Laboratorium 5 – Podstawowa konfiguracja zapory sieciowej opartej na strefach bezpieczeństwa

Cele ćwiczenia

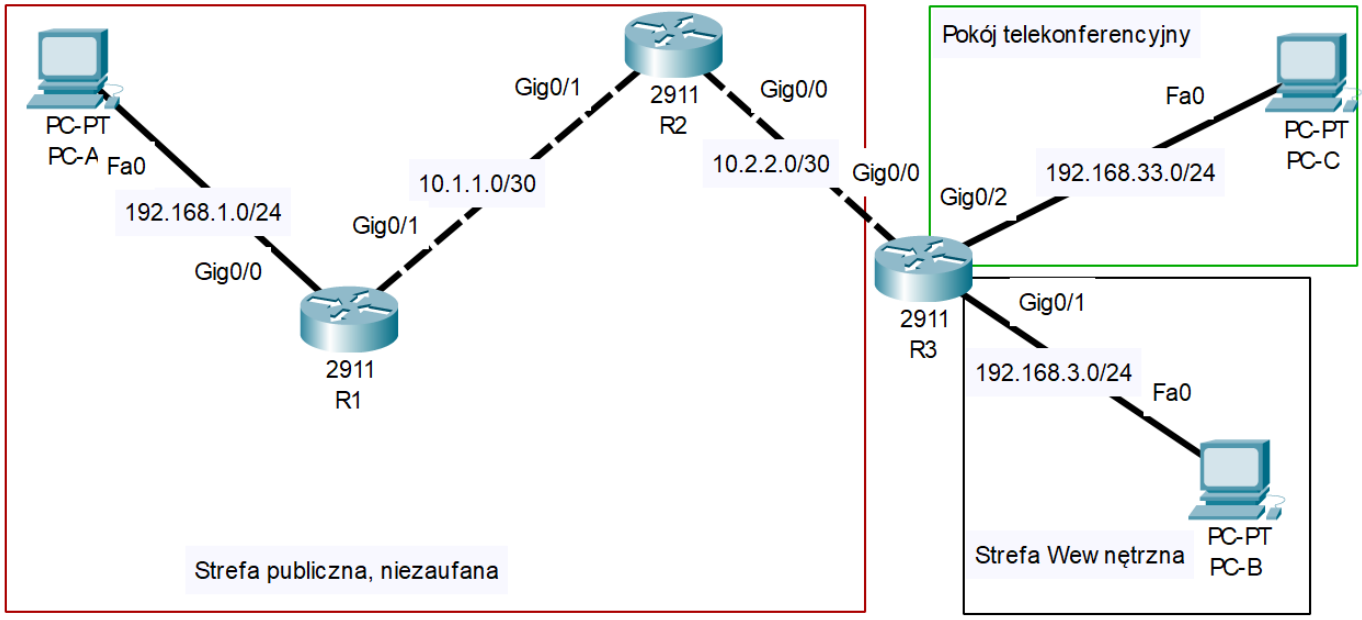
Celem ćwiczenia jest nabycie umiejętności konfigurowania stref bezpieczeństwa na ruterze pełniącym także funkcję zapory sieciowej. Cele szczegółowe są następujące:

1. Konfiguracja sieci z zaporą sieciową realizowaną jako funkcjonalność rutera
2. Konfiguracja stref bezpieczeństwa na poszczególnych interfejsach zapory sieciowe
3. Weryfikacja funkcjonalności zapory sieciowej opartej na strefach bezpieczeństwa

Opis topologii logicznej i fizycznej sieci

1. Komputer PC-A o adresie IP 192.168.1.10/24 połączony łączem FastEthernet0 z portem Gigabit Ethernet 0/0 rutera R1 o adresie 192.168.1.1/24.
2. Komputer PC-B o adresie IP 192.168.3.10/24 połączony łączem FastEthernet0 z portem Gigabit Ethernet 0/1 rutera R3 o adresie 192.168.3.1/24.
3. Komputer PC-C o adresie IP 192.168.33.10/24 połączony łączem FastEthernet0 z portem Gigabit Ethernet 0/2 rutera R3 o adresie 192.168.331/24.
4. Port Gigabit Ethernet 0/1 o adresie 10.1.1.1/30 rutera R1 połączony z portem Gigabit Ethernet 0/1 rutera R2 o adresie 10.1.1.2/30.
5. Port Gigabit Ethernet 0/0 o adresie 10.2.2.1/30 rutera R2 połączony z portem Gigabit Ethernet 0/0 rutera R3 o adresie 10.2.2.2/30.

