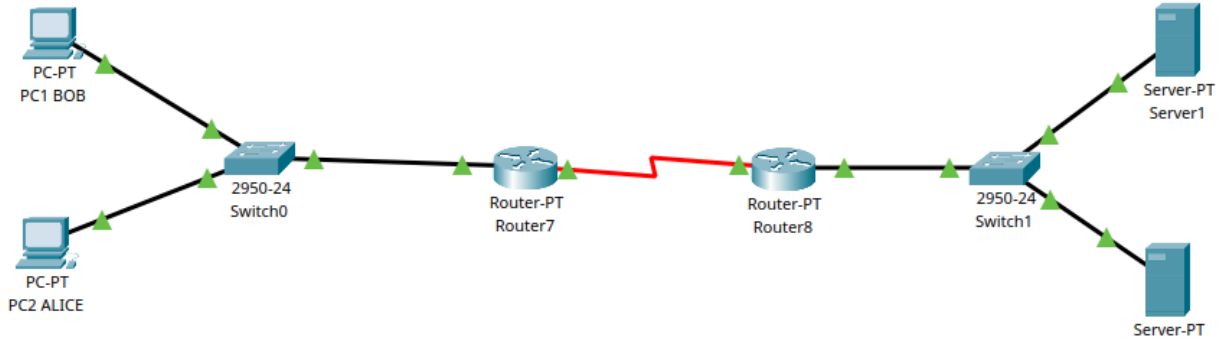


TP1

I. Manipulation : Mise en place du réseau



Le réseau une fois configuré.

Extrait du sh run :

```
interface FastEthernet0/0
ip address 15.0.0.254 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 11.0.0.1 255.0.0.0
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
ip classless
ip route 16.0.0.0 255.0.0.0 11.0.0.2
!
ip flow-export version 9

interface FastEthernet0/0
ip address 16.0.0.254 255.0.0.0
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 11.0.0.2 255.0.0.0
clock rate 2000000
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
ip classless
ip route 15.0.0.0 255.0.0.0 11.0.0.1
!
ip flow-export version 9

C 11.0.0.0/8 is directly connected, Serial2/0
C 15.0.0.0/8 is directly connected, FastEthernet0/0
S 16.0.0.0/8 [1/0] via 11.0.0.2

C 11.0.0.0/8 is directly connected, Serial2/0
S 15.0.0.0/8 [1/0] via 11.0.0.1
C 16.0.0.0/8 is directly connected, FastEthernet0/0
```

Connexion entre le PC1 et le Server1 :

```
C:\>ping 16.0.0.1

Pinging 16.0.0.1 with 32 bytes of data:

Reply from 16.0.0.1: bytes=32 time=12ms TTL=126
Reply from 16.0.0.1: bytes=32 time=1ms TTL=126
Reply from 16.0.0.1: bytes=32 time=1ms TTL=126
Reply from 16.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 16.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 3ms
```

II. Exercice 1 : Mise en place d'un filtrage avec les ACL simples

Créer une ACL simple nommée ACL#1 sur le routeur du site de gauche (coté PCs) avec la commande suivante :

```
Router(config)#ip access-list standard ACL#1
```

Configurer une « description » de votre ACL. Par exemple, « ACL pour interdire à Bob de sortir de son réseau ». Pour trouver comment faire, tapez « ? » après la commande suivante :

Parmi les commandes proposées, quelle est celle permettant de configurer une « description » pour cette ACL ?

C'est la commande remark.

Tapez cette commande et la description suggérée

```
Router(config-std-nacl)#remark Interdire a Bob de sortir de son reseau
```

Vous allez maintenant configurer les règles de cette ACL. Vous allez donc ajouter une règle pour interdire au PC1 de communiquer avec l'extérieur de son réseau. Pour ce faire, vous devez d'abord répondre aux questions suivantes :

Quelle action vous devez choisir entre : permit, deny et remark ?

Je vais utiliser deny pour interdire.

Donnez la syntaxe qui vous permet de désigner l'adresse de la machine de Bob (vous avez deux possibilités) ?

L'adresse est 15.0.0.1

Donnez la commande permettant d'interdire au PC de Bob de communiquer avec l'extérieur. Configurez votre routeur avec cette commande.

```
Router(config-std-nacl)#deny 15.0.0.1 0.0.0.0
```

Associez votre ACL à l'une des interfaces de votre routeur. Pour ce faire, vous devez d'abord répondre à la question suivante :

Sur quelle interface est-il le plus judicieux d'appliquer votre ACL ? Justifiez votre réponse.

