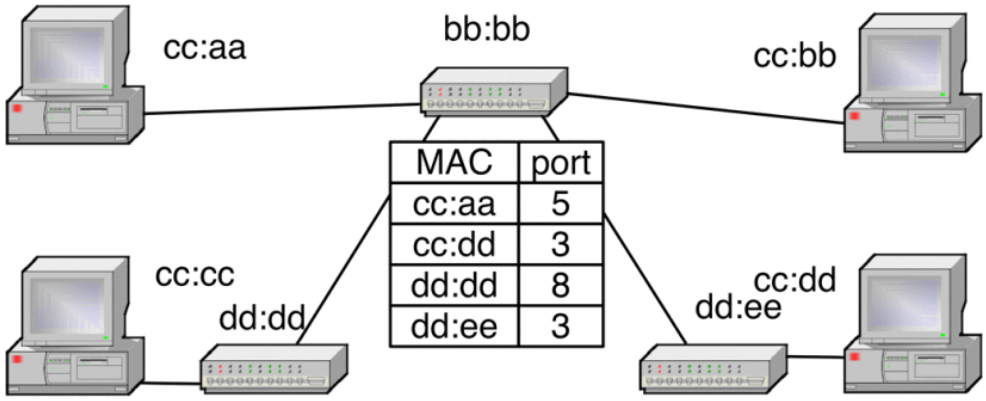


Рисунок 2.2 – Сегмент Ethernet з комутаторами і хостами(адреси подаються скорочено)

Комутатори також можна з’єднувати один з одним. Для комутатора інший комутатор – це лише кілька MAC-адрес за одним портом. Можливо і часто бажано побудувати сітчасту топологію комутаторі для збільшення надмірності. Канали, що з’єднують комутатори один з одним, часто називають магістральними, особливо коли передається трафік, зо належить кільком VLAN.

Зазвичай комутатори мають три рівня структури:

- Площина даних – в яких відбувається пересилання кадрі з одного порту на інший і зазвичай реалізована апаратно. Структура з’єднання, або шина заданої площини, має набагато вищу пропускну здатність, ніж порти введення/виводу комутатора. Це дає можливість декільком одночасним потокам проходити з повною потужністю лінії.
- Площина керування – в якому відбувається обробка кадрів,. Наприклад кадри, адреси яких не вказано в таблиці або повідомлення протоколу STP, які налаштовують мережу комутаторів. Зазвичай це робиться центральним процесором комутатора.
- Площа керування – використовується для налаштування таких функцій комутатора, як мережі VLAN. Реалізація зазвичай включає стек TCP/IP, інтерфейс командного рядка та агента простого протоколу керування мережею.

2.1.3 Віртуальна локальна мережа

VLAN використовують для поділу фізичної мережі на кілька логічних мереж. Кожен комутатор у мережі зберігає таблицю, яка пов’язує його порти з різними ідентифікаторами VLAN, що використовуються. Мотивація механізму VLAN полягає в підвищені ефективності шляхом обмеження розміру широкомовного домену, але він також використовується з метою безпеки. Хости в різних VLAN не можуть надсилати кадри один одному безпосередньо. На рис. 2.3 наведено приклад налаштування VLAN в локальній мережі.

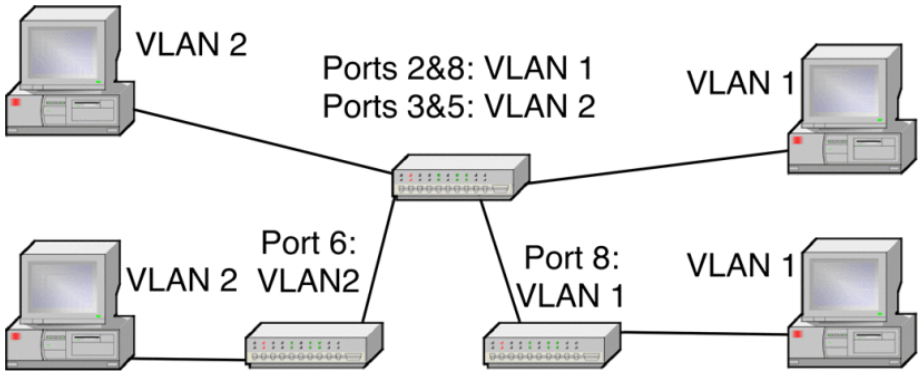


Рисунок 2.3 – Приклад налаштування VLAN в локальній мережі

Щоб розділити кадри під час передачі між комутаторами, механізм VLAN 802.1Q додає чотирьох байтовий тег VLAN всередині заголовка Ethernet після MAC-адресою відправника. IEEE 802.1ad додає другий тег для створення окремих локальних доменів і доменів VLAN провайдера. Перші два байти тегу VLAN містять значення 0x8100 для сповіщення комутаторів, що підтримують VLAN. Комутатори забезпечують дотримання меж цих локальних мереж, забезпечують додатковий захист. Тег додається, коли кадр надходить від хоста до першого комутатора, і віддаляється на останньому комутаторі перед доставкою до пункту призначення. За бажанням фрейми також можна доставити на хост із тегом, наприклад, якщо хост містить віртуальні хости.[2]

2.1.4 PoE

Power over Ethernet – це засіб забезпечення низкою напругою постійного струму для живлення пристроїв які підключені до локальної мережі через кабелі Ethernet.

Мережеві комутатори можна описати як обладнання джерела живлення (PSE), а пристрої PoE, такі як телефони VoIP, точки доступу Wi-Fi і камер відеоспостереження, можна описати як джерела живлення приладів. Для комутаторів без підтримки PoE, є джерело живлення середнього діапазону, відоме як інжектор живлення PoE, може використовуватися як PSE. Вони підключаються до зовнішнього джерела живлення. Також доступні розгалужувачі PoE, які поділяють дані та живлення від кабелю PoE і можуть використовуватися для живлення пристроїв які не мають доступу до розеток змінного струму. Інжектори і розгалужувачі PoE є недорогою альтернативою для оновлення застарілого обладнання.

Кабелі, які фізично з’єднують мережевий комутатор із пристроями в локальній мережі повинні відповідати стандартам: рівню продуктивності щодо пропускної здатності сигналу, затухання та перехресних перешкод і бути визначені категорією. Для живлення пристроїв PoE дві кручені пари використовуються для проведення низької напруги до кінцевого пристрою. Максимальна рекомендована довжина для PoE становить 100 м, в іншому випадку рекомендовано використовувати подовжувачі PoE.[3]

2.2 Протоколи 3 рівня

IP протокол є протоколом 3 рівня OSI який відповідає за доставку пакетів даних між любими вузлами в мережі через машрутизатори. Для цього кожен пристрій має IP-адресу, це унікальна адреса яка ідентифікує пристрій в мережі інтернет або в локальній адресі.

Щоб IP протокол 4 версій (IPv4) працював через Ethernet, потрібні два протоколи. Іноді їх називають протоколами рівня 2.5. Протокол динамічної конфігурації хоста(DHCP) використовується для запиту IP-адреса для хоста. Коли хост IPv4 без IP-адреси стає активним у сегменті Ethernet, він надсилає запит на сервери DHCP за допомогою широкомовної трансляції Ethernet. Отримавши одну або більше одноадресних відповідей, хост вибирає один сервер і запитує IP-адресу з одноадресним повідомленням, а в разі успіху отримує на деякий час IP-адресу та додаткову інформацію, таку як маска мережі та IP-адреса шлюзу(маршрутизатора). IP-адреси також можуть бути налаштовані статично на хості, у цьому випадку DHCP не потрібен.

Протокол розпізнавання адрес(ARP) необхідний для того, щоб IP працював на спільних носіях, такий як Ethernet, оскільки MAC-адреси мають бути зіставлені з відповідними IP-адресами. Коли хост бажає зв’язатися з іншими хостом у локальній мережі, наприклад шлюзом, він надсилає широкомовне повідомлення із запитом на MAC-адресу, яка відповідає IP-адресі в повідомлені. Хост, IP-адреса якого використовується, відповідає одноадресним повідомленням. Одержувач зберігає пару IP-адрес і MAC-адрес у таблиці (кеш ARP) протягом певного часу (зазвичай від 30 секунд до 5 хвилин, залежно від операційної системи). Реалізація, особливо старіші, часто не мають статусу, тому хост буде кешувати ARP-відповідь, навіть якщо їх не запитували.

IPv6 має схожі функції. Хости знаходяться за допомогою Neighbor Discovery Protocol(NDP), який використовує багатоадресну Ethernet (комутатори можуть використовувати багатоадресну передачу Ethernet як широкомовну розсилку, але використання адрес групової передачі допомагає мережевим картам хостів фільтрувати кадри) або за допомогою DHCPv6. Маршрутизатори IPv6 знаходяться шляхом прослуховування багатоадресних оголошень маршрутизатора, на основі яких хост може створити власну адресу IPv6 і використовувати NDP для перевірки її унікальності.

2.3 VPN

У теперішній час із запровадженням цифрових технологій на об’єктах критичної інфраструктури є велика потреба в обміну інформації між цими об’єктами. Але одного із головних умов зв’язку між ними є безпека передачі даних. Для безпечного налаштування зв’язку існує технологія віртуальної приватної мережі(VPN).

Віртуальні приватні мережі – це спосіб розширення приватної мережі через загальнодоступну мережу, таку як Інтернет. Потім користувачі можуть використовувати VPN для доступу до даних у приватній мережі через Інтернет, ніби вони безпосередньо підключені до приватної мережі. Розширення приватної мережі яке здійснюється за допомогою VPN, можна використовувати для віддаленого доступу до інших приватних мереж за допомогою тунелю VPN/ Тунель в мережі – це надійний спосіб надсилання даних, які зазвичай не підтримуються мережевим протоколом, шляхом перепакування даних у пакет до іншого протоколу. Якщо на двох маршрутизаторах налаштовано тунелювання, можна інкапсулювати дані для безпосереднього надсилання один одному через мережу Інтернет, а потім декапсулювати корисне навантаження, надіслане через тунель, щоб надіслати його далі до місця призначення.

Крім тунелювання приватних мереж, VPN може виконувати роль шифрування та забезпечення цілісності тунелю. VPN можна використовувати для відправлення конфіденційних даних у приватній мережі та забезпечення їх незмінності під час транспортування. На рис. 2.4 наведений приклад VPN мережі. Це додає додатковий рівень безпеки, не відкриваючи приватну мережу для публічного доступу, але водночас дає змогу отримати доступ до приватної мережі віддалено.[4]

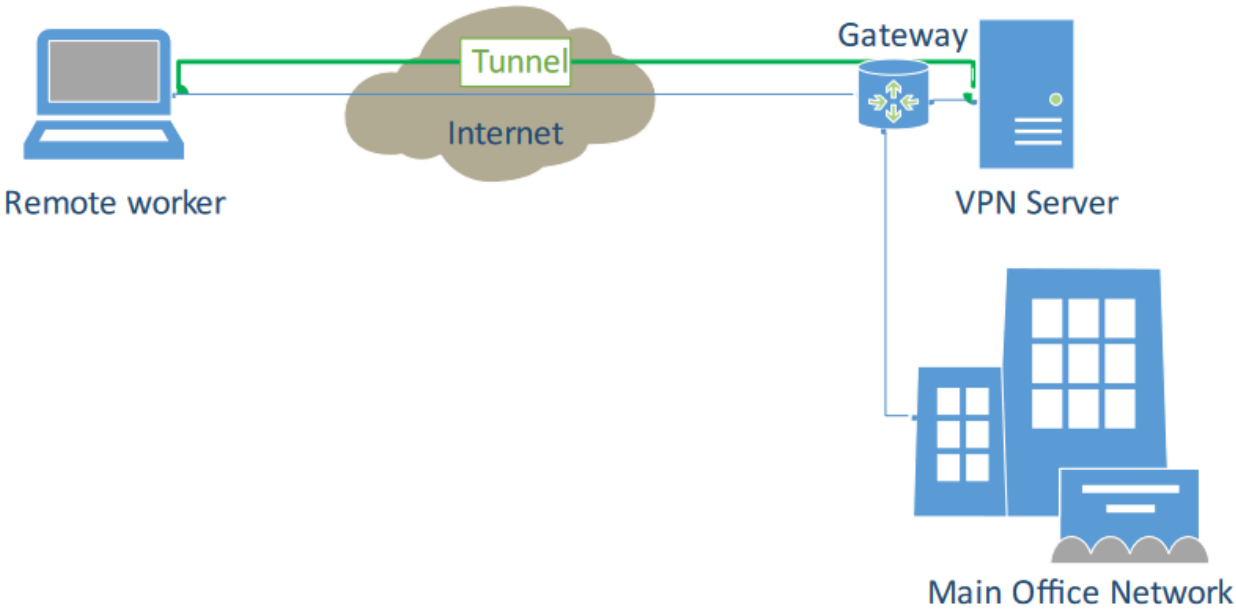


Рисунок 2.4 – Приклад VPN мережі між персональним комп’ютером і офісом

Є наступна класифікація VPN мережі за топологією:

1) Однорангова – встановлює безпечний тунель між двома комп’ютерами через публічну мережу. Для кожного кінця тунелю буде призначено IP-адресу, щоб два комп’ютера могли спілкуватися один з одним, ніби вони з’єднані фізичним кабелем Ethernet.
2) Клієнт-сервер – встановлює безпечний тунель між клієнтом VPN і певною приватною мережею з налаштованим VPN сервером. Клієнт може підключатися до всіх комп’ютерів у певні мережі. Потрібно також враховувати що трафік шифрується саме між клієнтом і сервером, а трафік між сервером і комп’ютерами в приватній мережі не відбувається.
3) Site-to-Site VPN – встановлює безпечний тунель між 2 приватними мережами через мережу Інтернет, де кінцевими точками тунелю є маршрутизатор або сервер з налаштованим VPN. Потрібно також враховувати що шифрування трафіку відбувається між пристроями з налаштованим VPN. На рис. 2.5 наведений приклад VPN Site-to-Site

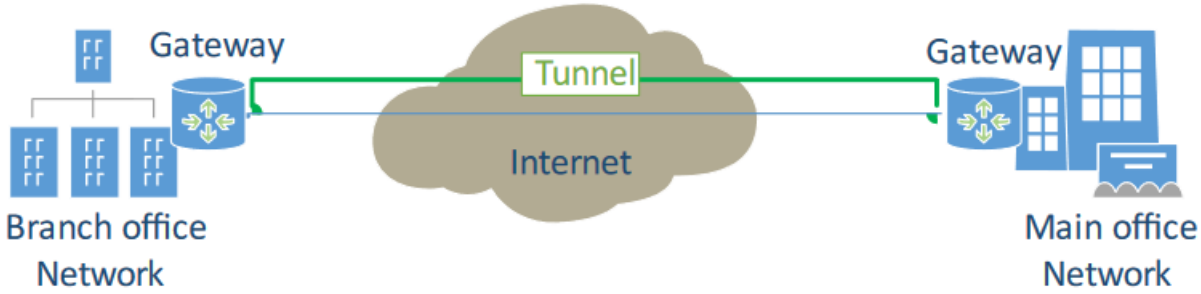


Рисунок 2.5 – VPN типу Site-to-Site

Вибір протоколу VPN залежить від типу трафіку, що надсилається через тунель. Протоколи VPN можна класифікувати відповідно до рівня OSI отриманих пакетів які використовуються для шифрування. Зараз існує 3 види VPN:

1) VPN рівня 2 – інкапсулює пакети на 2 рівні OSI: канальний рівень. Основні протоколи VPN рівня 2: MPLS VPN рівня 2, OpenVPN, PPTP і L2TP. Підтримує всі види трафіку такі як Frame Relay, асинхроний режим передачі і трафік Ethernet.
2) VPN рівня 3 – інкапсулює пакети на 3 рівні OSI: мережевий рівень. Основні протоколи VPN рівня 3: MPLS VPN рівня 3, OpenVPN, PPTP і L2TP. Він є дещо більш обмежений ніж VPN 2 рівня, і підтримує трафік IP-адресації, ICMP пакети тощо.
3) VPN рівня 4 – інкапсулює пакети на 4 рівні OSI: транспортний рівень. Основним використанням TLS є захист веб-трафіку, який передається через HTTP для формування HTTPS. Хоча TLS широко використовується, він може шифрувати лише пакети рівня 4, а не нижчі рівні. Це значно обмежує його застосування.[5]

Одна з причин використання VPN полягає в тому, що вона додає аспекти безпеки до мережевого з’єднання. Безпека в даному випадку означає захист мережевого трафіку щодо конфіденційності, цілісності та автентифікації. Конфіденційність досягається за допомогою шифрування. Якщо хтось отримає доступ до зашифрованих пакетів, надісланих через тунель VPN, він побачить лише зашифровані дані, які неможливо прочитати. Залежно від того який тип

шифрування використовується, його може бути дуже важко розшифрувати. Цілісність досягається за допомогою механізмів, які виявляють будь-які пакети підроблених. VPN використовують низку криптографічних алгоритмів і протоколів, щоб додати наприклад, механізмів автентифікації, щоб обмежити, хто може користуватися. Існує багато різних рівнів безпеки, які можна забезпечити різними програмами VPN.

Існують наступні VPN рішення:

1) PPTP – призначений для створення тунелю типу точка-точка. Протокол є одним із найстаріших протоколів. Використовує 1723 порт для зв'язку. Пакети даних що передаються через тунель інкапсульований. Найкраще підходить для додатків, де важлива швидкість. Використовує 128-бітне шифрування. Має низькі параметри безпеки і застарілості протоколу і наявних вразливостей.
2) L2TP – сам по собі не забезпечує жодного шифрування, але з використання протоколу IPSec досягається шифрування трафіку. Дані що передаються через протокол L2TP/IPSec, зазвичай двічі перевіряється тому і має високі параметри безпеки. Одним із недоліків є складність налаштування та підтримка VPN за допомогою цього методу.
3) OpenVPN – є opensource рішенням, тобто є можливість у спільноти перевіряти рішення на наявні вразливості і виправляти їх. Рішення використовує SSL/TLS для обміну ключами та шифрування. Також підтримує TCP, так і UDP протоколи, але за умовчання використовується UDP.
4) MPLS VPLS – є службою віртуально приватної мережі що пропонує багато точкове підключення на основі Ethernet через мережі IP або MPLS. Це дозволяє географічно рознесеним сайтам спільно використовувати широкомовний домен Ethernet, з'єднуючи користувачів через псевдодроти. Він часто використовується для

розширення послуг локальної мережі через мережу, надану постачальником послуг. [6]

Найголовніші умови для налаштування зв’язку між віддаленими об’єктами є високі параметри шифрування та аутентифікації, і можливість працювати на другому рівні OSI. Під ці всі параметри дуже добре підходить протокол OpenVPN, він має найвищі показники безпеки і також має високу сумісність з обладнанням і програмним забезпеченням.

2.4 SCADA

Диспетчерське управління і збір даних (SCADA) – це система для диспетчеризація інженерних систем. Цей комплекс технічних засобів необхідний для централізованого контролю та дистанційного регулювання інженерних комунікацій та обладнання.

Диспетчеризація і постійне проведення моніторингу необхідно для забезпечення безпечного функціонування об’єктів, економії ресурсів, забезпечення комфорту.

Промислові системи керування(ICS), включають як системи диспетчерського керування та збору даних(SCADA), так і розподілені системи керування (DCS) та системи керування процесами(PCS), а також інші конфігурації систем керування. Зокрема, системи SCADA є базовими компонентами моніторингу багатьох критичних інфраструктури, тоді як DCS і PCS з’єднують розподілені датчики, виконавчі механізми та керують процесами керування. ICS забезпечують моніторинг і контроль процесу в режимі реального часу, надаючи доступ віддаленим і локальним операторам через людино-машинні інтерфейси (HMI).

На рис. 2.6 наведена архітектура SCADA-системи.

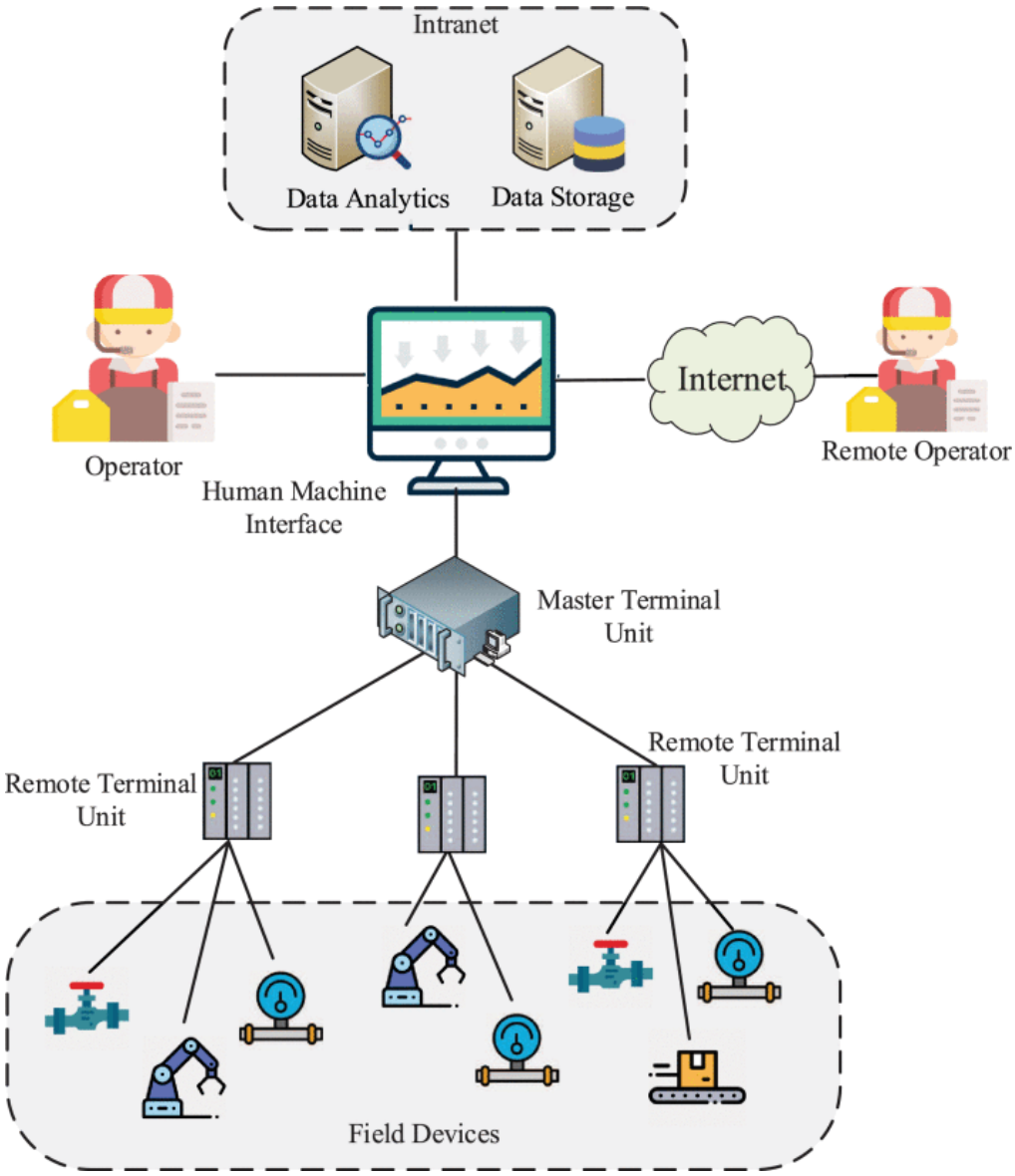


Рисунок 2.6 – Архітектура SCADA-системи

Типова структура SCADA-системи складається з наступних компонентів:

- Оператор – який відповідає за моніторинг системи, адресування сповіщень і виконання необхідних контрольних операцій. Оператор може перебувати в приміщені організацій або мати доступ до системи віддалено через Інтернет.
- HMI – який полегшує взаємодію між оператором і системою SCADA. HMI збирає інформацію з головного терміналу та належним чином перекладає команди керування.
- Сервери – які відповідають за збір і аналіз отриманих даних, які зібрані з польових пристроїв. Вони розташовані всередині організації.

