|  |  |
| --- | --- |
| **Politechnika Świętokrzyska**  **Wydział Elektrotechniki, Automatyki i Informatyki** | |
| **Bezpieczeństwo Infrastruktury Sieciowej** | |
| **Projekt** | |
| Skład zespołu: Dawid Jaszczyk, Diana Nowak, Dawid Bujak | |
| Grupa 1ID24A | Data: 10.10.2023 |
| Temat: Projekt infrastruktury sieciowej prywatnej przychodni lekarskiej (parter i piętro) | |

Repozytorium: <https://github.com/Dawol1/PrzychodniaBIS>

Spis treści

[1. Cel projektu 3](#_Toc153788676)

[2. Harmonogram prac 3](#_Toc153788677)

[3. Założenia sieci 3](#_Toc153788678)

[4. Opis zagrożeń 5](#_Toc153788679)

[5. Podział na podsieci 5](#_Toc153788680)

[6. Konfiguracja urządzeń 7](#_Toc153788681)

[7. Bezpieczeństwo sieci 14](#_Toc153788682)

[Radius 14](#_Toc153788683)

[DNS 15](#_Toc153788684)

[Firewall 17](#_Toc153788685)

[ACL 18](#_Toc153788686)

[Logowanie do R1 20](#_Toc153788687)

[SSH 20](#_Toc153788688)

[NTP 21](#_Toc153788689)

[AAA 22](#_Toc153788690)

[Port Monitor 22](#_Toc153788691)

[RIP 23](#_Toc153788692)

[OSPF 23](#_Toc153788693)

Spis ilustracji

[Rysunek 2.1 Schemat sieci 3](#_Toc138077825)

[Rysunek 5.1 Radius 13](#_Toc138077826)

[Rysunek 5.2 Syslog 13](#_Toc138077827)

[Rysunek 5.3 DNS - konfiguracja 14](#_Toc138077828)

[Rysunek 5.4 Uruchomiona strona 15](#_Toc138077829)

[Rysunek 5.5 Sprawdzenie działania firewall 16](#_Toc138077830)

[Rysunek 5.6 Efekt działania firewall 16](#_Toc138077831)

[Rysunek 5.7 ACL - ta sama podsieć 17](#_Toc138077832)

[Rysunek 5.8 ACL - inna podsieć 17](#_Toc138077833)

[Rysunek 5.9 ACL - drukarka w tej samej podsieci 18](#_Toc138077834)

[Rysunek 5.10 ACL - drukarka w innej podsieci 18](#_Toc138077835)

[Rysunek 5.11 Zabezpieczenie dostępu 19](#_Toc138077836)

[Rysunek 5.12 SSH 19](#_Toc138077837)

[Rysunek 5.13 NTP - konfiguracja 20](#_Toc138077838)

[Rysunek 5.14 NTP - sprawdzenie 20](#_Toc138077839)

[Rysunek 5.15 AAA 21](#_Toc138077840)

[Rysunek 5.16 Port monitor - konfiguracja 21](#_Toc138077841)

[Rysunek 5.17 Port monitor - sprawdzenie działania 22](#_Toc138077842)

# Cel projektu

W ramach projektu z zajęć „Wstęp do Cyberbezpieczeństwa” należy przygotować projekt sieci organizacji w programie Cisco Packet Tracer. Sieć ta musi odzwierciedlać prawdziwą topologię organizacji, czyli fizyczne odzwierciedlenie sprzętu komputerowego, połączeń oraz konfiguracji. Sieć musi zawierać także kilka protokołów zabezpieczających ją.

