|  |  |  |
| --- | --- | --- |
| **Politechnika Świętokrzyska**  Wydział Elektrotechniki, Automatyki i Informatyki | | |
| **Bezpieczeństwo Infrastruktury Sieciowej** – **Projekt** | | |
| **TEMAT:**  Projekt sieci dla biura rachunkowego | | **SKŁAD ZESPOŁU:**   * Przemysław Kałuziński (91271) * Jakub Kuśmierczyk (97504) * Michał Kaczor (91268) |
| **DATA:**  01.06.2025 | **GRUPA:**  1IZ22B |

Spis treści

[1. Wstęp 3](#_Toc186532071)

[2. Struktura sieci 4](#_Toc186532072)

[3. Podział na podsieci 5](#_Toc186532073)

[4. Adresacja 5](#_Toc186532074)

[5. Zabezpieczenia 7](#_Toc186532075)

[6. Routing RIP 8](#_Toc186532076)

[7. VLANy 9](#_Toc186532077)

[8. Serwer DHCP 9](#_Toc186532078)

[9. Konfiguracja urządzeń pod kątem dostępu SSH 11](#_Toc186532079)

[10. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS 13](#_Toc186532080)

[10.1. NTP 13](#_Toc186532081)

[10.2. Zarządzanie i raportowanie Cisco IOS 14](#_Toc186532082)

[11. Lokalny SPAN 16](#_Toc186532083)

[12. Lista kontroli ACL wewnątrz zabezpieczonej sieci 17](#_Toc186532084)

[13. Zabezpieczenia STP 18](#_Toc186532085)

[14. Uwierzytelnianie AAA na serwerze przy użyciu TACACS+ 20](#_Toc186532086)

[15. Zapora sieciowa typu Private and Public (ZPF) 21](#_Toc186532087)

[16. Demilitarized Zone (DMZ)/Zone-Based Policy 23](#_Toc186532088)

[17. Wnioski 24](#_Toc186532089)

# Wstęp

# Struktura sieci

# Podział na podsieci

# Adresacja

Poniżej znajdują się tabele adresacji dla poszczególnych podsieci w naszym projekcie. W przypadku, gdy jakiś interfejs nie posiada przydzielonych adresów IP lub jest nieaktywny, to nie został on uwzględniony.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | 3.0.0.2 | 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 (DHCP, SSH, NTP, CISCO IOS, TACACS+)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0 | 191.168.1.1 | 255.255.255.0 | -- |
| S0 | VLAN1 | 191.168.1.2 | 255.255.255.0 | 191.168.1.1 |
| PC0 | Fa0 | DHCP (191.168.1.10) | 255.255.255.0 | DHCP (191.168.1.1) |
| Server0 | Fa0 | 191.168.1.3 | 255.255.255.0 | 191.168.1.1 |
| PC1 | Fa0 | DHCP (191.168.1.11) | 255.255.255.0 | DHCP (191.168.1.1) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 2 (dwie standardowe 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 | Gig0/0 | 192.168.10.1 | 255.255.255.0 | -- |
| R3 | Gig0/1 | 192.168.20.1 | 255.255.255.0 | -- |
| S1 | -- | -- | -- | -- |
| S2 | -- | -- | -- | -- |
| PC2 | Fa0 | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| PC3 | Fa0 | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 3 (dwie rozszerzone ACL)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Se0/1/1 | 5.0.0.1 | 255.0.0.0 | -- |
| R4 | Se0/3/0 | 5.0.0.2 | 255.0.0.0 | -- |
| R4 | Gig0/0 | 193.168.10.1 | 255.255.255.0 | -- |
| R4 | Gig0/1 | 193.168.20.1 | 255.255.255.0 | -- |
| S3 | -- | -- | -- | -- |
| S4 | -- | -- | -- | -- |
| PC4 | Fa0 | 193.168.10.4 | 255.255.255.0 | 193.168.10.1 |
| PC5 | Fa0 | 193.168.20.5 | 255.255.255.0 | 193.168.20.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 4 (zabezpieczenia STP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R1 | Gig0/0 | 194.168.1.1 | 255.255.255.0 | -- |
| SCentral | -- | -- | -- | -- |
| S5 | -- | -- | -- | -- |
| S6 | -- | -- | -- | -- |
| S7 | -- | -- | -- | -- |
| S8 | -- | -- | -- | -- |
| PC6 | Fa0 | 194.168.1.6 | 255.255.255.0 | 194.168.1.1 |
| PC7 | Fa0 | 194.168.1.7 | 255.255.255.0 | 194.168.1.1 |
| PC8 | Fa0 | 194.168.1.8 | 255.255.255.0 | 194.168.1.1 |
| PC9 | Fa0 | 194.168.1.9 | 255.255.255.0 | 194.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 5 (FHRP - HSRP)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| HSRP (adres wirtualny) | -- | 195.168.1.1 | -- | -- |
| R1 (adres fizyczny) | Gig0/1 | 195.168.1.2 | 255.255.255.0 | -- |
| R2 (adres fizyczny) | Gig0/0 | 195.168.1.3 | 255.255.255.0 | -- |
| S9 | -- | -- | -- | -- |
| S10 | -- | -- | -- | -- |
| PC10 | Fa0 | 195.168.1.10 | 255.255.255.0 | 195.168.1.1 |
| PC11 | Fa0 | 195.168.1.11 | 255.255.255.0 | 195.168.1.1 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 6 (EtherChannel)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R2 | Gig0/1 | 196.168.1.1 | 255.255.255.0 | -- |
| S11 | -- | -- | -- | -- |
| S12 | -- | -- | -- | -- |
| S13 | -- | -- | -- | -- |
| PC12 | Fa0 | 196.168.1.12 | 255.255.255.0 | 196.168.1.1 |
| PC13 | Fa0 | 196.168.1.13 | 255.255.255.0 | 196.168.1.1 |