- Головний термінальний блок (MTU) – який відповідає за збір даних від віддалених терміналів, передачу їх до HMI та надсилання сигналів керування. Він також забезпечує високорівневе логіку керування системою.
- Віддалені термінали (RTU) – це пристрої які обмінюються даними та командами з MTU та надсилають певні сигнали керування на промислові пристрої.
- Промислові пристрої – розподілені по вій організації та складаються з пристроїв, які керують промисловими процесами і датчиків які збирають всю необхідну інформацію.

Для реалізації безперервного, надійного та ефективного зв'язку між вищезазначеними компонентами SCADA були розроблені певні протоколи зв'язку. Це протоколи враховують можливості обробки компонентів і комунікаційні вимоги промислових додатків. В табл. 2.1 будуть наведені існуючі протоколи з їх характеристиками.[7]

Таблиця 2.1 – Протоколи зв'язку SCADA

Протокол	Інтерфейс	Топологія	Швидкість передачі даних	Максимальна дистанція
BITBUS	Fieldbus	Bus	62.5Kbps, 375 Kbps, 1.5 Mbps	1200m
Modbus	Serial, Ethernet	Line, Star, Ring, Mesh	100 Mbps, 1 Gbps	1200m
PROFIBUS	Fielsbus	Point-to-Point, Bus with spur, Daisy-chain, Tree	9.6 Kbps to 12 Mbps	1200m, 15km for optical channel
PROFINET	Ethernet	Ring, Tree, Line, Star	100 Mbps, 1 Gbps	100m
EtherCAT	Ethernet	Ring, Line, Daisy-chain	100 Mbps, 1 Gbps	100m
WorldFIP	Fieldbus	Bus	31.25 Kbps, 1 Mbps, 2.5 Mbps, 5 Mbps	1km

Перевагами впровадження SCADA-систем є наступне:

- Повний контроль над усіма процесами, що відбувають в інженерних системах.
- Мінімізація впливу людського фактору, що може призводити до серйозних помилок.
- Оперативний збір фактичних даних в режимі реального часу.
- Архівування інформації для подальшого аналізу, стратегічного планування, фінансового обліку.
- Забезпечення безпеки за рахунок унеможливлення несанкціонованого доступу.

Диспетчеризація промислових об’єктів не просто дає можливість відразу дізнаватися про неполадки в тій чи іншій системі, а й дозволяє точно встановлювати локалізацію збоїв, їх причини. Відповідно, з’являється можливість усунути порушення у функціонування підсистем у найкоротші терміни.

Встановлення системи диспетчеризації об’єктів сприяє фінансовій економії. Вкладення у такі комплекси швидко окупаються за рахунок скорочення витрат на експлуатації об’єктів. Крім того, автоматизація більшості процесів дозволяє скоротити чисельність персоналу. [8]

2.5 Відеоспостереження

У наші дні системи відеоспостереження можна зустріти всюди. Їх головною задачею є спостереження і охорона важливих об’єктів. Система надає можливість слідкувати за пересуванням людей в середині і зовні будівлі, і можна прослідкувати щоб не відповідні особи не мали доступу до об’єкту у визначений час або певного місця. Загалом систему можна описати з точки зору її призначення, реалізації, топології та захисту.

За останні кілька десятиліть технології відеоспостереження еволюціонували від аналогових систем до систем з комутацією пакетів (з

підтримкою мереж IPv4 і IPv6). Аналогові системи використовували камери, які передають аналогові сигнали (зазвичай через коаксіальний кабель) на пристрою записую Атаки на ці системи були або відмовою в обслуговуванні шляхом перерізання проводів, введення відео шляхом перехоплення кабелю та фальсифікації запису шляхом фізичної взаємодії із записуючим пристроєм. Навпаки, системи на основі IP мають різноманітні топології та технології, що робить їх набагато складнішими та призводить до набагато більшої поверхні атаки (наприклад VPN, шлюзи, системи контролю доступу, тощо).

Система відеоспостереження складається з наступних елементів:

- Медіа сервер – який відповідає за отримання, зберігання, керування та перегляд записаних відеозаписів. Медіа сервер може бути як локальний, так і використовувати хмарні сервіси.
- IP-камера – пристрій який знімає відео. На ринку є дуже багато моделей які мають різні характеристики: способи підключення до мережі, якісь відео, підтримка зйомки у нічний час тощо.
- Термінал перегляду – це може бути пристрій або програма, яка використовується для підключення до IP-камер. Наприклад можна використовувати смартфони які можуть підключатися до камер.
- Інфраструктура мережі – елементи які підключають камери до мережі. Також включає в собі обладнання та канали віртуальної приватної мережі.

Є декілька способів розгортання IP-системи відеоспостереження:

- Фізично відкритий контур – коли мережеві хости мають публічні IP-адреси, це означає, що будь-хто з Інтернету може надсилати пакети на пристрої. На рис. 2.7 наведений приклад системи з відкритим контуром.

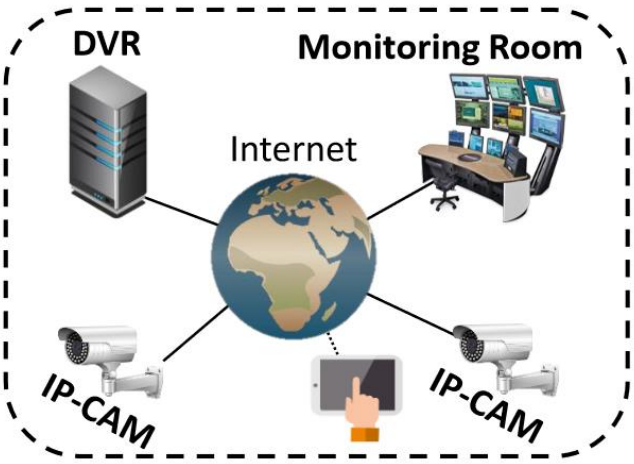


Рисунок 2.7 – Фізично відкритий контур

- Фізично замкнутий контур – коли мережеві хости в системі мають приватні IP-адреси, і коли система відеоспостереження не має доступу до інтернету. На рис. 2.8 наведений приклад з замкнутим контуром.

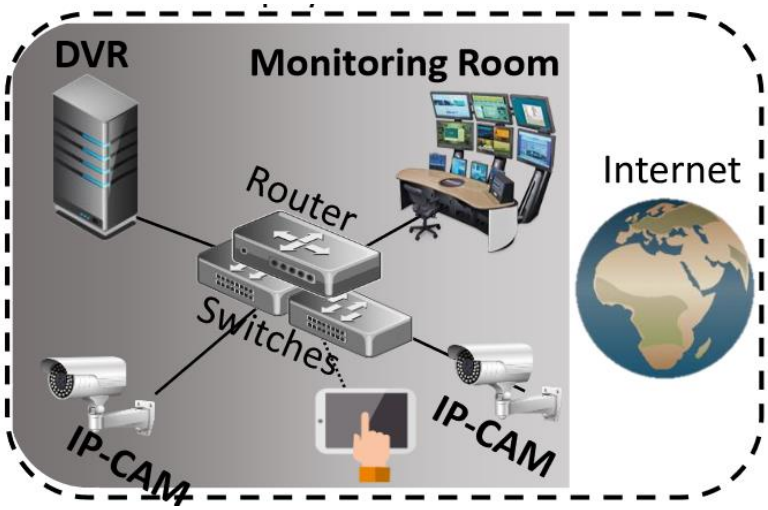


Рисунок 2.8 – Фізично замкнутий контур

- Віртуально замкнутий контур – коли хости в мережі мають приватні IP-адреси, і мережа підключена через інтернет за допомогою VPN. Це означає, що ніхто з Інтернету не може надсилати пакети на пристрої безпосередньо, якщо вони не надсилають пакети через VPN.На рис. 2.9 наведений приклад системи з віртуально замкнутим контуром. [9]

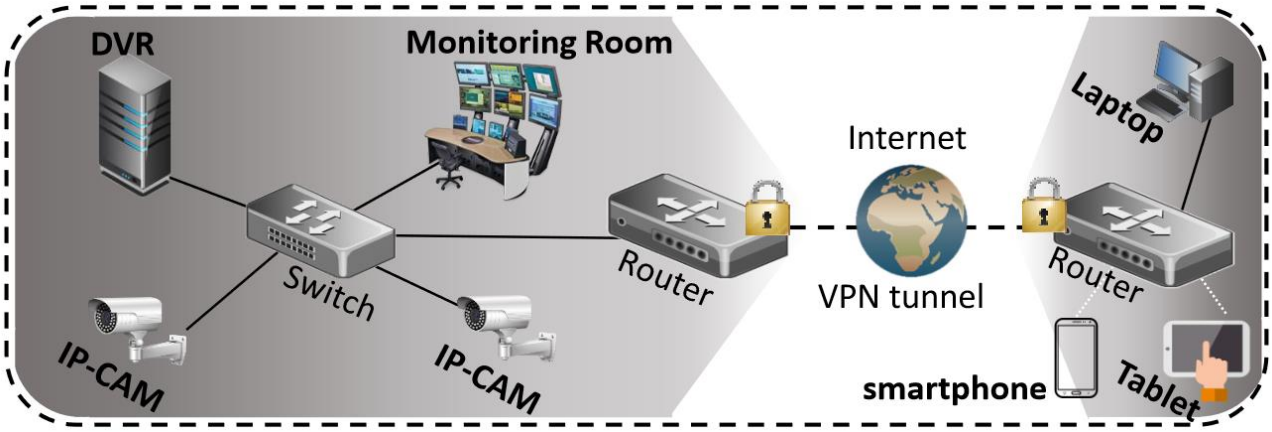


Рисунок – Віртуально замкнутий контур

Два найпоширеніші кодеки які використовують для систем відеоспостереження є H.264 і H.265. Відеокодек це програмне забезпечення, яке виконує функцію кодуванні і декодування цифрового відеосигналу. Кодування – це процес стиснення необробленого відеофайлу, що дозволяє зменшити розмір файлу майже без втрати інформаційної складової.

H.264 використовує блочно-орієнтовне кодування. Тобто він розвиває кожен кадр, на макроблоки(до 16x16 пікселів). На рис. 2.10 наведена схема макроблоків. Потім він використовує дані з поточного та попереднього кадрів для формування прогнозу руху, що у свою чергу, забезпечує більш ефективний процес кодування. Під час процесу декодування ці передбачення використовуються для реконструкції кожного макроблоку.

Рисунок 2.10 – Схема кодування H.264

H.265 він використовує одиниці дерева кодування(CTU), які не обов’язково мають однаковий розмір або форму. CTU можуть мати розміри від 4x4 пікселя і до 64x64 пікселів, що дозволяє програмі стискати дані набагато ефективніше. На рисунку 2.11 наведена схема CTU блоків. Крім боків різного розміру, кодек має більш ефективнішу технологію компенсації руху та передбачення.

Рисунок 2.11 – Схема кодування H.265

У табл. 2.2 наведено порівняння кодеків H.264 і H.265.

Таблиця 2.2 – Порівняння кодеків

	H.264(AVC)	H.265(HEVC)
Підтримувані формати контейнерів	mkv, mp4, qtff, asf, avi, mxf, ps, ts, m2ts, evo, 3gp, f4v	mkv, mp4, qtff, asf, avi, mxf, ps, ts, 3gp
Пропускна здатність для кодування відео у визначеній якості:		
480p	1,5 Мбіт/с	0,75 Мбіт/с
720p	3 Мбіт/с	1,5 Мбіт/с
1080p	6 Мбіт/с	4 Мбіт/с
4K	32 Мбіт/с	15 Мбіт/с
Максимальний FPS	59,94	300
Глибина кольору	8 біт	10 біт

В якості вибору кодеку для передачі відеосигналу, більше підходить H.265. Його головні переваги нижча пропускна здатність у порівнянні з конкурентом, що є дуже важливим при передачі сигналу через VPN мережу, де пропускна здатність є не високою. Єдиним недоліком є вищі вимоги для обладнання яке виконує функцію кодування і декодування.

2.6 Реалізація мережевої безпеки

2.6.1 Тріада інформаційної безпеки

Тріада інформаційної безпеки – це модель, яка є основою для розробки систем безпеки. Вона використовується для пошуку вразливостей і методів для створення рішень. Вона містить три основні компоненти:

1) Конфіденційність – вона передбачає використання обмеження доступу до інформації. Тільки довірені особи повинні мати доступ інформації, всім іншим заборонено дізнаватися про його вміст. Щоб досягти цього, доступ до інформації має контролюватися, щоб запобігти несанкціонованому обміну даними – навмисному чи випадковому.
2) Цілісність – це впевненість у тому, що інформація, до якої здійснюється доступ, не була змінена та справді відповідає призначенню. Цілісність даних підтримується, лише якщо вони автентичні, точні та надійні.
3) Доступність – означає, що будь-хто уповноважений на це, може отримати доступ до інформації та змінити її у відповідний проміжок часу.

Використання тріади інформаційної безпеки є необхідним, особливо тому, що кожен компонент є критичним. Однак це особливо корисно під час розробки систем, пов’язаних із класифікацією даних і керування дозволами та

привілеями доступу. [10]

2.6.2 Управління доступом

Після автентифікації користувача наступним кроком є переконатися, що він може отримати доступ лише до відповідних інформаційних ресурсів. Це робиться за допомогою контролю доступу.

Список контролю доступу (ACL) – його використовують для фільтрування пакетів на основі інформації в заголовку пакету. Тобто це список правил які можуть забороняти або дозволяти використовувати ресурси мережі: обмеження мережевого трафіку, керування потоком трафіку, забезпечення базового рівня безпеки, фільтрація трафіку, сканування вузлів у цілях доступу до мережевих послуг, надання пріоритету певним класам мережевого трафіку. На рис. 2.12 наведений приклад управління доступом для користувачів.

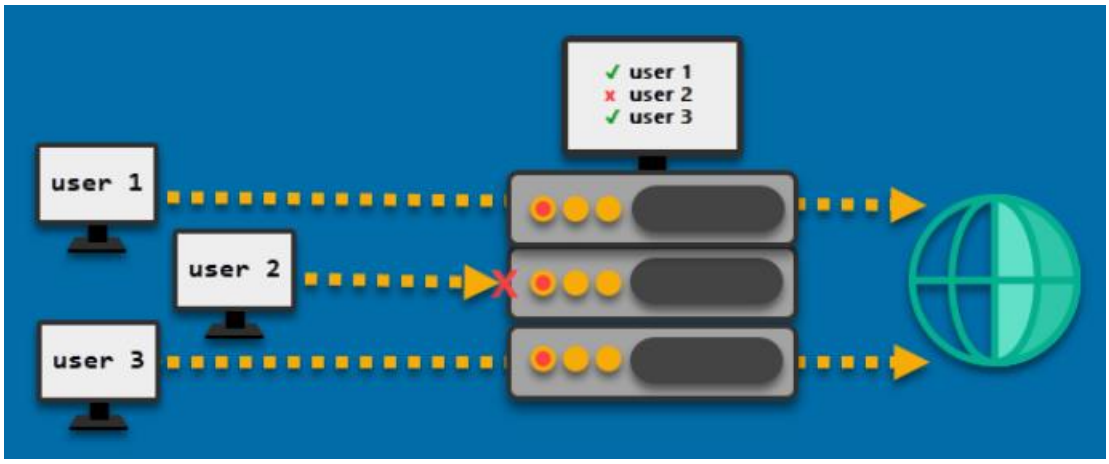


Рисунок 2.12 – Система управління доступом

ACL можна налаштувати для вхідної і вихідної фільтрації пакетів на маршрутизаторі:

- Вхідний – фільтрує пакети перед тим як направити пакети на вхідний інтерфейс. Він вигідний тим що позбавляє від додаткових витрати на пошук маршруту.

- Вихідний – фільтрує пакети після їх маршрутизації, не залежно від вхідного інтерфейсу. Найкраще використовувати коли один і той самий фільтри застосовується до пакетів, що надійшли від декількох вхідних інтерфейсів.

За замовчування ACL не налаштований на маршрутизаторі. І також фільтрація пакетів відбувається на 3 і 4 рівнях TCP/IP.

Існують наступні типи ACL:

- Стандартний – фільтрує трафік на основі IP-адреси джерела. Коли пакет намагається ввійти або залишити маршрутизатор, система перевіряє його IP-дані на відповідність правилам.
- Розширений – на відміну від стандартних списків контролю доступу, розширені ACL приймають правила на основі IP-адреси джерела і призначення. Крім того, розширені правила ACL можуть включати фільтрацію пакетів за типом протоколу, портами TCP або UDP тощо.
- Динамічний – це розширені списки з іменами, які містять правила ACL. Динамічний ACL вирішують проблеми, що виникають через зміну IP-адреси авторизованого хоста, наприклад, у разі фізичного переміщення довіреної машини. Для підтвердження особи клієнт повинен ввести свій логін і пароль. Якщо перевірка пройшла успішно, мережевий пристрій змінює свої правила доступу, щоб прийняти підключення з нової IP-адреси.
- Рефлексивний – у той час як стандартний ACL не відстежує сеанси, рефлективний ACL може обмежити трафік до сеансів, що надходять із хост-мережі. Рефлективний ACL не можна застосувати безпосередньо до інтерфейсу – замість цього він зазвичай вкладається в розширені іменований список доступу. Цей тип контролю доступу не підтримує програми, які змінюють номери портів під час сеансу. Наприклад FTP-клієнти.

- На основі часу – він дозволяє керувати доступом на основі часу. Наприклад організація може дозволити співробітникам доступ до певних місць в Інтернеті лише в обідній час.

Основною функцією ACL є захист мережі, але воно також корисний для інших аспектів контролю мережевого трафіку: блокування користувачів або трафік, спрощення ідентифікації хостів, покращення продуктивності мережі і допомого в запобіганні атак DoS і спуфінгу. [11]

2.6.3 Брандмауер

Брандмауери сьогодні є першою лінією захисту від серйозних атак, що впливають як на традиційні, так і на сучасні мережі, забезпечують захист внутрішніх мереж від зовнішніх(і ненадійних) мереж. Застосування ефективного набору практик і політик безпеки справді може забезпечити безпеку цих систем. Брандмауер мають дуже важливу функцію захисту, фільтрації та контроль всього трафіку, який надсилається та отримується з комп'ютера, внутрішніх локальних мереж або глобальної локальної мережі від несанкціонованих вторгнень або зовнішніх атак. На рис. 2.13 наведений приклад роботи брандмауера.

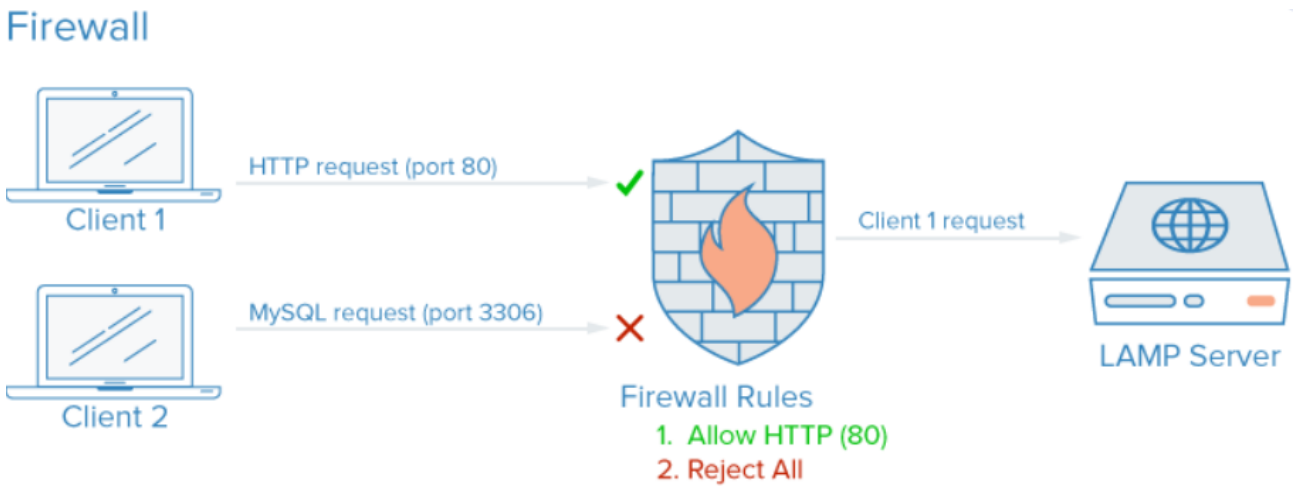


Рисунок 2.13 – Архітектура брандмауера

Брандмауери можуть являти собою апаратне забезпечення або програмне забезпечення пристрою, фільтрувати та контролювати інформацію, що надходить з Інтернету до приватної мережі, чи окремого комп'ютера. Брандмауер дозволяють вхід і/або вихід лише до даних, які вважаються безпечними та нешкідливими. Дані дозволені через серію інтернет протоколів(TCP/IP, UDP, ICMP тощо), у який кожен комп'ютер ідентифікується за допомого IP-адреси. Ці дані також називаються «пакетами даних», і ці пакети мають такі заголовки, які їх ідентифікують:

- IP-адреса відправника пакету
- IP-адреса одержувача пакетів
- Тип пакету
- Номер порту(який пов'язаний із певною службою або мережевою програмою)

Також брандмауери часто групуються в мережеві брандмауери та брандмауери на основі хоста: перші зазвичай працюють на апаратному забезпеченні та можуть обробляти дані з великої кількості серверів в одній або кількох мережах. Останні налаштовуються безпосередньо на хості або хмарному сервері, обмежуючи контролем трафіку, який генерується та доставляється на машину.

Брандмауери працюють на наступних рівнях OSI: мережевий, сеансовий і прикладний.

