TP15 : Listes de contrôle d’accès standards et étendues

Sommaire

1. ACL IPv4 standards

1. On configure les PC

2. On configure le routeur R1

a. On configure son nom d'hôte, on désactive la recherche DNS, on active le chiffrement des mots de passe

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
```

b. On protége l'accès enable avec le mot de passe class. On ajoute l'utilisateur admin avec le mot de passe cisco. On configure l'accès SSH avec l'utilisateur admin et la synchronisation des logs

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

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.exupery.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R1(config)#ip domain-name exupery.local
R1(config)#username admin secret cisco
```

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#logging synchronous
R1(config-line)#
```

c. On configure les interfaces du routeur (G0/0, G0/1 et S0/0/0)

```
R1(config)#int g0/0
R1(config-if)#ip address 192.168.11.254 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config)#int g0/1
R1(config-if)#ip address 192.168.12.254 255.255.255.0
R1(config-if)#no shutdown
```

```
R1(config)#int s0/0/0
R1(config-if)#ip address 10.0.12.1 255.255.255.252
R1(config-if)#no shutdown
```

Et on fait pareil pour R2 et R3

3. On configure le routeur R2 de manière analogue ainsi que les interfaces du routeur (L0, S0/0/0 et S0/0/1)

```
R2(config)#int s0/0/1
R2(config-if)#ip address 10.0.12.2 255.255.255.252
R2(config-if)#no shutdown


R2(config)#int s0/0/0
R2(config-if)#10.0.23.1 255.255.255.252
              ^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 10.0.23.1 255.255.255.252
R2(config-if)#no shutdown


R2(config)#int L0
R2(config-if)#ip address 200.0.0.1 255.255.255.255
R2(config-if)#no shutdown
```

4. On configure le routeur R3 de manière analogue ainsi que les interfaces du routeur (G0/0, G0/1 et S0/0/1)

je n'avais pas les captures de quand j'ai fait les commandes alors je suis aller voir dans le show run, les interfaces sont toute no shutdown bien sur

```
interface GigabitEthernet0/0
 ip address 192.168.21.254 255.255.255.0

interface GigabitEthernet0/1
 ip address 192.168.22.254 255.255.255.0


interface Serial0/0/1
 ip address 10.0.23.2 255.255.255.252
```

5. On configure RIPv2 sur les routeurs R1, R2 et R3.

R1 :

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.12.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 10.0.12.0
R1(config-router)#no auto-summary
```

R2 :

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.12.0
R2(config-router)#network 10.0.23.0
R2(config-router)#no auto-summary
R2(config-router)#default-information originate
```

R3 :

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 10.0.23.0
R3(config-router)#network 192.168.22.0
R3(config-router)#network 192.168.21.0
R3(config-router)#no auto-summary
```

On vérifie leur table de routage

R1 :

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.12.0/30 is directly connected, Serial0/0/0
L       10.0.12.1/32 is directly connected, Serial0/0/0
R       10.0.23.0/30 [120/1] via 10.0.12.2, 00:00:15, Serial0/0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0
L       192.168.11.254/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, GigabitEthernet0/1
L       192.168.12.254/32 is directly connected, GigabitEthernet0/1
R    192.168.21.0/24 [120/2] via 10.0.12.2, 00:00:15, Serial0/0/0
R    192.168.22.0/24 [120/2] via 10.0.12.2, 00:00:15, Serial0/0/0
R    200.0.0.0/24 is possibly down, routing via 10.0.12.2, Serial0/0/0
```

R2 :

```
R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.0.12.0/30 is directly connected, Serial0/0/1
L       10.0.12.2/32 is directly connected, Serial0/0/1
C       10.0.23.0/30 is directly connected, Serial0/0/0
L       10.0.23.1/32 is directly connected, Serial0/0/0
R    192.168.11.0/24 [120/1] via 10.0.12.1, 00:00:13, Serial0/0/1
R    192.168.12.0/24 [120/1] via 10.0.12.1, 00:00:13, Serial0/0/1
R    192.168.21.0/24 [120/1] via 10.0.23.2, 00:00:06, Serial0/0/0
R    192.168.22.0/24 [120/1] via 10.0.23.2, 00:00:06, Serial0/0/0
     200.0.0.0/32 is subnetted, 1 subnets
C       200.0.0.1/32 is directly connected, Loopback0
```

R3 :

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.0.12.0/30 [120/1] via 10.0.23.1, 00:00:08, Serial0/0/1
C       10.0.23.0/30 is directly connected, Serial0/0/1
L       10.0.23.2/32 is directly connected, Serial0/0/1
R    192.168.11.0/24 [120/2] via 10.0.23.1, 00:00:08, Serial0/0/1
R    192.168.12.0/24 [120/2] via 10.0.23.1, 00:00:08, Serial0/0/1
     192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.21.0/24 is directly connected, GigabitEthernet0/0
L       192.168.21.254/32 is directly connected, GigabitEthernet0/0
     192.168.22.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.22.0/24 is directly connected, GigabitEthernet0/1
L       192.168.22.254/32 is directly connected, GigabitEthernet0/1
```

