PiOSK projekt

Klinika medyczna

Klinika medyczna "HealthCare Plus"

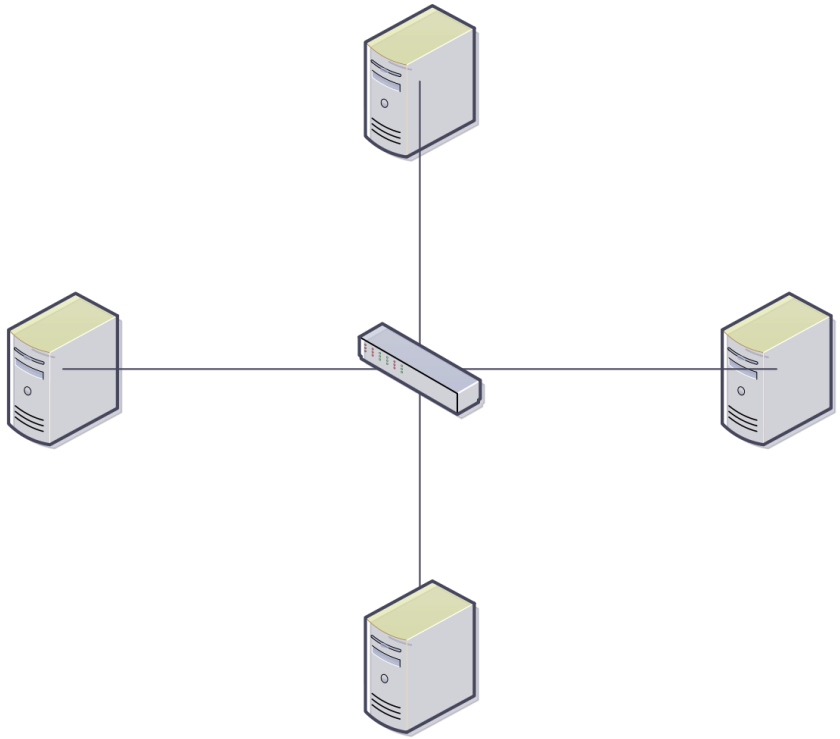
Naszym zadaniem było opracowanie projektu sieci dla małej kliniki która posiada 15 pracowników i 25 urządzeń takich jak komputery lekarzy i sprzęt medyczny.

Zadania które spełnia sieć

Zadaniem sieci jest szybki dostęp do informacji, przechowywanie i udostępnianie historii medycznych pacjentów oraz wyników badań.

Wybrana topologia

Po zapoznaniu się z wszystkimi topologiami uznaliśmy że najlepszym wyborem dla naszej kliniki jest topologia gwiazdy. Ponieważ jest to stabilne rozwiązanie, które zapewnia prosty dostęp do zarządzania siecią oraz pozwala na łatwe rozszerzenie sieci w przyszłości



Jaki sprzęt sieciowy?

Switch - 1000zł
Centralnym urządzeniem w topologii gwiazdy będzie główny switch.
Zdecydowaliśmy się na sprawdzony model cisco
WS-C2960X-24PS-L

Router - 1200zł
Chociaż topologia gwiazdy nie wymaga routera do przesyłania danych dodaliśmy urządzenie z funkcjami zabezpieczeń, takie jak firewall i VPN.
Co do routera zdecydowaliśmy się na
ASUS RT-AX88U

Jaki sprzęt sieciowy?

Access Point - 700zł
Klinika potrzebuje dostępu do sieci bezprzewodowej dla swojego personelu lub pacjentów
Naszym rekomendowanym access pointem będzie:
Ubiquiti UniFi AP-AC Pro

Magazyn danych w chmurze

Model sieci

Podsieć 1: Dla pracowników administracyjnych i biurowych
Adres IP: 172.17.10.0/24
Liczba adresów IP: 6

Przykładowe adresy IP:
Dla urządzeń: 172.17.10.2 - 172.17.10.4
Dla drukarek sieciowych: 172.17.10.5 - 172.17.10.6

Model sieci

Podsieć 2: Dla lekarzy i personelu medycznego
Adres IP: 172.17.20.0/24
Liczba adresów IP: 17

Przykładowe adresy IP:
Dla urządzeń: 172.17.20.2 - 172.17.20.9
Dla sprzętu medycznego: 172.17.20.10 - 172.17.20.18

Uzasadnienie

Izolacja sieci dla pracowników administracyjnych od sieci medycznej jest zalecana w celu ochrony danych pacjentów przed nieautoryzowanym dostępem oraz zminimalizowania ryzyka ataków na systemy informatyczne w obszarze opieki zdrowotnej. Taka separacja ułatwia także zarządzanie ruchem sieciowym

Model sieci

Podsieć bezprzewodowa 1: Dla pacjentów sieć publiczna
Oddzielona od pozostałych sieci dla jak największego bezpieczeństwa przez odosobniony VLAN.
Nazwa sieci: HealthCare_Public
Liczba adresów IP: Dynamiczna
Adresy przydzielane automatyczne za pomocą protokołu DHCP

Podsieć bezprzewodowa 2: Dla pracowników kliniki
Nazwa sieci: HealthCare_Internal
Zabezpieczona protokołem: WPA3
Liczba adresów IP: Dynamiczna
Adresy przydzielane automatyczne za pomocą protokołu DHCP

Uzasadnienie

Izolacja danych Każda podsieć jest dedykowana dla określonej grupy, co pomaga w zabezpieczeniu i izolacji danych.

