|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska**  Wydział Elektrotechniki, Automatyki i Informatyki | | |
| **Wprowadzenie do cyberbezpieczeństwa** – **Projekt** | | |
| **TEMAT:**  Projekt sieci dla biura rachunkowego | | **SKŁAD ZESPOŁU:**   * Przemysław Kałuziński (91271) * Jakub Kuśmierczyk () * Michał Kaczor (91268) |
| **DATA:**  15.01.2024 | **GRUPA:**  1IZ22B |

Spis treści

[1. Wstęp 3](#_Toc185619850)

[2. Struktura sieci 3](#_Toc185619851)

[3. Adresacja 3](#_Toc185619852)

[4. Podział na podsieci 3](#_Toc185619853)

[5. VLANy 3](#_Toc185619854)

[6. Serwer DHCP 3](#_Toc185619855)

[7. Konfiguracja urządzeń pod kątem dostępu SSH 3](#_Toc185619856)

[8. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS 3](#_Toc185619857)

[8.1. NTP 3](#_Toc185619858)

[8.2. CISCO IOS 3](#_Toc185619859)

[9. Lokalny SPAN 3](#_Toc185619860)

[10. Lista kontroli ACL wewnątrz zabezpieczonej sieci 3](#_Toc185619861)

[11. Zabezpieczenia STP 3](#_Toc185619862)

[12. Uwierzytelnianie AAA na serwerze przy użyciu TACACS+ 3](#_Toc185619863)

[13. Zapora sieciowa typu Private and Public (ZPF) 3](#_Toc185619864)

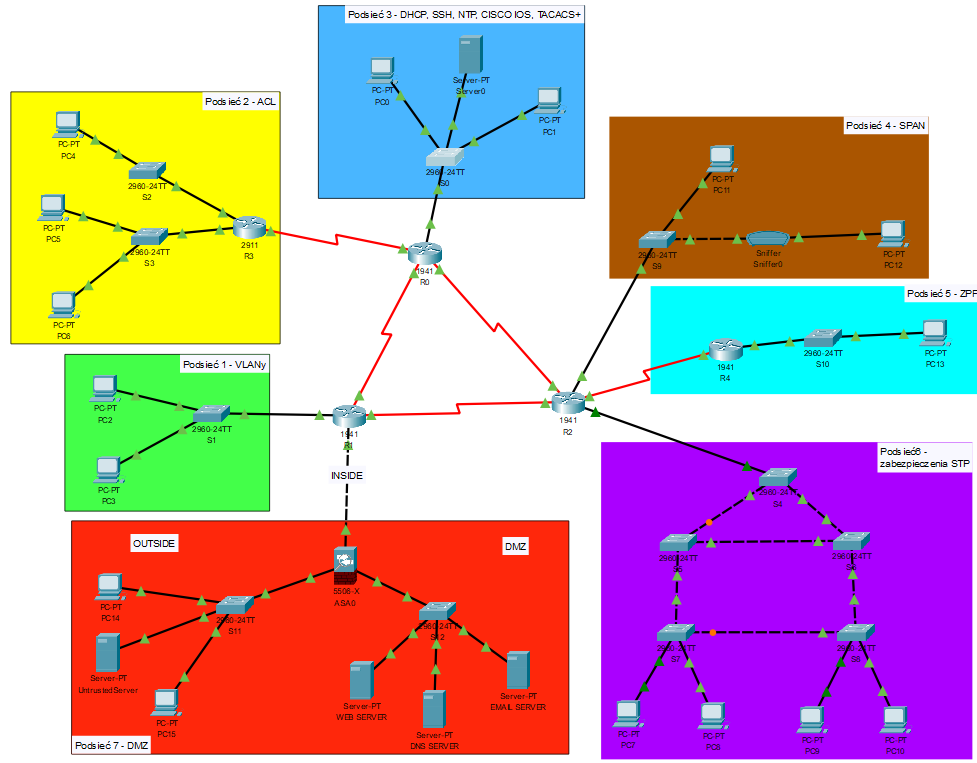
[14. Demilitarized Zone (DMZ)/Zone-Based Policy 3](#_Toc185619865)

[15. Wnioski 3](#_Toc185619866)

