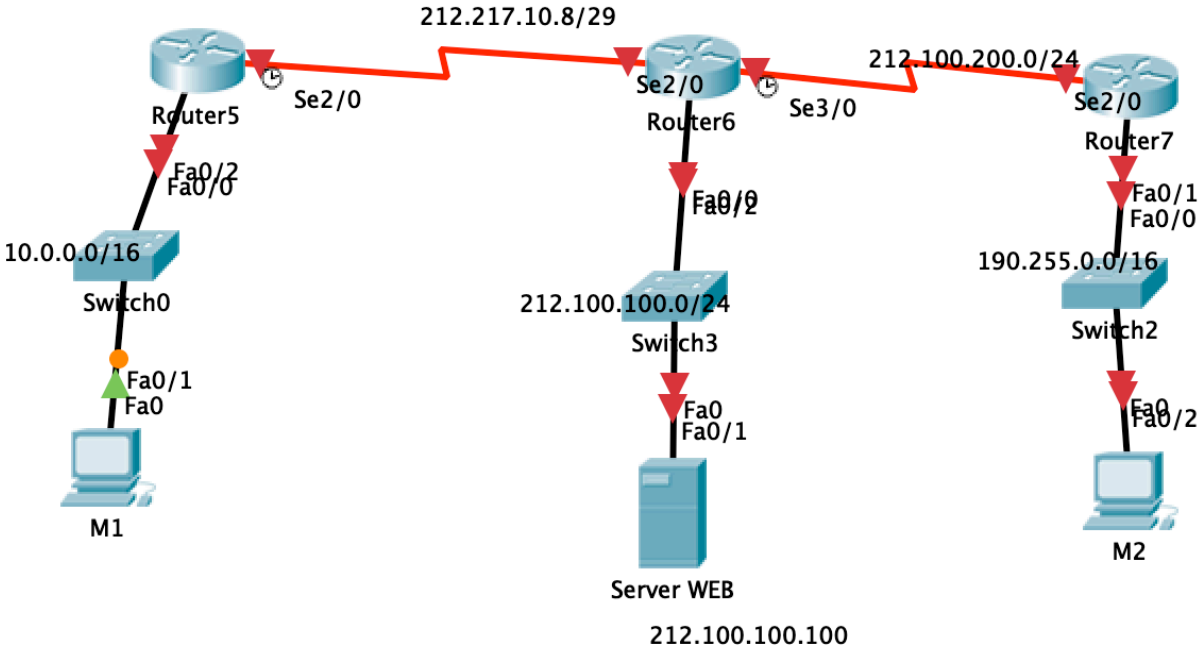
TP7 (solution)

Objectifs du TP : Configuration du protocole NAT et des listes de contrôle d'accès ACL.

Topologie :



A. Configuration du routeur et des équipements

1. Configurez toutes les interfaces des routeurs, des machines en respectant le plan d'adressage ci-dessus.

```
Router5(config)#interface Fa0/2
Router5(config-if)# ip address 10.0.0.1 255.0.0.0
Router5(config-if)#no shutdown
Router5(config-if)#exit

Router5(config)#interface Serial2/0
Router5(config-if)#ip address 212.217.10.9 255.255.255.248
Router5(config-if)#no shutdown
Router5(config-if)#clock rate 64000
Router5(config-if)#exit


Router6(config)#interface Fa0/2
Router6(config-if)# ip address 212.100.100.1 255.255.255.0
Router6(config-if)#no shutdown
Router6(config-if)#exit

Router6(config)#interface Serial2/0
Router6(config-if)#ip address 212.217.10.10 255.255.255.248
Router6(config-if)#no shutdown
Router5(config-if)#exit


Router6(config)#interface Serial3/0
```

```
Router6(config-if)#ip address 212.100.200.1 255.255.255.0
Router6(config-if)#clock rate 64000
Router6(config-if)#no shutdown
Router6(config-if)#exit

Router7(config)#interface Fa0/1
Router7(config-if)# ip address 190.255.0.0.1 255.255.0.0
Router7(config-if)#no shutdown
Router7(config-if)#exit

Router7(config)#interface Serial2/0
Router7(config-if)#ip address 212.100.200.2 255.255.255.0
Router7(config-if)#no shutdown
Router7(config-if)#exit
```

2. Configurez le routage statique sur les trois routeurs.

Router5 :

```
Router5(config-router)# ip route 212.100.100.0 255.255.255.0 212.217.10.10
Router5(config-router)# ip route 190.255.0.0 255.255.0.0 212.217.10.10
```

Router6 :

```
Router6(config-router)# ip route 10.0.0.0 255.0.0.0 212.217.10.1
Router6(config-router)# ip route 190.255.0.0 255.255.0.0 212.100.200.2
```

Router7 :

```
Router7(config-router)# ip route 10.0.0.0 255.0.0.0 212.100.200.1
Router7(config-router)# ip route 212.100.100.0 255.255.255.0 212.100.200.1
```