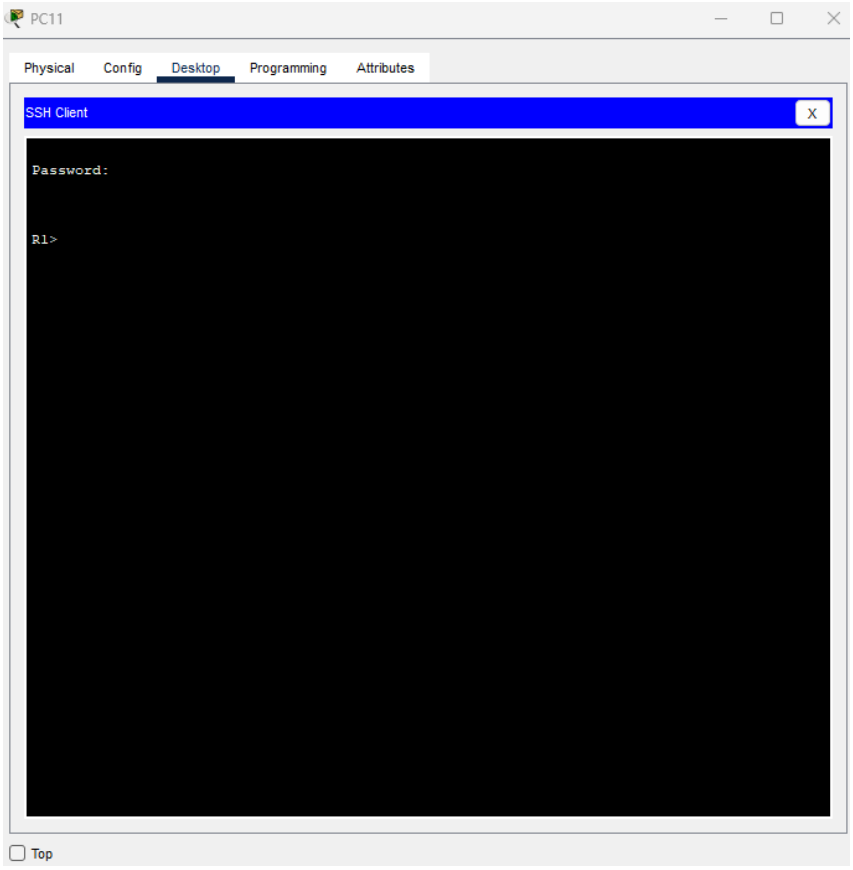
6. On vérifie la connectivité. Tous les PC doivent pouvoir se joindre et doivent également pouvoir accéder en SSH aux trois routeurs

PC12 peut bien ping les autres PC :

```
Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=17ms TTL=125
Reply from 192.168.21.1: bytes=32 time=17ms TTL=125
Reply from 192.168.21.1: bytes=32 time=21ms TTL=125
Reply from 192.168.21.1: bytes=32 time=21ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 21ms, Average = 19ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time=25ms TTL=125
Reply from 192.168.22.1: bytes=32 time=16ms TTL=125
Reply from 192.168.22.1: bytes=32 time=18ms TTL=125
Reply from 192.168.22.1: bytes=32 time=21ms TTL=125

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 25ms, Average = 20ms
```

Après avoir fait tout les tests tout les PC peuvent bien se ping

PC11 accède bien a R1, R2 et R3 en connexion ssh



7. On créer une liste de contrôle d'accès numérotée standard qui n'autorise l'accès au réseau 192.168.21.0/24 qu'aux hôtes des réseaux 192.168.11.0/24 et 192.168.12.0/24. La direction souhaite pouvoir connaître le nombre de tentatives refusées