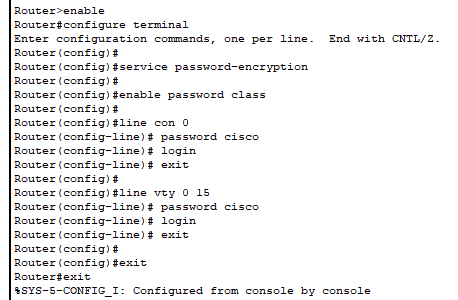
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Podsieć 7 (VLANy)** | | | | |
| **Sprzęt** | **Interfejs** | **Adres IP** | **Maska** | **Brama wyjściowa** |
| R0 | Gig0/0.10 | 197.168.1.1 | 255.255.255.0 | -- |
| R0 | Gig0/0.20 | 197.168.2.1 | 255.255.255.0 | -- |
| R0 | Gig0/0.30 | 197.168.3.1 | 255.255.255.0 | -- |
| S1 | VLAN1 | 197.168.1.10 | 255.255.255.0 | 197.168.1.1 |
| PC14 | Fa0 | 197.168.1.14 | 255.255.255.0 | 197.168.1.1 |
| PC15 | Fa0 | 197.168.1.15 | 255.255.255.0 | 197.168.1.1 |
| PC16 | Fa0 | 197.168.2.16 | 255.255.255.0 | 197.168.2.1 |
| PC17 | Fa0 | 197.168.2.17 | 255.255.255.0 | 197.168.2.1 |
| PC18 | Fa0 | 197.168.3.18 | 255.255.255.0 | 197.168.3.1 |
| PC19 | Fa0 | 197.168.3.19 | 255.255.255.0 | 197.168.3.1 |

# Zabezpieczenia

Urządzenia sieciowe w naszym projekcie zostały odpowiednio zabezpieczone przed nieautoryzowanym dostępem osób trzecich. Skonfigurowano między innymi zabezpieczenia dostępu do trybu uprzywilejowanego, portów konsolowych oraz wirtualnych terminali (VTY). W przypadku urządzenia router R0 zastosowano autoryzację przy użyciu TACACS+. Poniżej przedstawiono wykorzystane w projekcie dane uwierzytelniania oraz przykładową konfigurację zabezpieczeń na jednym z urządzeń.

Dla celów projektu zastosowano następujące hasła:

* **Dostęp do urządzenia:** username: cisco / hasło: cisco
* **Tryb uprzywilejowany (enable):** hasło: class
* **Dane dostępu do routera R0 (TACACS+):** username: ciscoTACACS / hasło: ciscoTACACS

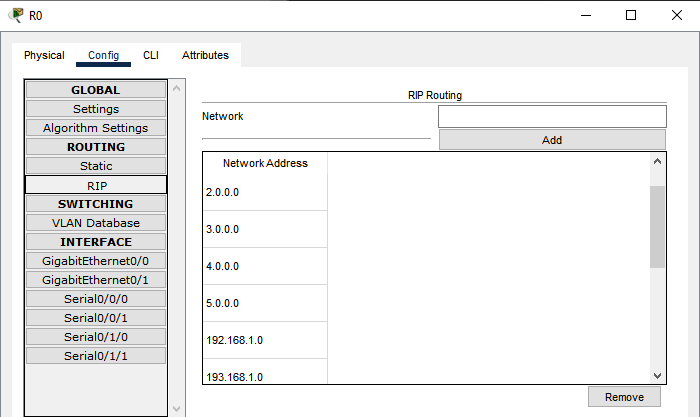


Przykładowa konfiguracja zabezpieczeń routera w naszej sieci

# Routing RIP

W celu umożliwienia routerom przesyłania pakietów między różnymi podsieciami oraz zapewnienia optymalnych tras do docelowych adresów w sieci, wykorzystaliśmy protokół RIP (Routing Information Protocol) do dynamicznego obliczania najlepszych tras przesyłania danych. RIP działa w oparciu o liczbę przeskoków (hop count), co czyni go prostym i łatwym w implementacji rozwiązaniem dla małych i średnich sieci. Dzięki automatycznej wymianie tablic routingu między routerami możliwe jest szybkie dostosowanie tras w przypadku zmian topologii, co stanowi istotną przewagę nad routingiem statycznym, który wymaga ręcznej konfiguracji i aktualizacji tras.

Poniżej przedstawiono przykładową konfigurację RIP dla jednego z routerów w naszej sieci.

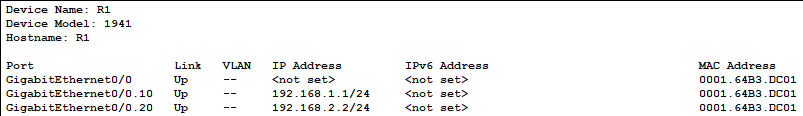


Przykładowa konfiguracja protokołu RIP dla jednego z routerów w naszej sieci

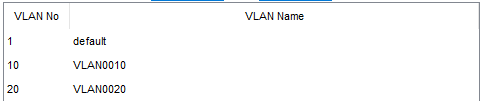
# VLANy

W ramach „Podsieci 1” zostały utworzone dwa VLAN-y: VLAN 10 i VLAN 20. Pozwoliło nam to na logiczne podzielenie fizycznej sieci na odseparowane segmenty. Dzięki temu urządzenia należące do różnych VLAN-ów mogą działać w tej samej fizycznej infrastrukturze, ale ich ruch sieciowy pozostaje oddzielony.