# Wstęp

COŚ

# Struktura sieci



# Adresacja

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Centrum sieci** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/0/0 | 1.0.0.2 | 255.0.0.0 | -- |
| R0 | Se0/0/1 | 5.0.0.1 | 255.0.0.0 | -- |
| R1 | Se0/0/0 | 1.0.0.1 | 255.0.0.0 | -- |
| R1 | Se0/0/1 | 2.0.0.1 | 255.0.0.0 | -- |
| R2 | Se0/0/0 | 2.0.0.2 | 255.0.0.0 | -- |
| R2 | Se0/0/1 | 3.0.0.1 | 255.0.0.0 | -- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 1 (VLANy)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/0.10 | 192.168.1.1 | 255.255.255.0 | -- |
| R1 | Gig0/0.20 | 192.168.2.2 | 255.255.255.0 | -- |
| S1 | Fa0/1 | -- | -- | -- |
| S1 | Fa0/2 | -- | -- | -- |
| S1 | Fa0/3 | -- | -- | -- |
| PC2 | Fa0 | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC3 | Fa0 | 192.168.2.10 | 255.255.255.0 | 192.168.2.2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 2 (ACL)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/1/0 | 4.0.0.1 | 255.0.0.0 | -- |
| R3 | Se0/3/0 | 4.0.0.2 | 255.0.0.0 | -- |
| R3 | Gig0/1 | 196.168.10.1 | 255.255.255.0 | -- |
| R3 | Gig0/2 | 196.168.20.1 | 255.255.255.0 | -- |
| S2 | -- | -- | -- | -- |
| S3 | -- | -- | -- | -- |
| PC4 | Fa0 | 196.168.10.3 | 255.255.255.0 | 196.168.10.1 |
| PC5 | Fa0 | 196.168.20.3 | 255.255.255.0 | 196.168.20.1 |
| PC6 | Fa0 | 196.168.20.4 | 255.255.255.0 | 196.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 3 (DHCP, NTP, CISCO IOS, TACACS+)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0 | 193.168.1.1 | 255.255.255.0 | -- |
| S0 | VLAN1 | 193.168.1.2 | 255.255.255.0 | 193.168.1.1 |
| PC0 | Fa0 | DHCP (193.168.1.5) | 255.255.255.0 | DHCP (193.168.1.1) |
| Server0 | Fa0 | 193.168.1.3 | 255.255.255.0 | 193.168.1.1 |
| PC1 | Fa0 | DHCP (193.168.1.4) | 255.255.255.0 | DHCP (193.168.1.1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 4 (SPAN)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/0 | 194.168.1.1 | 255.255.255.0 | -- |
| S9 | VLAN 1 | 194.168.1.2 | 255.255.255.0 | 194.168.1.1 |
| PC11 | Fa0 | 194.168.1.3 | 255.255.255.0 | 194.168.1.1 |
| Sniffer0 | -- | -- | -- | -- |
| PC12 | Fa0 | 194.168.1.4 | 255.255.255.0 | 194.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 5 (ZPF)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Se0/1/0 | 7.0.0.1 | 255.0.0.0 | -- |
| R4 | Se0/0/0 | 7.0.0.2 | 255.0.0.0 | -- |
| R4 | Gig0/0 | 198.168.1.1 | 255.255.255.0 | -- |
| S10 | -- | -- | -- | -- |
| PC13 | Fa0 | 198.168.1.3 | 255.255.255.0 | 198.168.1.1 |

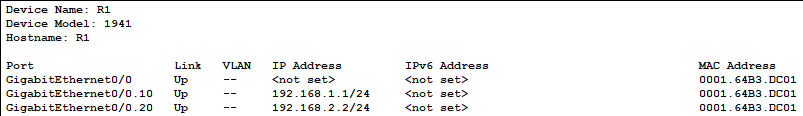
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 6 (STP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/1 | 195.168.1.1 | 255.255.255.0 | -- |
| S4 | -- | -- | -- | -- |
| S5 | -- | -- | -- | -- |
| S6 | -- | -- | -- | -- |
| S7 | -- | -- | -- | -- |
| S8 | -- | -- | -- | -- |
| PC7 | Fa0 | 195.168.1.10 | 255.255.255.0 | 195.168.1.1 |
| PC8 | Fa0 | 195.168.1.11 | 255.255.255.0 | 195.168.1.1 |
| PC9 | Fa0 | 195.168.1.12 | 255.255.255.0 | 195.168.1.1 |
| PC10 | Fa0 | 195.168.1.13 | 255.255.255.0 | 195.168.1.1 |