On fait en sorte que les listes de contrôle d'accès standards soit placées le plus près possible de la destination soit le réseau 192.168.21.0/24. On choisit donc l'interface G0/0 de R3 en sortie

```
R3(config)#access-list 1 permit 192.168.11.0 0.0.0.255
R3(config)#access-list 1 permit 192.168.12.0 0.0.0.255
R3(config)#access-list 1 deny any
```

```
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
```

Après avoir fait ça le réseau 192.168.21.0/24 ne doit plus être accessible depuis le PC22

```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Comme nous avons ajouter la dernière ACE (deny any), il est possible de visualiser les tentatives refusées

```
R3#sh access-lists
Standard IP access list 1
    10 permit 192.168.11.0 0.0.0.255
    20 permit 192.168.12.0 0.0.0.255
    30 deny any (4 match(es))
```

Le réseau doit naturellement être accessible depuis les deux LAN de R1. On test avec PC11 et PC12

ping depuis PC12 :

```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=8ms TTL=125
Reply from 192.168.21.1: bytes=32 time=7ms TTL=125
Reply from 192.168.21.1: bytes=32 time=16ms TTL=125
Reply from 192.168.21.1: bytes=32 time=7ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 16ms, Average = 9ms
```

ping depuis PC11 :

```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=23ms TTL=125
Reply from 192.168.21.1: bytes=32 time=24ms TTL=125
Reply from 192.168.21.1: bytes=32 time=12ms TTL=125
Reply from 192.168.21.1: bytes=32 time=16ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 24ms, Average = 18ms
```

Les pings marchent tout est bon

On créer une liste de contrôle d'accès standard nommée ACCESS_LAN11 qui n'autorise l'accès au réseau 192.168.11.0/24 qu'aux hôtes du réseau 192.168.22.0/24 ainsi qu'au PC21

On fait en sorte que les listes de contrôle d'accès standards doivent être placées le plus près possible de la destination, soit le réseau 192.168.11.0/24. Il faut donc choisir l'interface G0/0 de R1 en sortie

```
R1(config)#ip access-list standard ACCESS_LAN11
R1(config-std-nacl)#permit 192.168.22.0 0.0.0.255
R1(config-std-nacl)#permit host 192.168.21.1
R1(config-std-nacl)#exit
R1(config)#int g0/0
R1(config-if)#ip access-group ACCESS_LAN11 out
R1(config-if)#exit
```

On test un ping depuis PC21, PC22 et PC12 et on vérifie le nombre de paquets autorisés à l'aide de la commande sh access-lists

ping depuis PC21 :

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=25ms TTL=125
Reply from 192.168.11.1: bytes=32 time=10ms TTL=125
Reply from 192.168.11.1: bytes=32 time=18ms TTL=125
Reply from 192.168.11.1: bytes=32 time=15ms TTL=125

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 25ms, Average = 17ms
```

ping depuis PC22 :

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=9ms TTL=125
Reply from 192.168.11.1: bytes=32 time=7ms TTL=125
Reply from 192.168.11.1: bytes=32 time=8ms TTL=125
Reply from 192.168.11.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 9ms, Average = 7ms
```

ping depuis PC12 :

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

ça ne marche pas et c’est normal car le réseaux 12 n’est pas autorisé a accéder au réseaux 11

On fait donc un sh access-lists

```
R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit host 192.168.21.1 (4 match(es))
```

On voit bien le compteur du nombre de paquets autoriser pour chaque réseaux/hôte

On modifie la liste de contrôle d'accès standard nommée ACCESS_LAN11 afin de permettre à tous le réseau 192.168.21.0/24 (en plus du réseau 192.168.22.0/24) d'accéder au réseau 192.168.11.0/24. De plus, la direction souhaite également pouvoir connaître le nombre de tentatives refusées

On va donc supprimer la commande qui a permit la machine 21.1 d'accéder au réseaux 11 et on va en taper une autre qui cette fois va permettre a tous le réseaux 21 et pas seulement une machine de pouvoir accéder au réseaux 11 et on va aussi taper la commande qui va nous permettre d'avoir le compteur de refus (deny any)

```
R1(config)#ip access-list standard ACCESS_LAN11
R1(config-std-nacl)#no 20 permit host 192.168.21.1
R1(config-std-nacl)#20 permit 192.168.21.0 0.0.0.255
R1(config-std-nacl)#30 deny any
R1(config-std-nacl)#exit


R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit 192.168.21.0 0.0.0.255
    30 deny any
```

On effectue un ping de PC11 depuis PC12 et on vérifie le nombre de paquets refusés à l'aide de la commande sh access-lists

ping depuis PC12 vers PC11 :

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit 192.168.21.0 0.0.0.255
    30 deny any (4 match(es))
```