Skalowalność i wydajność Podział na podsieci pozwala na efektywne zarządzanie ruchem sieciowym i zapobieganie przeciążeniu sieci.

Łatwość zarządzania Prosta struktura podsieci ułatwia zarządzanie i konserwację sieci.

Oddzielenie sieci pracowników od sieci dla pacjentów: Utworzenie dwóch oddzielnych sieci bezprzewodowych pozwala na segregację urządzeń i użytkowników.

Protokoły używane w sieci

VLAN (Virtual Local Area Network) jest dobrym rozwiązaniem w małej sieci. VLAN pozwala na logiczne podzielenie jednej fizycznej sieci na kilka odrębnych segmentów, co może przynieść kilka korzyści:

-**Segmentacja ruchu**

-Bezpieczeństwo

-Łatwiejsze zarządzanie

-Optymalizacja wydajności

DHCP (Dynamic Host Configuration Protocol) do przydzielania automatycznych adresów IP
DNS (Domain Name System) do rozwiązywania nazw domen. Jest użyteczny w diagnostyce sieciowej i monitorowaniu ruchu sieciowego.

Protokoły używane w sieci

Dla Wi-Fi wykorzystamy

WPA3 najnowsza wersja, z zaawansowanymi protokołami szyfrowania, chroniące przed atakami typu "offline" i innymi nowoczesnymi technikami ataków.

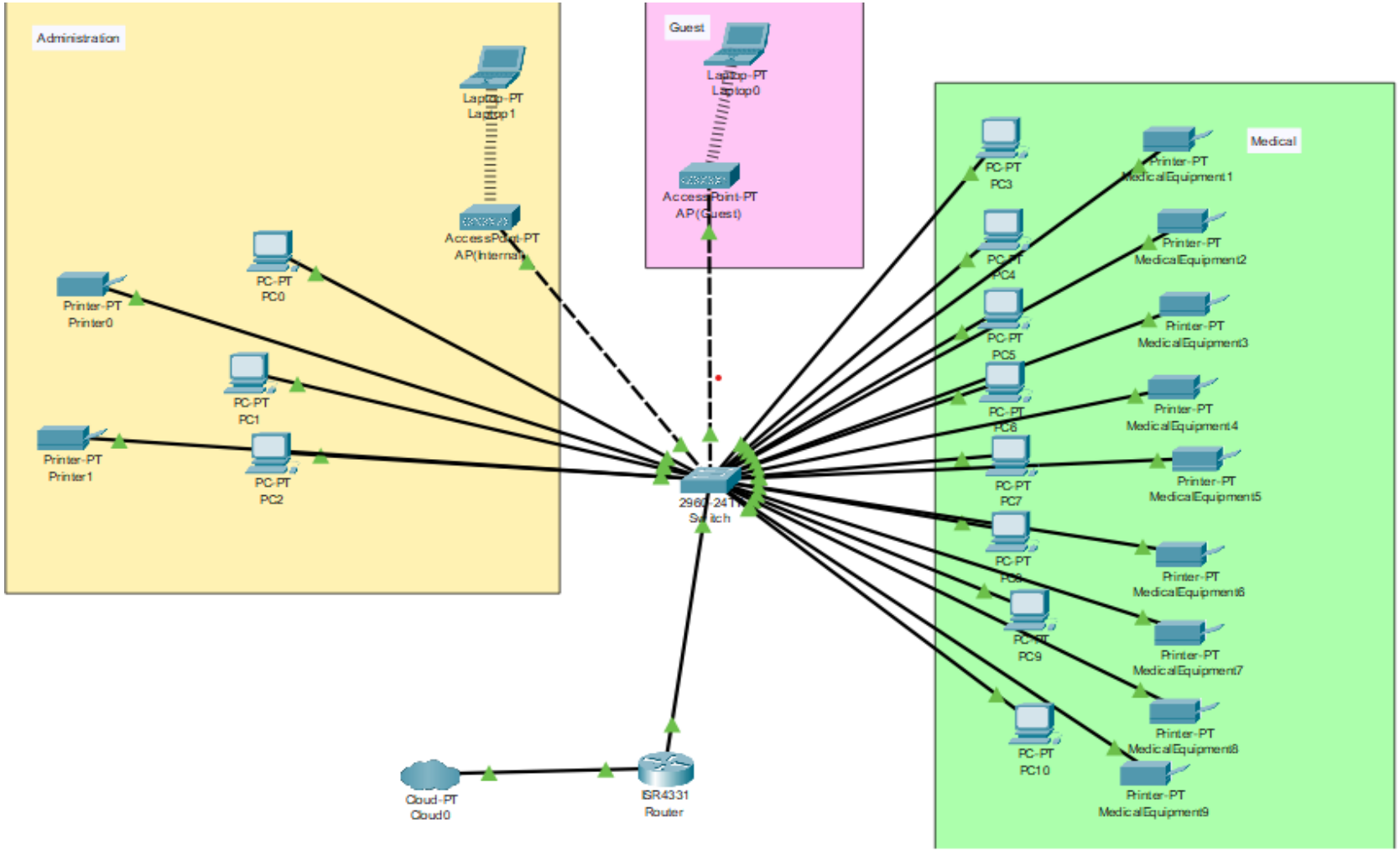
oraz zaimplementujemy **Firewall** na poziomie urządzeń i bramy sieciowej.