W naszym projekcie przypisano jeden komputer o adresie IP 192.168.1.10 do VLAN-u 10, a drugi komputer o adresie IP 192.168.2.10 do VLAN-u 20. Bramą dla pierwszego komputera jest adres 192.168.1.1, natomiast dla drugiego 192.168.2.2. Aby umożliwić komunikację między VLAN-ami, zastosowano trunking na kablu łączącym switch S1 z routerem R1. Jest to mechanizm, który pozwala na przesyłanie ruchu należącego do różnych VLAN-ów przez jeden wspólny interfejs, przy jednoczesnym oznaczaniu pakietów odpowiednimi tagami VLAN (przy użyciu standardu IEEE 802.1Q).



Konfiguracja adresów na routerze R1 połączonym ze switchem S1 w „Podsieci 1”

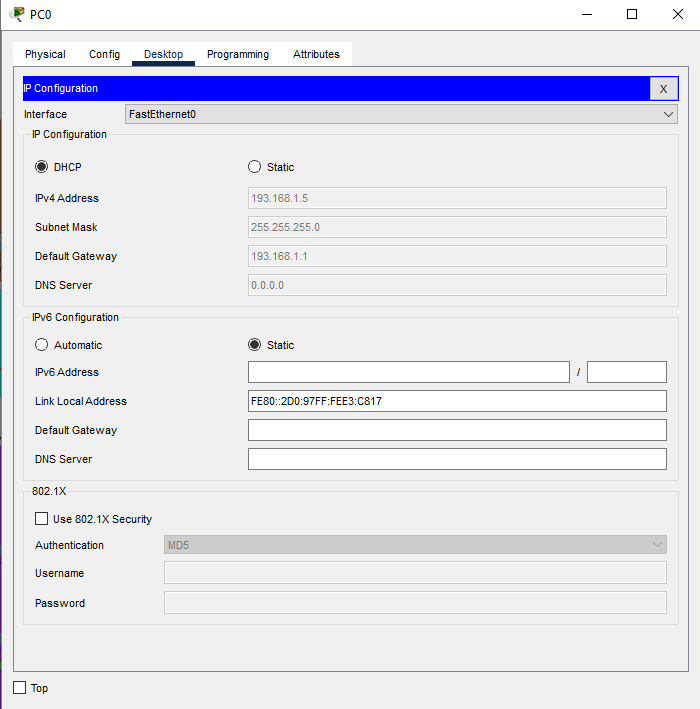


VLANy skonfigurowane na switchu S1

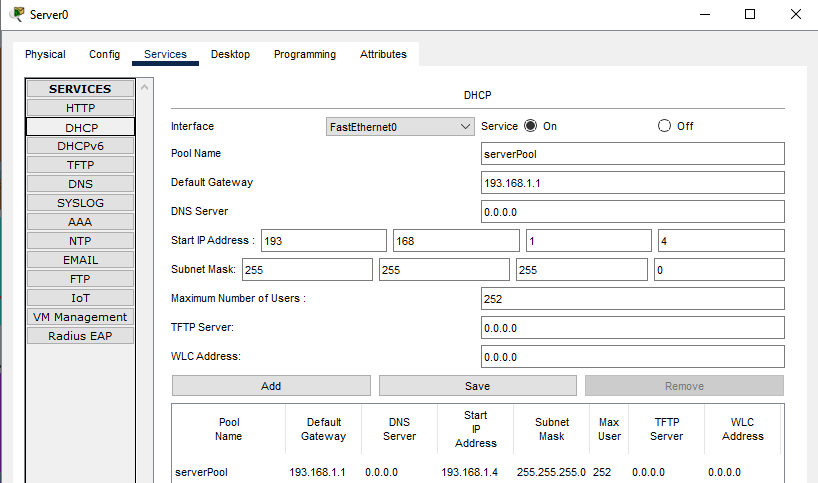
# Serwer DHCP

Serwer PT w „Podsieci 3” został skonfigurowany do automatycznego przydzielania adresów IP komputerom w sieci za pomocą protokołu DHCP (ang. Dynamic Host Configuration Protocol). DHCP pozwala na dynamiczne przypisywanie adresów IP, masek podsieci, bram domyślnych oraz serwerów DNS bez konieczności ręcznego konfigurowania tych parametrów na każdym urządzeniu.

Serwer wykorzystuje zdefiniowaną pulę adresów IP, z której losowo przydziela adresy do urządzeń w podsieci. Dzięki temu proces konfiguracji urządzeń sieciowych staje się szybszy, a zarządzanie adresacją w sieci bardziej efektywne. Poniżej przedstawiono przykładowy adres IP przypisany jednemu z hostów za pomocą tego protokołu.



Przykład działania protokołu DHCP dla hosta



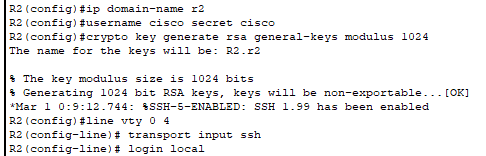
Konfiguracja protokołu DHCP na serwerze

# Konfiguracja urządzeń pod kątem dostępu SSH

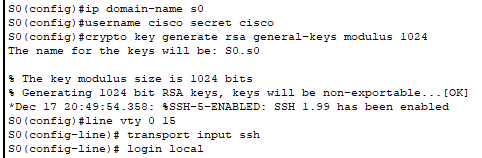
Dostęp SSH (ang. Secure Shell) zapewnia bezpieczny, szyfrowany kanał komunikacji z urządzeniami sieciowymi z poziomu innych urządzeń. W naszym przypadku do konfiguracji urządzeń pod kątem dostępu SSH wybraliśmy dwa urządzenia: router R2 oraz switch S0.