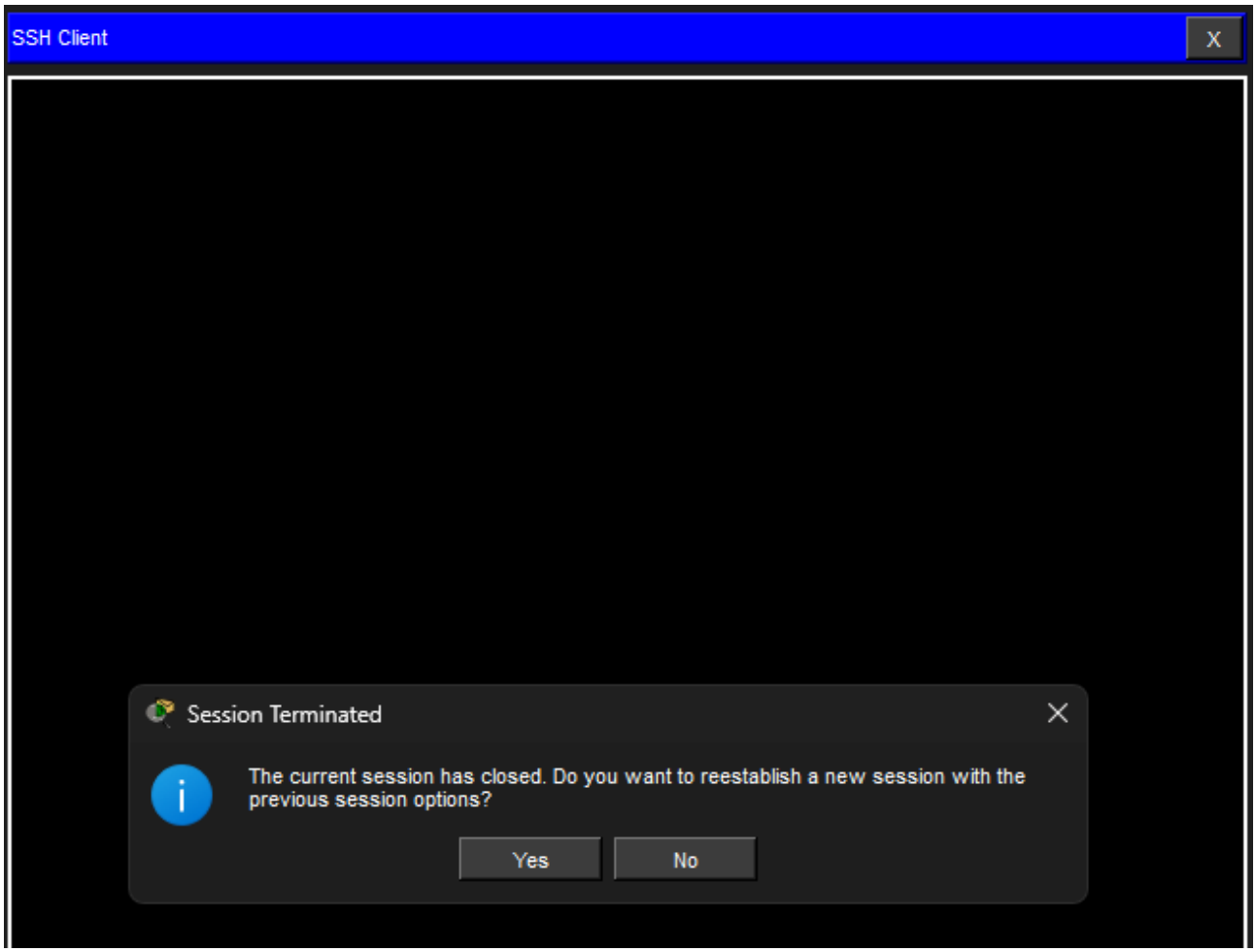
On voit bien le compteur de refus

On créer une liste de contrôle d’accès standard nommée ACCESS_SSH_ADMIN permettant de sécuriser les ports VTY des routeurs en n’autorisant que les accès SSH depuis le réseau 192.168.11.0/24

La liste de contrôle d’accès devra être créée sur tous les routeurs

```
R1(config)#ip access-list standard ACCESS_SSH_ADMIN
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#line vty 0 4
R1(config-line)#access-class ACCESS_SSH_ADMIN in
R1(config-line)#exit
```