Найпростішим типом брандмауера є з фільтрацією пакетів, який працює на 3 рівні OSI. За допомого IP створюється набір правил, які застосовуються до мережевого з'єднання, щоб приймати або відхиляти трафік. Брандмауери з фільтрацією пакетів дозволяють або забороняють трафік у мережевих IP протоколах, у джерелі та призначенні IP-адрес, включаючи поти та інші параметри заголовків TCP.

Цей брандмауер досить простий в налаштуванні, і він може допомогти відкинути весь непотрібний трафік, наприклад шкідливі пакети, що передаються через небезпечні порти, і джерело потенційної атаки. Однак,

оскільки правила фільтрації пакетів в загалом базується на IP-адресах, це не забезпечує повного захисту мережі.

Брандмауери перевірки стану працюють на 5 рівні моделі OSI. На відміну від фільтрації пакетів, перевірка з урахування стану може зберігати всю попередньо оброблену інформацію про пакети та перевіряти інформацію про вхідні та вихідні пакети, одночасно керуючи загрозами від пакета до пакета. З цієї причини цей брандмауер часто називають брандмауером динамічної фільтрації пакетів. Потенційною перевагою використання цього брандмауера є просте налаштування внутрішньої мережі, що дозволяє адміністраторам мережі встановлювати певні порти (і трафік), які вони хочуть залишати відкритим. Це запобігає ризикам спуфінгу та деяким методам злому, таким як сканування портів.

І останній брандмауер є програмного проксі, який є найбільш ефективним на сьогоднішній день. Проксі-сервер програми забезпечує безпеку на 7 рівні OSI. Він слідує механізму стану, але на відміну від перевірки стану, він працює як проксі-сервер мережі. Тобто він ж шлюзом, з поведінкою «людина посередині» від сервера до клієнта. Іншими словами, цей брандмауер не дозволяє будь-які пакети безпосередньо надсилати з програми до користувача і навпаки. Таким чином, проксі-сервер програми може перекладати адреси та виконувати будь-який додатковий контроль, перш ніж дозволити підключення до мережі.

Проксі-сервер програми забезпечує глибоку перевірку пакетів, запобігаючи атакам спуфінгу та іншим методам злому, таким як брандмауер перевірки стану, аде зберігаючи прийнятну продуктивність мережі. Крім того, проксі-сервер програми може блокувати небезпечні команди SQL та інші зловмисні атаки веб-програм, забезпечуючи таким чином ефективний рівень безпеки для різних мережевих топології, оптимальну ізоляцію безпеки та рівні анонімності. [12]

2.6.4 RADIUS

RADIUS – це мережевий протокол, який зазвичай використовується для автентифікації та авторизації користувачів, які намагаються підключитися до вбудованих маршрутизаторів, серверів та програмного забезпечення. Він визначає чи може користувач отримати доступ до локальної чи віддаленої мережі, визначає які привілеї йому надано в цій мережі, а потім записує активність користувача, коли він підключений до мережевого ресурсу.

Протокол використовує модель клієнт-сервер, і його три основні компоненти включають:

1) Клієнт – це пристрій, який шукає доступ до мережі
2) Сервер доступу до мережі – шлюз між користувачем і мережею.
3) Сервер RADIUS – який відповідає за автентифікацію, і гарантує, що користувачеві дозволено доступ до мережі з відповідним рівнями дозволів. Цей сервер також може надавати облікові функції.

В якості RADIUS-сервера може виступати маршрутизатор у якого вбудована дана функція. На рис. 2.14 наведений приклад роботи RADIUS-сервера.

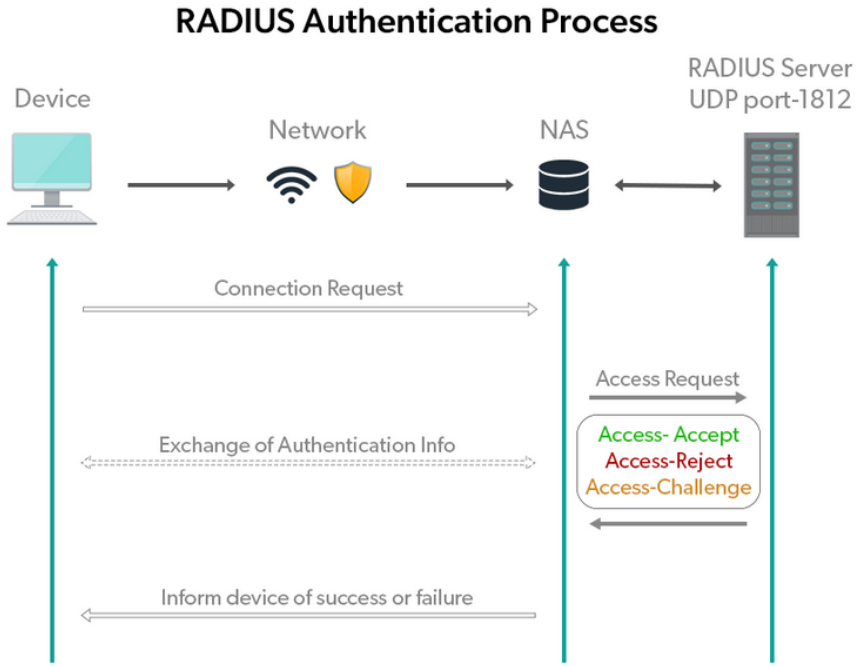


Рисунок 2.14 – Приклад роботи RADIUS

Принцип системи наступний, є користувач якому потрібен доступ до мережевого сервісу(наприклад NAS сервер). Клієнт відправляє інформацію о собі (ім’я користувача, пароль, тощо) до потрібного серверу разом із запитом доступу. Після того як сервер отримав запит, він просить визначити у RADIUS-серверу, чи дозволено користувачеві доступ до певного ресурсу, що називається автентифікацією. Якщо збіг встановлено, тоді сервер приймає користувача, надсилаючи підтвердження. Якщо збіг не встановлено, користувача буде відхиллено. Наприкінці транзакції сервер передає облікові дані до RADIUS-серверу, який документує транзакцію та дозволяє зберігати або пересилати дані транзакції. [13]

Висновки до розділу 2

В другому розділі були представлені теоретичні відомості щодо побудови локальної мережі для підприємства.

Були розглянуті протоколи і пристрої 2 і 3 рівня OSI, а саме комутатори і маршрутизатори, технологія PoE яка дозволяє подавати живлення через Ethernet кабель. Розглянув принцип розмежування мережі за допомогою VLAN.

За допомогою VPN можна зробити безпечне з’єднання між об’єктами, і досягаються такі аспекти як конфіденційності, цілісності та автентифікації. Так як безпечний зв’язок між об’єктами є дуже важливим. В якості протоколу для передачі трафіку було обране opensource рішення, а саме OpenVPN/

Розглянув принцип роботи і побудови системи диспетчерського управління і збору даних (SCADA) яка дозволить автоматизувати роботу котельної і зменшити використання ресурсів за допомогою інтелектуальної системи керування.

Був розглянутий принцип роботи системи відеоспостереження і можливості його застосування. Так як система є одним із елементів безпеки і

моніторингу за важливими об’єктами. Для передачі відеосигналу був обраний кодек H.265, який має невисокі показники пропускної здатності.

І також розглянуті методи реалізації мережевої безпеки на об’єктах, так як: система управління доступом, брандмауер, протокол RADIUS. Всі вони дозволяють зменшити імовірність втручання зловмисників в систему підприємства.

3 МОДЕРНІЗАЦЯ МЕРЕЖІ ЦЕНТРАЛЬНОГО ОФІСУ

3.1 Вимоги до локальної мережі

Під час модернізації локальної мережі офісу комунального підприємства повинна відповідати наступним вимогам:

- гарантувати передачу різного типу трафіку
- масштабування мережі без заміні обладнання і зміни в архітектурі, і також мати запас ємності по портам не менше 20%
- система аутентифікації і авторизації адміністраторів до спеціального мережевого обладнання
- передача пакетів в області протоколу IPv4, забезпечення IPv4 адресацій на інтерфейсах, а також можливість управління по IPv4, і також можливість підтримки протоколу IPv6
- користувачі мережі повинні мати безперебійний доступ до сервісів протягом робочого часу
- комунікаційне середовище реалізується на базі сучасних версій протоколу Ethernet

Мережеве обладнання повинно відповідати наступним вимогам:

- забезпечення сегментації мережі по технології VLAN
- захист мережі на рівні L2, від виникнення STP
- підтримка списку контроля доступу і також обмеження доступу, і забезпечення можливості підключення до порту на основі MAC-адреси робочий станції
- підтримка протоколів мережевої аутентифікації і авторизації
- підтримка протоколу управління (SSH)
- достатня кількість портів для підключення користувачів і периферійного обладнання
- з підтримкою PoE у випадку підключення камер відеоспостереження

Також є вимоги до встановлення бездротової мережі в офісі. Базою архітектури бездротової мережі вважається використання бездротових точок доступу. Узгодження контролю доступу до мережі, і можливості налаштування гостьової точки доступу для відвідувачів.

Займаючись питаннями телекомунікації потрібно також не забувати про систему безперебійного живлення. Під час зникнення живлення система безперебійного живлення повинна забезпечувати живленням мережевого телекомунікаційного і серверного обладнання на протязі 20 хвилин. Потужність акумулятора безперебійного живлення вибирається з розрахунку енергоживлення обладнання і резервом в 20%.

3.2 Розробка плану мережі

План мережі розробляється для 3 поверхової будівлі комунального підприємства «Покровськтепломережі». Ми маємо 48 робочих місць і з 16 робочими кабінетами, повний план будівлі винесено у ДОДАТОК Б. В кабінеті може знаходитися різна кількість робочих місць від 1 до 6. Кожен співробітник на робочому місці повинен мати доступ до мережі як локальної-кооперативної так і до зовнішньої. Також особа повина мати доступ до свої даних і пакету робочих програм, кооперативної пошті, до друкуючих пристроїв (МФУ). Крім цього, є необхідність в організації захисту, а саме монтажу камер відеоспостереження на будівлі і по поверхам. У табл. 3.1 наведено розподіл відділів між поверхами і кількості в них робітників.

Підприємство в офісі має наступний розподіл по відділам:

Таблиця 3.1 – Відділи і кількість людей

№	Відділ	Поверх	Кількість
1	Диспетчер	1	1
2	Охорони праці	1	2
3	Керівництво і приймальня	2	4
4	Енергетики	2	5
5	Конференц-зал	2	-
6	Виробничий	3	12
7	Плановий-економічний	3	5
8	Бухгалтерія	3	7
9	Юридичний	3	3
10	Абонентський	3	5
11	Відділ кадрів	3	1
12	Забезпечення	3	3

На рис. 3.1 наведено розподілення відділів в будівлі комунального підприємства:

Рисунок 3.1 – Розподілення відділів в будівлі

На підприємстві будуть використовуватися наступні мережеві рішення:

- Система відеоспостереження
- Маршрутизатор з функцією VPN для зв’язку з іншими об’єктами
- Міжмережевий екран
- NAS сервер для зберігання файлів і бекапів
- Сервер з базою даних(бухгалтерія, данні абонентів)

Отже мережа буде будуватися за топологією зірка, де до кожного комутатору будуть підключатися кінцеві пристрої(робочі станції, МФУ, тощо) і також бездротові точки доступу. А далі кожний комутатор буде підключений до головного комутатору, який вже з’єднаний з маршрутизатором через брандмауер.

Система відеоспостереження буде складатися з самого сервера який буде відповідати за збереження відеозаписів і перегляд самих камер. Загальна кількість камер буде 22 пристрою. Всі вони будуть підключені до виділеного комутатора який підтримує технологію PoE. На рис. 3.2 наведена узагальнена схема мережі.

Також до центрального комутатору під’єднані три сервера, які будуть виконувати наступні функції: Повний план мережі винесено у ДОДАТОК В.

- перший сервер це бази даних бухгалтерій і абонентського відділу і займається обробкою даних з котельних
- другий NAS сервер який відповідає за збереження файлів і бакепів робочих машин
- третій сервер відповідає за систему відеоспостереження

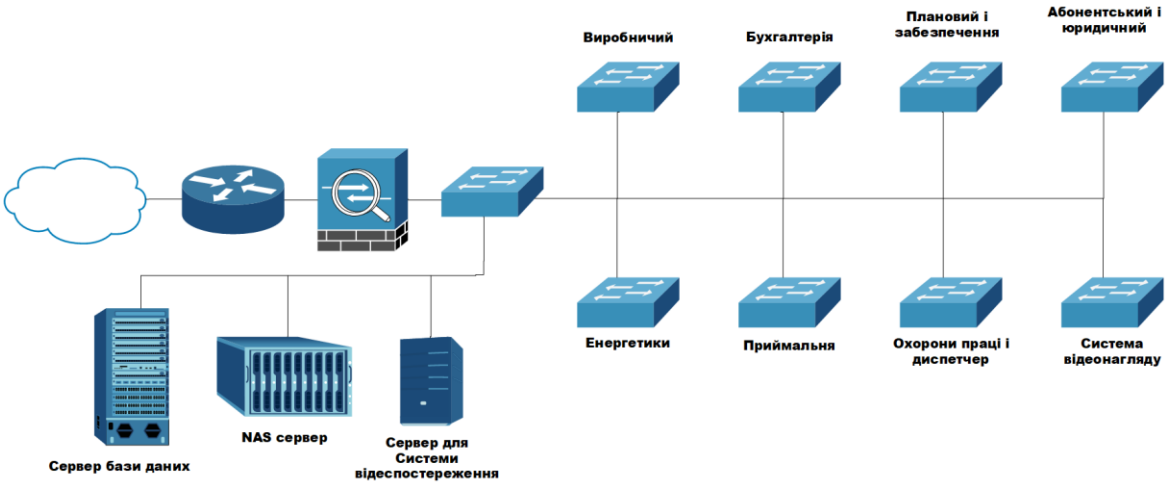


Рисунок 3.2 – Узагальнена схема мережі

3.3 Вибір устаткування

Дана мережа повинна повністю відповідати всім вимогам і мати високі показники надійності. Вище були описані всі критерії до мережі і також складений детальний план з усіма пристроями які будуть під’єднані до мережі. Тепер на основі всіх даних потрібно підібрати устаткування.

Для того щоб всі мережеві прилади працювали надійно і мали найкращу сумісність, потрібно обирати прилади одного вендора. Враховуючи потреби і параметри даної мережі, і вибору устаткування компанії мій вибір зупинився на «Ubiquiti». Ця компанія є відносно молода яка в теперішній час представляє велику кількість мережевого обладнання на ринку з високою якістю продукції. Також потужні можливості в налаштуванні і моніторингу мережевого трафіку.

В ролі маршрутизатору був вибраний «UniFi Security Gateway PRO (USG-PRO-4)» з будованим можливостями брандмауера і VPN. На рис. 3.3 наведено вигляд маршрутизатора, а в табл. 3.2 основні технічні характеристики.

Рисунок 3.3 – Маршрутизатор UniFi Security Gateway PRO (USG-PRO-4)

Таблиця 3.2 – Основні характеристики UniFi Security Gateway PRO (USG-PRO-4)

Порти Gigabit Ethernet	2 x 10/100/1000 Mbps
Combo-порти	2 x 10/100/1000 Mbps RJ45/SFP
Додаткові порти	USB, RJ45 Serial Port
Пропускна спроможність	4 Gbps
Пакетна продуктивність	2.4 Mpps
Процесор	Dual-Core 1 GHz, MIPS64 with Hardware Acceleration for Packet Processing
Обсяг ОЗП	2 GB
Флеш пам’ять	4 GB
Напруга споживання	max 40W
Операційна система	UniFi

Даний роутер також має такі можливості як: VPN Server, VLAN, QoS для VoIP і відео, моніторинг і аналіз мережі, веб-інтерфейс з налаштуванням мережі.

В якості комутатора була вибрана наступна модель: «UniFi Switch US-24-500W» з можливостями PoE. На рис. 3.4 наведено вигляд комутатора, а в табл. 3.3 основні технічні характеристики.

Рисунок 3.4 – Комутатор UniFi Switch US-24-500W

Таблиця 3.3 – Основні характеристики UniFi Switch US-24-500W

Порти Gigabit Ethernet	24 x 10/100/1000 Mbps
Порти SFP	2 x 1000 Mbps
Пропускна спроможність	26 Gbps
Пакетна продуктивність	38.69 Mpps
Комутаційна спроможність	52 Gbps
Power Over Ethernet (PoE)	POE+ IEEE 802.3af/at (Pins 1, 2+; 3, 6) 24VDC Passive PoE (Pins 4, 5+; 7, 8-)
Максимальна потужність на PoE+	34.2 W
Діапазон напруги в режимі 802.3at	50-57 V
Максимальна потужність Passive PoE	17 W
Діапазон напруги в режимі Passive PoE	20-27 V
Додаткові порти	RJ45 Serial Port
Операційна система	UniFi

В якості бездротових точок доступу були вибрані наступна модель пристрою: «UniFi 6 Lite (U6-Lite)» який має можливість підключення до мережі за допомогою PoE. На рис. 3.5 наведено вигляд бездротової точки доступа , а в табл. 3.4 основні технічні характеристики.

Рисунок 3.5 – Бездротова точка доступу UniFi 6 Lite (U6-Lite)

Таблиця 3.4 – Основні характеристики UniFi 6 Lite (U6-Lite)

Швидкість Wi-Fi	1500 Mbps
Порти Gigabit Ethernet	1 x 10/100/1000 Mbps
Джерело живлення	Живлення від 802.3af
Максимальна потужність споживання	12 W
Підтримка живлення	44-57 Vdc
Частота роботи	2.4 GHz/5GHz (дводіапазонний)
Потужність передавача	2.4 GHz – 23 dBm 5 GHz – 17 dBm
Коефіцієнт посилення	3 dBi
Wi-Fi стандарт	Wi-Fi 6 (802.11 ax)
Підтримка MIMO	MU-MIMO 2x2

Для системи відеоспостереження були вибрані наступні IP-камери UniFi Video Camera G3 Bullet (UVC-G3-BULLET), які мають можливість підключатися до мережі за допомогою 802.3af та 24V Passive PoE. На рис. 3.6 наведено вигляд IP-камери, а в табл. 3.5 основні технічні характеристики.

Рисунок 3.6 – IP-камера UniFi Video Camera G3 Bullet (UVC-G3-BULLET)

Таблиця 3.5 – Основні характеристики UniFi Video Camera G3 Bullet (UVC-G3-BULLET)

Порти Fast Ethernet:	1 x 10/100Mbps
Потужність	4 W З додатковим ІЧ модулем – 9 W
Розширення відео	1080p Full HD
Температура роботи	-20 – 50 ºС
Кути огляду	85° (H), 44.8° (V), 98.1° (D) 72° (H), 42.9° (V), 80.4° (D)
Об’єктив	f = 2.8 мм
Відеокодек	H.265

Також для системи відеоспостереження потрібен сервер який буде відповідати за запису та зберігання відео записів. Для цього було вибрано наступний сервер: UniFi Application Server XG (UAS-XG). Він має можливість на підключення двох жорстких дисків з великим об’ємом пам’яті. На рис. 3.7 наведено вигляд серверу відеоспостереження, а в табл. 3.6 основні технічні характеристики.

Рисунок 3.7 – Сервер UniFi Application Server XG (UAS-XG)

Таблиця 3.6 – Основні характеристики серверу UniFi Application Server XG (UAS-XG)

Процесор	Xeon-D 1521 4-core, 8 thread, 2.4 GHz
Обсяг ОЗП	32 GB
Flash пам’ять	M.2 SSD 120 GB
Жорсткий диск	2 x 2 TB HDDs
Інтерфейси	2 x 10GBase-T 1G/10G RJ45

	1GBase-T RJ45 IMPI Interface 2 x USB 2.0 2 x USB 3.0 VGA Display port
Операційна система	Ubuntu 16.04

Для зберігання файлів, і бекапів системи в мережі потрібен NAS-сервер. В якості серверу було вибрано наступне рішення: Synology RackStation RS422+. На рис. 3.8 наведено вигляд NAS-серверу, а в табл. 3.7 основні технічні характеристики.

Рисунок 3.8 – NAS-сервер Synology RackStation RS422+

Таблиця 3.7 Технічні характеристики NAS-серверу Synology RackStation RS422+

Кількість слотів для накопичувачів 3.5”	4 шт.
Підтримка RAID	RAID 0, RAID 1, RAID 5, RAID 10, JBOD, Basic, SHR, RAID 6
Інтерфейси	2 x 10/100/1000 Mbps RJ45 1 x USB 3.2
Процесор	AMD Ryzen R1600 2-core, 4 thread 2.6 GHz
Обсяг ОЗП	2 GB
Операційна система	DiskStation Manager

Сервер DELL EMC R240 який буде відповідальний за збереження і обробку бази даних бухгалтерії, абонентського відділу і даних с котельних. На рис. 3.9 наведено вигляд центрального серверу, а в табл. 3.8 основні технічні характеристики.

Рисунок 3.9 – Сервер DELL EMC R240

Таблиця 3.8 – Технічні характеристики серверу DELL EMC R240

Процесор	Intel Xeon E-2124 4-core 3.3 GHz
Обсяг ОЗП	8 GB, max – 64 GB
Кількість слотів для накопичувачів 3.5”	4 шт.
Інтерфейси	2 x 10/100/1000 Mbps RJ45 2 x USB 2.0 2 x USB 3.0 VGA COM – port
Операційна система	Ubuntu 18.04

3.4 Налаштування мережі

3.4.1 Налаштування VLAN

Для початку налаштування мережі, потрібно налаштувати пул адрес і надання відповідного VLAN для кожного відділу. Центральний офіс буде мати наступну мережу 192.168.0.0/24, з шлюзом 192.168.0.1. В табл. 3.9 буде предоставле розподіл адрес між робочими станціями між відділами. А на рис. 3.10 наведено зображення налаштування VLAN на маршрутизаторі.