Graficzną reprezentację opisanej topologii przedstawiono na poniższym rysunku.



Przebieg ćwiczenia

Połączenie urządzeń zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadanie adresów IP urządzeniom końcowym

1. Komputer PC-A

   Adres 192.168.1.10 z maską 24 bitową, brama domyślna 192.168.1.1/24

2. Komputer PC-B

   Adres 192.168.3.10 z maską 24 bitową, brama domyślna 192.168.3.1/24

3. Komputer PC-C

   Adres 192.168.33.10 z maską 24 bitową, brama domyślna 192.168.33.1/24

Nadanie adresów IP poszczególnym interfejsom ruterów R1, R2, R3.

```
R1(config)# interface g0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config)# interface g0/1
```

```
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# no shutdown
```

Wykonaj analogiczne czynności na ruterach R2 i R3.

Konfiguracja protokołu OSPF na ruterach R1, R2, R3 (nr procesu 1)

```
R1(config)# router ospf 1
R1(config-if)# network 192.168.1.0 0.0.0.255 area 0
R1(config-if)# network 10.1.1.0 0.0.0.3 area 0
```

Wykonaj te same czynności związane z konfiguracją protokołu OSPF na ruterach R2 i R3.

Konfiguracja dostępu do rutera R1.

Podaj nazwę domeny:

```
R1(config)# ip domain-name ioc.com
```

Skonfiguruj klucze kryptograficzne dla SSH:

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

Skonfiguruj konto **admin**i hasło **cisco**:

```
R1(config)# username admin secret cisco
```

Skonfiguruj **line console 0** tak, aby używała lokalnej bazy danych użytkowników do logowania. Wymuś automatyczne wylogowywanie po 5 minutach braku aktywności oraz automatyczne powtarzanie polecenia przerwanego przez komunikaty wyświetlane na linii konsoli.

```
R1(config)# line console 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
```

Skonfiguruj linie vty 0 4 tak, aby używały lokalnej bazy danych użytkowników do logowania. Linie vty powinny zezwalać tylko na połączenia SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

Skonfiguruj hasło do trybu uprzywilejowanego:

```
R1(config)# enable secret class
```

Konfigurowanie zapory opartej na strefach bezpieczeństwa ZPF

Aktywacja funkcjonalności zapory sieciowe na ruterze R3.

```
R3(config)# license boot module c2900 technology-package securityk9
R3(config)# copy run start
R3(config)# reload
```

Utworzenie stref bezpieczeństwa.

Poszczególne interfejsy rutera R3 dołączone są do 3 różnych stref bezpieczeństwa:

- G0/0 jest podłączony do Internetu. Ponieważ jest to sieć publiczna, jest uważana za niezaufaną i powinna mieć najniższy poziom bezpieczeństwa.
- G0/1 jest podłączony do sieci wewnętrznej. Sieć wewnętrzna powinna mieć najwyższy poziom bezpieczeństwa i powinna być dostępna tylko dla uwierzytelnionych pracowników.
- G0/2 jest podłączony do sali konferencyjnej, do której dostęp powinny mieć osoby także spoza organizacji.

W ćwiczeniu należy wdrożyć następującą politykę bezpieczeństwa:

- Ruch inicjowany w sieci publicznej nie powinien być dopuszczany do sieci wewnętrznej lub sali konferencyjnej.
- Ruch zwrotny (po zainicjowaniu sesji z sieci wewnętrznej i sali konferencyjnej) powinien być dozwolony.
- Urządzenia w sieci wewnętrznej R3 są uważane za zaufane i mogą inicjować ruch dowolnego typu (tcp, udp, icmp).
- Urządzenia w sieci sali konferencyjnej R3 są uważane za niezaufane i mogą inicjować tylko ruch sieciowy do Internetu (http, https, dns).
- Należy blokować ruch między siecią wewnętrzną a salą konferencyjną.

Poszczególne strefy bezpieczeństwa należy nazwać jako: **INSIDE**, **CONFROOM** oraz **INTERNET**:

```
R3(config)# zone security INSIDE
R3(config)# zone security CONFROOM
```

```
R3(config)# zone security INTERNET
```

Utworzenie polityki bezpieczeństwa.