Une fois appliqué à tous les routeurs, on va tenter de nous connecter en SSH avec PC12, 21 et 22 vers le routeur R1

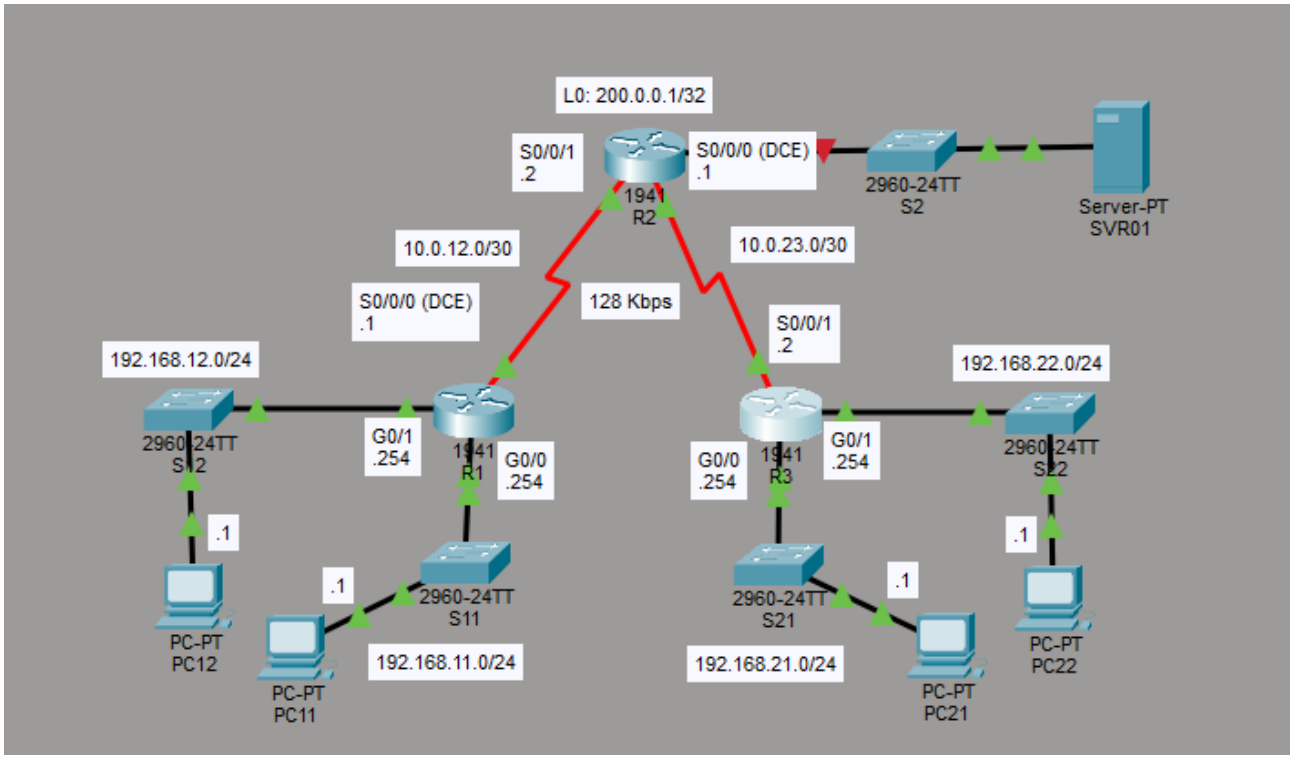


La connexion est refuser

Alors que si on essaye avec le PC11 la connexion est bien accepter

2. ACL IPv4 étendues

On reprend le fichier Cisco Packet Tracert de départ et on ajoute le serveur SRV01



1 Configurez les PC.

2 Configurez le routeur R1 :

a Configurez son nom d’hôte, désactivez la recherche DNS, activez le chiffrement des mots de passe.

b Protégez l’accès enable avec le mot de passe class. Ajoutez l’utilisateur admin avec le mot de passe cisco. Configurez l’accès SSH avec l’utilisateur admin et la synchronisation des logs.

c Configurez les interfaces du routeur (G0/0, G0/1 et S0/0/0).