Таблиця 3.9 – Розподіл адрес в центральному офісі

Відділ\місце	Адреса/пул адрес	VLAN
Шлюз	192.168.0.1	-
Сервери	192.168.0.2-4	1
Виробничий	192.168.0.5-19	31
Бухгалтерія	192.168.0.20-9	32
Плановий	192.168.0.30-6	33
Забезпечення	192.168.0.37-41	34
Кадрів	192.168.0.42	35
Абонентський	192.168.0.43-50	36
Юридичний	192.168.0.51-55	37
Енергетики	192.168.0.56-64	21
Приймальня	192.168.0.65-70	22
Охорони праці	192.168.0.71-74	11
Диспетчер	192.168.0.75-76	12
Wi-Fi	192.168.0.100-200	10
Відеоспостереження	192.168.0.77-99	20

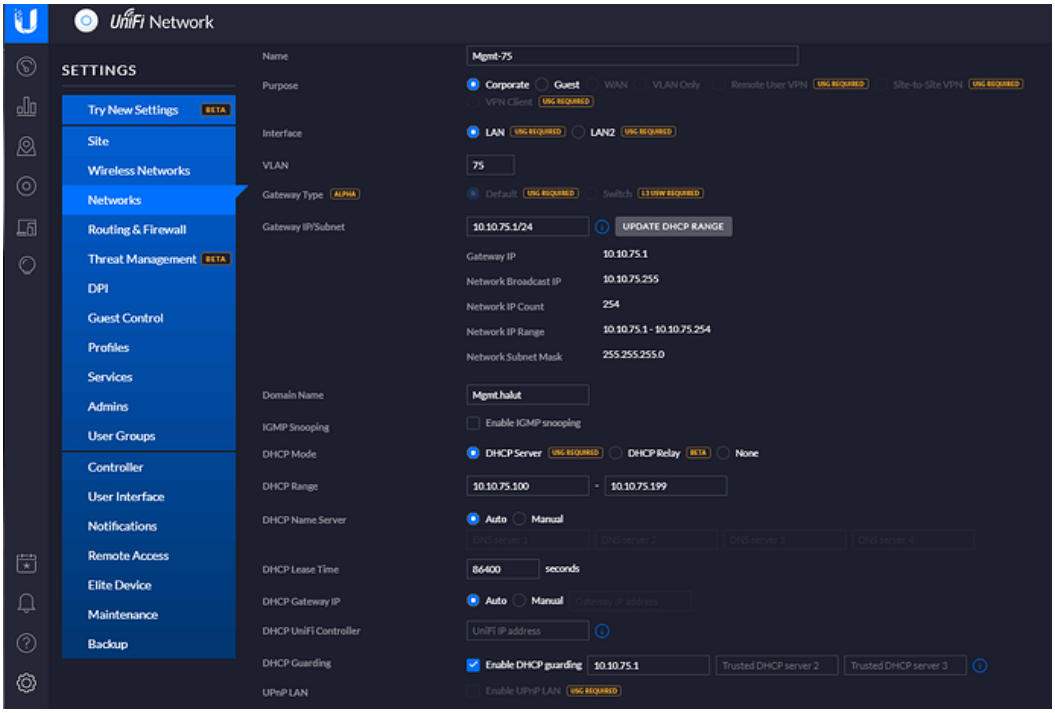


Рисунок 3.10 – Налаштування VLAN в UniFi

Операційна система UniFi надає налаштувати для VLAN мережі наступні параметри: назва мережі, тип мережі, інтерфейс, номер VLAN, діапазон адресів для DHCP.

Головна мета налаштування VLAN в мережі є розділення відділів між

собою, щоб кожен з них не мав доступу до інших. Єдине що кожен відділ має доступ до серверів для свої потреб.

3.4.2 Налаштування VPN

На маршрутизаторі потрібно налаштувати VPN для того щоб інші об’єкти підприємства могли з’єднуватися з центральним офісом. В якості протоколу для VPN мережі було обрано OpenVPN який є відритим рішенням і має найвищі показники безпеку, продуктивність і надійність в порівняні з L2TP/IPSec і PPTP.

На рис. 3.11 наведено налаштування RADIUS-серверу на маршрутизаторі.

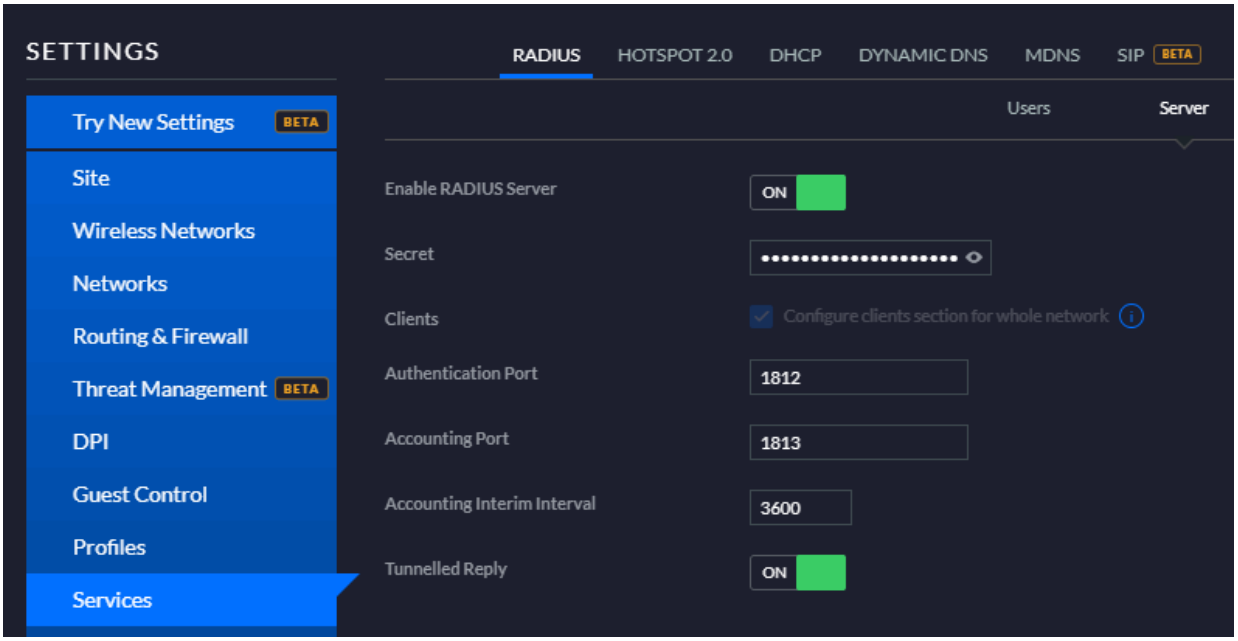


Рисунок 3.11 – Налаштування RADIUS

В пункті «Користувачі» потрібно добавити користувачі OpenVPN. Вказуємо інший VLAN з міркувань безпеки. На рис. 3.12 наведено налаштування користувача OpenVPN.

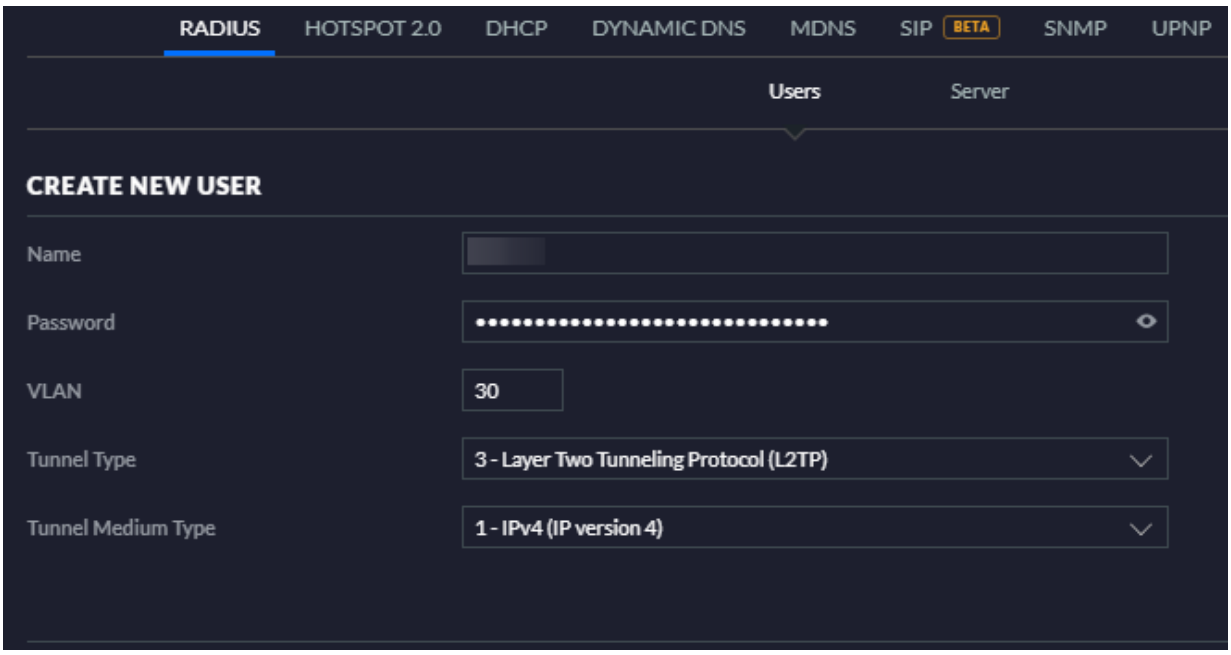


Рисунок 3.12 – Добавлення користувача OpenVPN

Для подальшого налаштування генерацію ключів за допомогою easy-rsa, потрібно увімкнути і налаштувати підключення SSH до маршрутизатору. На рис. 3.13 наведено налаштування SSH.

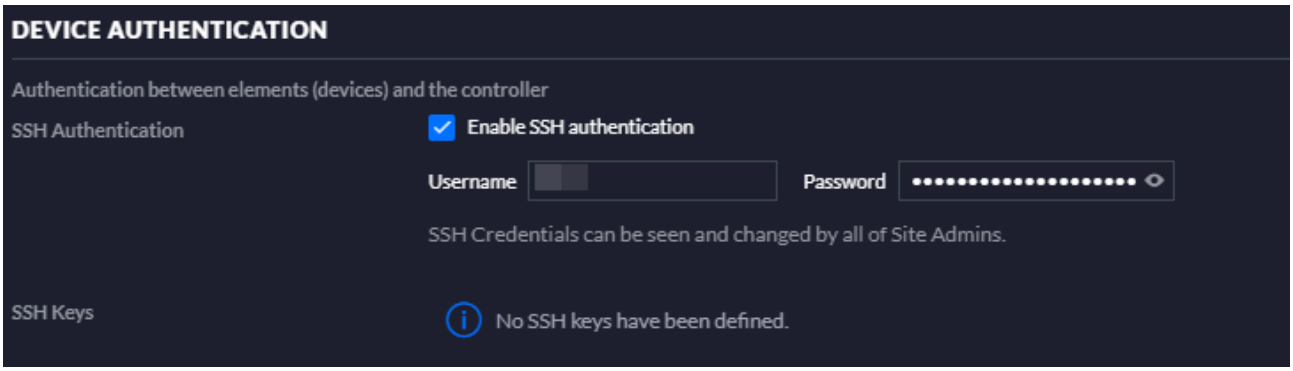


Рисунок 3.13 – Налаштування SSH

Повна генерація ключів для OpenVPN з командами винесено у ДОДАТОК Г. Де виконуються наступні дії: встановлення easy-rsa, ініціалізація PKI та створення сертифікатів і ключів ЦС, налаштування OpenVPN і збереження всіх змін.

Тепер є можливість створення VPN мережі на маршрутизаторі. Створюємо VPN типу Site-to-Site щоб у нас була можливість підключати

локальні мережі інших об’єктів. На рис. 3.14 наведено створення VPN мережі на маршрутизаторі.

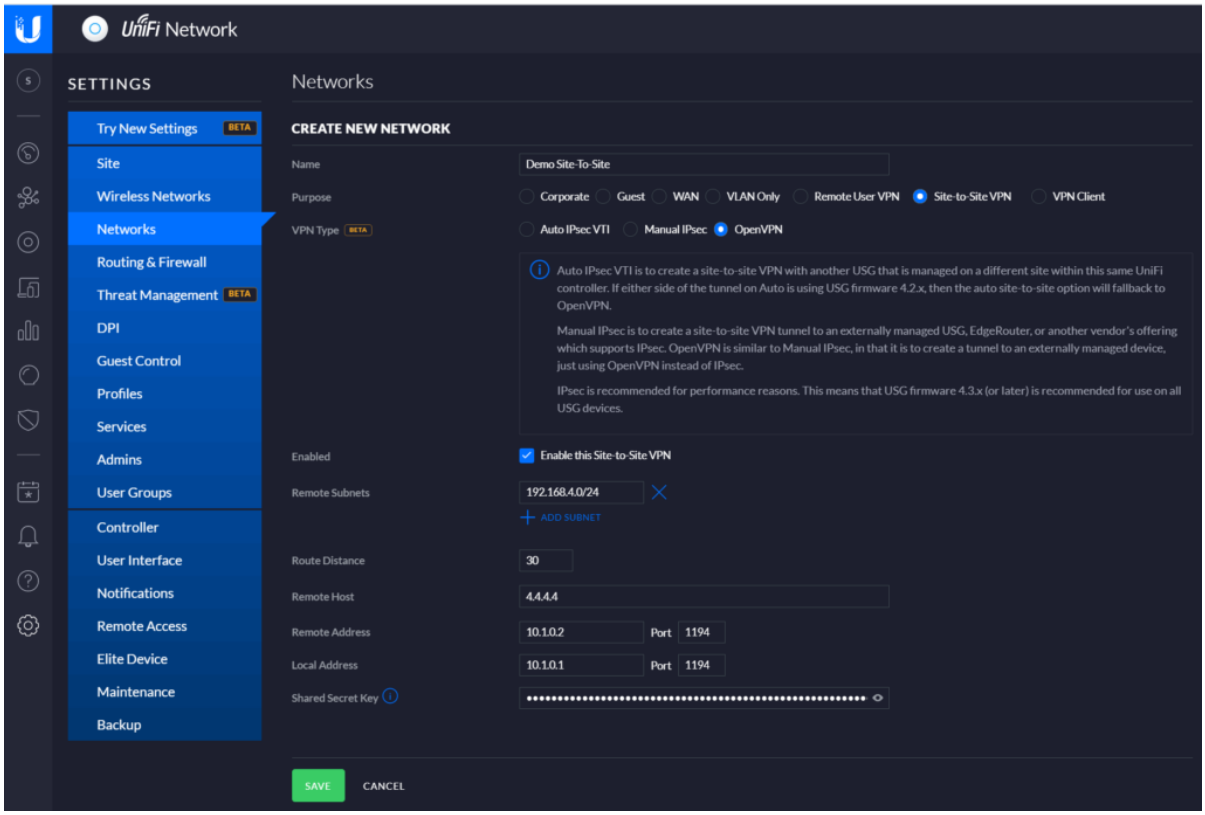


Рисунок 3.14 – Налаштування VPN на маршрутизаторі

Після створення і налаштування протоколу OpenVPN потрібно налаштувати правила брандмауера. Так як створений віртуальний інтерфейс vtun0 не відноситься до жодної групи інтерфейсів(WAN, LAN, GUEST). Щоб була можливість підключати інші мережі. І туди ми можемо добавити всі адреси об’єктів які будуть підключатися до нашої мережі. На рис. 3.15 наведено створення групи правил для VPN.

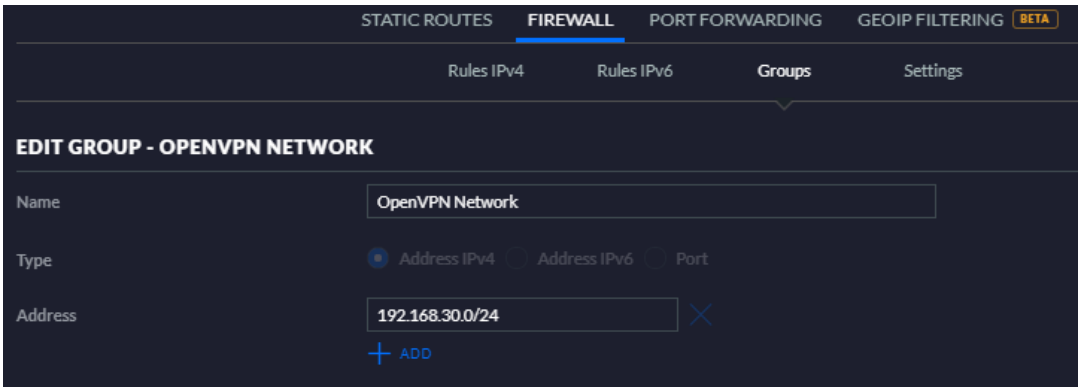


Рисунок 3.15 – Створення групи для VPN в брандмауере

Далі створюємо правило в LAN IN, щоб надати доступ до мережі користувачам VPN. На рис. 3.16 наведено створення правила для VPN.

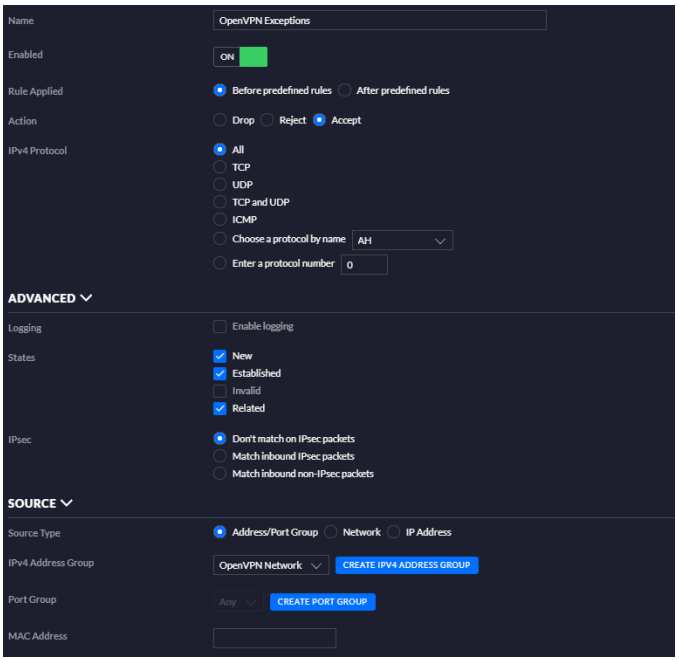


Рисунок 3.16 – Створення правило яке дозволяє з’єднання в брандмауері

Після створення правила, можна побачити в групі створені правила. На рис. 3.17 можна побачити створене правило.

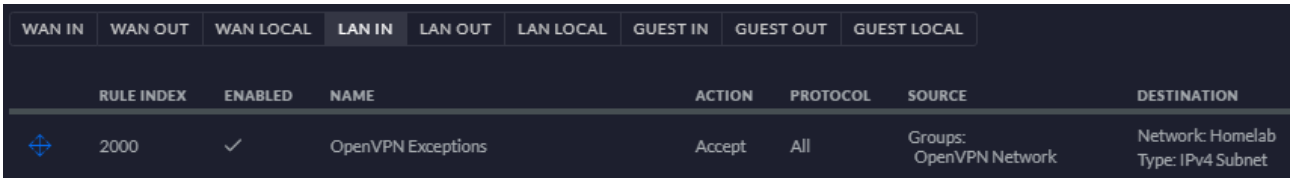


Рисунок 3.17 – Створене правило в LAN IN

Також потрібно створити правило яке буде відкидати будь-які з’єднання через OpenVPN яке не відноситься до наших об’єктів у тому випадку якщо зловмисник отримає дані для підключення. На рис. 3.18 наведено створення забороненого правила.

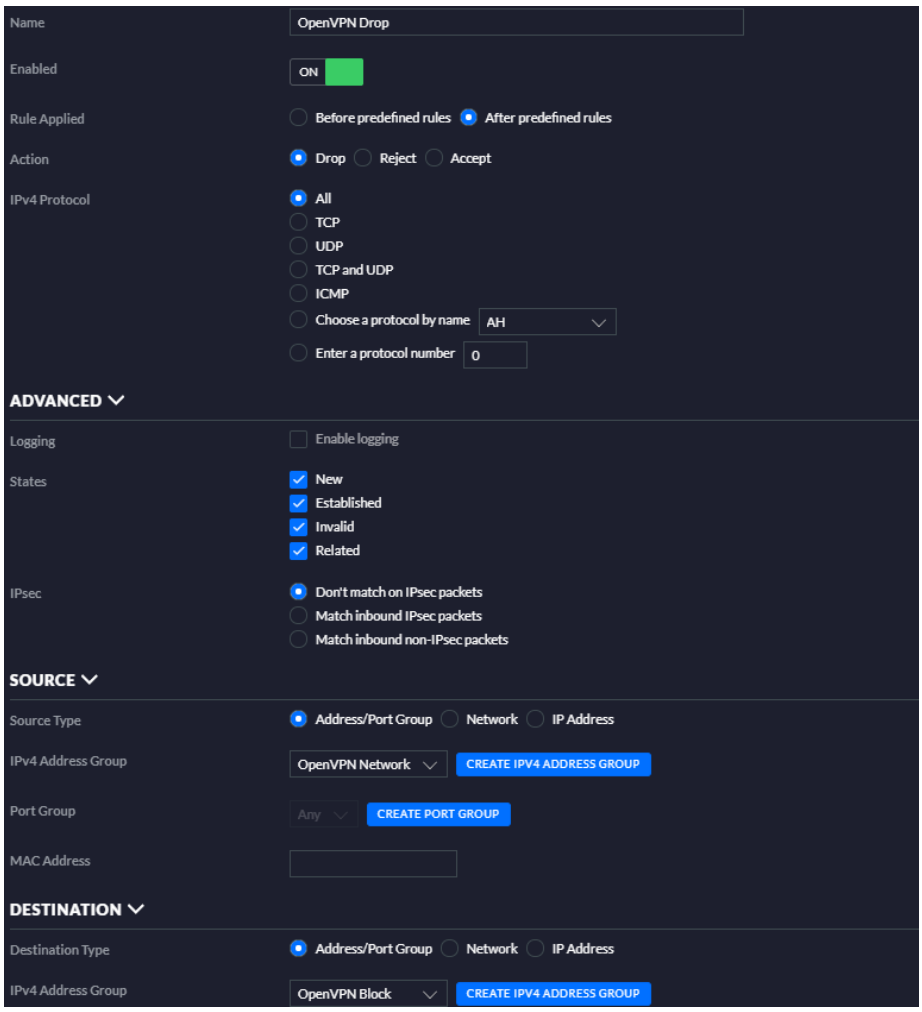


Рисунок 3.18 - Створення правило яке забороняє з’єднання інших користувачів в брандмауері

І останнє в налаштуванні в брандмауері для VPN, але менш важливе. Потрібно створити наступне правило LAN OUT, щоб забезпечити отримання вихідних пакетів. На рис. 3.19 наведено створення правила для вихідного трафіку.