C'est FastEthernet/0 car c'est celle ci qui a été configurée en lien avec le switch qui est connecté au réseau de Bob, donc ça permettra de le bloquer.

Appliquez maintenant votre ACL sur l'interface située du côté des PCs et dans le sens convenable en utilisant les commandes suivantes :

```
Router(config)#interface FastEthernet0/0
```

```
Router(config-if)#ip access-group ACL#1 in
```

Vérifiez la configuration de votre routeur. Donnez la commande qui vous a permis de le faire et le résultat de cette commande.

C'est la commande show access-lists

```
Router#show access-lists
Standard IP access list ACL#1
 10 deny host 15.0.0.1
```

Depuis le PC de Bob, faites les tests suivants :

Ping 15.0.0.2. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?

Lors du ping du 15.0.0.2 (Alice) il marche car Bob ne sort pas de son réseau.

```
C:\>ping 15.0.0.2

Pinging 15.0.0.2 with 32 bytes of data:

Reply from 15.0.0.2: bytes=32 time<1ms TTL=128
Reply from 15.0.0.2: bytes=32 time<1ms TTL=128
Reply from 15.0.0.2: bytes=32 time<1ms TTL=128
Reply from 15.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 15.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping 16.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?

Lors du ping du 16.0.0.1 (le Server1) il ne marche pas car Bob sort de son réseau.

```
C:\>ping 16.0.0.1

Pinging 16.0.0.1 with 32 bytes of data:

Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.

Ping statistics for 16.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Passez en mode simulation et vérifiez que vous obtenez le message suivant au niveau de votre routeur :

Je reçois bien ce message qui montre que c'est l'ACL#1 qui bloque la connexion.

PDU Information at Device: Router7

OSI Model Inbound PDU Details

At Device: Router7
Source: PC1 BOB
Destination: 16.0.0.1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3: IP Header Src. IP: 15.0.0.1, Dest. IP: 16.0.0.1 ICMP Message Type: 8	Layer3
Layer 2: Ethernet II Header 00D0.FF86.39A3 >> 0000.0C61.9660	Layer2
Layer 1: Port FastEthernet0/0	Layer1

1. The receiving port has an inbound traffic access-list with an ID of ACL#1. The device checks the packet against the access-list.
2. The packet matches the criteria of the following statement: deny host 15.0.0.1. The packet is denied and dropped.

Challenge Me << Previous Layer Next Layer >>

Depuis le PC d'Alice, faites les tests suivants :

Ping 15.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?

Lors du ping du 15.0.0.1 (Bob) il marche car Alice ne sort pas de son réseau.

```

C:\>ping 15.0.0.1

Pinging 15.0.0.1 with 32 bytes of data:

Reply from 15.0.0.1: bytes=32 time<1ms TTL=128
Reply from 15.0.0.1: bytes=32 time<1ms TTL=128
Reply from 15.0.0.1: bytes=32 time<1ms TTL=128
Reply from 15.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 15.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Ping 16.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?

Lors du ping du 16.0.0.1 (le Server1) il ne marche pas alors qu'Alice est sensée ne pas être concernée par l'ACL#1.

```

C:\>ping 16.0.0.1

Pinging 16.0.0.1 with 32 bytes of data:

Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.

Ping statistics for 16.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Passez en mode simulation et vérifiez que vous obtenez le message suivant au niveau de votre routeur :

J'obtiens bien le message suivant :

PDU Information at Device: Router7
OSI Model
Inbound PDU Details

At Device: Router7
Source: PC2 ALICE
Destination: 16.0.0.1

In Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 15.0.0.2, Dest. IP: 16.0.0.1 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.9777.D0D0 >> 0000.0C61.9660
Layer 1: Port FastEthernet0/0

Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

1. The receiving port has an inbound traffic access-list with an ID of ACL#1. The device checks the packet against the access-list.
2. The packet does not match the criteria of any statement in the access-list. The packet is denied and dropped by default.

Challenge Me
<< Previous Layer
Next Layer >>

Choisissez la règle à ajouter parmi les règles ci-dessous (4 des 5 règles répondent à la demande).

La meilleure règle à utiliser est “**permit 15.0.0.0 0.0.0.255**”.

```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#permit 15.0.0.0 0.0.0.255
```

La dernière règle est l’une de celles permettant de répondre à votre cahier de charges. Pourquoi cette règle répond à vos besoins ? Que se passe-t-il si cette règle était positionnée avant la première règle (celle créée pour interdire à Bob d’accéder à l’extérieur de son réseau) ?