3 Configurez le routeur R2 de manière analogue ainsi que les interfaces du routeur (G0/0, S0/0/0 et S0/0/1).

4 Configurez le routeur R3 de manière analogue ainsi que les interfaces du routeur (G0/0, G0/1 et S0/0/1).

Tout cela est déjà fait car on avait sauvegarder la configuration

5. Configurez OSPFv2 sur les routeurs R1, R2 et R3. On vérifiee leur table de routage

R1 :

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 10.0.12.0 0.0.0.3 area 0
R1(config-router)#passive-interface g0/0
R1(config-router)#passive-interface g0/1
```

table de routage :

```
R1#sh ip route ospf
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.0.23.0 [110/128] via 10.0.12.2, 00:11:50, Serial0/0/0
O    192.168.21.0 [110/129] via 10.0.12.2, 00:09:35, Serial0/0/0
O    192.168.22.0 [110/129] via 10.0.12.2, 00:09:35, Serial0/0/0
```

R2 :

```
R2(config)#int lo0
R2(config-if)#shut

 R2(config-if)#no ip address 200.0.0.1 255.255.255.0

 R2(config-if)#int G0/0
 R2(config-if)#ip address 200.0.0.1 255.255.255.0
 R2(config-if)#no shutdown

 R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0

 R2(config)#router ospf 1
```

```
R2(config-router)#network 10.0.12.0 0.0.0.3 area 0

R2(config-router)#network 10.0.23.0 0.0.0.3 area 0
R2(config-router)#default-information originate
```

table de routage :

```
R2#sh ip route ospf
O    192.168.11.0 [110/65] via 10.0.12.1, 00:13:10, Serial0/0/1
O    192.168.12.0 [110/65] via 10.0.12.1, 00:13:10, Serial0/0/1
O    192.168.21.0 [110/65] via 10.0.23.2, 00:10:47, Serial0/0/0
O    192.168.22.0 [110/65] via 10.0.23.2, 00:10:47, Serial0/0/0
```

R3 :

```
R3(config)#router ospf 1
*Mar 2 0:9:40.23: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config-router)#network 192.168.21.0 0.0.0.255 area 0
R3(config-router)#network 192.168.22.0 0.0.0.255 area 0
R3(config-router)#network 10.0.23.0 0.0.0.3 area 0
R3(config-router)#passive-interface g0/0

R3(config-router)#passive-interface g0/1
```

On vérifie leur table de routage (ici celle de R3)

```
R3#sh ip route ospf
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.0.12.0 [110/128] via 10.0.23.1, 22:35:19, Serial0/0/1
O    192.168.11.0 [110/129] via 10.0.23.1, 22:35:19, Serial0/0/1
O    192.168.12.0 [110/129] via 10.0.23.1, 22:35:19, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 10.0.23.1, 00:03:42, Serial0/0/1
```

6. On vérifie la connectivité. Tous les PC doivent pouvoir se joindre

Ping de PC11 a tout les autres :

```
C:\>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:

Reply from 192.168.12.1: bytes=32 time<1ms TTL=127
Reply from 192.168.12.1: bytes=32 time<1ms TTL=127
Reply from 192.168.12.1: bytes=32 time<1ms TTL=127
Reply from 192.168.12.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=12ms TTL=125
Reply from 192.168.21.1: bytes=32 time=2ms TTL=125
Reply from 192.168.21.1: bytes=32 time=2ms TTL=125
Reply from 192.168.21.1: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 4ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time=11ms TTL=125
Reply from 192.168.22.1: bytes=32 time=11ms TTL=125
Reply from 192.168.22.1: bytes=32 time=2ms TTL=125
Reply from 192.168.22.1: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 6ms
```

PC11 vers le SRV01 :

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 200.0.0.2: bytes=32 time=1ms TTL=126
Reply from 200.0.0.2: bytes=32 time=16ms TTL=126
Reply from 200.0.0.2: bytes=32 time=6ms TTL=126
Reply from 200.0.0.2: bytes=32 time=6ms TTL=126

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 7ms
```

Après avoir réaliser tout les test tout les PC peuvent bien se ping

7. On créer une liste de contrôle d’accès étendue numérique qui n’autorise, pour les réseaux 192.168.11.0/24 et 192.168.12.0/24, que l’accès aux hôtes du réseau 192.168.21.0/24. La direction souhaite pouvoir connaître le nombre de tentatives refusées

Les listes de contrôle d’accès étendues doivent être placées le plus près possible de la source soit dans notre cas les réseaux 192.168.11.0/24 et 192.168.12.0/24. Deux possibilités s’offrent à nous :

• soit créer deux ACL placées respectivement sur les interfaces G0/0 et G0/1 de R1 en entrée ;

• soit créer une ACL placée sur l’interface S0/0/0 de R1 en sortie.