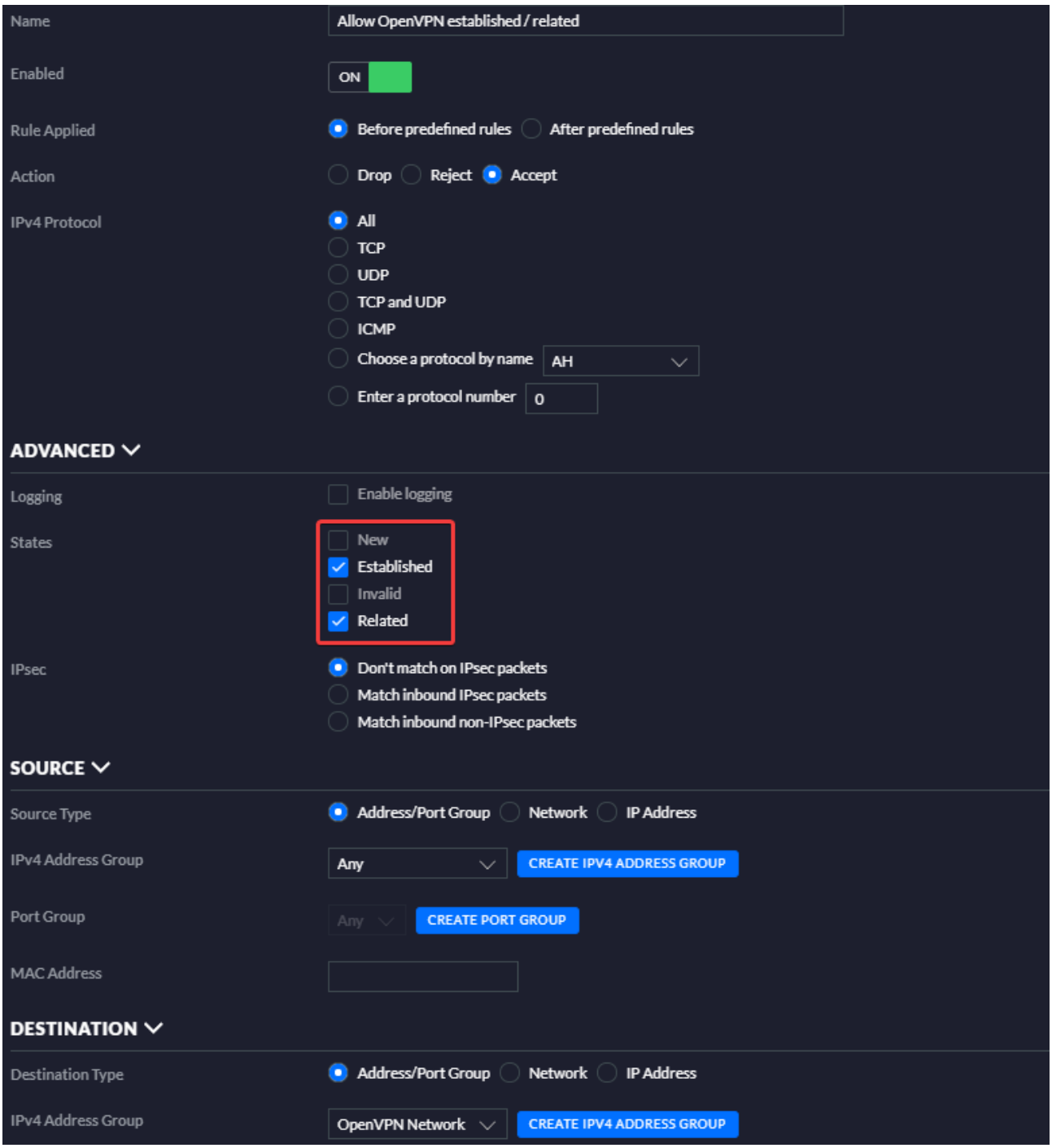


Рисунок 3.19 – Створення правила в LAN OUT

Після всіх налаштувань потрібно перевірити роботу протоколу OpenVPN. Для цього нам потрібно здійснити підключення з іншої мережи за допомогою програмного забезпечення від OpenVPN яке можна встановити на Windows 10. На рис. 3.20 наведено працездатність VPN з’єднання.

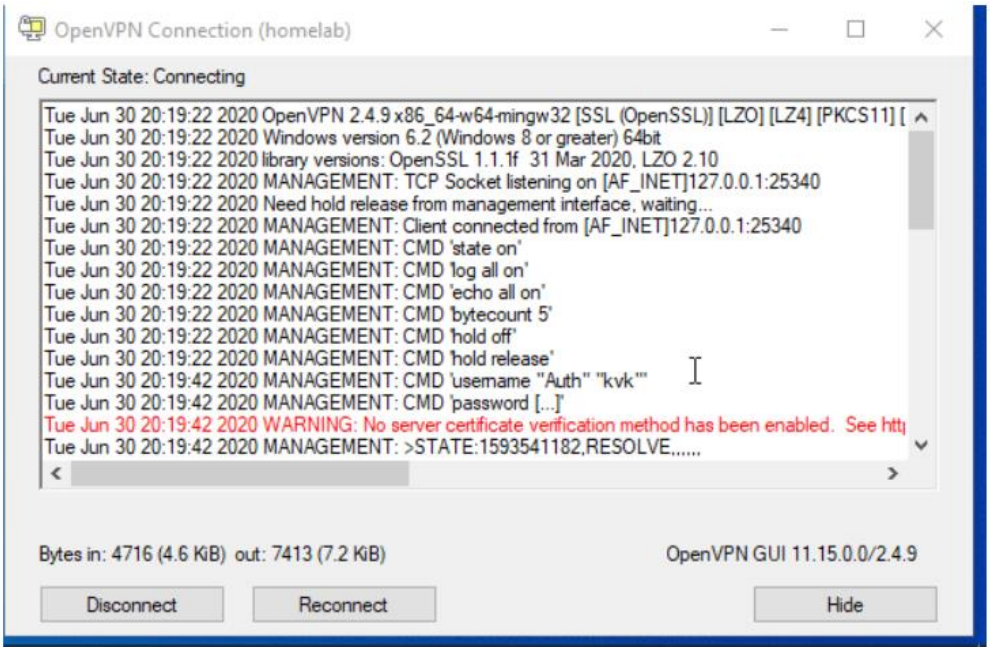


Рисунок 3.20 – Перевірка роботи OpenVPN на персональному комп’ютері

3.4.3 Налаштування системи відеоспостереження

Всі 22 камери відеоспостереження будуть підключені до одного комутатора, і з’єднанні вони будуть за допомогою PoE. Тобто нам не потрібно буде підводити окремо лінію живлення до камери, так як живлення буде відбуватися через кабель Ethernet.

Після підключення камер до мережі, ми відразу на сервері відеоспостереження можем побачити підключені до мережі камери, і всі їх мережеві параметри такі як: MAC-адреса, IP-адреса і швидкість передачі. На рис. 3.21 наведено перелік камер які підключені до мережі.

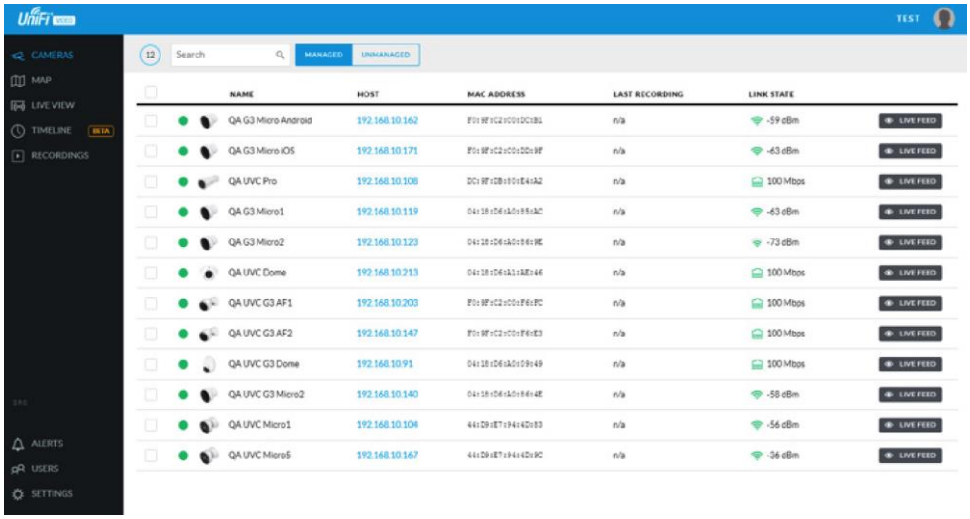


Рисунок 3.21 – Перелік камер які підключені до локальної мережі

Сервер відеоспостереження має наступні можливості. Один із головних це режим Live View, дозволяє переглядати відео з ками в реальному часі. Це використовується охороною і іншими працівниками для контролю за безпекою і виробничими процесами. На рис. 3.22 наведено режим Live View.

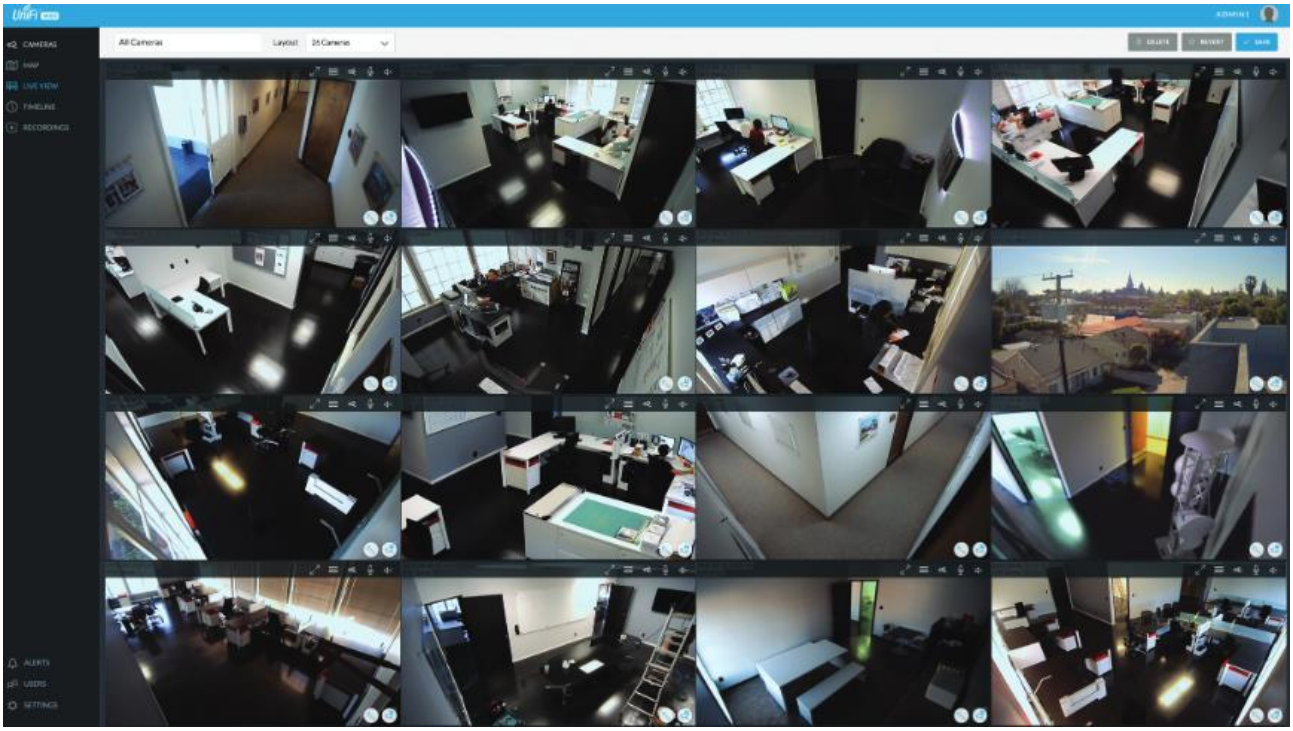


Рисунок 3.22 – Режим Live View

Наступна із найважливіших функції це можливість запису відео і

подальший його перегляд. Система UniFi може підтримувати наступні режими запису камери: «Завжди», «Ніколи», «Виявлення». Останній режим починає записувати відео у момент коли виявляє рухи в області запису, цей режим дозволяє зекономити місце на збережені відеофайлів.

Також є можливість редагування якості записаних файлі, а саме: змінення роздільної здатності, зміна бітрейту, зміна FPS.

Сервер надає наступні можливості для перегляду відеофайлів. Одна із функції, це перегляд відео запису з камеру в режимі «таймлайн». На часовій шкалі можна побачити в які моменти відбувались рух в полі зору камери. На рис. 3.23 наведено режим таймлайну.

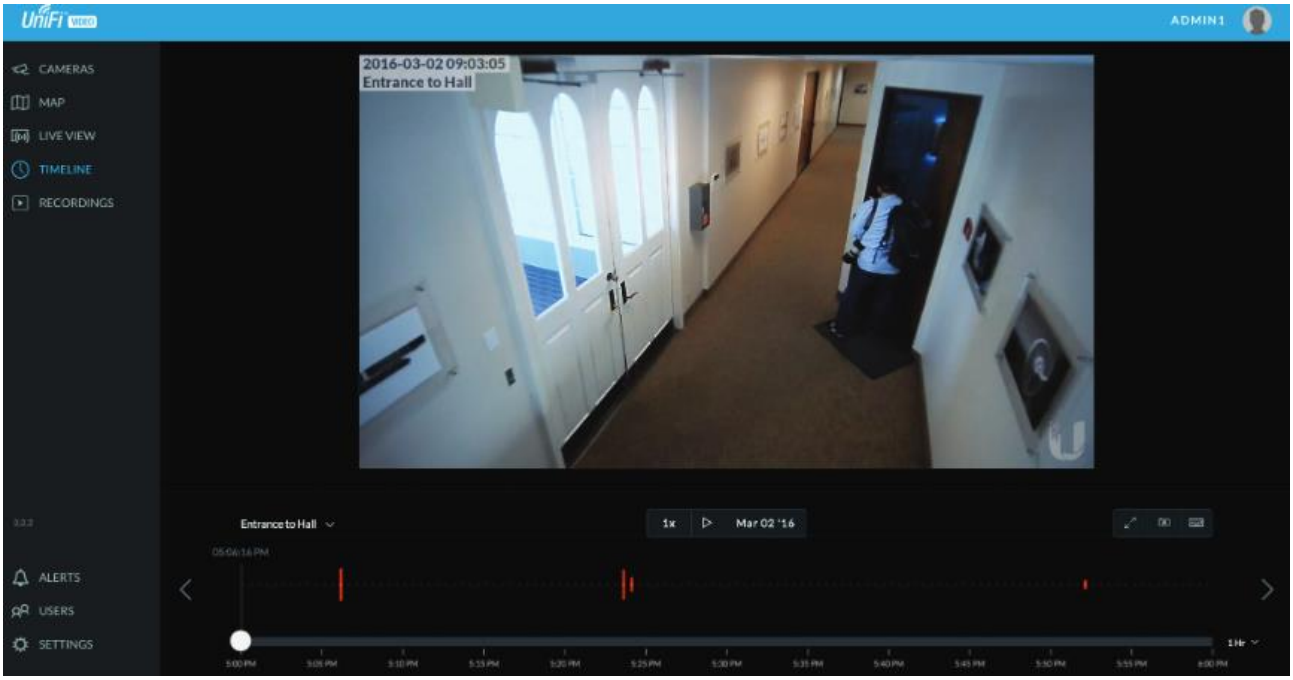


Рисунок 3.23 – Режим таймлайн

Другий режим перегляду відео записів, дозволяє переглядати всі наявні файли в хронологічному порядку. На екрані ми можем побачити час о котрі було записано відео, місце положення камери і тривалість відео. На рис. 3.24 наведено режим перегляду записаних відео.

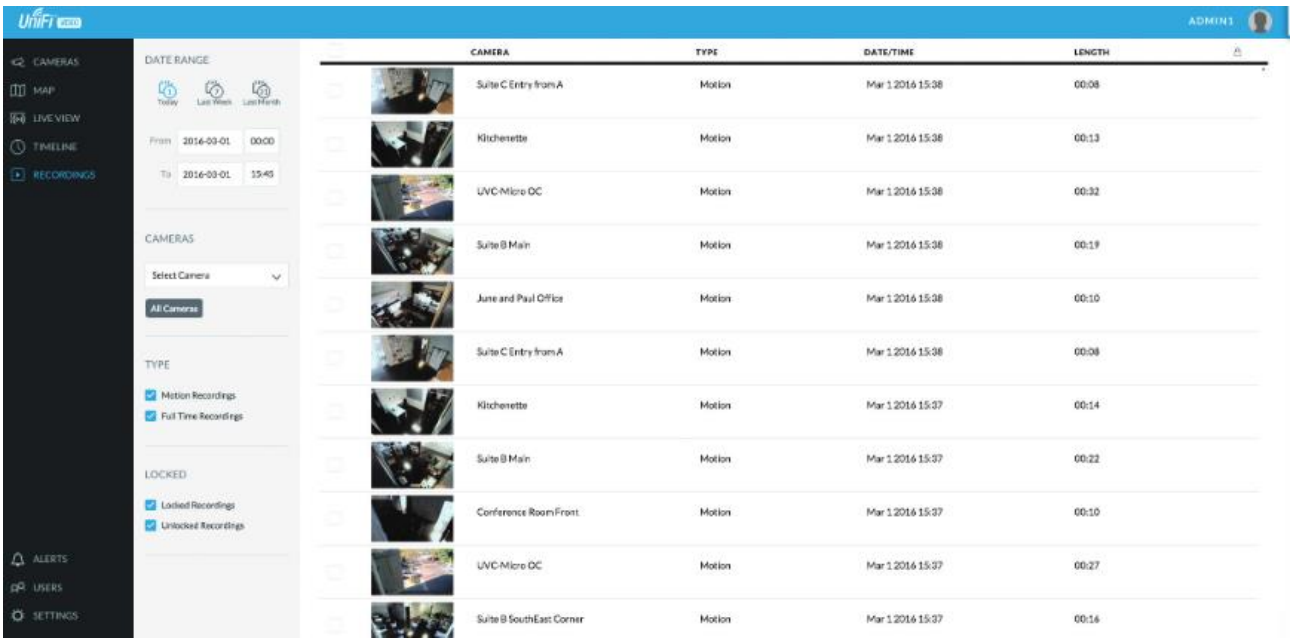


Рисунок 3.24 – Перегляд записаних відео

Одна із головних особливостей для системи відеоспостереження від UniFi, це карта об’єкту на якій можна розташовувати всі наявні камери. Це дає можливість для розуміння де саме розташовані камери і також їх поле зору. На рис. 3.25 наведено режим карти з розташуваннями камери і полем зору.

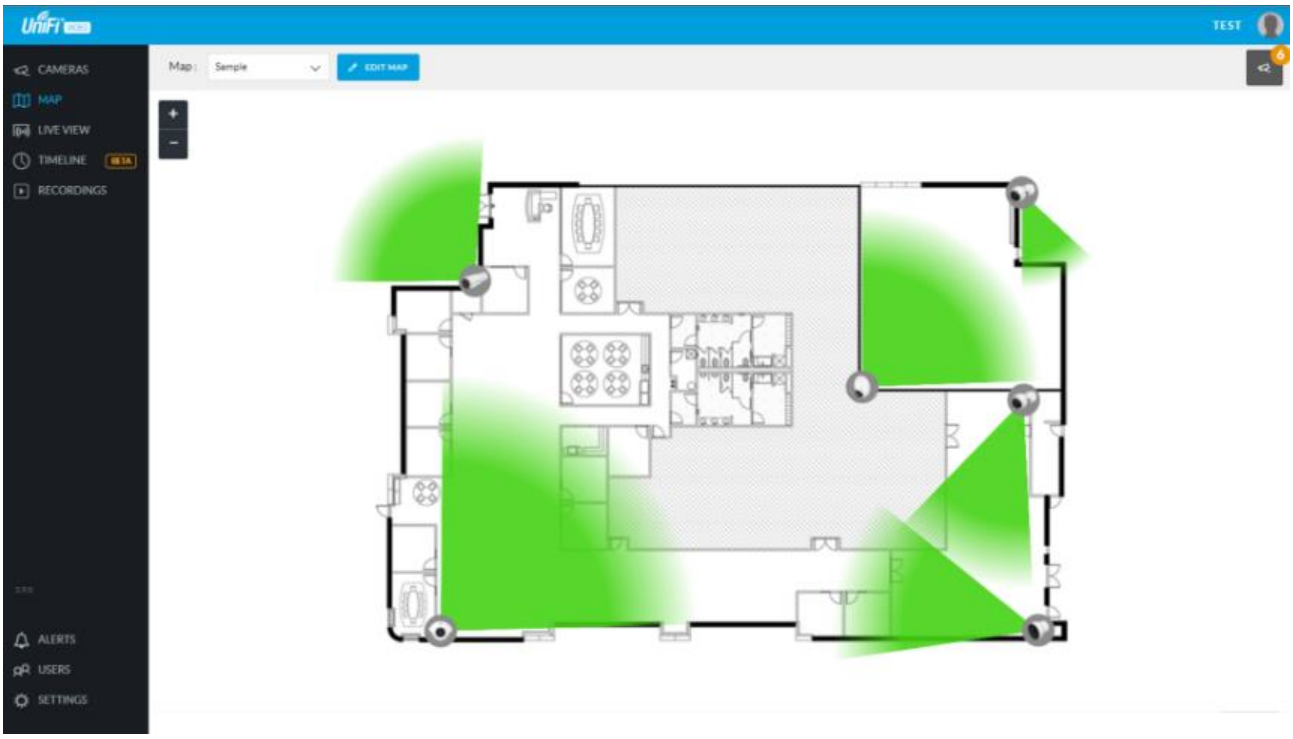


Рисунок 3.25 – Приклад карти об’єкту з камерами відеоспостереження

3.4.4 Налаштування бездротової мережі

Загальна кількість бездротових точок доступу 7 штук. На підприємстві будуть тільки дві бездротові мережі, одна робоча до якої зможуть підключатися співробітники і гостьова мережа до якої будуть підключатися люди які не є співробітниками і вона буде відокремлена. Тобто користувачі гостьової мережі не зможуть з’єднатися з серверами і камерами на підприємстві. На рис. 3.26 наведено сторінку налаштування Wi-Fi точок доступу.

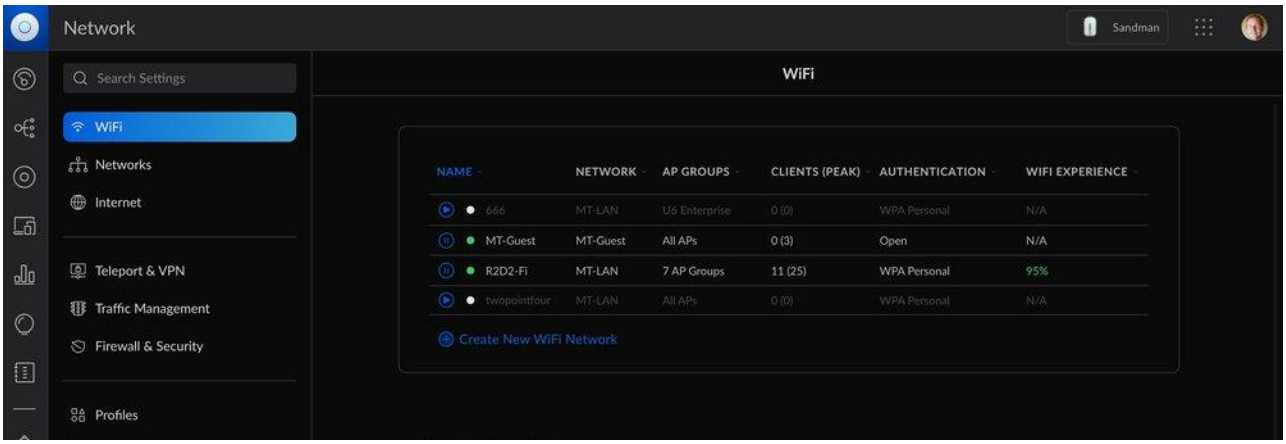


Рисунок 3.26 – Сторінка налаштування Wi-Fi

На початку конфігурації бездротової точки доступу потрібно задати назву точки доступу, пароль і до якої мережі відноситься Wi-Fi. На рис. 3.27 наведена сторінка створення Wi-Fi мережі.