Konfiguracja zarówno routera, jak i switcha przebiegała w podobny sposób. Najpierw należało ustawić nazwę domeny, która jest wymagana do wygenerowania klucza kryptograficznego. Następnie utworzono użytkownika o nazwie „cisco” z przypisanym zaszyfrowanym hasłem „cisco”. Kolejnym krokiem było wygenerowanie 1024-bitowego klucza RSA, niezbędnego do działania protokołu SSH.

Po wygenerowaniu klucza skonfigurowano linie VTY, umożliwiając dostęp do urządzeń za pomocą SSH. Linie VTY zostały dostosowane tak, aby wykorzystywały dane uwierzytelniające wcześniej utworzonego użytkownika. Szczegółowy przebieg konfiguracji dla urządzeń został przedstawiony w formie screenów z terminala poniżej.

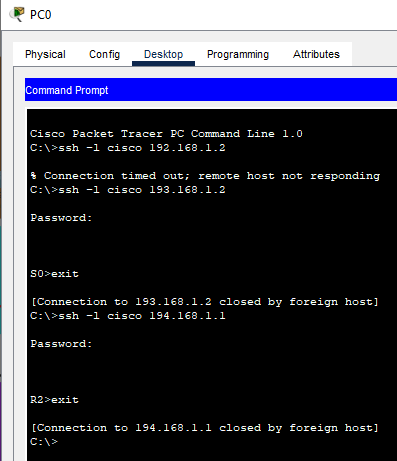


Konfiguracja routera pod kątem dostepu SSH



Konfiguracja switcha pod kątem dostępu SSH

W celu zaprezentowania poprawności działania dostępu SSH, ustanowiono połączenie ze switchem S0 oraz następnie z routerem R2 z poziomu terminala CMD komputera PC0. Dzięki temu istnieje możliwość konfiguracji urządzeń sieciowych pośrednio z poziomu innych urządzeń – tak jak w tym przypadku, można konfigurować S0 lub R2 z terminala komputera PC0.



Logowanie poprzez SSH do switcha oraz routera

# Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

## NTP

Network Time Protocol (NTP) to protokół służący do synchronizacji zegarów systemowych w urządzeniach sieciowych. Zapewnia dokładne i spójne ustawienia czasu w całej infrastrukturze, co ma kluczowe znaczenie dla działania usług sieciowych, takich jak logowanie zdarzeń, uwierzytelnianie czy analiza ruchu sieciowego. NTP działa w modelu hierarchicznym, gdzie serwery wyższego poziomu synchronizują się z zegarami atomowymi lub GPS, a urządzenia w sieci lokalnej pobierają czas od lokalnych serwerów NTP, minimalizując opóźnienia.

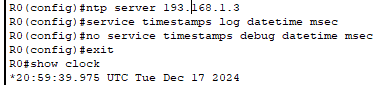
W celu konfiguracji protokołu NTP w naszej sieci należało zacząć od włączenia usługi NTP na serwerze znajdującym się w „Podsieci 3” oraz ustawienia bieżącego czasu, wobec którego będą synchronizowane pozostałe urządzenia.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

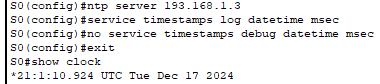
Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Włączenie usługi NTP na serwerze

Następnie na routerze i switchu ustawiono adres IP serwera NTP oraz włączono funkcję logowania ze znacznikami czasu, które zawierają dokładne informacje o dacie oraz godzinie.



Konfiguracja NTP na routerze oraz weryfikacja działania (sprawdzenie czasu)

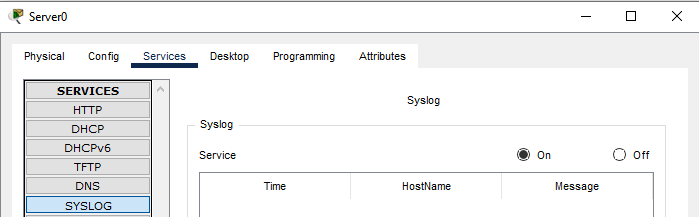


Konfiguracja NTP na switchu oraz weryfikacja działania (sprawdzenie czasu)

## Zarządzanie i raportowanie Cisco IOS

Cisco IOS wspiera efektywne zarządzanie siecią dzięki funkcji rejestrowania zdarzeń (syslog) i konfiguracji serwerów logów. Funkcja pozwala na przesyłanie zdarzeń z urządzeń sieciowych do zdalnego serwera, co ułatwia późniejsze zarządzanie logami i ich analizę.