La première solution est préférable car le trafic non désiré ne transite pas inutilement par le routeur

```
R1(config)#access-list 111 permit ip 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
R1(config)#access-list 111 deny ip any any
R1(config)#access-list 112 permit ip 192.168.12.0 0.0.0.255 192.168.21.0 0.0.0.255
R1(config)#access-list 112 deny ip any any
R1(config)#int g0/0
R1(config-if)#ip access-group 111 in
R1(config-if)#int g0/1
R1(config-if)#ip access-group 112 in
```

Le serveur SRV01 ainsi que le PC22 ne doivent plus être accessibles depuis le PC11 ni depuis le PC12 mais en revanche le PC21 doit toujours être joignable depuis PC11 et PC12

depuis PC11 vers SRV01 :

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

c’est pareil pour le PC12

depuis PC11 vers PC21 :

```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=16ms TTL=125
Reply from 192.168.21.1: bytes=32 time=14ms TTL=125
Reply from 192.168.21.1: bytes=32 time=12ms TTL=125
Reply from 192.168.21.1: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 16ms, Average = 13ms
```

c’est pareil pour le PC12

8. On créer une liste de contrôle d’accès étendue nommée WEB qui n’autorise les hôtes du réseau 192.168.22.0/24 qu’à accéder à Internet en HTTP et HTTPS. Les ping doivent également fonctionner

Les listes de contrôle d’accès étendues doivent être placées le plus près possible de la source soit dans notre cas le réseau 192.168.22.0/24. Il faut donc travailler sur R3. Il est alors possible de créer une ACL placée soit sur l’interface S0/0/1 de R3 en sortie soit sur l’interface G0/1 de R3 en entrée.

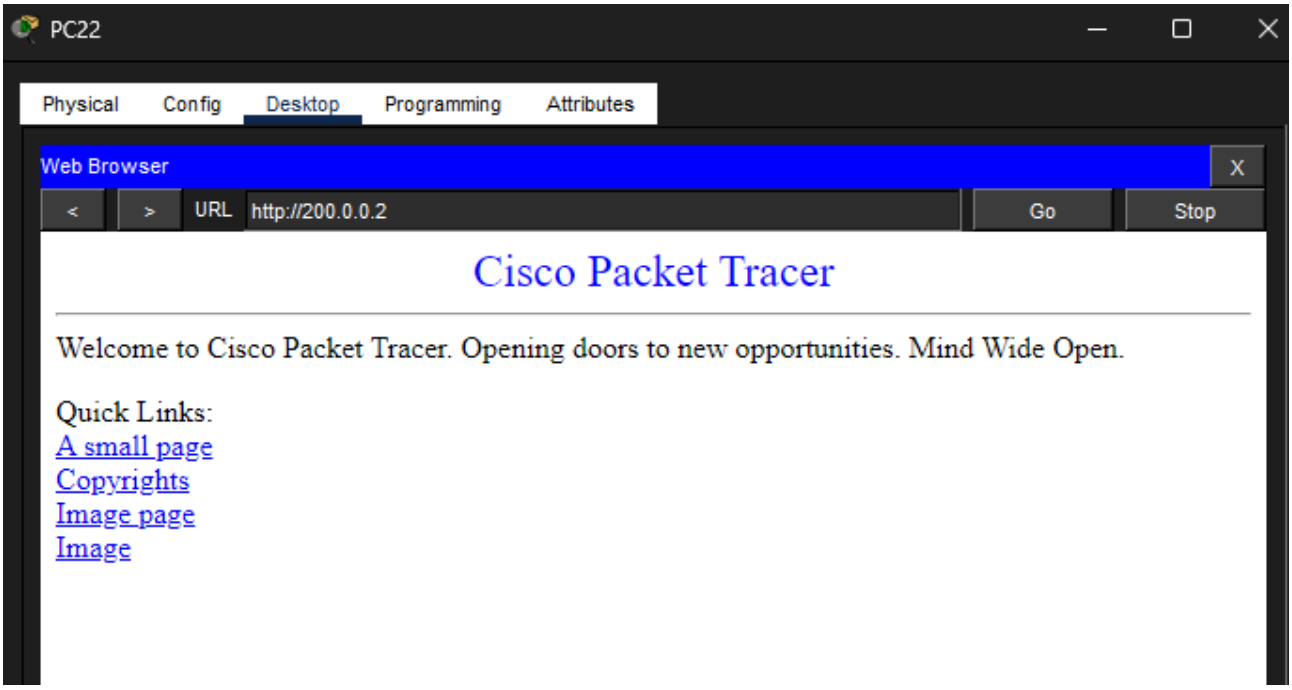
La deuxième solution est préférable car le trafic non désiré ne transite pas inutilement par le routeur. De plus cette solution ne perturbera pas le trafic du réseau 192.168.21.0/24.

```
R3(config)#ip access-list extended WEB
R3(config-ext-nacl)#permit icmp 192.168.22.0 0.0.0.255 any echo
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq www
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq 443
R3(config-ext-nacl)#exit
```

```
R3(config)#int g0/1
R3(config-if)#ip access-group WEB in
R3(config-if)#exit
```

