

Politechnika Świętokrzyska Wydział Elektrotechniki, Automatyki i Informatyki		
Wprowadzenie do cyberbezpieczeństwa – Projekt		
TEMAT: Projekt sieci dla biura rachunkowego		SKŁAD ZESPOŁU: <ul style="list-style-type: none">• Przemysław Kałuziński (91271)• Jakub Kuśmierczyk (97504)• Michał Kaczor (91268)
DATA: 15.01.2024	GRUPA: 1IZ22B	

2

Spis treści

1. Wstęp	3
2. Struktura sieci	4
3. Podział na podsieci.....	5
4. Adresacja.....	5
5. Zabezpieczenia	7
6. Routing RIP	8
7. VLANy	9
8. Serwer DHCP	9
9. Konfiguracja urządzeń pod kątem dostępu SSH.....	11
10. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS	13
10.1. NTP	13
10.2. Zarządzanie i raportowanie Cisco IOS	14
11. Lokalny SPAN	16
12. Lista kontroli ACL wewnątrz zabezpieczonej sieci.....	17
13. Zabezpieczenia STP	18
14. Uwierzytelnianie AAA na serwerze przy użyciu TACACS+	20
15. Zapora sieciowa typu Private and Public (ZPF)	21
16. Demilitarized Zone (DMZ)/Zone-Based Policy	23
17. Wnioski.....	24