W celu implementacji tego rozwiązania w naszej sieci, podobnie jak w przypadku konfiguracji NTP, pierwszym krokiem było włączenie usługi SYSLOG na serwerze w „Podsieci 3”



Włączenie usługi SYSLOG na serwerze

Następnie, z wykorzystaniem komendy logging na routerze oraz switchu, został określony adres serwera z włączoną usługą logowania, co umożliwiło przesyłanie logów systemowych z tych urządzeń do centralnego serwera syslog,

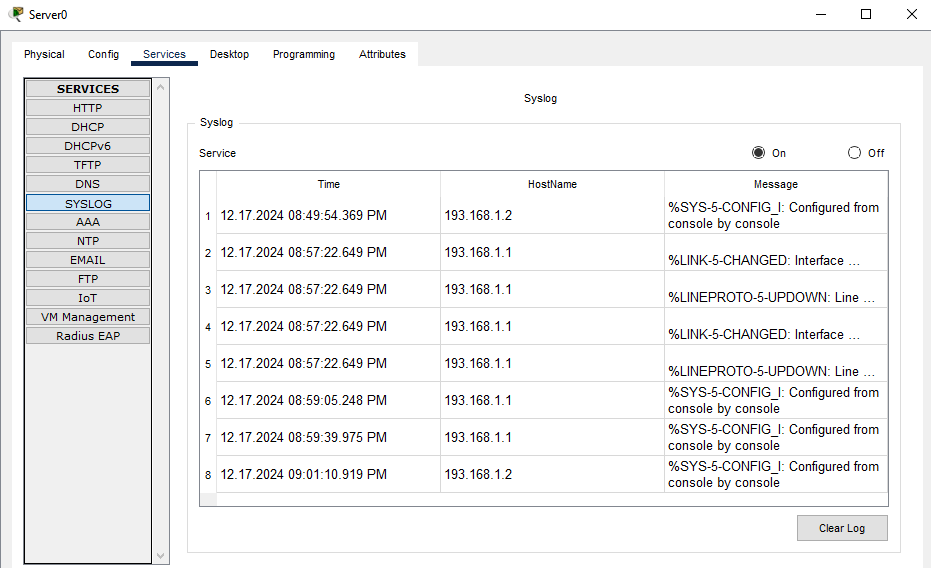


Konfiguracja SYSLOG na switchu



Konfiguracja SYSLOG na routerze

Aby zweryfikować poprawność działania opcji rejestrowania zdarzeń systemowych, wystarczyło przejść do zakładki SYSLOG na serwerze w „Podsieci 3”. Jak można zaobserwować na poniższym zrzucie ekranu, na serwer spłynęły wszystkie logi dotyczące zmian w konfiguracji wybranych urządzeń sieciowych.

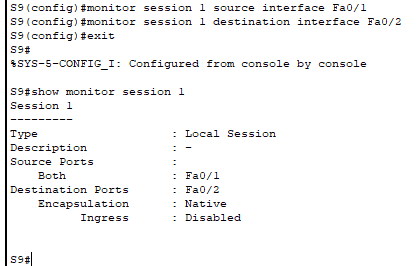


Logi z routera oraz switcha, które spłynęły na główny serwer

# Lokalny SPAN

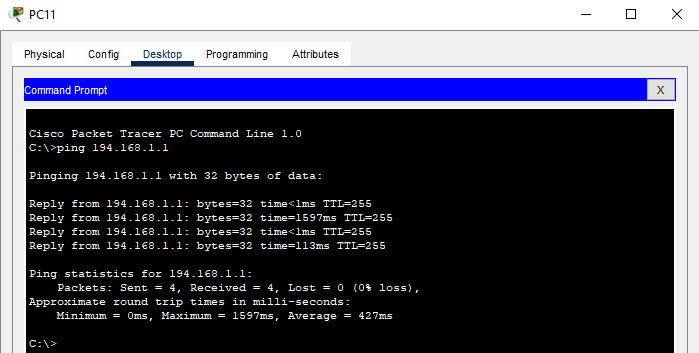
Lokalny SPAN to funkcja dostępna w przełącznikach sieciowych, która umożliwia monitorowanie ruchu sieciowego na wybranych portach. Ruch ten jest kopiowany na dedykowany port monitorujący, do którego można podłączyć urządzenie analizujące, takie jak sniffer czy IDS.

W naszym przypadku konfiguracja lokalnego SPAN wykonana została w „Podsieci 4”. Urządzenie switch S9 zostało skonfigurowany tak, by ruch z portu FastEthernet 0/1 był kopiowany i przesyłany na port FastEthernet 0/2.

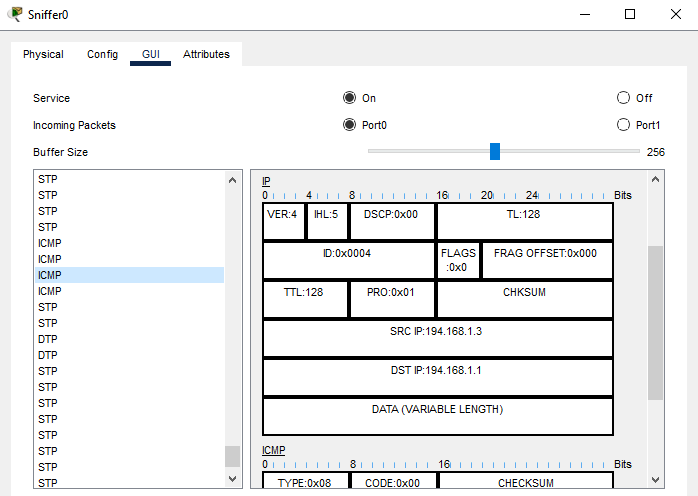


Konfiguracja lokalnego SPAN na switchu S9

W celu weryfikacji poprawności działania należało najpierw wygenerować jakiś ruch sieciowy na porcie FastEthernet 0/1. Zapingowanie routera R2 z poziomu wiersza poleceń CMD na komputerze PC11 pozwoliło na przesłanie pakietów ICMP, które następnie można było przechwycić na Snifferze.