On test l’accès HTTP et ICMP au serveur Web SRV01

Test de PC22 a SRV01 (HTTP) :



Test de PC22 a SRV01 (ICMP) :

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 200.0.0.2: bytes=32 time=9ms TTL=126
Reply from 200.0.0.2: bytes=32 time=6ms TTL=126
Reply from 200.0.0.2: bytes=32 time=6ms TTL=126
Reply from 200.0.0.2: bytes=32 time=6ms TTL=126

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 9ms, Average = 6ms
```

Les pings ont parfaitement réussi

9. On créer une liste de contrôle d'accès nommée WEB_RETOUR qui autorise uniquement le retour du trafic initié depuis l'intérieur du réseau 192.168.22.0/24. Il faut faire attention à ne pas bloquer l'accès au réseau 192.168.21.0/24 depuis les réseaux 192.168.11.0/24 et 192.168.12.0/24

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#permit tcp any 192.168.22.0 0.0.0.255 established
R3(config-ext-nacl)#exit
R3(config)#int g0/1
R3(config-if)#ip access-group WEB_RETOUR out
R3(config-if)#exit
```

Après avoir encodé cette ACL, le retour des ping ne passe plus ! En effet, ICMP n'utilise pas de notion d'établissement (ne relève pas d'une connexion TCP) !

On modifie la liste de contrôle d'accès standard nommée WEB_RETOUR afin de pouvoir connaître le nombre de tentatives refusées et d'autoriser les retours de ping.

On vérifie au préalable les ACE présentes :

```
R3#sh access-lists
Extended IP access list WEB
    10 permit icmp 192.168.22.0 0.0.0.255 any echo
    20 permit tcp 192.168.22.0 0.0.0.255 any eq www
    30 permit tcp 192.168.22.0 0.0.0.255 any eq 443
Extended IP access list WEB_RETOUR
    10 permit tcp any 192.168.22.0 0.0.0.255 established
```

Ainsi que les ACL attachées à une interface

```
R3#sh ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.22.254/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is WEB_RETOUR
  Inbound  access list is WEB
```

La liste d'accès modifiée est la suivante

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#20 deny ip any any
R3(config-ext-nacl)#exit
```

On test maintenant avec une requête ping depuis PC22 et on regarde les compteurs des A

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

La requête ICMP ne passe effectivement pas

```
R3#sh access-lists WEB_RETOUR
Extended IP access list WEB_RETOUR
    permit tcp any 192.168.22.0 0.0.0.255 established
    deny ip any any (3 match(es))
```

Pour permettre le retour des requêtes ICMP, voici la solution

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#15 permit icmp any 192.168.22.0 0.0.0.255 echo-reply
```

On test à nouveau le ping et on regarde les compteurs de l'ACL WEB_RETOUR

```
R3#sh access-lists WEB_RETOUR
Extended IP access list WEB_RETOUR
    permit tcp any 192.168.22.0 0.0.0.255 established
    permit icmp any 192.168.22.0 0.0.0.255 echo-reply (4 match(es))
    deny ip any any (3 match(es))
```

Les retours de ping passent désormais

10. On modifie la liste de contrôle d’accès nommée WEB afin de permettre à tout le réseau 192.168.22.0/24 d’accéder également à Internet en POP3. De plus, la direction souhaite également pouvoir connaître le nombre de tentatives refusées.

```
R3(config)#ip access-list extended WEB
R3(config-ext-nacl)#permit tcp 192?
A.B.C.D
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq pop3
R3(config-ext-nacl)#deny ip any any
```

Comme la demande d’autorisation du protocole POP3 pour le réseau 192.168.22.0/24 n’est en contradiction avec aucune commande précédente de la liste de contrôle d’accès WEB, il suffit d’ajouter la permission en fin d’ACL. Enfin, il convient d’ajouter un refus explicite en fin de liste pour comptabiliser toutes les tentatives refusées