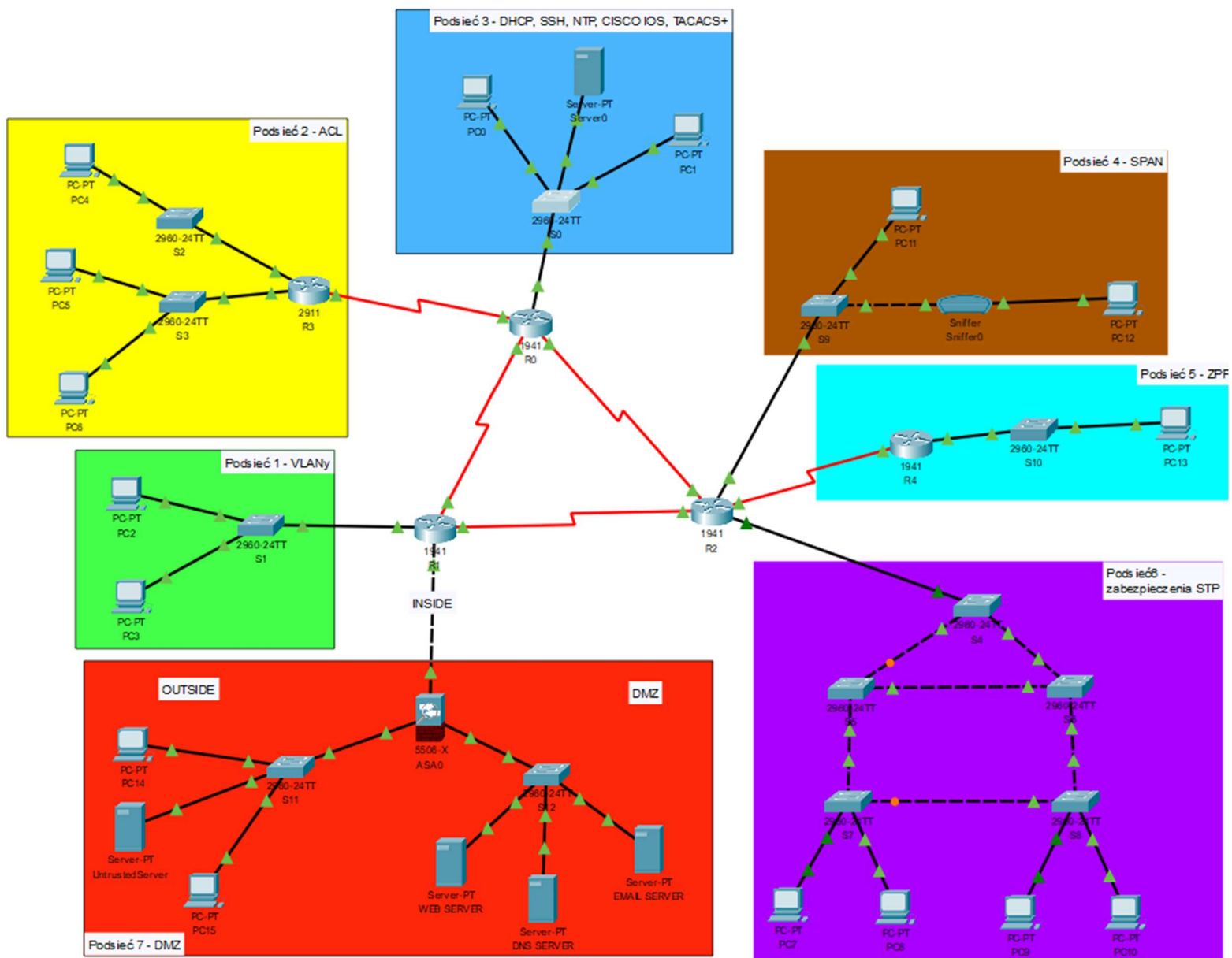
3

1. Wstęp

Tematem naszego projektu było zaprojektowanie struktury sieci dla biura rachunkowego. W ramach realizacji zadania należało opracować schemat sieci oraz odpowiednio skonfigurować urządzenia wchodzące w jej skład. Do prac nad projektem wykorzystano oprogramowanie Cisco PacketTracer. Konfiguracja miała obejmować implementację następujących rozwiązań (w tabeli zaznaczono również, które z nich udało się zrealizować):

Wymagania na ocenę 3.0	
Adresacja	✓
Podział na podsieci	✓
VLANy	✓
Serwer DHCP	✓
Konfiguracja urządzeń pod kątem dostępu SSH.	✓
Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS.	✓
Implementacja lokalnego SPAN.	✓
Implementacja co najmniej jednej listy kontroli dostępu ACL wewnątrz zabezpieczonej sieci.	✓
Wymagania na ocenę 4.0	
Realizacja wymagań na ocenę 3.0.	✓
Implementacja zabezpieczeń STP.	✓
Konfiguracja uwierzytelniania AAA na serwerze przy użyciu TACACS+ lub RADIUS.	✓
Zaprojektowanie zapory sieciowej typu Private and Public.	✓
Wymagania na ocenę 5.0	
Realizacja wymagań na ocenę 3.0 oraz 4.0.	✓
Zaprojektowanie zapory sieciowej typu Demilitarized Zone (DMZ)/Zone-Based Policy.	✓
Konfiguracja i weryfikacja sieci VPN IPsec.	✗

Na obrazie poniżej przedstawiono strukturę naszego projektu sieci.



5

3. Podział na podsieci

Jednym z zadań był podział głównej sieci na podsieci. Wykorzystaliśmy tę możliwość, aby rozdzielić sieć na mniejsze segmenty, z których każdy odpowiada za inną funkcjonalność. Dzięki temu udało się uniknąć nadmiernego obciążenia pojedynczych urządzeń oraz poprawić czytelność i organizację konfiguracji. Każda z podsieci została oznaczona innym kolorem, tak jak to można zauważyć na poprzednim zdjęciu, aby podkreślić ich rozłączność. Dodatkowo przy każdej z podsieci znajduje się krótka notatka, która informuje o zaimplementowanych w niej rozwiązaniach.

Jesteśmy świadomi, że w rzeczywistych zastosowaniach takie podejście nie jest w pełni profesjonalne, ponieważ każda podsieć powinna być w pełni skonfigurowana i w pełni zintegrowana z całą infrastrukturą. Tylko w ten sposób można zagwarantować poprawność działania oraz bezpieczeństwo całej sieci. Jednak w ramach projektu przyjęte rozwiązanie miało na celu przede wszystkim zademonstrowanie naszej umiejętności implementacji wybranych funkcjonalności i osiągnięcia założonych celów.

4. 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	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

5. 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

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#service password-encryption
Router(config)#
Router(config)#enable password class
Router(config)#
Router(config)#line con 0
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
Router(config)#
Router(config)#line vty 0 15
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
Router(config)#
Router(config)#exit
Router#exit
%SYS-5-CONFIG_I: Configured from console by console