# Harmonogram prac

|  |  |
| --- | --- |
| **Data** | **Planowane wykonane czynności** |
| 10.10.2023 | Ustalenie tematu projektu oraz jego zakresu, a także harmonogramu. |
| 14.11.2023 | Określnie wymagań, jakie mogą czekać wykreowaną sieć. Gotowy schemat infrastruktury sieciowej w programie Cisco Packet Tracer. Przydzielenie sieci, podsieci, zaadresowanie urządzeń, konfiguracja serwera DHCP, konfiguracja poziomów dostępowych na urządzeniach sieciowych, dynamiczne protokoły routingu. Weryfikacja z wymagania projektu oraz z harmonogramem. |
| 19.12.2023 | Dalszy rozwój projektu. Konfiguracja różnych usług, m.in. Syslog, NTP, AAAA, listy ACL, VLANY, RIP, OSPF. Weryfikacja z wymagania projektu oraz z harmonogramem. |
| 16.01.2023/23.01.2023 | Weryfikacja działania skonfigurowanego projektu sieci, a także weryfikacja z wymaganiami i harmonogramem. Prezentacja oraz obrona gotowego projektu. |

# Założenia sieci

Naszym tematem projektowanej topologii sieci jest przychodnia medyczna. W tej organizacji zakładamy, że sprzęt komputerowy czy sieciowy będzie rozmieszczony na parterze oraz 1 piętrze. Topologia przedstawia się następująco:

Obraz zawierający diagram, linia, design

Opis wygenerowany automatycznie

Rysunek . Schemat sieci

Mamy tutaj podział na 2 piętra.

**Parter:**

* Księgowość
  + S0
  + PC0
  + PC1
  + Printer0
* Baza danych/archiwum
  + Server0
  + S1
* Gabinet1
  + S2
  + PC3
  + PC4
  + Printer1
* Obsługa klienta / rejestracja
  + S3
  + PC5
  + PC6
  + PC7
  + Printer2
* R0

**Pierwsze piętro:**

* Administracja
  + R3
  + S6
  + PC2
* Gabinet 2
  + S4
  + Laptop0
  + Laptop1
  + Printer3
* Gabinet 3
  + S5
  + Laptop2
  + Laptop3
  + Printer4
* R1
* R3

Pomiędzy parterem a pierwszym piętrem występuje łączenie poprzez routery.

# Opis zagrożeń

Jak każda infrastruktura, tworzony projekt też będzie podatny na przeróżne zagrożenia.

Pierwszym potencjalnym zagrożeniem jest dostęp osób z zewnątrz do serwera a tym samym do danych medycznych.

Drugim potencjalnym zagrożeniem są ataki DDoS, którą mogą obciążyć całą sieć, spowolnić ją lub nawet doprowadzić do awarii.

Kolejnym potencjalnym zagrożeniem jest nieautoryzowany dostęp pracowników. Nie każdy pracownik musi mieć dostęp do wszystkiego, a jedynie do niezbędnych zasobów. Należy więc zadbać o to, aby uprawnienia były odpowiednio nadane. W sieci przewidywane są także komputery dla pacjentów, które szczególnie trzeba zabezpieczyć przed ewentualną niechcianą ingerencją.

Innym potencjalnym zagrożeniem jest ryzyko przechwycenia danych pacjentów, ze względu na brak szyfrowania komunikacji.

Jeszcze innym zagrożeniem jest nieautoryzowany dostęp. Brak odpowiednich mechanizmów uwierzytelniania i autoryzacji może prowadzić do nieautoryzowanego dostępu do danych pacjentów.

Wszystkie zagrożenia są dosyć niebezpieczne i mogą być fatalne w skutkach. Należy więc zadbać o prawidłowe zabezpieczenie, co pozwoli na ich wyeliminowaniem lub zminimalizowanie.

# Podział na podsieci

W projektowanej sieci zastosowaliśmy następujący podział:

* **Parter**
  + Adres sieci: 192.168.1.0
  + Maska: 255.255.255.0

Podział na podsieci:

* **Obsługa klienta / rejestracja**
  + Adres sieci: 192.168.1.0
  + Maska: 255.255.255.248
* **Księgowość**
  + Adres sieci: 192.168.1.8
  + Maska: 255.255.255.248
* **Baza danych / archiwum**
  + Adres sieci: 192.168.1.24
  + Maska: 255.255.255.248
* **Gabinet** **1**
  + Adres sieci: 192.168.1.16
  + Maska: 255.255.255.248
* **Połączenie pomiędzy routerami**
  + Adres sieci: 192.168.1.32
  + Maska: 255.255.255.252
* **Połączenie pomiędzy routerami**
  + Adres sieci: 192.168.1.36
  + Maska: 255.255.255.248
* **Pierwsze piętro**
  + Adres sieci: 192.168.2.0
  + Maska: 255.255.255.0