Skonfiguruj politykę bezpieczeństwa, realizującą zasady przesyłania ruchu opisane powyżej:

```
R3(config)# class-map type inspect match-any INSIDE_ZONE
R3(config-cmap)# match protocol tcp
R3(config-cmap)# match protocol udp
R3(config-cmap)# match protocol icmp

R3(config)# class-map type inspect match-any CONFROOM_ZONE
R3(config-cmap)# match protocol http
R3(config-cmap)# match protocol https
R3(config-cmap)# match protocol dns

R3(config)# policy-map type inspect INSIDE_TO_INTERNET
R3(config-pmap)# class type inspect INSIDE_ZONE
R3(config-pmap-c)# inspect
R3(config)# policy-map type inspect CONFROOM_TO_INTERNET
R3(config-pmap)# class type inspect CONFROOM_ZONE
R3(config-pmap-c)# inspect
```

Tworzenie par stref bezpieczeństwa.

Należy stworzyć pary stref bezpieczeństwa, opisujące politykę przesyłania ruchu w każdym z kierunków – każda para opisuje zasady dla ruchu jednokierunkowego, od pierwszego elementu pary (inicjującego ruch) do drugiego elementu pary. W ćwiczeniu należy utworzyć dwie pary stref bezpieczeństwa:

INSIDE_TO_INTERNET: dla ruchu inicjowanego z sieci wewnętrznej do Internetu (dopuszczony),

CONFROOM_TO_INTERNET: dla ruchu inicjowanego z pokoju konferencyjnego do Internetu (dopuszczony).

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE
destination INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET source
CONFROOM destination INTERNET
```

Sprawdź poprawność utworzenia par stref bezpieczeństwa:

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy not configured

Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy not configured
```

Przyporządkowanie polityki bezpieczeństwa do par stref bezpieczeństwa.

Zastosuj policy-maps do poszczególnych par stref bezpieczeństwa:

```
R3(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE
destination INTERNET
R3(config-sec-zone-pair)# service-policy type inspect
INSIDE_TO_INTERNET
R3(config)# zone-pair security CONFROOM_TO_INTERNET source
CONFROOM destination INTERNET
R3(config-sec-zone-pair)# service-policy type inspect
CONFROOM_TO_INTERNET
```

Sprawdź poprawność przypisania polityk bezpieczeństwa do par stref bezpieczeństwa:

```
R3# show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET

Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET
R3# show policy-map type inspect zone-pair sessions
policy exists on zp INSIDE_TO_INTERNET
 Zone-pair: INSIDE_TO_INTERNET
```

```
    Service-policy inspect : INSIDE_TO_INTERNET

      Class-map: INSIDE_PROTOCOLS (match-any)
        Match: protocol tcp
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol udp
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
        Inspect

      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          0 packets, 0 bytes

  policy exists on zp CONFROOM_TO_INTERNET
   Zone-pair: CONFROOM_TO_INTERNET

    Service-policy inspect : CONFROOM_TO_INTERNET

      Class-map: CONFROOM_PROTOCOLS (match-any)
        Match: protocol http
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: protocol https
          0 packets, 0 bytes
          30 second rate 0 bps
```

```
        Match: protocol dns
          0 packets, 0 bytes
          30 second rate 0 bps
        Inspect

      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          0 packets, 0 bytes
```

Przyporządkuje interfejsy rutera R3 do odpowiednich stref bezpieczeństwa.

Przyporządkuj interfejs G0/2 rutera R3 do strefy bezpieczeństwa **CONFROOM**:

```
R3(config)# interface g0/2
R3(config-if)# zone-member security CONFROOM
```

Przyporządkuj interfejs G0/1 rutera R3 do strefy bezpieczeństwa **INSIDE**:

```
R3(config)# interface g0/1
R3(config-if)# zone-member security INSIDE
```

Przyporządkuj interfejs G0/0 rutera R3 do strefy bezpieczeństwa **INTERNET**:

```
R3(config)# interface g0/0
R3(config-if)# zone-member security INTERNET
```

Sprawdzenie poprawności przyporządkowania interfejsów do stref bezpieczeństwa.

```
R3(config)# show zone security
zone self
  Description: System defined zone

zone INSIDE
  Member Interfaces:
    GigabitEthernet0/1

zone CONFROOM
  Member Interfaces:
    GigabitEthernet0/2
```

```
zone INTERNET
  Member Interfaces:
    GigabitEthernet0/0
```

Zweryfikuj poprawność działania zapory sieciowej opartej na strefach bezpieczeństwa

Sprawdź łączność w obu kierunkach pomiędzy każdą parą komputerów PC-A, PC-B, PC-C za pomocą polecenia **ping**. Wyjaśnij, dlaczego w pewnych relacjach polecenie ping zakończyło się sukcesem, a w innych nie.