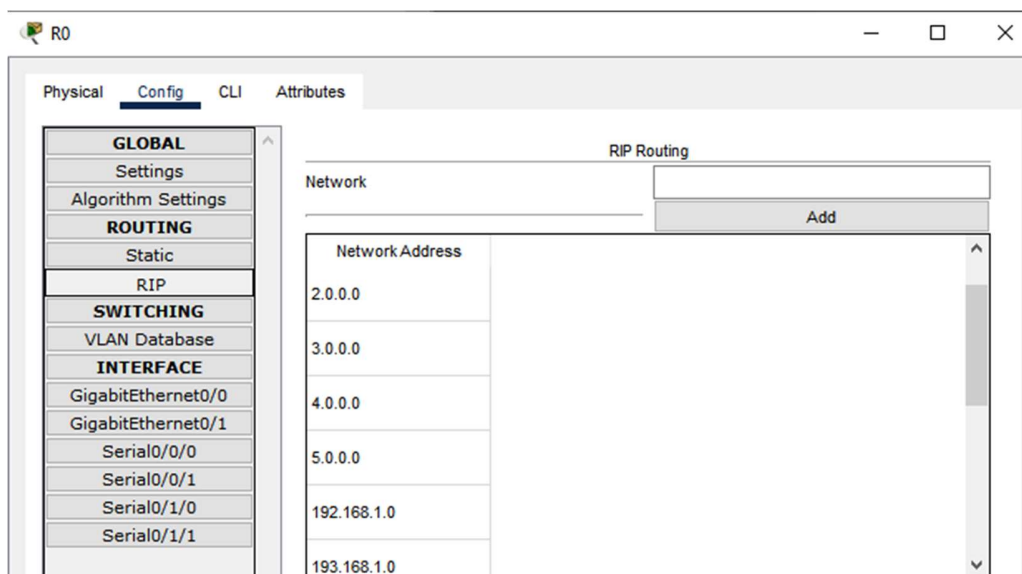
```

Przykładowa konfiguracja zabezpieczeń routera w naszej sieci

6. 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

7. 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).

Device Name: R1						
Device Model: 1941						
Hostname: R1						
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address	
GigabitEthernet0/0	Up	--	<not set>	<not set>	0001.64B3.DC01	
GigabitEthernet0/0.10	Up	--	192.168.1.1/24	<not set>	0001.64B3.DC01	
GigabitEthernet0/0.20	Up	--	192.168.2.2/24	<not set>	0001.64B3.DC01	

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

VLAN No	VLAN Name
1	default
10	VLAN0010
20	VLAN0020

VLANy skonfigurowane na switchu S1

8. 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.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 193.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 193.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2D0:97FF:FEE3:C817

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Przykład działania protokołu DHCP dla hosta

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 193.168.1.1

DNS Server: 0.0.0.0

Start IP Address: 193 168 1 4

Subnet Mask: 255 255 255 0

Maximum Number of Users: 252

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	193.168.1.1	0.0.0.0	193.168.1.4	255.255.255.0	252	0.0.0.0	0.0.0.0

Konfiguracja protokołu DHCP na serwerze

9. 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.

```
R2(config)#ip domain-name r2
R2(config)#username cisco secret cisco
R2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R2.r2

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:9:12.744: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#line vty 0 4
R2(config-line)# transport input ssh
R2(config-line)# login local
```

Konfiguracja routera pod kątem dostępu SSH

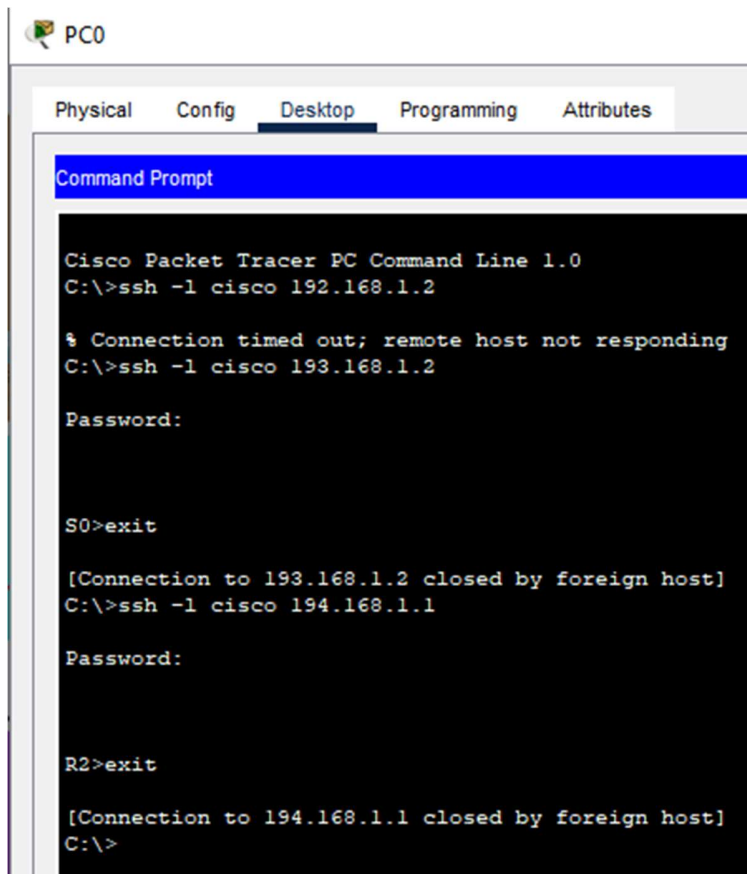
```
S0(config)#ip domain-name s0
S0(config)#username cisco secret cisco
S0(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S0.s0