Podział na podsieci:

* **Gabinet** 1
  + Adres sieci: 192.168.2.0
  + Maska: 255.255.255.248
* **Księgowość**
  + Adres sieci: 192.168.2.8
  + Maska: 255.255.255.248
* **Połączenie pomiędzy routerami**
  + Adres sieci: 192.168.2.16
  + Maska: 255.255.255.248
* **Administracja**
  + Adres sieci: 192.168.2.24
  + Maska: 255.255.255.248

# Konfiguracja urządzeń

**Server0**

* Brama: 192.168.1.25
* Serwer DNS: 0.0.0.0
* FastEthernet0
  + Adres:192.168.1.26
  + Maska: 255.255.255.252
* Uruchomiony serwer DNS: strona.pl na adresie 192.168.1.26
* Uruchomiony firewall – możliwość dostępu do strony ale brak możliwości pingowania serwera
* Uruchomione AAA, serwer Radius
  + Nazwa hosta: R1
  + Adres: 192.168.1.25
  + Typ: Radius
  + Hasło/klucz: cisco
  + Użytkownicy
    - Nazwa: user
    - Hasło: cisco
* Uruchomiony serwer Syslog
* Uruchomiony serwer NTP
  + Klucz: 1
  + Hasło: cisco

**PC0**

* Brama: 192.168.1.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.10
  + Maska: 255.255.255.248

**PC2**

* Brama: 192.168.1.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.11
  + Maska: 255.255.255.248

**Printer0**

* Brama: 192.168.1.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.10
  + Maska: 255.255.255.248

**S0**

* VLAN1
  + Adres:192.168.1.13
  + Maska: 255.255.255.248
* Konfiguracja ssh
  + Nazwa : user
  + Hasło: haslo
* Konfiguracja Port Monitor – z portów FastEthernet3/1 i FastEthernet1/1 na port FastEthernet2/1.

**Printer0**

* Brama: 192.168.1.25
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.16
  + Maska: 255.255.255.248

**S1**

* VLAN1
  + Adres:192.168.1.27
  + Maska: 255.255.255.248
* Konfiguracja ssh
  + Nazwa : user
  + Hasło: haslo

**S2**

* VLAN1
  + Adres:192.168.1.22
  + Maska: 255.255.255.248
* Konfiguracja ssh
  + Nazwa : user
  + Hasło: haslo

**PC3**

* Brama: 192.168.1.17
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.18
  + Maska: 255.255.255.248

**PC4**

* Brama: 192.168.1.17
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.19
  + Maska: 255.255.255.248

**Printer1**

* Brama: 192.168.1.17
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.20
  + Maska: 255.255.255.248

**S3**

* VLAN1
  + Adres:192.168.1.6
  + Maska: 255.255.255.248
* Konfiguracja ssh
  + Nazwa : user
  + Hasło: haslo

**Printer1**

* Brama: 192.168.1.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.5
  + Maska: 255.255.255.248

**PC5**

* Brama: 192.168.1.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.2
  + Maska: 255.255.255.248

**PC6**

* Brama: 192.168.1.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.3
  + Maska: 255.255.255.248

**PC7**

* Brama: 192.168.1.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.1.4
  + Maska: 255.255.255.248
* Zabroniony dostęp przez ACL (brak możliwość komunikacji z siecią, komputer dla pacjentów)