3. Tester l'état de votre connexion des machines vers le serveur.

```
M1>ping 190.255.0.2 (M2)
Pinging 190.255.0.2 with 32 bytes of data: Reply from 190.255.0.2: bytes=32 time=13ms TTL=125
Reply from 190.255.0.2: bytes=32 time=2ms TTL=125 Reply from 190.255.0.2: bytes=32
time=11ms TTL=125 Reply from 190.255.0.2: bytes=32 time=10ms TTL=125 Ping statistics for
190.255.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in
milli-seconds: Minimum = 2ms, Maximum = 13ms, Average = 9ms

M1>ping 212.100.100.2 (WEB)
Pinging 212.100.100.2 with 32 bytes of data: Reply from 212.100.100.2: bytes=32 time=12ms
TTL=126 Reply from 212.100.100.2: bytes=32 time=13ms TTL=126 Reply from 212.100.100.2:
bytes=32 time=10ms TTL=126 Reply from 212.100.100.2: bytes=32 time=11ms TTL=126 Ping
statistics for 212.100.100.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate
round trip times in milli-seconds: Minimum = 10ms, Maximum = 13ms, Average = 11ms
```

B. Configuration du protocole NAT/PAT/ACL

1. Avant de commencer cette partie, supprimez du routeur 7 la route qui mène au réseau 10.0.0.0 ?

```
Router7(config-router)# no ip route 10.0.0.0 255.0.0.0 212.100.200.1
```

2. Testez la connexion de la machine M1 vers M2 ? ……non

```
M1>ping 190.255.0.2
```

Pinging 190.255.0.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 190.255.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

3. Testez la connexion de la machine M2 vers M1 ? ……Non……

M2>ping 10.0.0.2

Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Ping statistics for 10.0.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

4. Configurez le NAT surchargé sur le routeur 5

Router5(config) # **access-list** *1* **permit** *10.0.0.0 0.0.255.255*

Router5(config) # **ip nat inside source list** *1* **interface** *serial 2/0* **overload**

Que signifie le mot clé **overload** ? surchage

Interface d'entrée au réseau privée

Router5(config) # **int** *fa0/2*

Router5(config-if) # **ip nat inside**

Interface de sortie du réseau privée vers le publique via S2/0

Router5(config) # **int** *s2/0*

Router5(config-if) # **ip nat outside**

- Quelles sont les machines qui sont autorisées à faire du NAT ?

La liste des machines autorisées à faire de la traduction x.y.z.t (x=10, y=0, 0=<z<=255, 0=<t<=254)

5. Faites un ping de la machine M2 vers M1.

M2>ping 10.0.0.2 (M1)
Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Reply from 190.255.0.1: Destination host unreachable. Ping statistics for 10.0.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

6. Faites un ping de la machine M1 vers M2.

M1>ping 190.255.0.2 (M2)

Reply from 190.255.0.2: bytes=32 time=20ms TTL=125 Reply from 190.255.0.2: bytes=32 time=11ms TTL=125 Reply from 190.255.0.2: bytes=32 time=4ms TTL=125 Reply from 190.255.0.2: bytes=32 time=13ms TTL=125 Ping statistics for 190.255.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 4ms, Maximum = 20ms, Average = 12ms

7. Consultez la table des translations NAT

Router5 **#show ip nat translations**

```
Inside global     Inside local      Outside local     Outside global
icmp 212.217.10.9:45 10.0.0.2:45    190.255.0.2:45  190.255.0.2:45
icmp 212.217.10.9:46 10.0.0.2:46 190.255.0.2:46 190.255.0.2:46
icmp 212.217.10.9:47 10.0.0.2:47 190.255.0.2:47 190.255.0.2:47
icmp 212.217.10.9:48 10.0.0.2:48 190.255.0.2:48 190.255.0.2:48
```

8. Changez l'adresse IP de la machine M1 par 10.1.0.2, puis faites un ping sur M2. Consultez à nouveau la table des translations NAT ? Pourquoi la translation n'a pas pu eu lieu ?

   M1>ping 190.255.0.2

   Pinging 190.255.0.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 190.255.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

   Router5 **#show ip nat translations**

   La traduction ne marche pas.

   Pourquoi la translation n'a pas pu eu lieu ?

9. Remettez l'ancienne adresse IP (10.0.0.2) à M1. Réalisez un mappage statique pour que la machine M1 devienne visible depuis l'extérieur ?

