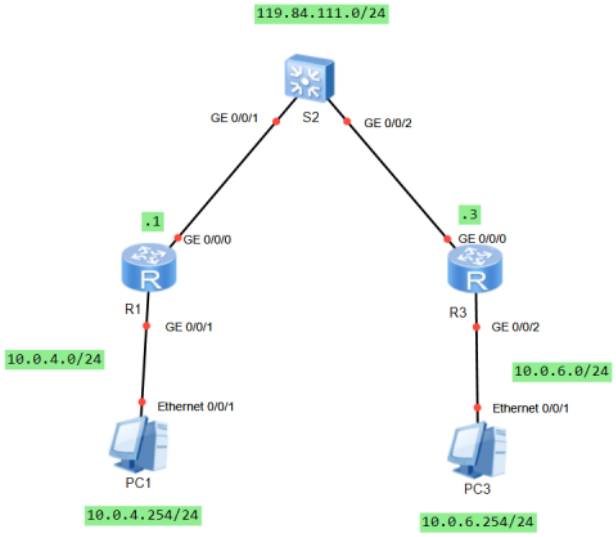
Lab 9 Konfiguracja mechanizmu NAT (Network Address Translation)

Cele

W ćwiczeniu będzie trzeba wykonać następujące zadania:

- **Umożliwić tłumaczenie adresów pomiędzy sieciami (NAT).**
- **Skonfigurować Easy IP.**

Topologia



Scenariusz

W celu zaoszczędzenia zakresów publicznych adresów IP W sieciach wewnętrznych zastosowano adresację prywatną. Wykorzystując mechanizm NAT możliwe będzie zapewnienie łączności pomiędzy sieciami wewnętrzymi (prywatnymi) a siecią publiczną. Routery R1 oraz R3 reprezentują routery brzegowe dla oddziałów formy. Administrator sieci został poproszony o skonfigurowanie mechanizmu NAT na routerze R1 w celu umożlwienia tłumaczenia adresów IP. Na routerze R3 zostanie skonfigurowane rozwiązanie easyIP NAT.

Zadania

Krok 1 Przygotowanie.

```
[Huawei]sysname R1
[Rl]inter GigabitEthernet0/0/1
[Rl-GigabitEthernet0/0/1]ip address 10.0.4.1 24

[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24
```

Ustaw adresy IP, maski podsieci oraz bramy domyślne na komputerach PC1 i PC3.

Krok 2 Konfiguracja publicznych adresów IP

```
[Rl]interface GigabitEthernet0/0/0
[Rl-GigabitEthernet0/0/0]ip address 119.84.111.1 24

[R3]interface GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24

[S2]interfae vlanif1
[S2-Vlanif1]ip address 119.84.111.2 24
```

Zweryfikuj czy R1 ma dostęp do komputera PC1 I routera R3.

```
<Rl>ping 10.0.4.254
  PING 10.0.4.254: 56 data bytes, press CTRL_C to break
    Reply   from10.0.4.254: bytes=56 Sequence=l ttl=255 time=23 ms
    Reply   from10.0.4.254: bytes=56 Sequence=2 ttl=254 time=l ms
    Reply   from10.0.4.254: bytes=56 Sequence=3 ttl=254 time=l ms
    Reply   from10.0.4.254: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply   from10.0.4.254: bytes=56 Sequence=5 ttl=254 time=l ms
   -  10.0.4.254 ping statistics --
     5 packet(s) transmitted
     5 packet(s) received
     0.00% packet loss

     round-trip min/avg/max = 1/7/23 ms
```

```
<Rl>ping 119.84.111.3
PING 119.84.111.3: 56 data bytes, press CTRL_C to break
Reply from 119.84.111.3: bytes=56 Sequence=l ttl=255 time=l ms
Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=10 ms
Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=l ms
Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=l ms
Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms

 ---  119.84.111.3 ping statistics --
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/10 ms
```

Krok 3 Konfiguracja list kontroli dostępu na R1 i R3.