Si cette règle (“**permit 15.0.0.0 0.0.0.255**”) était placée avant le deny, alors Bob ne serait pas bloqué et pourrait sortir de son réseau, parce que les ACL sont lues de manière séquentielle.

En mode simulation, vérifiez que vous obtenez bien le message suivant au niveau du routeur côté PCs :

J’obtiens bien le message suivant :

The screenshot displays the 'PDU Information at Device: Router7' window. It has three tabs: 'OSI Model', 'Inbound PDU Details', and 'Outbound PDU Details'. The 'OSI Model' tab is active, showing a comparison between 'In Layers' and 'Out Layers'. The 'In Layers' section lists Layer 7, Layer 6, Layer 5, Layer 4, Layer 3 (IP Header Src. IP: 15.0.0.2, Dest. IP: 16.0.0.1 ICMP Message Type: 8), Layer 2 (Ethernet II Header 0001.9777.D0D0 >> 0000.0C61.9660), and Layer 1 (Port FastEthernet0/0). The 'Out Layers' section lists Layer 7, Layer 6, Layer 5, Layer 4, Layer 3 (IP Header Src. IP: 15.0.0.2, Dest. IP: 16.0.0.1 ICMP Message Type: 8), Layer 2 (HDLC Frame HDLC), and Layer 1 (Port(s): Serial2/0). Below the layers, a list of five events is shown: 1. The receiving port has an inbound traffic access-list with an ID of ACL#1. The device checks the packet against the access-list. 2. The packet matches the criteria of the following statement: permit 15.0.0.0 0.0.0.255. The packet is permitted. 3. The device looks up the destination IP address in the CEF table. 4. The CEF table does not have an entry for the destination IP address. 5. The device looks up the destination IP address in the routing table. At the bottom, there are buttons for 'Challenge Me', '<< Previous Layer', and 'Next Layer >>'.

Donnez le résultat de cette commande sur votre routeur et expliquez à quoi correspondent les « matches ».

Les “matches” correspondent au nombre de fois où la règle de l’ACL a été déclenchée.

```
Router#show access-lists ACL#1
Standard IP access list ACL#1
  deny host 15.0.0.1 (4 match(es))
  permit 15.0.0.0 0.0.0.255 (4 match(es))
```

Configurez votre ACL sur l'interface de sortie avec les commandes suivantes :

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip access-group ACL#1 in
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip access-group ACL#1 out
```

Faites les tests nécessaires pour prouver le bon fonctionnement de cette nouvelle solution de filtrage.

L'ACL existe toujours.

```
Router#show access-lists
Standard IP access list ACL#1
  10 deny host 15.0.0.1 (4 match(es))
  20 permit 15.0.0.0 0.0.0.255 (4 match(es))
```

Bob arrive à se connecter avec Alice mais pas à contacter le Server1. Donc ça marche toujours.

Alice arrive à se connecter à Bob et au Server1. Donc ça marche toujours.

<pre>C:\>ping 15.0.0.2 Pinging 15.0.0.2 with 32 bytes of data: Reply from 15.0.0.2: bytes=32 time<1ms TTL=128 Reply from 15.0.0.2: bytes=32 time<1ms TTL=128 Reply from 15.0.0.2: bytes=32 time<1ms TTL=128 Reply from 15.0.0.2: bytes=32 time<1ms TTL=128 Ping statistics for 15.0.0.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>ping 16.0.0.1 Pinging 16.0.0.1 with 32 bytes of data: Reply from 15.0.0.254: Destination host unreachable. Reply from 15.0.0.254: Destination host unreachable. Reply from 15.0.0.254: Destination host unreachable. Reply from 15.0.0.254: Destination host unreachable. Ping statistics for 16.0.0.1: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</pre>	<pre>C:\>ping 15.0.0.1 Pinging 15.0.0.1 with 32 bytes of data: Reply from 15.0.0.1: bytes=32 time=16ms TTL=128 Reply from 15.0.0.1: bytes=32 time<1ms TTL=128 Reply from 15.0.0.1: bytes=32 time<1ms TTL=128 Reply from 15.0.0.1: bytes=32 time<1ms TTL=128 Ping statistics for 15.0.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 16ms, Average = 4ms C:\>ping 16.0.0.1 Pinging 16.0.0.1 with 32 bytes of data: Reply from 16.0.0.1: bytes=32 time=14ms TTL=126 Reply from 16.0.0.1: bytes=32 time=1ms TTL=126 Reply from 16.0.0.1: bytes=32 time=17ms TTL=126 Reply from 16.0.0.1: bytes=32 time=6ms TTL=126 Ping statistics for 16.0.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 17ms, Average = 9ms</pre>
--	---

Expliquer les différences entre cette solution de filtrage et la solution configurée précédemment.

Avec l'ACL en entrée, le trafic indésirable est bloqué avant même d'atteindre le routeur, ce qui économise des ressources.

Avec l'ACL en sortie, le trafic arrive sur le routeur mais est bloqué au moment de quitter vers l'extérieur.

III. Exercice 2 : Mise en place d'un filtrage avec les ACL étendues

Pour commencer, supprimez le filtrage de l'exercice précédent avec la commande suivante