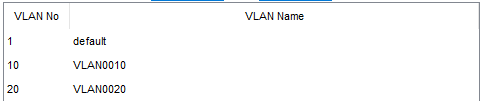
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 7 (DMZ)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/1 | 197.168.10.1 | 255.255.255.0 | -- |
| ASA0 | Gig1/1 | 197.168.10.2 | 255.255.255.0 | -- |
| ASA0 | Gig1/2 | 203.0.113.1 | 255.255.255.0 | -- |
| ASA0 | Gig1/3 | 197.168.20.1 | 255.255.255.0 | -- |
| S11 | -- | -- | -- | -- |
| S12 | -- | -- | -- | -- |
| PC14 | Fa0 | 203.0.113.2 | 255.255.255.0 | 203.0.113.1 |
| UntrustedServer | Fa0 | 203.0.113.3 | 255.255.255.0 | 203.0.113.1 |
| PC15 | Fa0 | 203.0.113.4 | 255.255.255.0 | 203.0.113.1 |
| WEB SERVER | Fa0 | 197.168.20.2 | 255.255.255.0 | 197.168.20.1 |
| DNS SERVER | Fa0 | 197.168.20.3 | 255.255.255.0 | 197.168.20.1 |
| EMAIL SERVER | Fa0 | 197.168.20.4 | 255.255.255.0 | 197.168.20.1 |

# Podział na podsieci

# VLANy

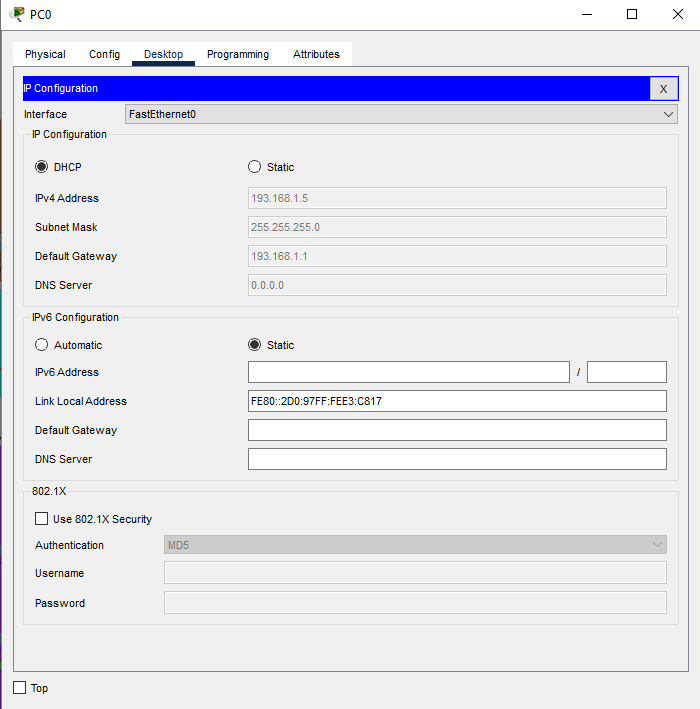
W podsieci Network 2 zostały stworzone dwa VLAN-y: VLAN 10 i VLAN 20. Jeden komputer o adresie IP 192.168.1.10 jest w VLAN-ie 10, natomiast drugi komputer o adresie IP 192.168.2.10 jest w VLAN-ie 20. Pierwszy komputer ma bramę 192.168.1.1, natomiast drugi 192.168.2.2. Kabel, który łączy switch z routerem jest trunkingowy, co oznacza, że należy do wszystkich VLAN-ów. Na routerze interfejs podłączony do switcha skonfigurowano tak, że dla VLAN-u 10 ma adres IP 192.168.1.1, a dla VLAN-u 20 192.168.2.2. Przedstawiono konfigurację adresów na routerze na rysunku poniżej. Na drugim rysunku przedstawiono utworzone VLAN-y na switchu.