**R1**

* Ethernet0/0
  + Adres:192.168.1.1
  + Maska: 255.255.255.248
* Ethernet0/1
  + Adres:192.168.1.9
  + Maska: 255.255.255.248
* Ethernet0/2
  + Adres:192.168.1.25
  + Maska: 255.255.255.252
* Ethernet0/3
  + Adres:192.168.1.17
  + Maska: 255.255.255.248
* Ethernet0/4
  + Adres:192.168.1.33
  + Maska: 255.255.255.252
* Routing statyczny
  + 192.168.2.0/24 przez port 192.168.1.34
* RIP
  + 192.168.1.0
* OSPF
  + 192.168.1.0
* ACL
  + Numer listy: 1
    - Zabroniona komunikacja dla PC7 (komputer dla pacjentów)
      * Standard IP access list 1
        + 10 deny host 192.168.1.4 (16 match(es))
        + 20 permit any (16 match(es))
  + Numer listy : 2
    - Zabroniona komunikacja z drukarkami poza tymi, które znajdują się w danej podsieci
      * Standard IP access list 2
        + 10 deny host 192.168.1.12 (3 match(es))
        + 20 deny host 192.168.1.20 (7 match(es))
        + 30 deny host 192.168.1.5
        + 40 deny host 192.168.2.4
        + 50 deny host 192.168.2.12
        + 60 permit any (23 match(es))
* Synchronizacja z serwerem NTP
* Username: user
* Hasło: cisco
* Hasło do trybu enable: cisco

**R2**

* Ethernet0/0
  + Adres:192.168.1.34
  + Maska: 255.255.255.252
* Ethernet0/1
  + Adres:192.168.2.1
  + Maska: 255.255.255.248
* Ethernet0/2
  + Adres:192.168.2.9
  + Maska: 255.255.255.248
* Ethernet0/3
  + Adres:192.168.2.17
  + Maska: 255.255.255.248
* Routing statyczny
  + 192.168.1.0/24 przez port 192.168.1.33
  + 192.168.2.24/29 przez port 192.168.2.18
* RIP
  + 192.168.1.0
  + 192.168.2.0
* OSPF
  + 192.168.1.0
  + 192.168.2.0
* ACL
  + Numer listy: 1
    - Zabroniona komunikacja dla PC7 (komputer dla pacjentów)
      * Standard IP access list 1
        + 10 deny host 192.168.1.4 (32 match(es))
        + 20 permit any (39 match(es))Numer listy : 2
    - Zabroniona komunikacja z drukarkami poza tymi, które znajdują się w danej podsieci
      * Standard IP access list 2
        + 10 deny host 192.168.1.12
        + 20 deny host 192.168.1.20
        + 30 deny host 192.168.1.5
        + 40 deny host 192.168.2.4 (4 match(es))
        + 50 deny host 192.168.2.12 (4 match(es))
        + 60 permit any (16 match(es))
* Synchronizacja z serwerem NTP
* Username: user
* Hasło: cisco
* Hasło do trybu enable: cisco

**R3**

* Ethernet0/0
  + Adres:192.168.2.18
  + Maska: 255.255.255.252
* Ethernet1/0
  + Adres:192.168.2.25
  + Maska: 255.255.255.248
* Routing statyczny
  + 192.168.1.0/24 przez port 192.168.2.17
* RIP
  + 192.168.2.0
* OSPF
  + 192.168.2.0
* Synchronizacja z serwerem NTP
* Username: user
* Hasło: cisco
* Hasło do trybu enable: cisco

**S6**

* VLAN1
  + Adres:192.168.2.27
  + Maska: 255.255.255.248

**PC2**

* Brama: 192.168.2.17
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.26
  + Maska: 255.255.255.248

**S4**

* VLAN1
  + Adres:192.168.2.5
  + Maska: 255.255.255.248

**Printer3**

* Brama: 192.168.2.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.4
  + Maska: 255.255.255.248

**Laptop1**

* Brama: 192.168.2.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.3
  + Maska: 255.255.255.248

**Laptop0**

* Brama: 192.168.2.1
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.2
  + Maska: 255.255.255.248

**S5**

* VLAN1
  + Adres:192.168.2.13
  + Maska: 255.255.255.248

**Printer4**

* Brama: 192.168.2.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.12
  + Maska: 255.255.255.248

**Laptop2**

* Brama: 192.168.2.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.10
  + Maska: 255.255.255.248

**Laptop3**

* Brama: 192.168.2.9
* Serwer DNS: 192.168.1.26
* FastEthernet0
  + Adres:192.168.2.11
  + Maska: 255.255.255.248