```
Router(config)#interface Serial2/0
Router(config-if)#no ip access-group ACL#1 out
```

Ajoutez une ACL étendue nommée ACL#2 sur votre routeur. Cette ACL sera composée de plusieurs règles et positionnée du côté des PCs.

```
Router(config)#ip access-list extended ACL#2
```

Ajoutez à votre ACL une règle pour interdire à tous les PCs du réseau 15.0.0.0/8 d'accéder au service web du Server1. Vous devez spécifier tous les paramètres permettant d'identifier le protocole, les adresses IP sources et destination et les ports sources et destination. Donnez la règle que vous avez ajoutée en expliquant tous ses paramètres.

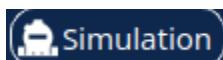
```
Router(config-ext-nacl)#deny tcp 15.0.0.0 0.255.255.255 host 16.0.0.1 eq 80
Router(config-ext-nacl)#deny tcp 15.0.0.0 0.255.255.255 host 16.0.0.1 eq 443
```

On **deny** tous les paquets **tcp** qui viennent du réseau **15.0.0.0** avec le masque **0.255.255.255** vers le **host 16.0.0.1** (Server1) avec les ports **80** (HTTP) et **443** (HTTPS).

Appliquez l'ACL#2 sur l'interface située du côté des PCs en utilisant la commande suivante :

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group ACL#2 in
```

Passez en mode simulation. Appliquez un filtre pour ne visualiser que les paquets TCP.



Utilisez le client http des PC pour solliciter l'URL 16.0.0.1. Vous devriez obtenir le message suivant au niveau de votre routeur :

PDU Information at Device: Router7

OSI Model Inbound PDU Details

At Device: Router7
Source: PC1 BOB
Destination: 16.0.0.1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3: IP Header Src. IP: 15.0.0.1, Dest. IP: 16.0.0.1	Layer3
Layer2: Ethernet II Header 00D0.FF86.39A3 >> 0000.0C61.9660	Layer2
Layer1: Port FastEthernet0/0	Layer1

1. The receiving port has an inbound traffic access-list with an ID of ACL#2. The device checks the packet against the access-list.
2. The packet matches the criteria of the following statement: deny tcp 15.0.0.0 0.255.255.255 host 16.0.0.1 eq www. The packet is denied and dropped.

Challenge Me << Previous Layer Next Layer >>

Que se passe-t-il lorsque vos PCs sollicitent l'URL 16.0.0.2 ?
Il se passe la même chose car ce serveur est aussi bloqué.

PDU Information at Device: Router7

OSI Model Inbound PDU Details

At Device: Router7
Source: PC1 BOB
Destination: 16.0.0.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3: IP Header Src. IP: 15.0.0.1, Dest. IP: 16.0.0.2	Layer3
Layer2: Ethernet II Header 00D0.FF86.39A3 >> 0000.0C61.9660	Layer2
Layer1: Port FastEthernet0/0	Layer1

1. The receiving port has an inbound traffic access-list with an ID of ACL#2. The device checks the packet against the access-list.
2. The packet does not match the criteria of any statement in the access-list. The packet is denied and dropped by default.

