LABORATORIUM PROJEKTOWANIE I OBSŁUGA SIECI KOMPUTEROWYCH II

Data wykonania ćwiczenia:	27.04.2023
Rok studiów:	3
Semestr:	6
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	9

Temat: Packet Tracer - Konfigurowanie statycznego NAT / Packet Tracer – Konfigurowanie dynamicznego NAT

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Packet Tracer - Konfigurowanie statycznego NAT

W sieciach komputerowych z protokołem IPv4, klienci i serwery używają adresów prywatnych. Zanim pakiety z prywatnej sieci zostaną wysłane przez Internet, to ich prywatne adresy muszą zostać zamienione na adresy publiczne. Serwery, do których wymagany jest dostęp z zewnątrz firmy, zazwyczaj używają jednocześnie adresów i prywatnych i publicznych. W tym ćwiczeniu skonfigurujesz statyczny NAT, dzięki czemu urządzenia znajdujące się w sieci zewnętrznej będą mogły uzyskać dostęp do serwera w sieci wewnętrznej poprzez jego adres publiczny.

Część 1: Testowanie dostępu bez mechanizmu NAT

Krok 1: Spróbuj połączyć się z serwerem Server1 używając trybu Simulation Mode.

a) Przełącz w tryb Simulation.

b) Z komputera PC1 lub laptopa L1 spróbuj połączyć się przeglądarką ze stroną internetową serwera Server1 dostępną pod adresem 172.16.16.1. Kliknij przycisk Capture Forward, zauważ, że pakiety nigdy nie opuszczają chmury internetowej. Próba powinna zakończyć się niepowodzeniem.

c) Wyjdź z trybu Simulation.

d) Z komputera PC1 wykonaj ping do interfejsu R1 S0/0/0 (209.165.201.2). Wykonanie polecenia ping powinno zakończyć się sukcesem.

Krok 2: Wyświetl tablicę routingu R1 i zawartość pliku konfiguracji bieżącej running-config.

a) Wyświetl bieżącą konfigurację routera R1. Zauważ, że nie ma tam żadnych poleceń dotyczących konfiguracji NAT. Łatwym sposobem potwierdzenia tego jest wydanie następującego polecenia:

```
R1# show run | include nat
```

b) Sprawdź, czy tablica routingu nie zawiera wpisów odnoszących się do adresów sieci IP dla PC1 i L1.

```
R1# show ip nat translations
```

Część 2: Konfigurowanie statycznego NAT

Krok 1: Wykonaj instrukcje konfigurujące statyczny NAT.

Wykorzystaj podaną topologię. Utwórz statyczne mapowanie dla serwera Server1 między adresem wewnętrznym a adresem zewnętrznym.

```
R1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

Krok 2: Wykonaj konfigurację interfejsów.

a) Skonfiguruj interfejs G0/0 jako wewnętrzny interfejs NAT.

```
R1(config)# interface g0/0
R1(config-if)# ip nat inside
```

b) Skonfiguruj interfejs publiczny s0/0/0 jako interfejs zewnętrzny.

```
R1(config)# interface s0/0/0
R1(config-if)# ip nat outside
```

Część 3: Testowanie dostępu z uruchomionym mechanizmem NAT

Krok 1: Sprawdź połączenie ze stroną internetową serwera Server1.

a) Otwórz wiersz poleceń na PC1 lub L1 i za pomocą komendy ping sprawdź połączenie z publicznym adresem serwera Server1. Test powinien zakończyć się powodzeniem.

b) Upewnij się, że zarówno PC1 , jak i L1 mają teraz dostęp do strony internetowej serwera Server1.

Krok 2: Wyświetl translacje NAT.

Użyj następujących poleceń, aby zweryfikować statyczną konfigurację NAT na R1:

```
show running-config
show ip nat translations
show ip nat statistics
```

Packet Tracer – Konfigurowanie dynamicznego NAT

Część 1: Konfiguracja dynamicznego NAT

Krok 1: Konfiguracja dozwolonego ruchu.

Na R2, skonfiguruj standardową listę ACL 1 zezwalającą na ruch dla adresów należących do przestrzeni 172.16.0.0/16.

```
R2(config)# access-list 1 permit 172.16.0.0 0.0.255.255
```

Krok 2: Konfiguracja puli adresów NAT.

Skonfiguruj R2 z pulą NAT, która używa dwóch adresów w przestrzeni adresowej 209.165.200.228/30.

```
R2(config)# ip nat pool ANY_POOL_NAME 209.165.200.229 209.165.200.230 netmask
255.255.255.252
```

Zauważ, że w topologii są trzy adresy sieciowe, które powinny być przekształcane zgodnie z utworzoną listą ACL.

Co się stanie, jeśli więcej niż 2 urządzenia spróbują uzyskać dostęp do Internetu?

Nadprogramowe urządzenia nie otrzymają dostępu dopóki zwolni się jakiś adres

Krok 3: Powiązanie listy ACL1 z pulą NAT.

Wprowadź polecenie kojarzące ACL 1 z utworzoną pulą translacji NAT.

```
R2(config)# ip nat inside source list 1 pool ANY_POOL_NAME
```

Krok 4: Konfiguracja interfejsów NAT.

Stosując właściwe polecenia NAT skonfiguruj interfejsy R2 oznaczając je, jako połączone do wewnątrz i połączone na zewnątrz.

```
R2(config)# interface s0/0/0
R2(config-if)# ip nat outside
R2(config-if)# interface s0/0/1
R2(config-if)# ip nat inside
```

Część 2: Weryfikacja implementacji NAT

Krok 1: Uzyskaj dostęp do usług przez Internet.

Korzystając z przeglądarki internetowej na L1, PC1 lub PC2 uzyskaj dostęp do strony internetowej na serwerze Server1.

Krok 2: Wyświetl translacje NAT.

Wyświetl odwzorowania NAT na R2. Zidentyfikuj wewnętrzny adres źródłowy komputera i przetłumaczony adres z puli NAT w danych wyjściowych polecenia.

```
R2# show ip nat translations
```