Wysyłanie poleceń „ping” z PC11 do routera R2



Pakiety przechwycone przez Sniffera

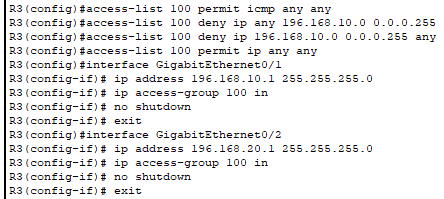
# Lista kontroli ACL wewnątrz zabezpieczonej sieci

Listy kontroli dostępu (ACL, ang. Access Control Lists) to mechanizm stosowany w sieciach komputerowych w celu definiowania reguł dostępu do zasobów i filtrowania ruchu sieciowego. ACL pozwalają określać, jakie typy ruchu są dozwolone, a jakie powinny zostać zablokowane, na podstawie takich parametrów jak adresy IP, protokoły czy porty.

W naszym projekcie rozwiązanie to zostało zaimplementowane w „Podsieci 2” na urządzeniu router R3. Najpierw utworzono listę ACL z następującymi regułami:

* permit icmp any any – zezwala na cały ruch ICMP w sieci (np. pingowanie urządzeń).
* deny ip any 196.168.10.0 0.0.0.255 – blokuje cały ruch IP skierowany do podsieci 196.168.10.0/24.
* deny ip 196.168.10.0 0.0.0.255 any – blokuje cały ruch wychodzący z tej samej podsieci do dowolnego celu.
* permit ip any any – zezwala na cały pozostały ruch, który nie został wcześniej zablokowany przez reguły.

Po skonfigurowaniu reguł lista ACL została przypisana do odpowiednich interfejsów routera R3, umożliwiając kontrolę ruchu przychodzącego lub wychodzącego na danym interfejsie, zgodnie z określonymi zasadami.



Ustawianie list kontrolnych ACL dla routera R3

# Zabezpieczenia STP

W celu zapewnienia stabilności i bezpieczeństwa działania protokołu STP (Spanning Tree Protocol) w „Podsieci 6”, przeprowadzono konfigurację urządzeń, definiując główne węzły drzewa oraz implementując mechanizmy ochronne. Na początku jako główny węzeł drzewa (root) wybrano switch S4, a jako drugorzędny węzeł główny (root-secondary) skonfigurowano switch S5. W ten sposób zapewniliśmy celową redundancję, która zapewnia poprawność działania sieci nawet w przypadku awarii głównego urządzenia.

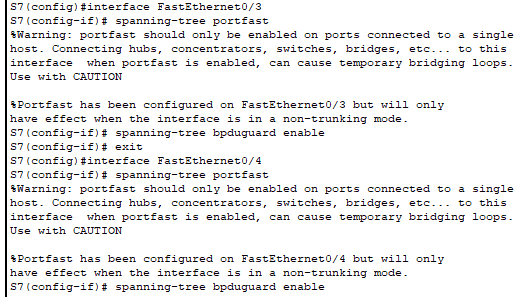


Konfiguracja urządzenia switch S4 jako głównego węzła drzewa (root)

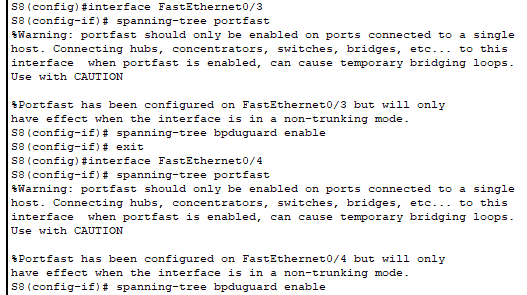


Konfiguracja urządzenia switch S5 jako drugorzędnego węzła drzewa (root-secondary)

Dodatkowo, na przełącznikach S7 i S8 zastosowano funkcje PortFast oraz BPDU Guard. PortFast pozwala na szybkie przełączanie portów do stanu przekazywania (forwarding), co jest szczególnie przydatne na portach końcowych, podczas gdy BPDU Guard zapobiega wprowadzaniu zmian w topologii przez nieautoryzowane urządzenia.

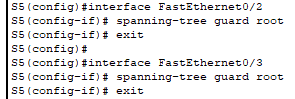


Konfiguracja PortFast oraz BPDU Guard na urządzeniu switch S7



Konfiguracja PortFast oraz BPDU Guard na urządzeniu switch S8

Na koniec na urządzeniach switch S5 i S6 skonfigurowano funkcję Root Guard na wybranych portach, aby zabezpieczyć główną strukturę drzewa przed potencjalnym przejęciem roli głównego węzła przez inne urządzenia. Taka konfiguracja pozwala na ochronę stabilności sieci oraz minimalizację ryzyka zakłóceń spowodowanych przez nieprawidłowe lub złośliwe działanie.