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Dec 17 20:49:54.358: %SSH-5-ENABLED: SSH 1.99 has been enabled
S0(config)#line vty 0 15
S0(config-line)# transport input ssh
S0(config-line)# login local
```

Konfiguracja switcha pod kątem dostępu SSH

12

W celu zaprezentowania poprawności działania dostępu SSH, ustawiono 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.



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 192.168.1.2

% Connection timed out; remote host not responding
C:\>ssh -l cisco 193.168.1.2

Password:

S0>exit

[Connection to 193.168.1.2 closed by foreign host]
C:\>ssh -l cisco 194.168.1.1

Password:

R2>exit

[Connection to 194.168.1.1 closed by foreign host]
C:\>
```

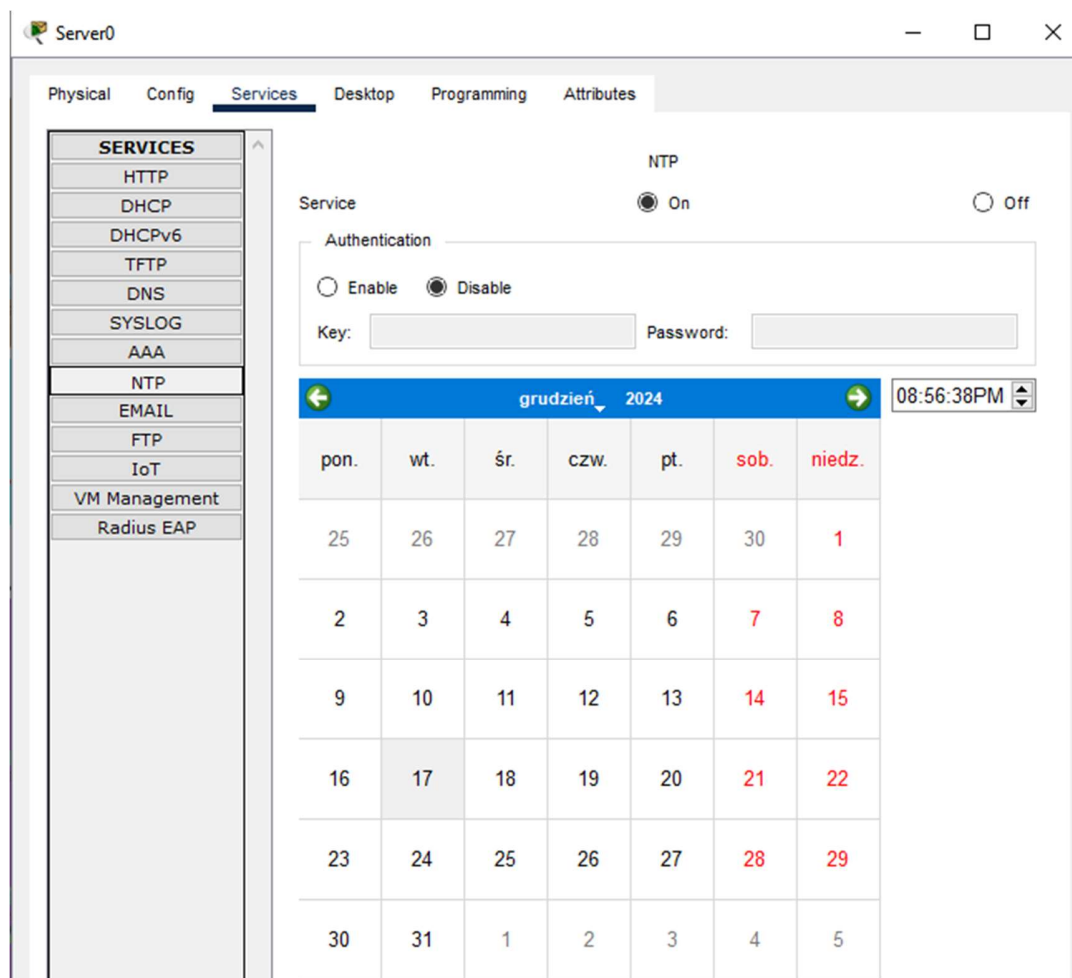
Logowanie poprzez SSH do switcha oraz routera

10. Konfiguracja NTP oraz zarządzania i raportowania CISCO IOS

10.1. 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 „Podsięci 3” oraz ustawienia bieżącego czasu, wobec którego będą synchronizowane pozostałe urządzenia.