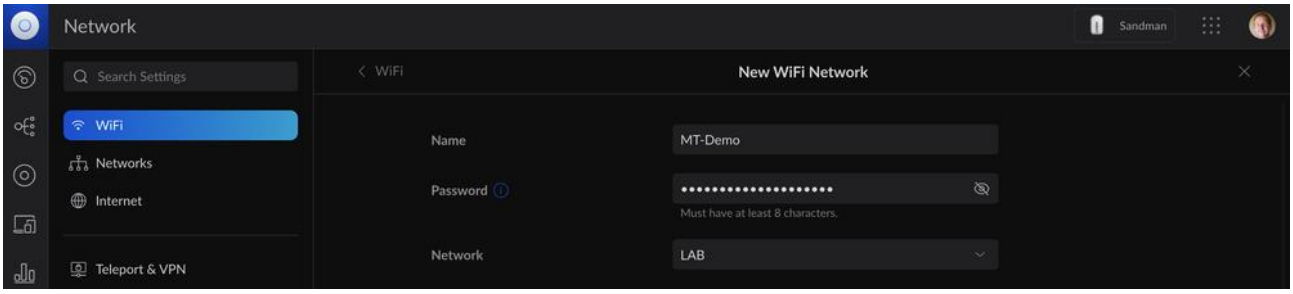


Рисунок 3.27 – Початкові налаштування точки доступу

В наступних пунктах налаштовуємо діапазон роботи точки доступу, це

може бути 2,4 і/або 5 ГГц. Тип який може бути стандартним і гостьовим. Смуга керування надає можливості клієнтським пристроям автоматично підключатися до потрібного діапазону. Також є можливість вказати пропускну здатність для мережі, яку ми можемо обмежити для гостьової мережі, щоб вони не навантажували локальну мережу. Є можливість ізолювати клієнтські пристрої, щоб вони не мали можливість з'єднуватися між собою. На рис. 3.28 наведено налаштування діапазону роботи точки доступу.

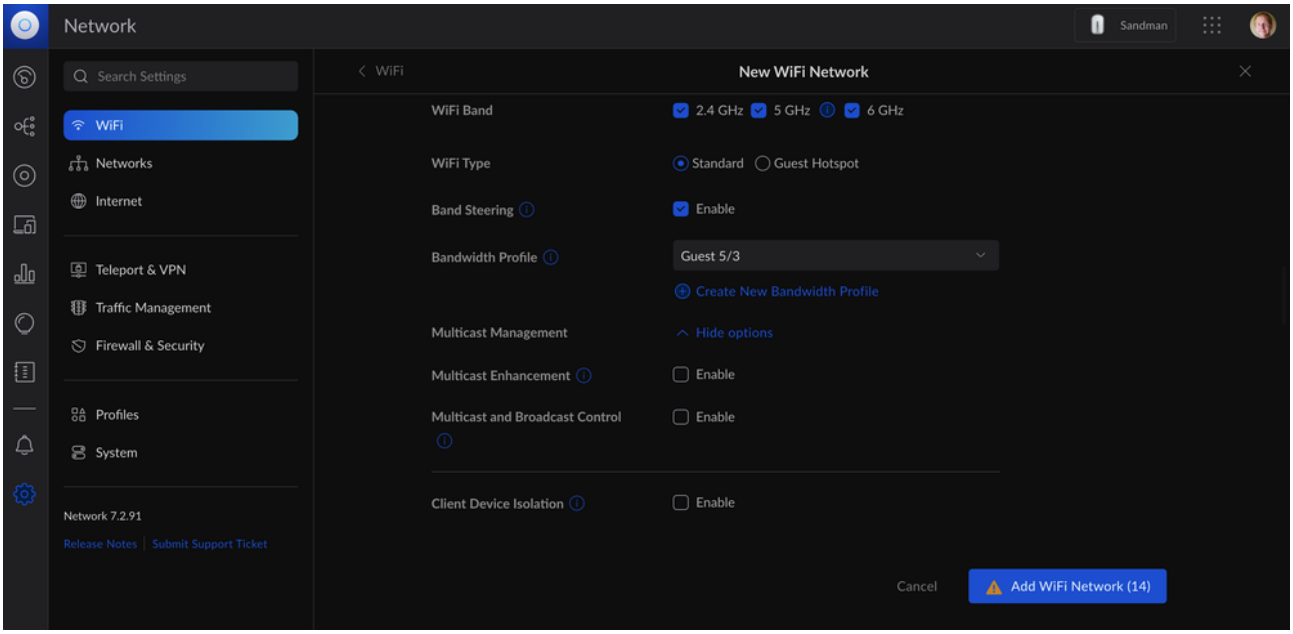


Рисунок 3.28 – Налаштування точки доступу

Далі надається можливість налаштувати параметри безпеки для точки доступу. Визначити протокол безпеки в бездротової мережі, що є дуже важливим для зменшення імовірності підключення зайвих користувачів. Також ми можемо приховати назву Wi-Fi мережі, якщо потрібно щоб її не було видно і для того щоб до неї підключитися потрібно вводити назву і пароль. На рис. 3.29 наведено налаштування параметрів підключення точки доступу.

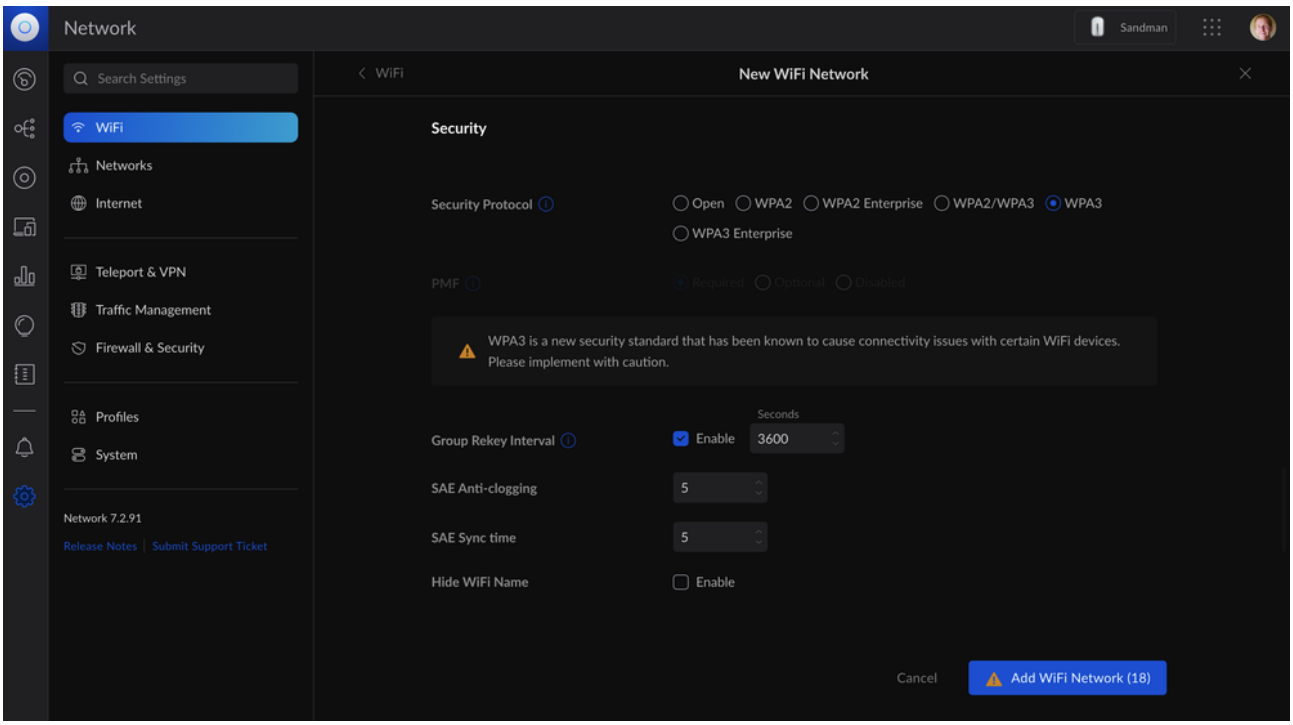


Рисунок 3.29 – Параметри підключення точки доступу

Фільтрація пристроїв надає можливість налаштування підключення до точки доступу тільки для довірених пристроїв. Налаштувати фільтрацію можна за допомогою наступних параметрів: MAC-адреса, профілі RADIUS, аутентифікація RADIUS MAC, формат MAC-адреси. На рис. 3.30 наведено параметри безпеки точки доступу.

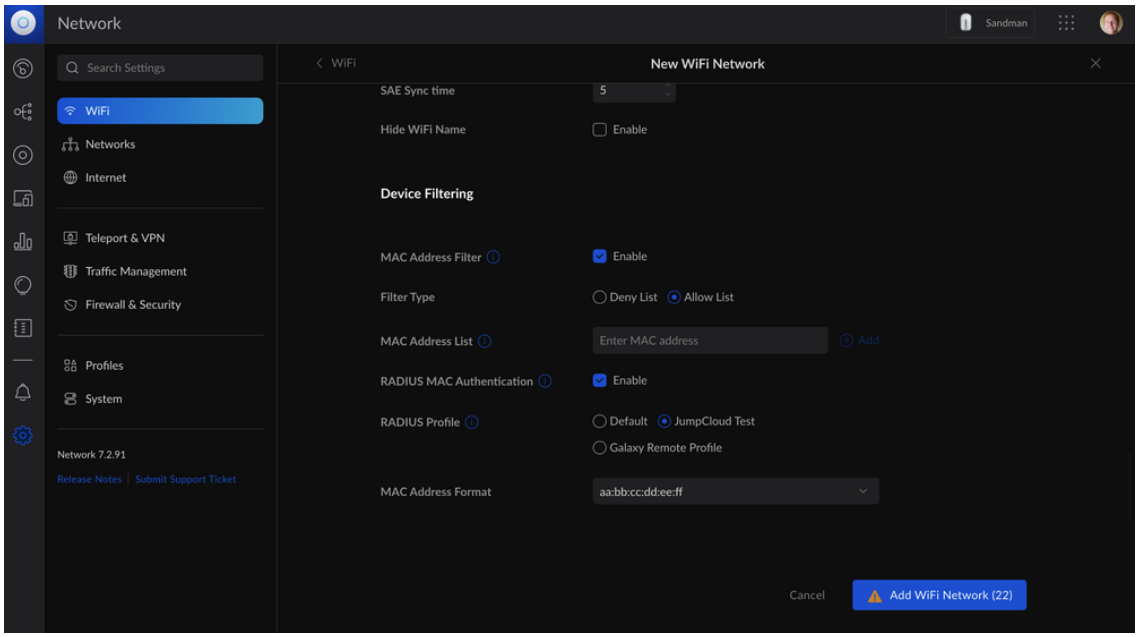


Рисунок 3.30 – Параметри безпеки точки доступу

Точки доступу від UniFi також надають доступ налаштування часу роботи Wi-Fi мережі на визначений час. Наприклад можна задати щоб Wi-Fi працював протягом робочого дня, а в кінці робочого дня він вимикається. На рис. 3.31 наведено налаштування часу роботи Wi-Fi мережі.

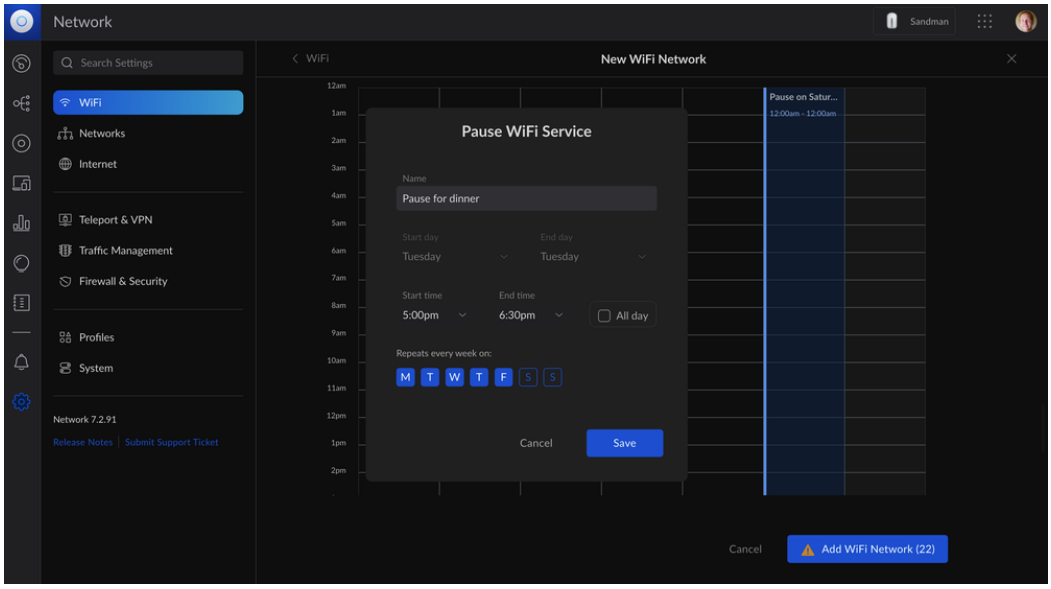


Рисунок 3.31 – Налаштування часу роботи точки доступу

3.4.5 Налаштування серверів

NAS сервер від Synology надає наступні можливості для корпоративної мережі:

- Файлове сховище з підтримкою технології RAID
- Бекап робочих пристроїв і файлів
- Поштовий сервер
- Месенджер для обміну повідомленнями в середині підприємства
- Спільна робота над офісними документами

На NAS сервері буде організовано RAID 6, для якого потрібно 4 жорстких диска. Головною особливістю RAID 6 є забезпечення працездатності системи після виходу із ладу двох дисків. Тобто ми маємо високий рівень відмовостійкості і швидкості обробки запитів. Але дана система має свої

недоліки, а саме: невелика швидкість запису і читання при одиничних запитах даних невеликого об’єму і тяжка процедура відновлення даних.

Операційна система Synology надає можливість розмежувати доступ до папок для кожної групи користувачів. Також є можливість задання максимального об’єму які можуть вони використовувати, доступ до визначених сервісів. На рис. 3.32 наведено створення груп користувачів на NAS-сервері.

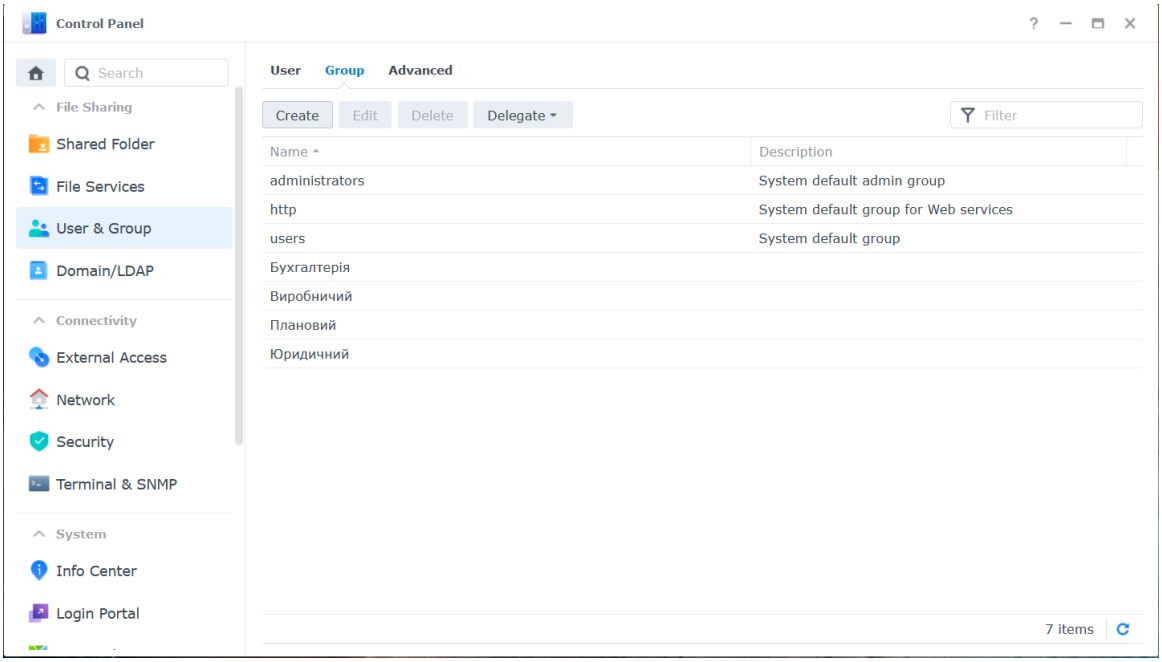


Рисунок 3.32 – Створення груп користувачів

Система дуже гнучка в налаштуванні правил доступу для користувачів і груп користувачів. Це дає великі можливості тонкого налаштування доступу групи користувачів до файлового сховища.

На сервері DELL EMC R240 буде розгорнута операційна система Ubuntu 18.04. Він буде виступати в якості серверу з базою даних, який буде зберігати дані від наступного програмного забезпечення:

- UA-бюджет – бухгалтерська програма яка забезпечує автоматизацію бухгалтерського та фінансового обліку, розрахунку заробітної плати та ведення кадрового обліку

- M.E.Doc – програмне забезпечення для електронного документу обігу та для подання звітності до контролюючих органів.
- Комунальне підприємство Універсальна Система Обліку – програмне забезпечення для нарахування абонентської плати для абонентів і формування квитанції
- SCADA zenon – програмне забезпечення для моніторингу системи автоматизації котельної. Більше детально розкриття системи в 4 розділу.

3.4.6 Налаштування параметрів безпеки

Маршрутизатор від UniFi надає наступні можливості для налаштування безпеки в мережі, а саме: RADIUS-сервер, брандмауер, фільтрація через GeoIP, DNS-фільтри, ACL.

Використання RADIUS, надає можливість прив’язати своє середовище UniFi до Active Directory для використання збережених ідентифікаційних даних для додаткових можливостей автентифікації. На рис. 3.33 наведено створення нового RADIUS профілю.

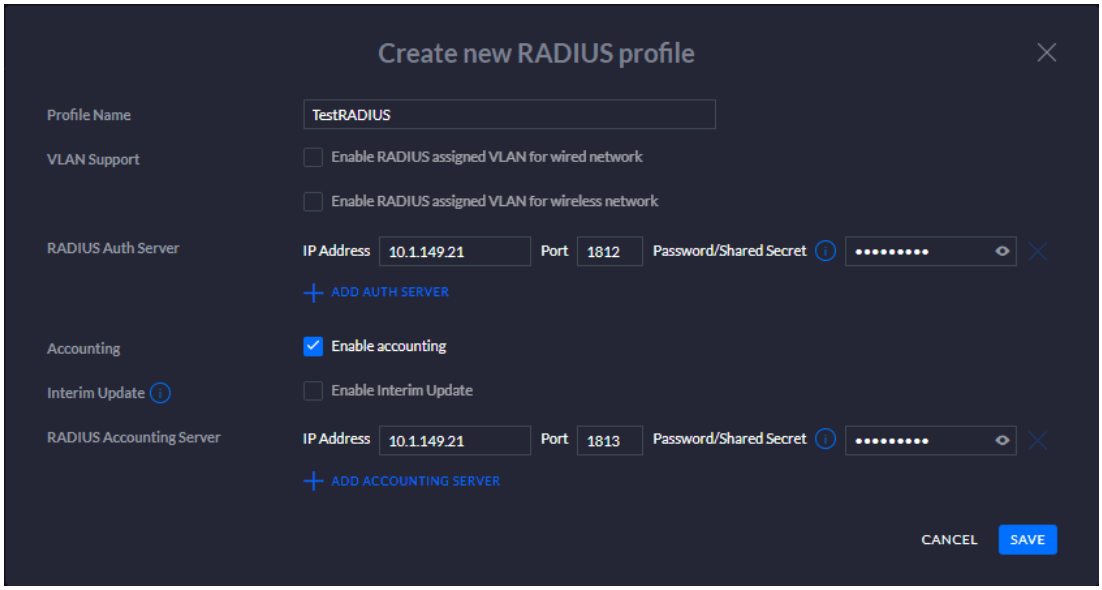


Рисунок 3.33 – Приклад налаштування RADIUS профіля

В налаштуванням брандмауера є можливість налаштування рівня чутливості системи. Чим вище рівень безпеки тим сильніше перевіряє маршрутизатор пакети, і при підозрі зловмисного трафіку буде блокувати його. На рис. 3.34 наведено налаштування рівнів чутливості брандмауера.

Рисунок 3.34 – Налаштування рівнів чутливості

Також UniFi надає можливості блокування трафіку з визначених країн. Це робиться для запобігання DDoS атаки, так як з визначених країн вона може проводитися. А також для блокування доступу до веб-сторінок визначених країн. На рис. 3.35 наведено список заблокованих країн через GeoIP.

Рисунок 3.35 – Заблоковані країни

Ще можна налаштувати напрямок фільтрації трафіку GeoIP. Що дозволяє переглядати сторінки в визначених країнах, але забороняє отримувати трафік від них. На рис. 3.36 наведено налаштування напрямку руху для визначених країн.

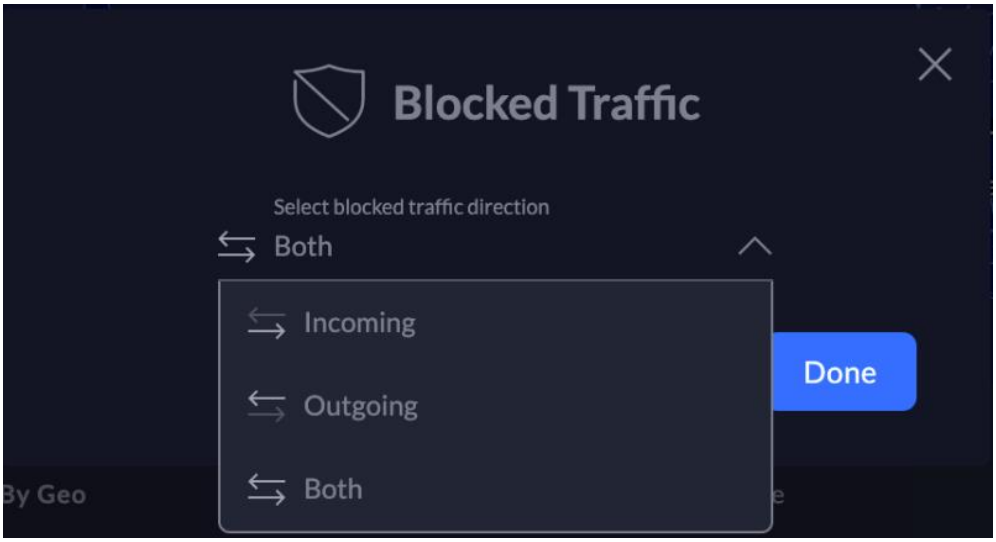


Рисунок 3.36 – Налаштування напрямку руху

Функція DNS-фільтру дозволяє вибирати рівні фільтрації для кожної мережі. Тобто можна налаштувати щоб фільтр блокував доступ до фішингу, спаму, зловмисного програмного забезпечення та шкідливих доменів. Є можливість підключити DNS-фільтр до бази даних яка оновлює свій вміст щогодини. На рис. 3.37 наведено налаштування DNS-фільтру для маршрутизатору.