Konfiguracja Root Guard na urządzeniu switch S5

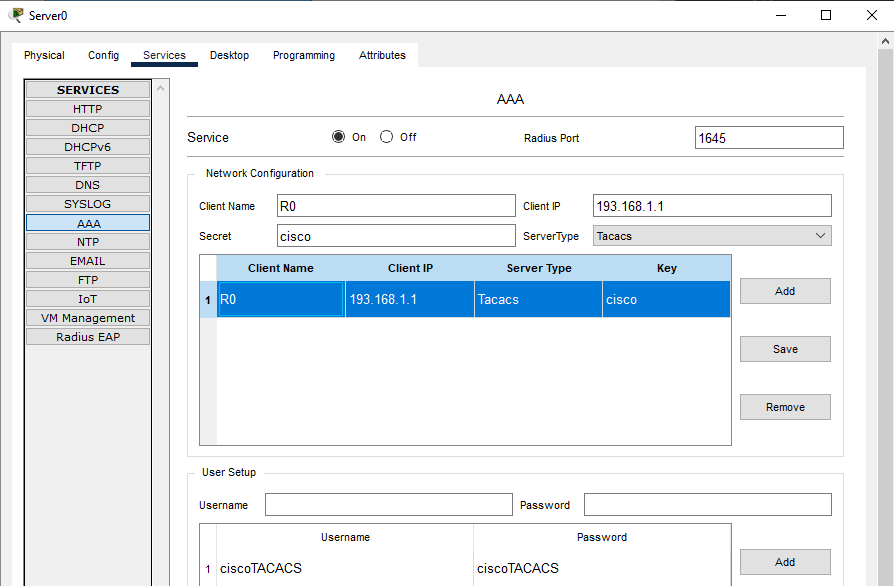


Konfiguracja Root Guard na urządzeniu switch S6

# Uwierzytelnianie AAA na serwerze przy użyciu TACACS+

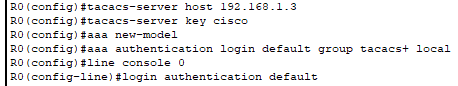
W celu zwiększenia bezpieczeństwa dostępu do urządzeń sieciowych, zaimplementowano uwierzytelnianie AAA (Authentication, Authorization, and Accounting) przy użyciu protokołu TACACS+ (Terminal Access Controller Access-Control System Plus).

Pierwszym krokiem było włączenie usługi uwierzytelniania AAA na serwerze zlokalizowanym w „Podsieci 3” oraz wybranie metody TACACS+. Następnie dodano dane urządzenia (routera R0) korzystającego z usługi uwierzytelniania, w tym adres IP oraz hasło współdzielone dla komunikacji między serwerem a routerem. Dla celów projektu hasło to: ciscoTACACS.



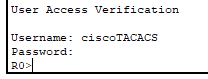
Konfiguracja uwierzytelniania AAA przy użyciu TACACS+ na serwerze

Dalsza konfiguracja dotyczyła już routera R0. Na urządzeniu włączono funkcję AAA, co umożliwiło korzystanie z zewnętrznych serwerów uwierzytelniania, a następnie zdefiniowano serwer TACACS+ poprzez wskazanie jego adresu IP, hasła współdzielonego oraz portu komunikacji. Ostatecznie router został skonfigurowany tak, aby logowanie do urządzenia odbywało się z wykorzystaniem serwera TACACS+, a nie lokalnie na urządzeniu.



Konfiguracja TACACS+ na routerze R0

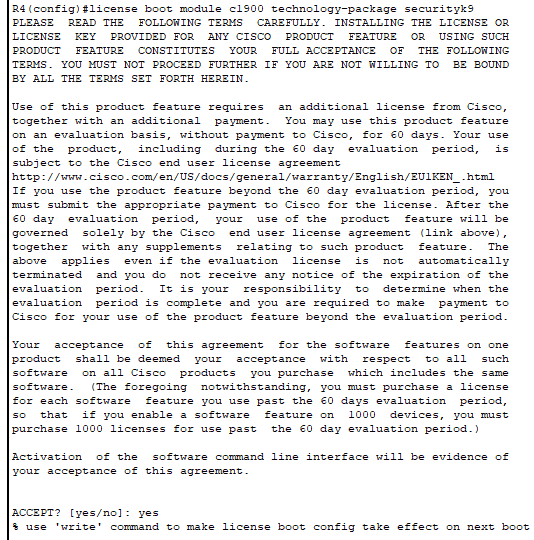
Po zakończeniu konfiguracji dostęp do routera wymaga podania danych uwierzytelniających skonfigurowanych na serwerze TACACS+. Dzięki temu wszystkie próby logowania są rejestrowane i mogą być monitorowane na serwerze, co zwiększa kontrolę oraz bezpieczeństwo sieci.



Zabezpieczony dostęp wykorzystujący uwierzytelnianie TACACS+

# Zapora sieciowa typu Private and Public (ZPF)

Do utworzenia zapory sieciowej typu Zone-Based Policy Firewall (ZPF) konieczne było zastosowanie pakietu funkcjonalności ***license boot module c1900 technology-package securityk9*** który aktywuje wymagane możliwości bezpieczeństwa na urządzeniu.



Aktywacja pakietu funkcjonalności dla zapory sieciowej ZPF na routerze R4

Pierwszym krokiem w konfiguracji zapory było utworzenie dwóch stref: wewnętrznej (Private) i zewnętrznej (Public). Zdefiniowanie tych stref umożliwia segmentację ruchu i ustanowienie zasad bezpieczeństwa dla komunikacji między nimi. Następnie skonfigurowano listę kontroli dostępu (ACL), która pozwala na ruch wychodzący z sieci wewnętrznej do sieci zewnętrznej, zapewniając jednocześnie podstawowe filtrowanie ruchu.



Tworzenie stref

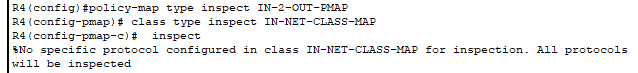


Lista kontroli określająca zasady ruchu sieci wewnętrznej

W kolejnym kroku utworzono klasyfikator ruchu typu ***class-map***, który definiuje ruch bazujący na wcześniej zdefiniowanej liście kontroli ACL. Klasyfikator ten pozwala na przypisanie zasad bezpieczeństwa do wybranych kategorii ruchu. Na podstawie klasyfikatora ruchu skonfigurowano mapę zasad (***policy-map***), która określa kontrolę dostępu opartą na kontekście dla określonego ruchu sieciowego, np. zezwalając na ruch inicjowany z sieci wewnętrznej i blokując nieautoryzowany ruch przychodzący z sieci zewnętrznej.