Skonfiguruj rozszerzoną ACL na R1 dla adresów IP z sieci podłączonej do interfejsu G0/0/1 routera R1, uwzględniając dowolny adres IP docelowy.

```
[Rl]acl 3000
[Rl-acl-adv-3000]rule 5 permit ip source 10.0.4.0 0.0.0.255 destination any
[Rl-acl-adv-3000]rule 10 deny ip
```

Skonfiguruj standardową ACL na R3 dla źródłowych adresów IP 10.0.6.0/24.

```
[R3]acl 2000
[R3-acl-basic-2000]rule permit source 10.0.6.0 0.0.0.255
```

Krok 4 Konfiguracja dynamicznego NAT.

Skonfiguruj dynamiczny NAT na GigabitEthernet0/0/0 toutera R1.

```
[R1]nat address-group 1 119.84.111.240 119.84.111.243
[Rl]interface GigabitEthernet 0/0/0
[Rl-GigabitEthernetO/O/O]nat outbound 3000 address-group 1
```

Zweryfikuj czy grupa adresów została skonfigurowana prawidłowo.

```
<Rl>display nat address-group
     NAT Address-Group Information:

     Index Start-address       End-address

     1      119.84.111.240   119.84.111.243

     Total : 1
```

Sprawdź połączenie z komputera PC1 do adresu 119.84.111.3.

```
<PCl>ping 119.84.111.3
  PING 119.84.111.3: 56 data bytes, press CTRL_C to break
    Request time out
    Reply from  119.84.111.3:bytes=56  Sequence=2 ttl=254 time=l ms
    Reply from  119.84.111.3:bytes=56  Sequence=3 ttl=254 time=l ms
    Reply from  119.84.111.3:bytes=56  Sequence=4 ttl=254 time=l ms
    Reply from  119.84.111.3:bytes=56  Sequence=5 ttl=254 time=l ms

   -- 119.84.111.3 ping statistics  -
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

W celu weryfikacji działania NAT wyświetl ACL skonfigurowaną na routerze R1.

```
<Rl>display acl 3000
Advanced ACL 3000, 2 rules
Acl's step is 5
rule 5 permit ip source 10.0.4.0 0.0.0.255 (1 matches)
rule 10 deny ip
<Rl>display nat session all
  NAT Session Table Information:

    Protocol                 ICMP(1)
    SrcAddr Vpn              10.0.  4.254
    DestAddr Vpn             119.84.111.3
    Type Code Icmpld         8   0   44003
    NAT-Info
      New SrcAddr            119.84.111.242
      New DestAddr
      New Icmpld             10247



  Total : 1
```

Jeśli jako wynik polecenia nei wyświetli się ICMP należy zwiększyć jego czas podtrzymania z 20s do 300s. Należy użyć poniższego polecenia:

```
[Rl]firewall-nat session icmp aging-time 300
```

Konfiguracji easyIP na interfejsie Gigabit Ethernet 0/0/0 routera R3, dokonujemy przy użyciu poniższego polecenia (wiążemy z mechanizmem NAT listę ACL 2000).

```
[R3-GigabitEthernet0/0/0]nat outbound 2000
```

Testowanie połączenia z PC3 do R1 przez R3.

```
<PC3>ping 119.84.111.1
PING 119.84.111.1: 56 data bytes, press CTRL C to break
Reply from 119.84.111.1: bytes=56  Sequence=l ttl=254 time=l ms
Reply from 119.84.111.1: bytes=56  Sequence=2 ttl=254 time=l ms
Reply from 119.84.111.1: bytes=56  Sequence=3 ttl=254 time=l ms
Reply from 119.84.111.1: bytes=56  Sequence=4 ttl=254 time=l ms
Reply from 119.84.111.1: bytes=56  Sequence=5 ttl=254 time=l ms


   -- 119.84.111.1 ping statistics  --
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

<R3>display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
rule 5 permit source 10.0.6.0 0.0.0.255 (1 matches)

<R3>display nat outbound acl 2000


NAT Outbound Information:

Interface                 Acl          Address-group/IP/Interface
                                      Type

GigabitEthernet0/0/0 2000                        119.84.111.3 easyip
```