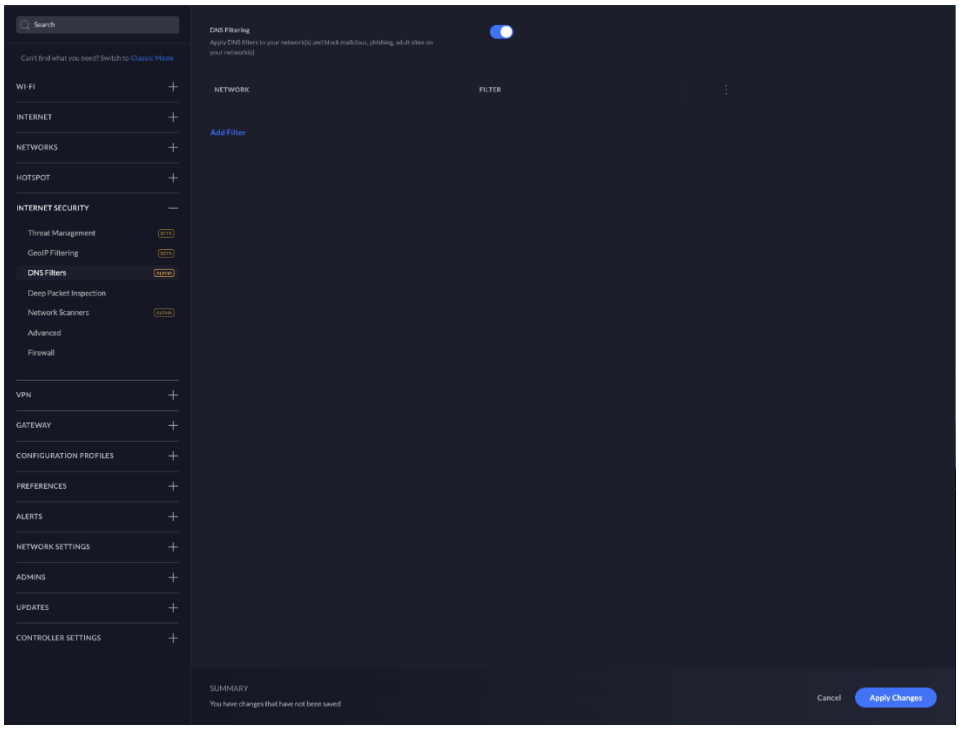


Рисунок 3.37 – Налаштування DNS-фільтру

Висновки до розділу 3

В третьому розділі випускної кваліфікаційної роботи були проведена робота з модернізації мережі центрального офісу і запровадження нових мережевих технології і безпеки.

Була розроблена новий план мережі з розподіленням відділів. Також було запроваджено розподілення між відділами за допомогою VLAN. Проведений підбір мережевого і серверного обладнання.

Проведено налаштування VPN серверу на базі маршрутизатора з використанням протоколу OpenVPN. Налаштування правил в брандмауері для VPN мережі для вхідного і вихідного трафіку.

Розгорнута система відеоспостереження і підключення IP-камер до серверу. Проведена налаштування відео серверу і алгоритми запису відео з камер.

Було проведено налаштування бездротових точок доступу. Створено дві мережі, одна для працівників і друга гостьова. Також виставлені всі параметри безпеки для Wi-Fi мережі, а саме: протокол безпеки, параметри авторизації і час роботи мережі.

Також було проведення налаштування центрального і NAS серверів в мережі. Встановлені всі необхідні параметри авторизації, створення груп користувачів відносно відділів і надані відповідні ролі доступу до пристроїв.

І на кінець були проведені заходи з організації мережевої безпеки. Були налаштовані наступні параметри: RADIUS-серверу, брандмауер, фільтрація через GeoIP і DNS-фільтри.

4 МОДЕРНІЗАЦІЯ МЕРЕЖІ КОТЕЛЬНИХ

4.1 Структура локальної мережі котелень

Вимоги до локальної мережі котельних повністю відповідають вимогам локальної мережі центрального офісу, але має декілька додаткових вимог:

- мати високоякісний зв’язок з центральним офісом
- безпечний і зашифрований зв’язок з серверами підприємства
- відмово стійкість мережі
- можливість автономної роботи

План мережі для всіх котельних буде типовим. В кожній котельні буде до 5 робочих місць для співробітників, які будуть виконувати наступні задачі: робота з електронними листами, доступ до центральних серверів підприємства, формування звітів, готування звітів і також контроль роботи котельні. Кількість камер відеоспостереження які будуть використовувати на кожну котельню в середньому 6 штук.

Для автоматизації управління котельними будуть використовуватися SCADA системи. Головною метою їх запровадження є: підвищення надійності роботи котельних, економія використання ресурсів і також їх точний облік. За рахунок використання автоматизованої системи управління можна досягнути найвищих рівнів безпеки при експлуатації котельної. В рис. 4.1 наведений типовий план мережі для котельні.

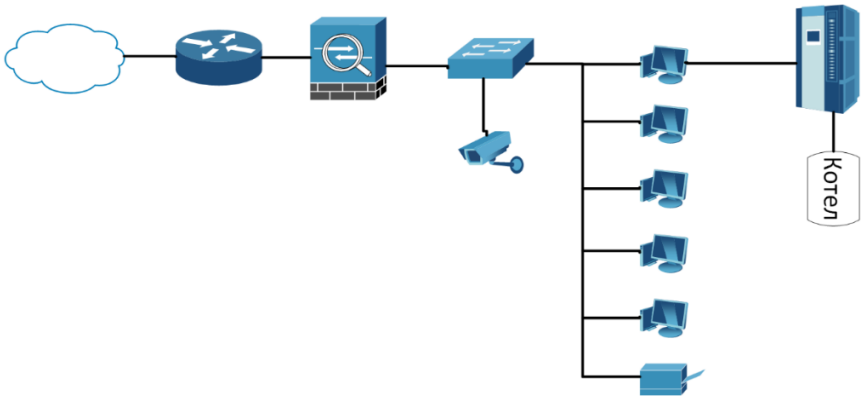


Рисунок 4.1 – Типовий мережевий план котельні

Мережеве устаткування буде використовуватися яке було вибране в розділі 3, воно повністю відповідає вимогам мережі і також дозволяє підтримувати єдність мережі що дозволить найкраще працювати мережі.

4.2 Запровадження SCADA

4.2.1 Вимоги до системи автоматизації

Даний проект реалізується на спільній інтеграції технічних засобів автоматизації і програмного забезпечення, яка дозволяє здійснювати експлуатацію котельній без постійної участі обслуговуючого персоналу. Всі технологічні параметри, сигнали про поточний стан обладнання котельні, у тому числі сигнали про несправність, заносяться до журналів диспетчерського пункту оператора, яким може виступати персональна робоча станція (ПК), так і HMI-панель.

АСУ поділяється на підсистему захисту, що включає пристрої сигналізації, та підсистему регулювання, що включає пристрої керування. Регулювання забезпечує оптимальний режим горіння за рахунок підтримки відповідного розрідження в топці та витрати повітря, необхідної температури води, тиску/витрати тепломережі. Підсистема безпеки забезпечує запобіганням

аваріям при порушені нормального режиму роботи котлів.

Система автоматизацій відповідає наступним критеріям:

- висока надійність;
- наочність та повнофункціональний інтерфейс оператора;
- використання сучасних технічних засобів;
- зниження експлуатаційних витрат;
- передача даних на віддалений сервер;

Дана автоматична система управління повинна виконувати наступні функції:

1. Ручний пуск котла з контролем наступних параметрів:
    a. обов’язкова робота димососа і вентилятора при розпалі;
    b. наявність полум’я на пальнику після розпалу;
2. Автоматична і ручне регулювання навантаження по температурі води на виході котла, шляхом керування шибером вентиляторами і газової заслінки;
3. Автоматичне або ручне регулювання розрізу в топці шляхом керування шибером димососа;
4. Автоматичний захист і зупинка котла при виявлені аварійних ситуації;
5. Автоматичне переключення роботи котлоагрегатів у відповідність заданим розкладам або у випадку аварійної зупинці одного із них;
6. Дистанційне управління регулюючими виконавчими механізмами;
7. Реалізація АРМ оператора з візуальним відображенням хода технологічного процесу на екрані ПК і/або панелі, а саме:
    a. цифровий покази датчиків
    b. стан виконавчих механізмів;
    c. попереджуючих повідомлення о аварійних ситуаціях в технологічному процесі;
    d. забезпечення системи безпеки: автентифікації і авторизації;
    e. видача журналів звітів у відповідних формах;
    f. ведення журнал всіх дій операторів і події в системі;

8. Для здійснення оперативного керування агрегатом у ручному режимі (у випадку аварійних ситуації) передбачається встановлення елементів управління виконавчими механізмами у шафах управління;
9. Виконання алгоритмів аварійних захистів котла при:
    a. різкому зміненні тиску газу;
    b. зниження тиску повітря;
    c. зниження тяги;
    d. виході температури води за аварійні межі;
    e. зникнення полум’я на пальнику;
    f. припинення роботи димососа;
    g. зупинка системи подачі повітря;

Аварійний захист повинен передбачати закриття клапанів подачі газу, продування котла, видачу відповідного повідомлення оператору та задіяння звукової сигналізації. Стан усіх датчиків-реле, що використовуються в системі, дублюватися на робочий станції оператора у вигляді псевдо схеми, при цьому аварійні ділянки повинні підсвічуватися.

4.2.2 Опис системи автоматизації

В якості програмного забезпечення для візуалізації, диспетчерського керування, збору та аналізу даних буде використовуватися рішення від COPA-DATA GmbH. Система zenon повістю вирішує всі задачі, що ставляться перед HMI та SCADA системами. ПЗ надає можливості здійснювати зручне та наочне керування, чітку взаємодію всіх інженерних комплексів, автоматичну адаптацію, інтелектуалізацію режимів роботи підсистеми. Базується на стандартних відкритих технологіях та пропонує величезний набір простих у використанні графічних функцій для побудови системи візуалізації. Система має можливість розгортання на робочих комп’ютерах. [14]

Система zenon має наступні особливості:

- Відкрита архітектура – можливість використання при розробці незалежних програм, створення макросів.
- Автоматичне проектування – наявність великої кількості шаблонів стандартних зображень і форм користувача яка дозволяє здійснювати проектування в автоматичному режимі.
- Широкі комунікаційні можливості – має високу сумісність з апаратними засобами системи автоматизації, підтримує велику кількість інтерфейсів і комунікаційних протоколів.
- Гнучкість системи – XML технологія дозволяє імпортувати/експортувати в систему управління як окремі частини проекту, так і весь проект. Розширення системи здійснюється без необхідності змінювати або переробляти існуючий проект.
- Багатокористувацька розробка – система дозволяє здійснювати розподілену розробку проектів, завдяки чому не існує жорсткої прив’язки до одного робочого місця. Проектувальники можуть розподілити між собою об’єм робіт і займатися конкретно своєю частиною проекту.

Виконувати функції модульної системи керування буде PLC VIPA 200V. ПЛК призначена для реалізації централізованих і розподілених систем керування. Пристрій побудований за модульним принципом. Це дає можливість оптимально підбирати склад модулів для вирішення завдань і гнучко модифікувати його при розширені або зміні вимог до системи. На рис. 4.2 наведена модульна система керування. А в табл. 4.1 технічні характеристики.

Рисунок 4.2 – Модульна система керування PLC VIPA 200V з сигнальними модулями

Таблиця 4.1 – Технічні характеристики PLC VIPA 200V

Кількість входів/виходів	дискретні – до 1024 I/O аналогові – до 128 I/O
Організація	модульна конструкція (до 32 модулів розширення)
Об’єм пам’яті	32-128 кБ
Час виконання операції	з бітами – 0,25 мкс зі словами – 1,2 мкс
Таймер/лічильники	128/256
Програмування	WinPLC7 від VIPA STEP7 від Siemens
Функціональні блоки/функції/блоки даних	1024/1024/2047
Інтерфейс	MP2I (MPI+PPI)
Підтримка мереж	Profibus DP slave

Місцеве керування виконуватиме панель оператора VIPA OP03, яка використовується для відображення і управління невеликим

користувальницькими застосунком. ПО дозволяє відображати текстову повідомлення о статусі, режимі, аваріях і також задавати параметри за допомогою навігаційних і функціональних кнопках. На рис. 4.3 наведена панель оператора. А в табл. 4.2 технічні характеристики.

Рисунок 4.3 – Панель оператора VIPA OP03

Таблиця 4.2 – Технічні характеристики VIPA OP03

Дисплей	2 x 20 символів
Інтерфейс	MP^{2}I
Об’єм пам’яті	256 кБ
Кількість змінних	4096

В загалом система буде складатися з наступних приладів. На нижньому рівні буде встановлений модульна система керування PLC VIPA 200V з набором модулів вводів-виводів(до 20 аналогових і 32 дискретних параметрів, а також 25 аварійних) в якому реалізуються всі функції регулювання. Місцеве керування буде виконуватися з панелі оператора VIPA OP03.

Верхній рівень реалізується на базі робочого комп’ютера з встановленим програмним забезпечення. На рис.4.4 наведений інтерфейс системи керування котельною.

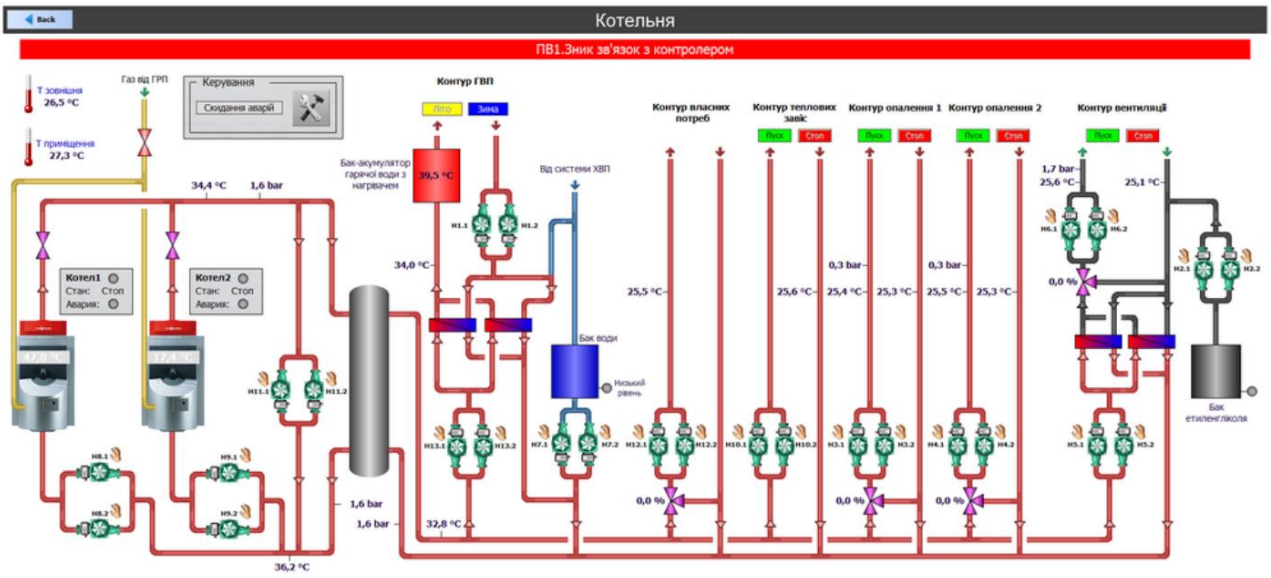


Рисунок 4.4 – Інтерфейс системи керування котельною

В системі будуть використовуватися наступні пристрої:

- Система насосів – які відповідають за подачу холодної води до котлів і відводу гарячої води до тепломережі
- Система вентиляції – яка відповідає за подачу повітря до котла і система відводу продуктів згоряння
- Система подачі газу – яка відповідає за концентрацію подачі газу і її обліку
- Система датчиків – які відповідають за збір наступних даних з різних ділянок системи: температури, тиску і об’єму який проходить через труби
- Нагрівач – який відповідає за регулювання потужності котла

4.3 Налаштування мережі

Отже кожна котельня буде мати мережу з наступним адресом 192.168.n.0, де n – відповідає номеру котельні(від 1 до 20). В кожній котельні буде єдина VLAN, так як нема потреби в розділені мережі.

Надалі потрібно підключити локальну мережу котельні за допомогою

VPN до центрального офісу. Для цього вводимо глобальну адресу мережі, і пароль який ми створили. На рис. 4.5 наведено підключення до VPN мережі центрального офісу.

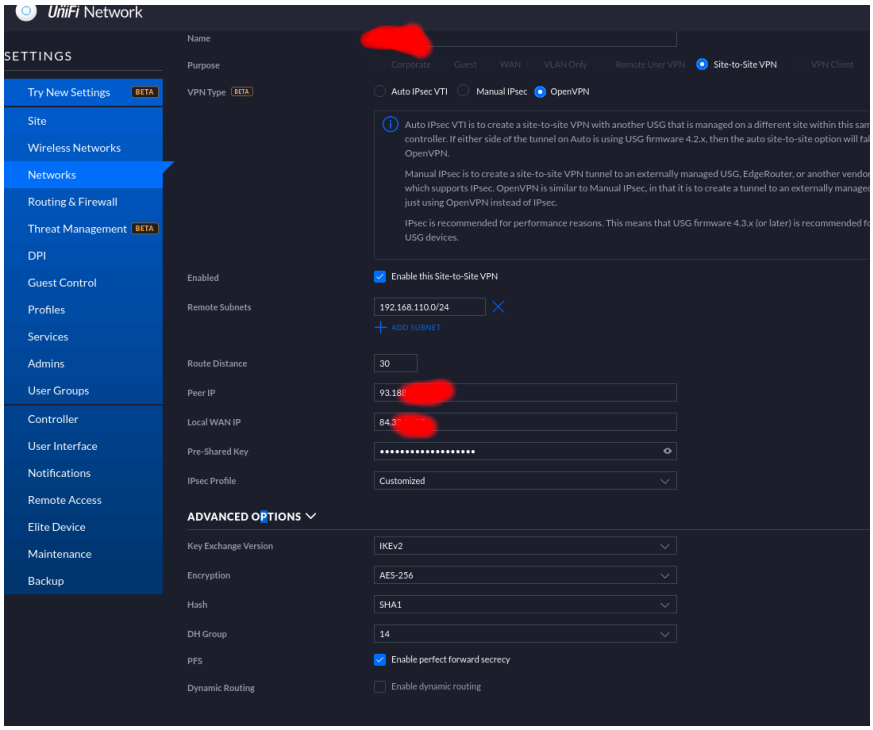


Рисунок 4.5 – Підключення до VPN мережі

Далі вже по прикладу налаштування мережі в розділі 3 проводимо наступні роботи в котельних:

- Налагодження і підключення системи відеоспостереження до серверу який буде зберігати записи
- Налаштування бездротової точки доступу. Єдиною відмінністю буде те що на котельних буде відсутня гостьова мережа, задля безпеки локальної мережі. Тільки довірені користувачі можуть підключаються до мережі.
- Налаштування зв’язку SCADA системи з центральним сервером для передачі даних з датчиків.
- Підключення робочих комп’ютерів до NAS серверу, для обміну файлами і бекапів системи

- Налаштування RADIUS-серверу, на підключення робочого пристрою і серверу до SCADA системи котла
- Налаштування брандмауера на найвищий рівень чутливості трафіку
- Включити блокування країн
- Активація DNS-фільтру

Висновок до розділу 4

В четвертому розділі випускної кваліфікаційної роботи була проведена робота з модернізації мережі котельних і запровадження SCADA системи для керування котельною.

Проведена робота з побудови плани мережі і її налаштування. Проведено підключення локальної мережі котельної до центрального офісу за допомогою технології VPN.

Запроваджена SCADA система для керування котельною, вибір необхідно устаткування і опис її роботи. Також підключення системи до робочого комп’ютера оператора і центрального серверу на який будуть відправляти дані о роботі котельної.

ВИСНОВКИ

В ході виконання випускної кваліфікаційної роботи за рівнем «магістр», було виконано дослідження об’єктів КП «Покровськтепломережа». Проведений аналіз телекомунікаційну мережі і систему управління котлами. Було виділені недоліки і складений план по модернізації мережі.

Під час модернізації телекомунікаційної мережі, було складений новий план мережі з розподіленням користувачів між відділами для найкращого управляння. Налаштований VPN зв’язок між центральним офісом і котельнями для обміну конфіденційними даними і моніторингу за робочими процесами. Також було запроваджені дії для посилення телекомунікаційної мережі для запобігання кібератак. Побудова і налаштування системи відеоспостереження з можливостю запису і зберігання файлів. Встановлення і налаштування серверів для зберігання робочих файлів і бази даних для програмного забезпечення.