**DHCP**

R1

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Rysunek . DHCP R1

R2

Obraz zawierający tekst, Czcionka, zrzut ekranu, numer

Opis wygenerowany automatycznie

Rysunek . DHCP R2

R3

Obraz zawierający tekst, Czcionka, zrzut ekranu, linia

Opis wygenerowany automatycznie

Rysunek . DHCP R3

# Bezpieczeństwo sieci

## Radius

Próbujemy z R2 połączyć się z serwerem

Obraz zawierający tekst, zrzut ekranu, linia

Opis wygenerowany automatycznie

Rysunek . Radius

Sprawdzanie działania serwera Syslog

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . Syslog

## DNS

Na serwerze pod adresem strona.pl uruchomiona jest usługa DNS. Widnieje strona przychodni pod adresem 192.168.1.26 lub nazwą DNS, czyli strona.pl.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Opis wygenerowany automatycznie

Rysunek . DNS - konfiguracja

Po wejściu na adres strona.pl widnieje taka strona.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie

Rysunek . Uruchomiona strona

## Firewall

Na serwerze Server0 skonfigurowana jest usługa firewall. Oznacza to, że nikt nie może pingować sewera, jednak może korzystać z usług na nim uruchomionych, np. DNS.

Sprawdzamy więc poprawność. Z PC1 uruchamiamy stronę strona.pl.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie

Rysunek . Sprawdzenie działania firewall

A teraz spróbujmy użyć polecenia ping z PC1 do serwera.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Rysunek . Efekt działania firewall

Jak widać konfiguracja działa poprawnie.

## ACL

Na routerach zostały skonfigurowane listy ACL.

Ograniczenie dotyczy PC7, który nie może pingować się poza podsiecią, w której się znajduje.

Ping do PC6 znajdującego się w tej samej podsieci.

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . ACL - ta sama podsieć

Ping do PC1 znajdującego się poza podsiecią.

Obraz zawierający tekst, oprogramowanie, Strona internetowa, Ikona komputerowa

Opis wygenerowany automatycznie

Rysunek . ACL - inna podsieć

Jak widać lista ACL działa poprawnie.

Inną konfiguracją listy jest ograniczenie możliwości pingowania drukarki to tej samej podsieci. Oznacza to, że komputery mogą pingować drukarkę w tej samej podsieci, jednak drukarkę znajdującą się w innej podsieci już nie.

Wybierzmy dla przykładu Gabinet 2.

Pingujemy z Laptopa0 do Printer3.

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . ACL - drukarka w tej samej podsieci

Jak widać ping działa poprawnie. A teraz załóżmy, że z laptopa0 chcemy spingować Printer0 znajdującą się w Księgowości.

Obraz zawierający elektronika, tekst, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . ACL - drukarka w innej podsieci

Jak widać ping jest nieosiągalny.

Tak samo ograniczenie analogicznie wygląda dla pozostałych drukarek.

Lista ACL 2 jak widać działa.

## Logowanie do R1

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie

Rysunek . Zabezpieczenie dostępu

Logowanie do R1 zabezpieczone jest nazwą user i hasłem cisco.

## SSH

Na switchach zostały skonfigurowane SSH.

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . SSH

Danymi do logowania jest user oraz hasło haslo.

## NTP

Skonfigurowany został również serwer NTP.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie

Rysunek . NTP - konfiguracja

Sprawdzenie konfiguracji

Obraz zawierający tekst, Czcionka, zrzut ekranu, linia

Opis wygenerowany automatycznie

Rysunek . NTP - sprawdzenie

## AAA

Skonfigurowano również AAA.

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Opis wygenerowany automatycznie

Rysunek . AAA

## Port Monitor

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Rysunek . Port monitor - konfiguracja

Wszystkie dane przychodzące do księgowości kopiowane są więc port FastEthernet2/1.

Obraz zawierający tekst, diagram, linia, zrzut ekranu

Opis wygenerowany automatycznie

Rysunek . Port monitor - sprawdzenie działania

Jak widać konfiguracja działa poprawnie.

## RIP

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Rysunek . Konfiguracja RIP

## OSPF

Obraz zawierający tekst, zrzut ekranu, Czcionka, linia

Opis wygenerowany automatycznie

Rysunek . Konfiguracja OSPF