Zabezpieczenia sieci

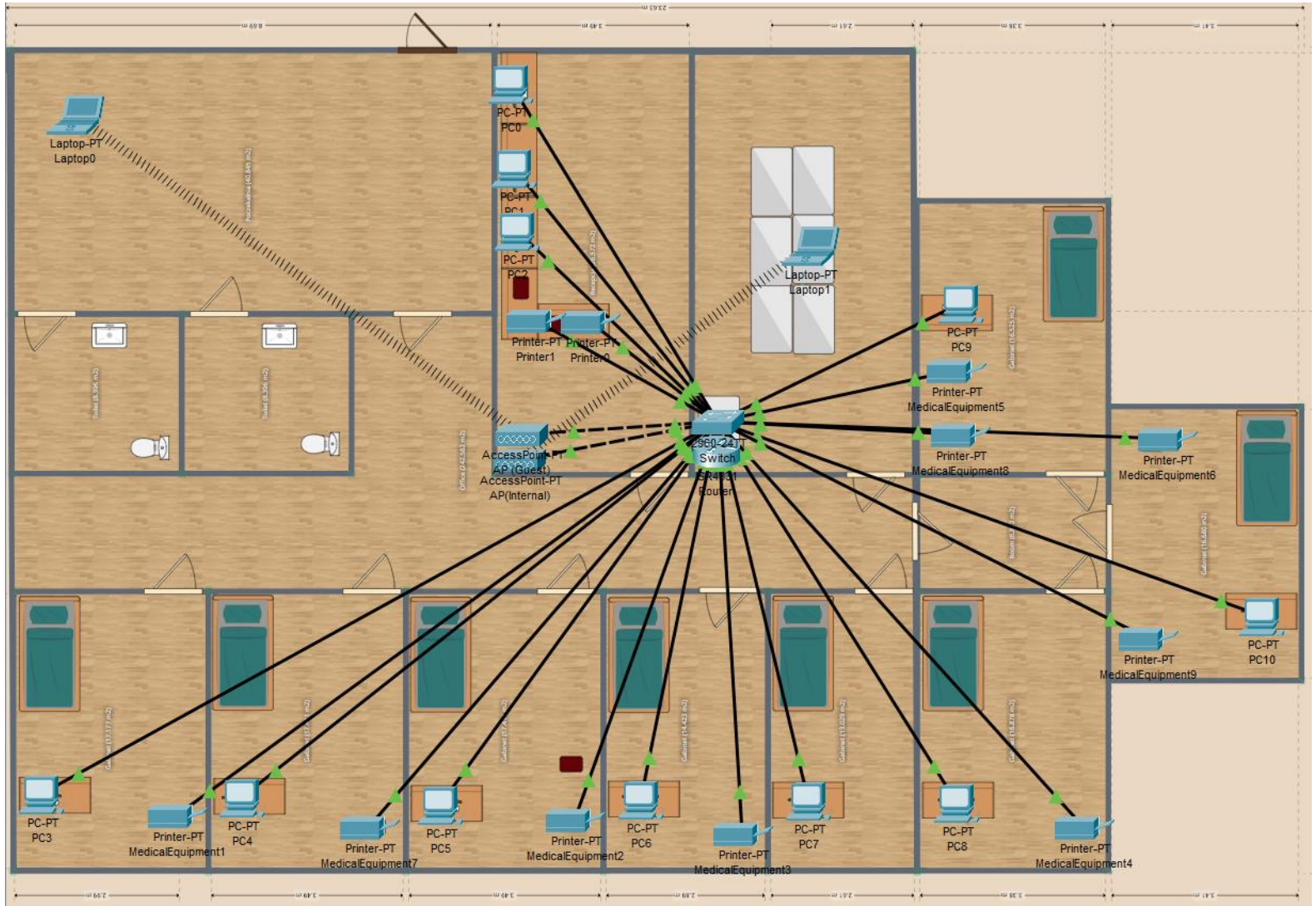
firewall - administrator ma możliwość określać jaki ruch powinien być przez firewall przepuszczany a jaki blokowany
IPS – system Intrusion Prevention wykorzystuje technologię wykrywania i blokowania ataków ASQ
serwer VPN - pozwala na tworzenie bezpiecznych połączeń, tzw. kanałów VPN
Technologia SFTP - to protokół zapewniający bezpieczny transfer plików między urządzeniami w sieci.

Fizyczny model naszej kliniki

Topologia sieci kliniki



Topologia sieci rzutowana na fizyczny model



Dziękujemy za uwagę