На котельних була запроваджена диспетчерська система управління і збору даних. Вона дозволяє зменшити людський фактор під час аварійних ситуації, проводити моніторинг за робочими процесами і також дозволити зменшити використання ресурсів для роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ethernet Tutorial – Part I: Networking Basics [Електронний ресурс] – Режим доступу: https://www.lantronix.com/resources/networking-tutorials/ethernet-tutorial-networking-basics/ – Дата доступу: Грудень 2022. Назва з титул. Екрана

2. A Survey of Ethernet LAN Security [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/abstract/document/6407456 – Дата доступу: Грудень 2022. Назва з титул. Екрана

3. Power Over Ethernet (PoE) Technical Overview [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/339055006_Power_Over_Ethernet_PoE_Technical_Overview – Дата доступу: Грудень 2022. Назва з титул. Екрана

4. VIRTUAL PRIVATE NETWORKS: An Analysis of the Performance in State-of-the-Art Virtual Private Network solutions in Unreliable Network Conditions [Електронний ресурс] – Режим доступу: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1367277&dswid=-3460 – Дата доступу: Грудень 2022. Назва з титул. Екрана

5. Technical Overview of Virtual Private Networks(VPNs) [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/274929918_Technical_Overview_of_Virtual_Private_NetworksVPNs – Дата доступу: Грудень 2022. Назва з титул. Екрана

6. Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/339761254_Comparative_Analysis_of_Site-to-Site_Layer_2_Virtual_Private_Networks – Дата доступу: Грудень 2022. Назва з титул. Екрана

7. A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/abstract/document/9066892#full-text-header – Дата доступу: Грудень 2022. Назва з титул. Екрана

8. Towards explainable AI-assisted operations in District Heating Systems [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2405896321007606 – Дата доступу: Грудень 2022. Назва з титул. Екрана

9. The Security of IP-Based Video Surveillance Systems [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/343902531_The_Security_of_IP-Based_Video_Surveillance_Systems – Дата доступу: Грудень 2022. Назва з титул. Екрана

10. What is the Information Security Triad? [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/cia-triad – Дата доступу: Грудень 2022. Назва з титул. Екрана

11. What is ACL in Networking & How to Implement It? [Електронний ресурс] – Режим доступу: https://phoenixnap.com/kb/acl-network – Дата доступу: Грудень 2022. Назва з титул. Екрана

12. Firewall Best Practices for Securing Smart Healthcare Environment: A Review [Електронний ресурс] – Режим доступу: https://www.mdpi.com/2076-3417/11/19/9183 – Дата доступу: Грудень 2022. Назва з титул. Екрана

13. What is the RADIUS Protocol? [Електронний ресурс] – Режим доступу: https://jumpcloud.com/blog/what-is-the-radius-protocol – Дата доступу: Грудень 2022. Назва з титул. Екрана

14. SADA система Zenon [Електронний ресурс] – Режим доступу: https://www.copa-data.com.ua/ - Дата доступу: Грудень 2022. Назва з титул Екрана

ДОДАТОК А

Охорона праці та безпека під час експлуатації теплових мереж і установок

А.1 Заходи з електробезпеки

Заходи безпеки призначені для запобігання можливості контакту людини з струмоведучими частинами. Все для того щоб виключити можливість контакту з струмоведучими частинами оператора, вимикач встановлюється в закритому положенні, використовується блоковий вузол, а рівень обладнання відповідає IP44 (це 4-рівневий захист жорсткість). Відповідно до ПУЕ-87 і ГОСТ 14254.80.

Відповідно до ГОСТ 12.2.007ю0-75* ми приймаємо I клас захисту від ураження електричними струмом операторів.

Забезпечити безпеку тіла людини при контакті з не струмопровідними металевими частинами електрообладнання, щоб запобігти випадковому пробою його ізоляції та генерації на ній електричного потенціалу. Пристрій живиться від заземленої мережі з напругою нейтралі 220 В і частотою 50 Гц.

Оскільки напруга нижче 1000 В, але вище 42 В, згідно ГОСТ 12.1.030-81, необхідно використовувати занулення для запобігання ураження електричним струмом, оскільки люди можуть доторкнутися до металевих конструкцій і металевих конструкції заземленого електронного обладнання.

Нуль означає підключення до металевого циферблата захисного провідника, який може бути під напругою.

Відповідно до способу захисту ГОСТ 12.2.007.0.75 наша протиударна система віднесена до 1 класу.

В електроустановках при роботі напругах від 24 до 380 В змінного струму та в ситуаціях підвищеної небезпеки використовувати повторне захисне заземлення (ізольована нейтраль). Повторне захисне заземлення захищає персонал від ураження електричним струмом у разі зіткнення з

непровідними металевими частинами, які можуть стати під напругою через порушення ізоляції.

Основним джерелом живлення в приміщені є однофазна мережа. Напруга змінного струму 220 В, нейтральна земля, частота 50 Гц, потужність 2 кВт. Живлення забезпечується електричними приладом, а джерело живлення має регульовану напругу під навантаженням. Напруга мережі подається на розподільний пристрій.

Всередині організації прокладіть шину захисного заземлення згідно ГОСТ 12.1.030-81. Шина металева закріплена на заземленому нульовому провіднику електроустановки. Опір заземлювача, підключеного до нейтральної точки, не більше 0.6 Ом. Захищені шини доступні для огляду.

Використання високовольтного обладнання вимагає такого застереження:

- Не підключати та не від’єднувати кабелі, коли живлення увімкнено
- Роботи з технічного обслуговування на ремонту можна проводити тільки при вимкненому живленні
- Не відкривати кришку, коли живлення увімкнено
- Працювати може персонал, підготовлений приймальною комісією та прийнятий на роботу відповідно до ПУЕ-87

А.2 Пожежна безпека

Контроль пожежної безпеки для операторів повинен відповідати ГОСТ 12.1.004-91. Слід продумати системи протипожежного захисту та організаційного-технічні заходи.

Перелік причин пожежі в диспетчерській:

- Перевантаження
- Високий опір перехідних процесів

- Недотримання протипожежних правил при будівництві опалювальних і вентильованих будівель і споруд
- Порушення протипожежних правил
- Коротке замикання
- Поганий контакт з’єднання
- Порушення ізоляції провідника

В системі повинні бути встановлені такі компоненти протипожежного захисту:

- Електрообладнання класи захисту IP54
- Перемикання проводів за допомогою роз’ємів
- Система протипожежного захисту – Вуглекислотний вогнегасник ОУ-5
- Пожежна сигналізація з датчиком КІ-1
- Телефон встановлено в межах досягності

Несучі та захищені сталеві конструкції повинні бути захищені вогнезахисними матеріалами.

Для нормальної евакуації людей під час пожежі передбачені такі умови: ширина дверей – 2 м., висота – 2м., ширина коридору – 1,5 м.

Організаційно-технічні заходи щодо пожежної безпеки полягають у інструкції ПБ і навчання персоналу організаційним правилам безпеки та діям у разі пожежі.

А.3 Заходи безпеки при користуванні котлом

Водогрійні котли є об’єктом підвищеної небезпеки, тому їх монтаж, підготовка до роботи та експлуатації повинні бути організовані у суворій відповідності до цієї інструкції, паспорта та чинних «Правил пристрою та безпечної експлуатації водогрійних котлів та парових котлів», затверджених держтехнаглядом.

До роботи з котлом допускаються особи, які пройшли спеціальну підготовку, інструктаж щодо заходів безпеки та проведені наказом щодо організації (установи), що експлуатує цей котел.

Пуск котла у роботу допускається після їх огляду відповідно до правил технічного огляду комісією підприємства (установи), призначеної наказом.

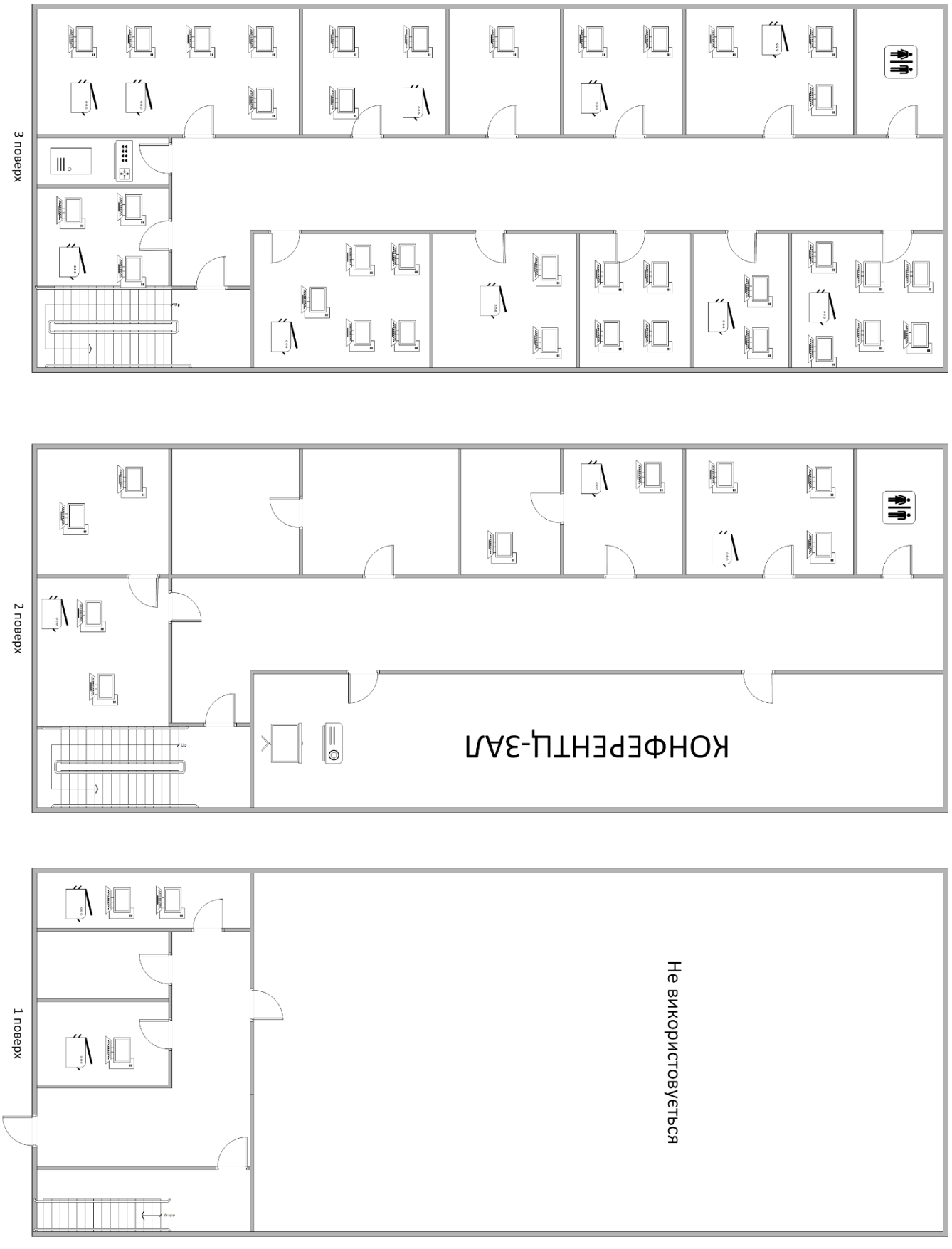
Забороняється експлуатувати несправні котли та котли, у паспортах яких немає дозволу комісії, зробленого на підставі проведеного огляду та технічного огляду.

Котел повинен бути негайно зупинений у випадку:

- Якщо температура води або тиск у системі різко підвищуються і продовжують зростати, незважаючи на вжиті заходи (зменшення подачі палива, зменшення тяги та дуття)
- Якщо підживлення системи довго не з’являється води з сигнальної трубки розширювача
- При виявлені пошкодження котла із сильним витоком води
- Під час вибуху газів у газоходах
- При пошкоджені кладки або обмуровки, що загрожують обвалами, при розжарюванні до червоних елементів котла або каркаса
- При горінні сажі та частинок палива газоходах

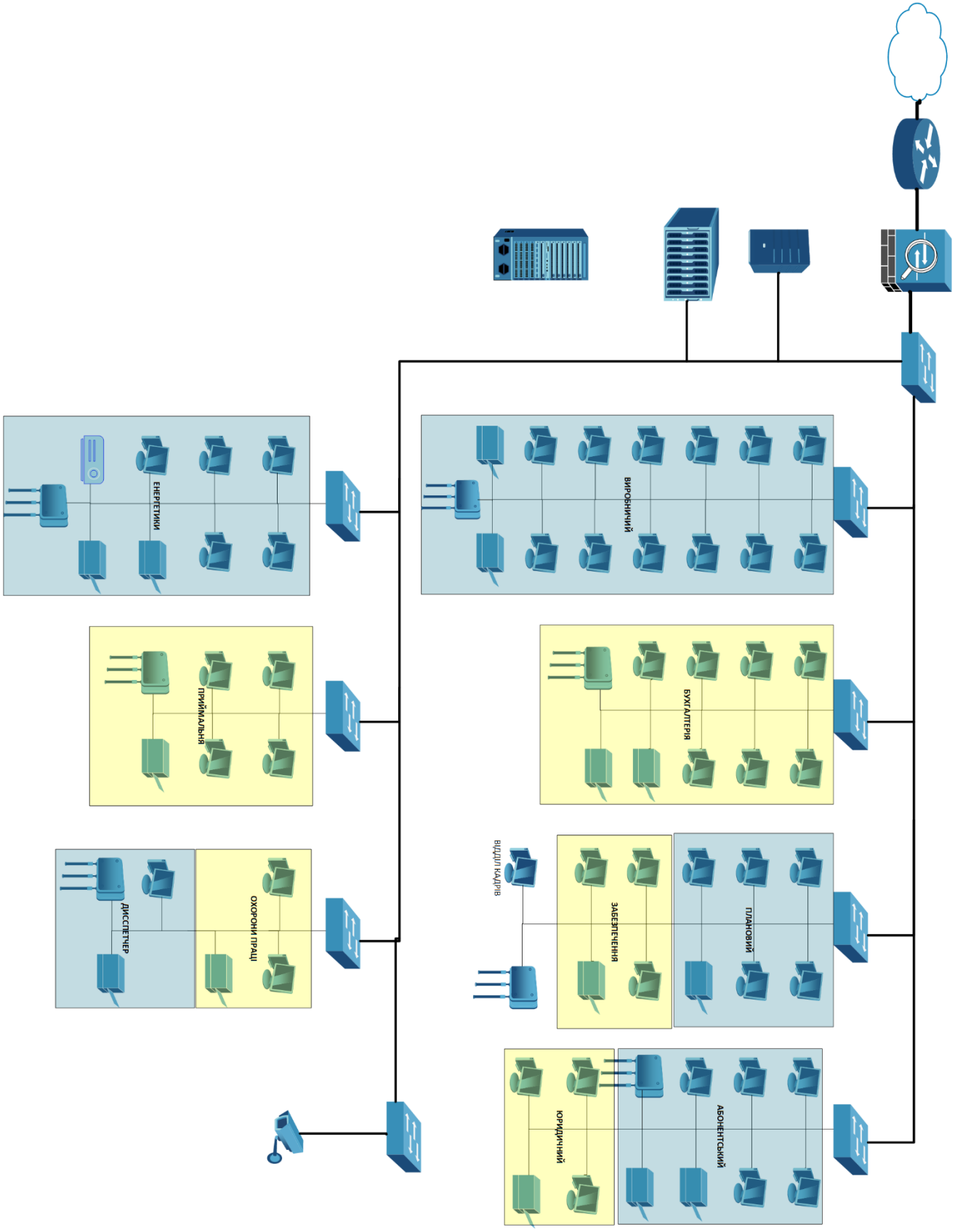
ДОДАТОК Б

План будівлі



ДОДАТОК В

План мережі



ДОДАТОК Г

Налаштування генерації ключів для OpenVPN

Г.1 – Лістинг команд які використовуються для налаштування генерації ключів для протоколу OpenVPN через SSH

1. Завантаження і встановлення easy-rsa

```
sudo bash
curl -O http://ftp.us.debian.org/debian/pool/main/e/easy-rsa/easy-rsa_2.2.2-1_all.deb
sudo dpkg -i easy-rsa_2.2.2-1_all.deb
```

2. Ініціалізація PKI та створення сертифікатів і ключів ЦС

```
cd /usr/share/easy-rsa
. vars
./clean-all
./build-ca

./build-key-server server

./build-dh
```

3. Після створення ключів і сертифікаті, потрібну буде задати назву для VPN. Згенеровані ключі перенести в /config/auth/keys/

```
mkdir /config/auth/keys/
cp keys/* /config/auth/keys/
```

4. Налаштування OpenVPN

```
configure
set interfaces openvpn vtun0 mode server
set interfaces openvpn vtun0 server subnet 192.168.0.0/24
set interfaces openvpn vtun0 tls ca-cert-file /config/auth/keys/ca.crt
set interfaces openvpn vtun0 tls cert-file /config/auth/keys/server.crt
set interfaces openvpn vtun0 tls key-file /config/auth/keys/server.key
set interfaces openvpn vtun0 tls dh-file /config/auth/keys/dh2048.pem
set interfaces openvpn vtun0 encryption aes128
set interfaces openvpn vtun0 openvpn-option "--keepalive 8 30"
set interfaces openvpn vtun0 openvpn-option "--comp-lzo"
set interfaces openvpn vtun0 openvpn-option "--duplicate-cn"
set interfaces openvpn vtun0 openvpn-option "--user nobody --group nogroup"
set interfaces openvpn vtun0 openvpn-option "--plugin /usr/lib/openvpn/openvpn-auth-
pam.so openvpn"
set interfaces openvpn vtun0 openvpn-option "--client-cert-not-required --username-as-
common-name"
set interfaces openvpn vtun0 openvpn-option "--verb 1"
set interfaces openvpn vtun0 openvpn-option "--proto udp6"
set interfaces openvpn vtun0 openvpn-option "--port 1194"
set interfaces openvpn vtun0 openvpn-option "--push redirect-gateway def1"
set interfaces openvpn vtun0 openvpn-option "--push dhcp-option DNS 8.8.8.8"
set interfaces openvpn vtun0 openvpn-option "--push dhcp-option DNS 8.8.4.4"
```

5. Налаштування брандмауера, щоб приймав з’єднання OpenVPN через

інтерфейс WAN

```
set firewall name WAN_LOCAL rule 20 action accept
set firewall name WAN_LOCAL rule 20 description "Allow OpenVPN clients in"
set firewall name WAN_LOCAL rule 20 destination port 1194
set firewall name WAN_LOCAL rule 20 log disable
set firewall name WAN_LOCAL rule 20 protocol udp
```

6. Налаштування трафіку від користувачів OpenVPN до інтернету

```
set service nat rule 5010 description "Masquerade for WAN"
set service nat rule 5010 outbound-interface eth0
set service nat rule 5010 type masquerade
commit
save
exit
```

7. Створення файлу конфігурації .ovpn

```
client
float
dev tun

remote vpn.hostname.com 1194 udp

auth-nocache
resolv-retry infinite
nobind
persist-key
persist-tun
auth-user-pass
cipher AES-128-CBC
comp-lzo
verb 3
<ca>
-----BEGIN CERTIFICATE-----
INSERT YOUR CERT HERE
-----END CERTIFICATE-----
</ca>
```

```
# this is an random certificate. The .ovpn file needs one, but does not use it, so you can leave this as is
<cert>
-----BEGIN CERTIFICATE-----
MIIB1jCCAT+gAwIBAgIEAmLSTjANBgkqhkiG9w0BAQUFADAVMRMwEQYDVQQDEwpP
cGVuVlBOIENBMB4XDTEzMDExNzAyMTExMloXDTIzMDEyMjAyMTExMlowKDEmMCQG
A1UEAxQdZnJyaWN0aW9uQGdtYWlsLmNvbV9BVVRPTE9HSU4wgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALVEXIZYYu1Inmejuo4Si6Eo5AguTX5sg1pGbLkJSTR4
BXQsy6ocUnZ9py8htYkipkUUhjY7zDu+wJlUtWnVCwCYtewYfEc/+azH7+7eU6ue
T2K2IKdik1KWhdtNbaNphVvSlgdyKiuZDTCedptgWyiL50N7FMcUUMjjXYh/hftB
AgMBAAGjIDAeMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMA0GCSqGSIb3
DQEBBQUAA4GBABhVzSYXHlQEPNaKGmx9hMwwnNKcHgD9cCmC9lX/KR2Y+vT/QGxK
7sYlJInb/xmpa5TUQYc1nzDs9JBps1mCtZbYNNDpYnKINAKSDsM+KOQaSYQ2FhHk
bmBZk/K96P7VntzYI5S02+hOWnvjq5Wk4gOt1+L18+R/XujuxGbwnHW2
-----END CERTIFICATE-----
</cert>

# this is an random key. The .ovpn file needs one, but does not use it, so you can leave this as is
<key>
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALVEXIZYYu1Inmej
uo4Si6Eo5AguTX5sg1pGbLkJSTR4BXQsy6ocUnZ9py8htYkipkUUhjY7zDu+wJlU
tWnVCwCYtewYfEc/+azH7+7eU6ueT2K2IKdik1KWhdtNbaNphVvSlgdyKiuZDTCe
dptgWyiL50N7FMcUUMjjXYh/hftBAgMBAAECgYEAsNjgOEYVRhEaUlzfzmpzhakC
SKT8AALYaAPbYO+ZVzJdh8mIbg+xuF7A9G+7z+5ZL35lrpXKnONuvmlxkK5ESwvV
Q7EOQYCZCqa8xf3li3GUBLwcwXKtOUr3AYXhdbOh2viQdisD4Ky7H6/Nd3yMc3bu
R4pErmWeHei+l6dIwAECQQDqljNxi9babmHiei6lHaznCMg5+jfAyDXgHvO/afFr
1bDQVDTDK+64kax4E9pvDZC6B/HGse9hOUGWXTjb0WZBAkEAxdAw/14iJIUcE5sz
HDy2R0RmbUQYFjrNgBCi5tnmr1Ay1zHAs1VEF+Rg5IOtCBO50I9jm4WCSwCtN6zF
FoFVAQJAUGfBJDcZIm9ZL6ZPXJrqS5oP/wdLmtFE3hfd1gr7C8oHu7BREWB6h1qu
8c1kPlI4+/qDHWaZtQpJ977mITOJwQJAMcgUHKAm/YPWLgT31tpckRDgqgzh9u4z
e1A0ft5FlMcdFFT8BuWlblHWJIwSxp6YO6lqSuBNiuyPqxw6uVAxAQJAWGxOgn2I
fGkWLLw4WMpkFHmwDVTQVwhTpmMP8rWGYEdYX+k9HeOJyVMrJKg2ZPXOPtybrw8T
PUZE7FgzVNxypQ==
-----END PRIVATE KEY-----
</key>
```

8. Налаштування Radius для автентифікації

```
auth sufficient pam_radius_auth.so debug
account sufficient pam_permit.so
session sufficient pam permit.so
```

9. Збереження налаштувань

```
mkdir /config/scripts/ovpn_radius_config
cp /etc/pam_radius_auth.conf /config/scripts/ovpn_radius_config/pam_radius_auth.conf
cp /etc/pam.d/openvpn /config/scripts/ovpn radius config/openvpn
```

```
#!/bin/vbash
readonly logFile="/var/log/postprovision.log"

source /opt/vyatta/etc/functions/script-template

echo "$(date) - Beginning post provision steps" >> ${logFile}
#restore the ssmtp configuration

cp -f /config/scripts/ovpn_radius_config/pam_radius_auth.conf /etc
cp -f /config/scripts/ovpn_radius_config/openvpn /etc/pam.d/openvpn

#the following lines remove the postprovision scheduled task
#do not modify below this line

configure >> ${logFile}
delete system task-scheduler task postprovision >> ${logFile}
commit >> ${logFile}
save >> ${logFile}
#exit

#end no edit

exit

echo "$(date) - Finished post provision steps" >> ${logFile}
```

```
#!/bin/vbash
readonly logFile="/var/log/postreboot.log"

source /opt/vyatta/etc/functions/script-template

#restore the radius configuration
echo "Copying PAM and OpenVPN config files" >> ${logFile}
cp -f /config/scripts/ovpn_radius_config/pam_radius_auth.conf /etc
cp -f /config/scripts/ovpn radius config/openvpn /etc/pam.d/openvpn
```