Włączenie usługi NTP na serwerze

14

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.

```
R0(config)#ntp server 193.168.1.3
R0(config)#service timestamps log datetime msec
R0(config)#no service timestamps debug datetime msec
R0(config)#exit
R0#show clock
*20:59:39.975 UTC Tue Dec 17 2024
```

Konfiguracja NTP na routerze oraz weryfikacja działania (sprawdzenie czasu)

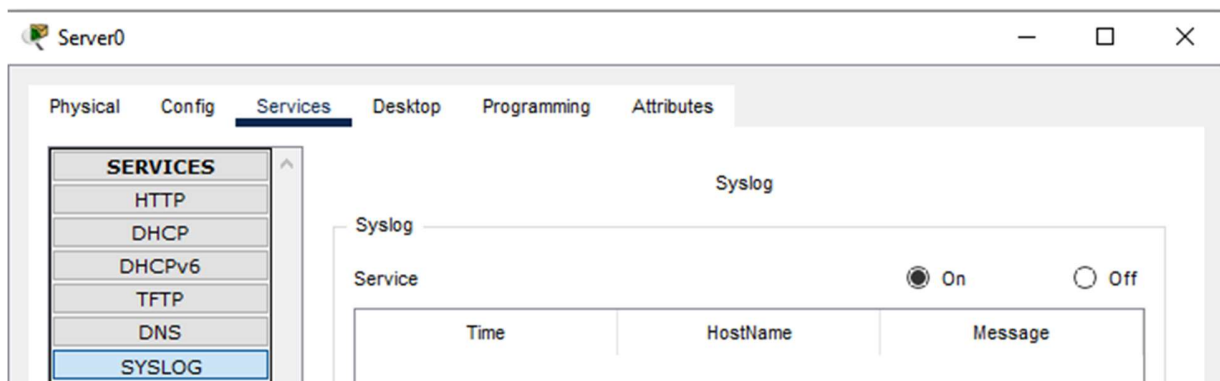
```
S0(config)#ntp server 193.168.1.3
S0(config)#service timestamps log datetime msec
S0(config)#no service timestamps debug datetime msec
S0(config)#exit
S0#show clock
*21:1:10.924 UTC Tue Dec 17 2024
```

Konfiguracja NTP na switchu oraz weryfikacja działania (sprawdzenie czasu)

10.2. 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,

```
S0(config)#logging 193.168.1.3
S0(config)#exit
S0#
*Dec 17, 21:02:25.022: SYS-5-CONFIG_I: Configured from console by console
```

Konfiguracja SYSLOG na switchu

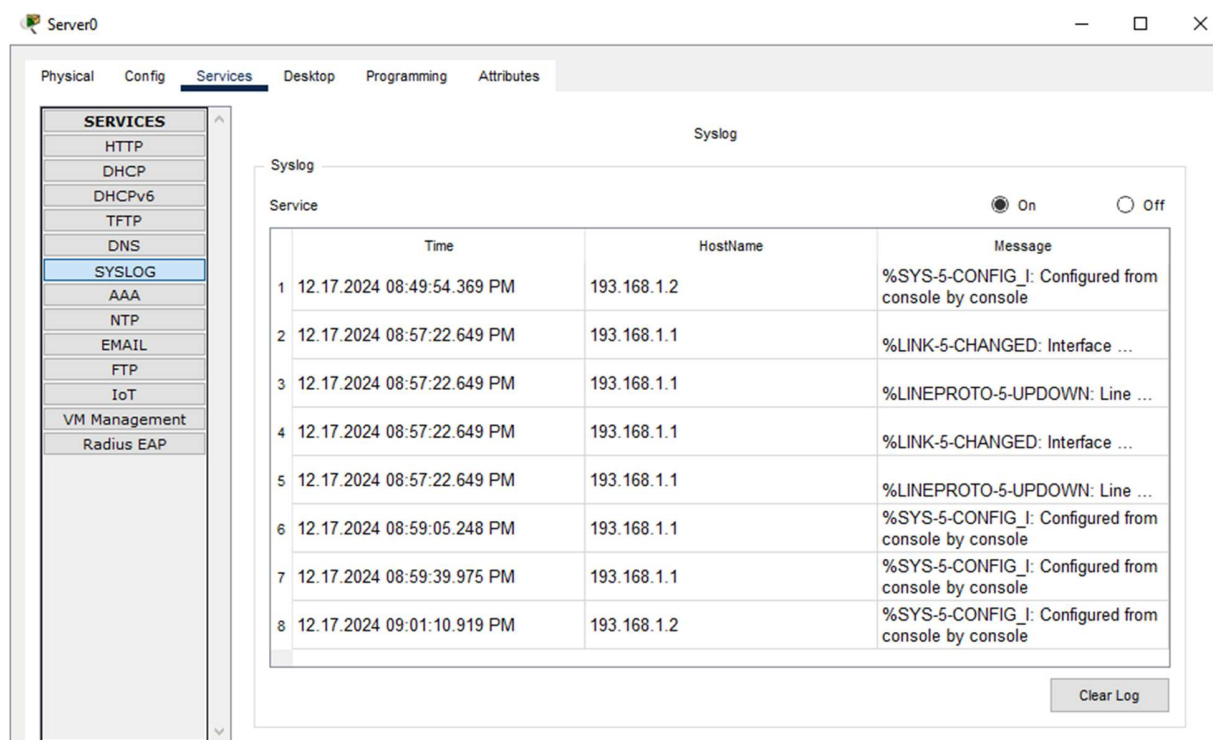
```

R0(config)#logging 193.168.1.3
R0(config)#exit
R0#
*Dec 17, 21:03:01.033: SYS-5-CONFIG_I: Configured from console by console

