Slajd 2

Zadaniem naszej grupy było stworzenie sieci obsługującej Klinikę medyczną

"HealthCare Plus"

Slajd 3

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 i zapewnia zgodność z przepisami dotyczącymi ochrony danych medycznych.

Slajd 4

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

Slajd 5

WS-C2960X-24PS-L

- **Zaawansowane funkcje warstwy 2 i warstwy 3:**
- **Power over Ethernet Plus (PoE+):**
- **Wysoka moc wyjściowa PoE na port:**
- **Wsparcie dla różnych rodzajów interfejsów:**
- **Zaawansowane zarządzanie siecią:**
- **Wsparcie dla różnorodnych urządzeń:**

ASUS RT-AX88U

- **Standard Wi-Fi 6 (802.11ax):**
- **Prędkość transmisji bezprzewodowej 6000 Mb/s:**
- **Zabezpieczenia bezprzewodowe:**
- **Obsługa wielu trybów pracy:**
- **Zarządzanie i konfiguracja:**
- **Obsługa VPN, QoS, serwery sieciowe:**
- **Obsługa IPv6:**
- **Dodatkowe funkcje i zabezpieczenia:**

Slajd 6

Ubiquiti UniFi AP-AC Pro

- **Standard Wi-Fi ac i wysoka wydajność:**
- **Zastosowanie technologii 3x3 MIMO:**
- **Dwa gigabitowe porty Ethernet:**
- **Odporność na warunki zewnętrzne:**
- **Produkt Ubiquiti i serwery UniFi:**
- **Wysoka reputacja na rynku:**

Magazyn danych

Po długiej analizie możliwości zdecydowaliśmy się na rozwiązanie w chmurze głównie ze względu na swoją cenę w implementacji, są to koszta rutynowe ale zdecydowanie mniejsze niż lokalny server.

1. Bezpieczeństwo danych: Usługi chmurowe często oferują wysoki poziom zabezpieczeń, w tym szyfrowanie danych, kontrolę dostępu i systemy monitorowania.
2. Dostępność i skalowalność: Rozwiązania w chmurze mogą zapewnić wysoką dostępność danych oraz elastyczność w zakresie skalowania zasobów w zależności od potrzeb, co jest ważne w przypadku wzrostu liczby pacjentów i danych medycznych.
3. Redundancja i backup danych: Usługi chmurowe często zapewniają automatyczne tworzenie kopii zapasowych, co minimalizuje ryzyko utraty danych.
4. Koszty: Rozwiązania chmurowe często wymagają niższych kosztów początkowych niż zakup i utrzymanie własnej infrastruktury serwerowej.

Slajd 7

Dla urządzeń podłączonych do naszej sieci zdecydowaliśmy się na podział jej na 3 podsieci, 2 używane głównie przewodowo i 1 bezprzewodowo za pomocą vlanów.

Pierwszą siecią jest sieć administracyjna stworzona dla pracowników na recepcji

Slajd 8

Druga jest sieć dla personelu medycznego

Slajd 9

Istotną kwestią tutaj jest brak połączenia trunk, jest to świadoma decyzja poniważ 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

Recepcja powinna mieć dostęp tylko do podstawowych informacji pacjentów koniecznych do rejestrowania terminów wizyt.

Lekarze powinni jako jedyni mieć dostęp do historii medycznej pacjentów aby chronić dane osobowe.

Slajd 10

W przypadku sieci bezprzewodowych, mamy sieć wewnętrzną i publiczną gdzie sieć publiczna ze względów bezpieczeństwa jest całkowicie odizolowana od reszty sieci

Slajd 11

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.

Slajd 12

- VLAN (Podział sieci na podsieci)
- DHCP (Dynamiczne rozdzielanie adresów)
- DNS (Diagnostyka sieci)

Slajd 13

Jako główne zabeczpieczenie sieci bezprzewodowej wewnętrznej użyjemy protokół WPA3 ora zaporę sieciową

Slajd 14

- 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.

Slajd 15

Fizyczna prezentacja modelu naszej kliniki

Slajd 16

Topologia naszej sieci