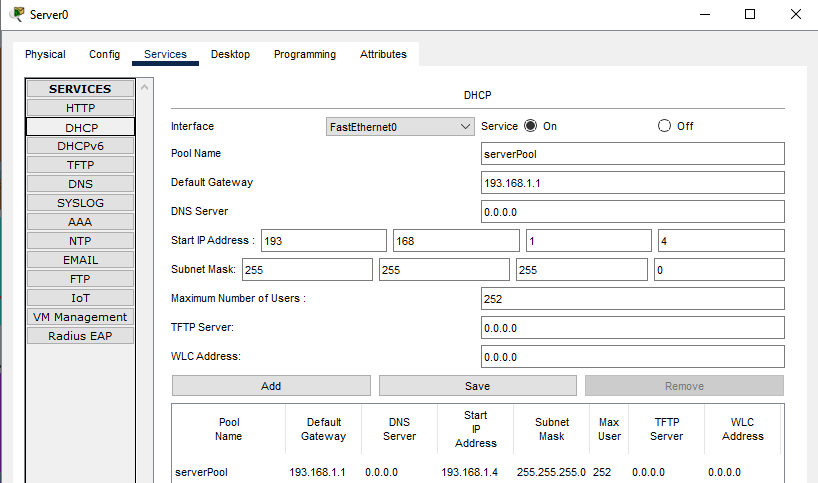




# Serwer DHCP

Serwer w podsieci *„Podsieć 3”* został skonfigurowany tak, by przydzielać komputerom adresy z puli adresów przy pomocy protokołu DHCP. Poniżej przedstawiono przykładowy adres IP hosta uzyskany z wykorzystaniem protokołu DHCP.

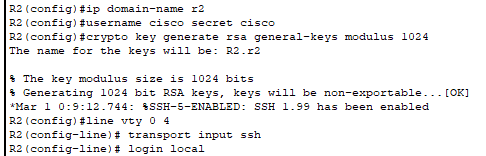


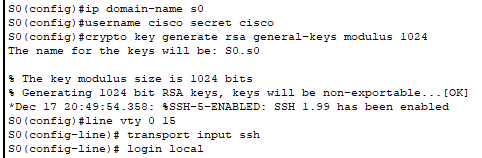


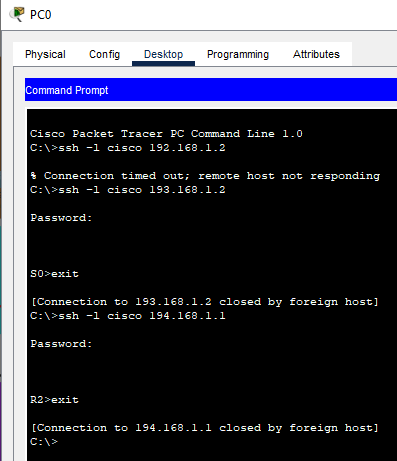
# Konfiguracja urządzeń pod kątem dostępu SSH

Do wykonania konfiguracji urządzeń pod kątem dostępu do SSH wybraliśmy urządzenia: Router2 oraz Swtich1.

W przypadku routera jak i switcha konfiguracja wyglądała bardzo podobnie. Na początku określona została nazwa domeny, po czym utworzony został użytkownik z loginem cisco i zaszyfrowanym hasłem cisco. Następnie utworzony został 1024-bitowy klucz RSA. W kolejnym kroku wykonana została konfiguracja linii VTY w celu umożliwienia dostępu do urządzeń z wykorzystaniem SSH z wykorzystaniem danych utworzonego wcześniej użytkownika. Poniżej przedstawiona została szczegółowa konfiguracja routera oraz switcha.