```

Konfiguracja SYSLOG na routerze

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



Logi z routera oraz switcha, które spłynęły na główny serwer

11. 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.

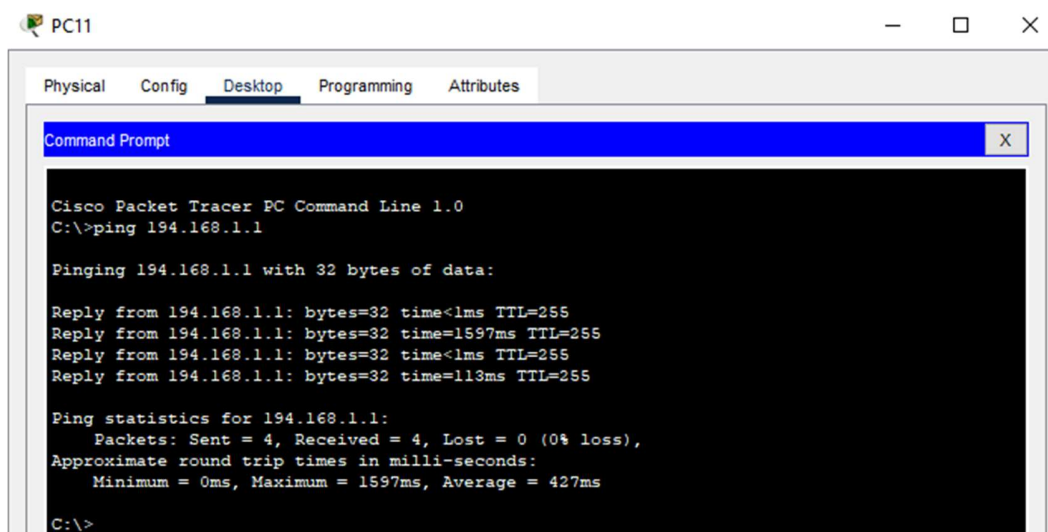
W naszym przypadku konfiguracja lokalnego SPAN wykonana została w „Podsieci 4”. Urządzenie switch S9 zostało skonfigurowane tak, by ruch z portu FastEthernet 0/1 był kopiowany i przesyłany na port FastEthernet 0/2.

```
S9(config)#monitor session 1 source interface Fa0/1
S9(config)#monitor session 1 destination interface Fa0/2
S9(config)#exit
S9#
%SYS-5-CONFIG_I: Configured from console by console

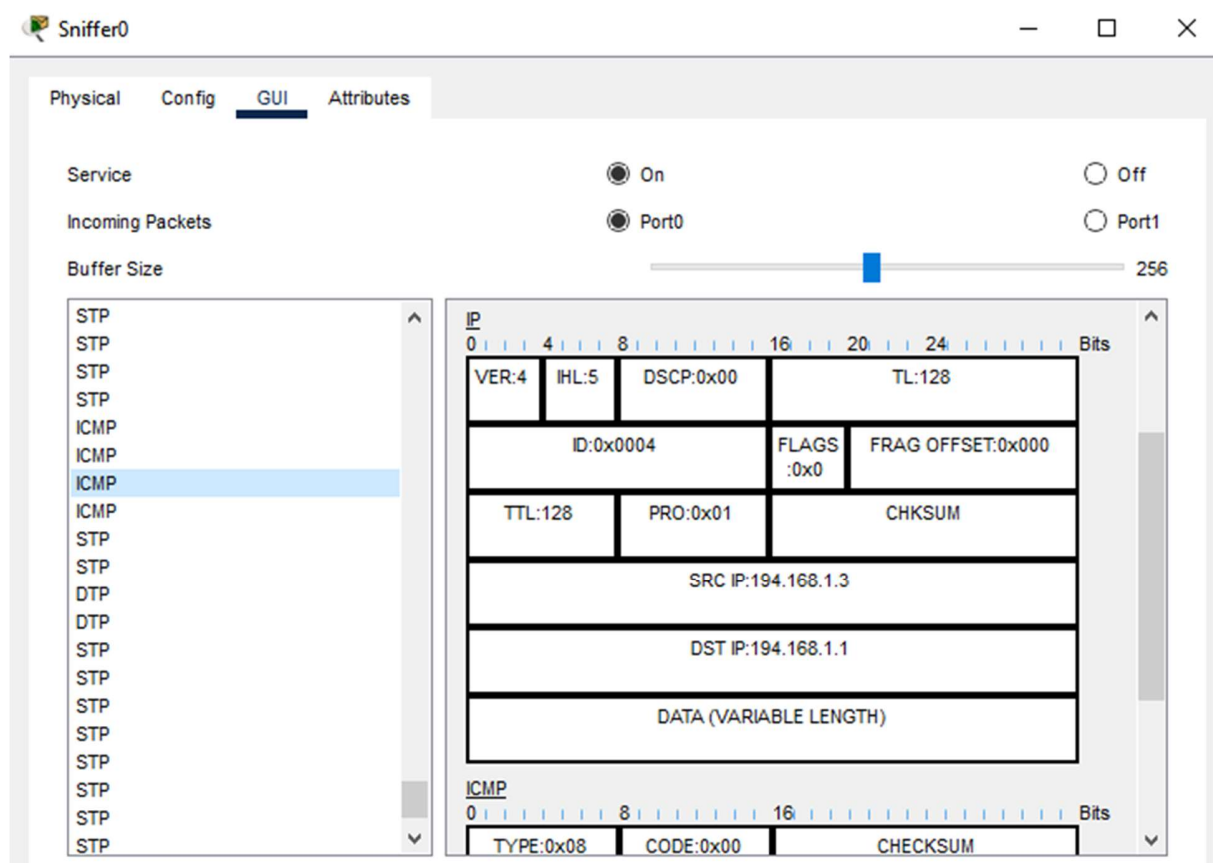
S9#show monitor session 1
Session 1
-----
Type                : Local Session
Description          : -
Source Ports         :
    Both             : Fa0/1
Destination Ports    : Fa0/2
    Encapsulation     : Native
    Ingress           : Disabled
S9#
```