   Router5 #ip nat inside source static 10.0.0.2 212.217.10.12

10. Testez de nouveau un ping de la machine M2 vers M1 en utilisant sa nouvelle adresse publique (212.217.10.12) ?

    M2>ping 212.217.10.12

    Reply from 212.217.10.12: bytes=32 time=3ms TTL=125 Reply from 212.217.10.12: bytes=32 time=2ms TTL=125 Reply from 212.217.10.12: bytes=32 time=3ms TTL=125 Reply from 212.217.10.12: bytes=32 time=12ms TTL=125 Ping statistics for 212.217.10.12: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 12ms, Average = 5ms

11. Consultez la table des translations NAT

    Router5 #show ip nat translations

```
Inside global  Inside local  Outside local  Outside global
icmp 212.217.10.12:65 10.0.0.2:65 190.255.0.2:65 190.255.0.2:65
icmp 212.217.10.12:66 10.0.0.2:66 190.255.0.2:66 190.255.0.2:66
icmp 212.217.10.12:67 10.0.0.2:67 190.255.0.2:67 190.255.0.2:67
icmp 212.217.10.12:68 10.0.0.2:68 190.255.0.2:68 190.255.0.2:68
--- 212.217.10.12  10.0.0.2 --- ---
```

12. Ecrivez une ACL étendue (en trois lignes) qui permet de bloquer les machines dont les IPs varient de **10.0.0.2** à 10.0.0.19 et qui autorise le reste ? Testez votre ACL ?

    Il s'agit du routeur 5.
    ACL = une liste de règles séquentielles.
    N(ACL étendue)> 99.

Règle 1 : Autoriser l'interface 10.0.0.1 à sortir du routeur 5.
Router5(config)#access-list 102 permit ip 10.0.0.1 0.0.0.0 (host) any
Règle 2 : Bloquer toutes les machines dont les IPs varient de **10.0.0.2** à 10.0.0.19
10.0.0.0000 0010 à 10.0.0.00010011 (masque générique 0.0.0.00011111 (31))
Router5(config)#access-list 102 deny ip 10.0.0.2 0.0.0.31 any
(plage d'adresses de 10.0.0.1 à 10.0.0.19)
Règle 3 : autorise le reste
Router5(config)#access-list 102 permit ip any any
Une ACL n°102 est crée.

L'interface d'application de la liste (interface de sortie):
Router5(config)#int serial2/0
Router5(config-if)#ip access-group 102 out
Router5(config-if)#exit
Router5#show ip access-list
Extended IP access list 102
10 permit ip host 10.0.0.1 any
20 deny ip 10.0.0.0 0.0.0.31 any
30 permit ip any any (7 match(es))

Test de votre ACL
M1> Ping @IP_M2

C:\>ping 190.255.0.2 Pinging 190.255.0.2 with 32 bytes of data: Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Ping statistics for 190.255.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Supprimer la liste 102.

13. En utilisant une ACL étendue, écrivez une ACL interdit toute communication de M1 vers M2. Testez votre ACL ?

Router(config)#access-list 103 deny ip 10.0.0.2 0.0.0.0 190.255.0.2 0.0.0.0
Router(config)#access-list 103 permit ip any any

Router(config)#int serial2/0
Router(config-if)#ip access-group 103 out

Test

Pinging 190.255.0.2 with 32 bytes of data: Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Reply from 10.0.0.1: Destination host unreachable. Ping statistics for 190.255.0.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Supprimer la liste 103.

14. Ecrire une ACL qui limite l'accès telnet sur les deux routeurs à la machine M1. Testez votre ACL ?

```
Router(config)#access-list 104 permit TCP 10.0.0.2 0.0.0.0  any  eq telnet (23)
Router(config)#access-list 104 deny TCP 10.0.0.0  0.0.255.255  any   eq telnet (23)

Router(config)#access-list 104 permit ip 10.0.0.0 0.0.255.255  any

Router(config)#int serial2/0
Router(config-if)#ip access-group 104 out
Router(config-if)#exit
```

Vérification :

```
Extended IP access list 104
10 permit tcp host 10.0.0.2 any eq telnet
20 deny tcp 10.0.0.0 0.0.255.255 any eq telnet
30 permit ip 10.0.0.0 0.0.255.255 any
```

Test

Configurer une session virtuelle sur R6 (VTY).

M1>telnet 212.217.10.10

>telnet 212.217.10.10 Trying 212.217.10.10 ...Open User Access Verification Password: Router>

15. Ecrire sur le routeur 6, une ACL qui permet d'autoriser uniquement l'accès au serveur WEB à partir des autres routeurs ?

```
Router6(config)#access-list 105 permit tcp any 212.100.100.100 0.0.0.0 eq HTTP (80)
Router6(config)#access-list 105 deny ip any   212.100.100.0 0.0.0.255

Router6(config)#int gigabitEthernet 0/0
Router6(config-if)#ip access-group 105 out
Router6(config-if)#exit
```

Test

M1>ping 212.100.100.100

Pinging 212.100.100.100 with 32 bytes of data: Reply from 212.217.10.10: Destination host unreachable. Reply from 212.217.10.10: Destination host unreachable. Reply from 212.217.10.10: Destination host unreachable. Reply from 212.217.10.10: Destination host unreachable. Ping statistics for 212.100.100.100: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

M1>WEB http:// 212.100.100.100

Cisco Packet Tracer Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.