Utworzenie klasyfikatora ruchu typu class-map

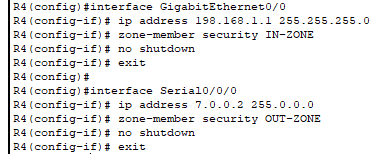


Tworzenie mapy zasad policy-map

Ostatecznie zapora została wdrożona poprzez określenie pary stref i przypisanie mapy zasad regulującej ruch pomiędzy nimi. Do każdej strefy przypisano odpowiednie interfejsy routera, co zapewnia fizyczne połączenie z segmentami sieci oraz implementację zasad bezpieczeństwa. Dzięki tej konfiguracji sieć wewnętrzna została skutecznie zabezpieczona przed nieautoryzowanym dostępem, a jednocześnie zapewniono kontrolowany dostęp do zasobów zewnętrznych.



Utworzenie pary stref i przypisanie zasad obsługi ruchu

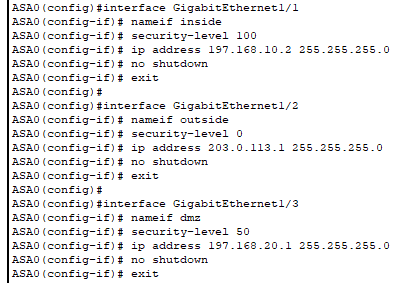


Przypisanie interfejsów do poszczególnych stref

# Demilitarized Zone (DMZ)/Zone-Based Policy

Demilitarized Zone (DMZ) to wydzielony segment sieci, który umożliwia umieszczanie serwerów dostępnych zarówno dla sieci wewnętrznej, jak i zewnętrznej, zapewniając jednocześnie izolację i dodatkowy poziom bezpieczeństwa.

Konfiguracja rozpoczęła się od utworzenia trzech stref: **Inside**, **Outside** oraz **DMZ**, przypisując im odpowiednie interfejsy sieciowe. Interfejs przypisany do strefy Inside posiada najwyższy poziom bezpieczeństwa (100) i stanowi połączenie z routerem R1 obsługującym sieć wewnętrzną. Interfejs przypisany do strefy Outside ma najniższy poziom bezpieczeństwa (0) i jest odpowiedzialny za komunikację z siecią zewnętrzną. Interfejs przypisany do strefy DMZ, gdzie umieszczono serwery WEB, DNS oraz EMAIL, posiada pośredni poziom bezpieczeństwa (50).



Konfiguracja interfejsów dla poszczególnych stref

Na przełącznikach stref DMZ i Outside utworzono odpowiednie VLAN-y, aby oddzielić ruch sieciowy w obu segmentach. Dla strefy Outside, do której podłączono urządzenia zewnętrzne, w tym **UntrustedServer**, skonfigurowano **VLAN 10**. Z kolei dla strefy DMZ, gdzie znajdują się serwery, utworzono **VLAN 20**. Dzięki temu każdy segment sieci może być logicznie odseparowany, co zapewnia lepszą kontrolę nad ruchem sieciowym.



Tworzenie VLAN 10 (dla sieci zewnętrznej)



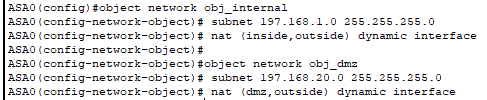
Tworzenie VLAN 20 (dla DMZ)

Aby umożliwić komunikację między sieciami, skonfigurowano statyczne trasy routingu. Dodano trasę domyślną dla ruchu wychodzącego ze strefy Outside do internetu oraz trasę do sieci wewnętrznej przez router R1.



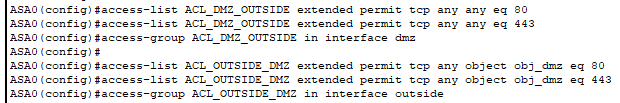
Konfiguracja tras statycznych

Ponadto wdrożono translację adresów NAT w celu ochrony wewnętrznych adresów IP przed bezpośrednią ekspozycją. Ruch z sieci wewnętrznej (Inside) oraz DMZ został zmapowany na zewnętrzny adres IP przypisany do interfejsu strefy Outside, co pozwoliło na bezpieczny dostęp do internetu.



Konfiguracja NAT

W ostatnim etapie skonfigurowano reguły kontroli dostępu ACL, które określają zasady ruchu między strefami. Ruch wychodzący z DMZ do sieci zewnętrznej ograniczono do usług HTTP (port 80) oraz HTTPS (port 443). Z kolei dla ruchu z sieci zewnętrznej do DMZ dopuszczono jedynie dostęp do serwerów w DMZ na tych samych portach. Dzięki temu ograniczono możliwość nieautoryzowanego dostępu do strefy DMZ, zapewniając jednocześnie dostępność niezbędnych usług dla użytkowników zewnętrznych.



Dostęp dla ruchu z DMZ do zewnętrznej sieci oraz z zewnętrznej sieci do DMZ (ograniczony do serwisów)

# Wnioski

W ramach realizacji projektu udało nam się zbudować i skonfigurować funkcjonalną sieć, spełniającą niemal wszystkie założenia początkowe. Zrealizowano kluczowe elementy infrastruktury oraz wdrożono rozwiązania zgodne z wymaganiami na ocenę 3, 4, a także część założeń na ocenę 5. Niestety, nie udało się wdrożyć VPN Ipsec, co stanowi jedyny brakujący element w pełnym spektrum założeń projektu.

Pomimo tego, projekt spełnia postawione cele funkcjonalne i pokazuje skuteczność zastosowanych rozwiązań oraz naszą umiejętność ich implementacji.