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

12. 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 „Podsieli 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.

```
R3(config)#access-list 100 permit icmp any any
R3(config)#access-list 100 deny ip any 196.168.10.0 0.0.0.255
R3(config)#access-list 100 deny ip 196.168.10.0 0.0.0.255 any
R3(config)#access-list 100 permit ip any any
R3(config)#interface GigabitEthernet0/1
R3(config-if)# ip address 196.168.10.1 255.255.255.0
R3(config-if)# ip access-group 100 in
R3(config-if)# no shutdown
R3(config-if)# exit
R3(config)#interface GigabitEthernet0/2
R3(config-if)# ip address 196.168.20.1 255.255.255.0
R3(config-if)# ip access-group 100 in
R3(config-if)# no shutdown
R3(config-if)# exit
```

Ustawianie list kontrolnych ACL dla routera R3

13. 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.

```
S4(config)#spanning-tree mode pvst
S4(config)#spanning-tree vlan 1 root primary
```

Konfiguracja urządzenia switch S4 jako głównego węzła drzewa (root)

```
S5(config)#spanning-tree mode pvst
S5(config)#spanning-tree vlan 1 root secondary
```

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.

```
S7(config)#interface FastEthernet0/3
S7(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
S7(config-if)# spanning-tree bpduguard enable
S7(config-if)# exit
S7(config)#interface FastEthernet0/4
S7(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
S7(config-if)# spanning-tree bpduguard enable
```

Konfiguracja PortFast oraz BPDU Guard na urządzeniu switch S7

```
S8(config)#interface FastEthernet0/3
S8(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
S8(config-if)# spanning-tree bpduguard enable
S8(config-if)# exit
S8(config)#interface FastEthernet0/4
S8(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
S8(config-if)# spanning-tree bpduguard enable
```

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.

```
S5(config)#interface FastEthernet0/2
S5(config-if)# spanning-tree guard root
S5(config-if)# exit
S5(config)#
S5(config)#interface FastEthernet0/3
S5(config-if)# spanning-tree guard root
S5(config-if)# exit
```

Konfiguracja Root Guard na urządzeniu switch S5

```
S6(config)#interface FastEthernet0/3
S6(config-if)# spanning-tree guard root
S6(config-if)# exit
```

Konfiguracja Root Guard na urządzeniu switch S6

14. 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.

The screenshot shows the configuration interface for a server named 'Server0'. The 'Services' tab is selected, and the 'AAA' service is configured. The 'Network Configuration' section includes fields for 'Client Name' (R0), 'Client IP' (193.168.1.1), 'Secret' (cisco), and 'Server Type' (Tacacs). A table below lists the configuration for the client R0. The 'User Setup' section shows a user named 'ciscoTACACS' with the same password.