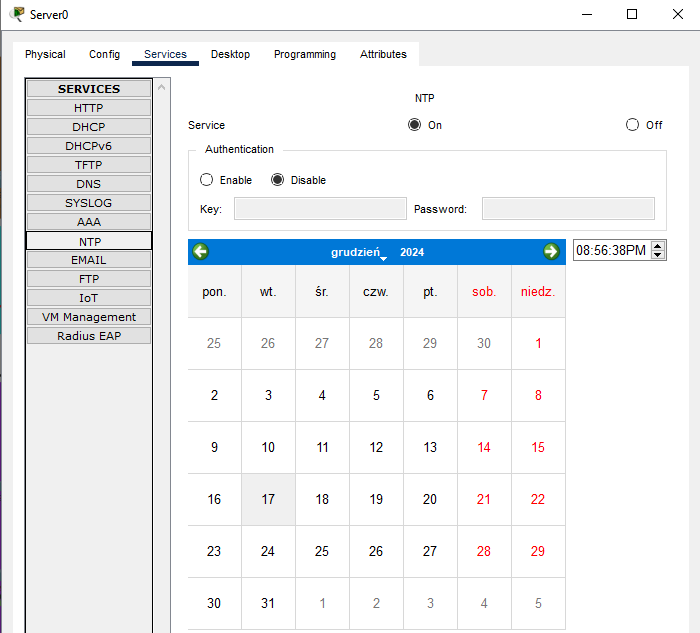




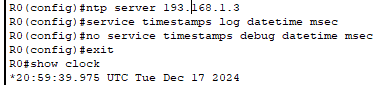
# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

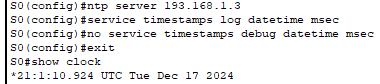
## NTP

Na początku na serwerze włączona została usługa NTP oraz ustawiony został aktualny czas.



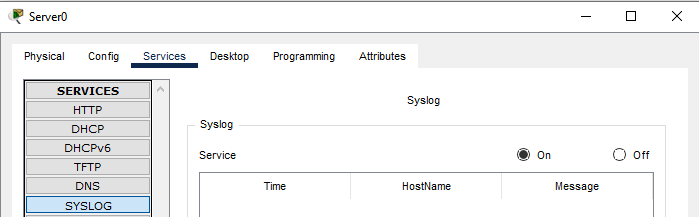
Następnie na routerze jak i na switchu określony został adres ip serwera ntp wraz z konfiguracją logowania pod kątem dołączania znaczników czasu zawierających datę, godzinę oraz milisekundy.





## CISCO IOS

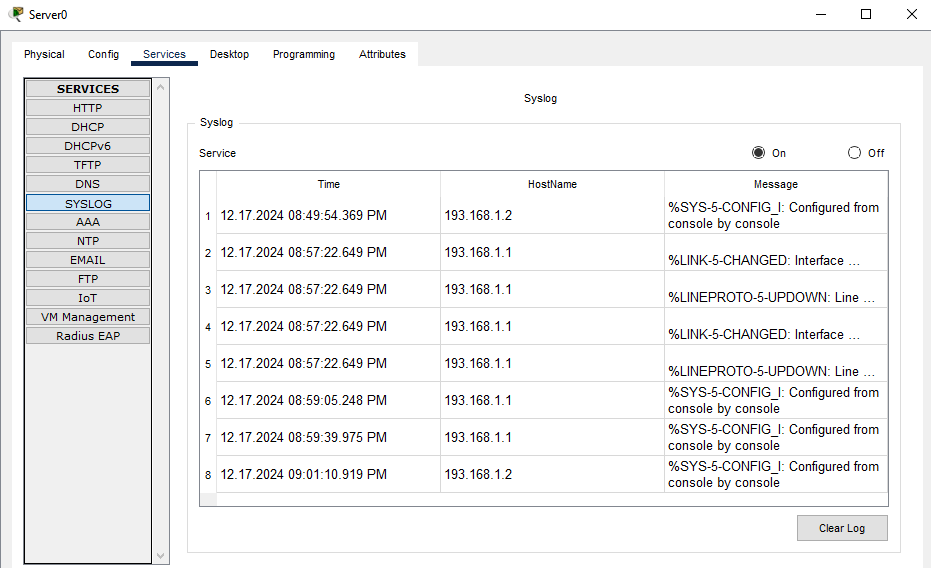
Podobnie, jak w przypadku konfiguracji NTP, pierwszym krokiem było włączenie usługi CISCO IOS na serwerze.



Następnie, z wykorzystaniem komendy *logging* na routerze oraz switchu określony został adres serwera z włączoną usługą logowania.







# Lokalny SPAN

# Lista kontroli ACL wewnątrz zabezpieczonej sieci

# Zabezpieczenia STP

# Uwierzytelnianie AAA na serwerze przy użyciu TACACS+

# Zapora sieciowa typu Private and Public (ZPF)

# Demilitarized Zone (DMZ)/Zone-Based Policy

# Wnioski