	Client Name	Client IP	Server Type	Key
1	R0	193.168.1.1	Tacacs	cisco

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.

```
R0(config)#tacacs-server host 192.168.1.3
R0(config)#tacacs-server key cisco
R0(config)#aaa new-model
R0(config)#aaa authentication login default group tacacs+ local
R0(config)#line console 0
R0(config-line)#login authentication default
```

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.

```
User Access Verification

Username: ciscoTACACS
Password:
R0>
```

Zabezpieczony dostęp wykorzystujący uwierzytelnianie TACACS+

15. 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.

```
R4(config)#license boot module c1900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

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.

```
R4(config)#zone security IN-ZONE
R4(config-sec-zone)# exit
R4(config)#zone security OUT-ZONE
R4(config-sec-zone)# exit
```

Tworzenie stref


```
R4(config)#access-list 101 permit ip 198.168.1.0 0.0.0.255 any
```

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.

```
R4(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R4(config-cmap)# match access-group 101
R4(config-cmap)# exit
```

Utworzenie klasyfikatora ruchu typu class-map

```
R4(config)#policy-map type inspect IN-2-OUT-PMAP
R4(config-pmap)# class type inspect IN-NET-CLASS-MAP
R4(config-pmap-c)# inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
```

Tworzenie mapy zasad policy-map

Ostatecznie zaporą 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.

```
R4(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R4(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
R4(config-sec-zone-pair)# exit
```

Utworzenie pary stref i przypisanie zasad obsługi ruchu

```
R4(config)#interface GigabitEthernet0/0
R4(config-if)# ip address 198.168.1.1 255.255.255.0
R4(config-if)# zone-member security IN-ZONE
R4(config-if)# no shutdown
R4(config-if)# exit
R4(config)#
R4(config)#interface Serial0/0/0
R4(config-if)# ip address 7.0.0.2 255.0.0.0
R4(config-if)# zone-member security OUT-ZONE
R4(config-if)# no shutdown
R4(config-if)# exit
```

Przypisanie interfejsów do poszczególnych stref

16. 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).

```
ASA0(config)#interface GigabitEthernet1/1
ASA0(config-if)# nameif inside
ASA0(config-if)# security-level 100
ASA0(config-if)# ip address 197.168.10.2 255.255.255.0
ASA0(config-if)# no shutdown
ASA0(config-if)# exit
ASA0(config)#
ASA0(config)#interface GigabitEthernet1/2
ASA0(config-if)# nameif outside
ASA0(config-if)# security-level 0
ASA0(config-if)# ip address 203.0.113.1 255.255.255.0
ASA0(config-if)# no shutdown
ASA0(config-if)# exit
ASA0(config)#
ASA0(config)#interface GigabitEthernet1/3
ASA0(config-if)# nameif dmz
ASA0(config-if)# security-level 50
ASA0(config-if)# ip address 197.168.20.1 255.255.255.0
ASA0(config-if)# no shutdown
ASA0(config-if)# exit
```

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.

```
S11(config)#vlan 10
S11(config-vlan)# name Outside_Network
```

Tworzenie VLAN 10 (dla sieci zewnętrznej)

```
S12(config)#vlan 20
S12(config-vlan)# name DMZ_Network
```

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.

```
ASA0(config)#route outside 0.0.0.0 0.0.0.0 203.0.113.2
ASA0(config)#route inside 197.168.1.0 255.255.255.0 197.168.10.1
```

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.

```
ASA0(config)#object network obj_internal
ASA0(config-network-object)# subnet 197.168.1.0 255.255.255.0
ASA0(config-network-object)# nat (inside,outside) dynamic interface
ASA0(config-network-object)#
ASA0(config-network-object)#object network obj_dmz
ASA0(config-network-object)# subnet 197.168.20.0 255.255.255.0
ASA0(config-network-object)# nat (dmz,outside) dynamic interface
```

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.

```
ASA0(config)#access-list ACL_DMZ_OUTSIDE extended permit tcp any any eq 80
ASA0(config)#access-list ACL_DMZ_OUTSIDE extended permit tcp any any eq 443
ASA0(config)#access-group ACL_DMZ_OUTSIDE in interface dmz
ASA0(config)#
ASA0(config)#access-list ACL_OUTSIDE_DMZ extended permit tcp any object obj_dmz eq 80
ASA0(config)#access-list ACL_OUTSIDE_DMZ extended permit tcp any object obj_dmz eq 443
ASA0(config)#access-group ACL_OUTSIDE_DMZ in interface outside
```

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

17. 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.