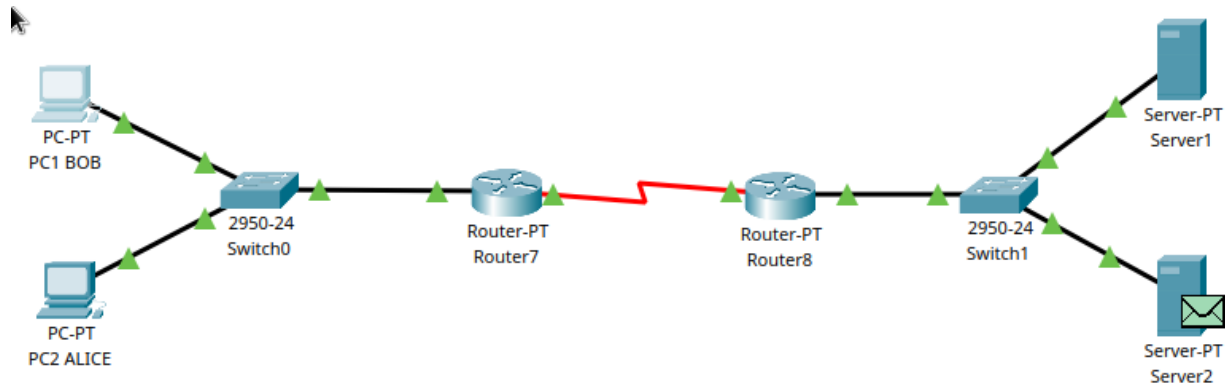
Challenge Me << Previous Layer Next Layer >>

Ajoutez donc une règle pour autoriser l'accès aux autres serveurs. Donnez la règle ajoutée et prouvez le bon fonctionnement de votre solution de filtrage.

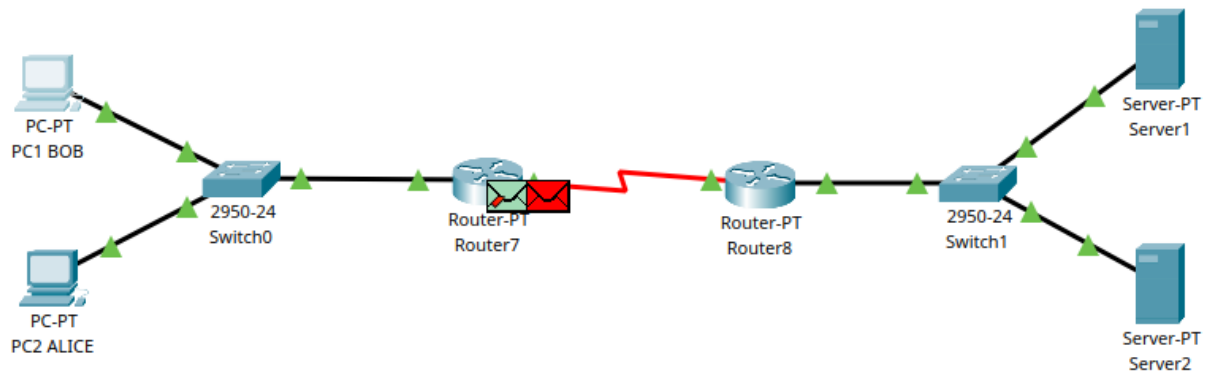
La nouvelle règle pour autoriser l'accès aux autres serveurs est :

```
Router(config-ext-nacl)#permit tcp 15.0.0.0 0.255.255.255 any eq 80
```

Avec http://16.0.0.2 , la connexion s'établit.



Mais avec 16.0.0.1, elle ne fonctionne toujours pas.



Que se passe-t-il si vous « pinguez » les serveurs depuis les PCs ?

Si on ping les serveurs depuis les PCs, la connexion ne s'établit pas :

```
C:\>ping 16.0.0.1

Pinging 16.0.0.1 with 32 bytes of data:

Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.

Ping statistics for 16.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 16.0.0.2

Pinging 16.0.0.2 with 32 bytes of data:

Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.
Reply from 15.0.0.254: Destination host unreachable.

Ping statistics for 16.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Car l'ACL bloque tout ce qui n'est pas autorisé donc elle bloque les ping.

TP2

I. Manipulation : Mise en place du réseau

Configurez les PCs et les Serveurs (adresse IP et passerelle).

PC0 :

IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0
<input checked="" type="radio"/> Static	
Default Gateway	192.168.1.254

PC1 :

IPv4 Address	192.168.3.1
Subnet Mask	255.255.255.0
<input checked="" type="radio"/> Static	
Default Gateway	192.168.3.254

Configurez les interfaces des routeurs

IP Configuration	
IPv4 Address	192.168.1.254
Subnet Mask	255.255.255.0

IP Configuration	
IPv4 Address	192.168.3.254
Subnet Mask	255.255.255.0

Configurez les 2 routeurs avec pour chacun, une route par défaut vers l'autre routeur.

Configurez une route statique par défaut sur votre routeur (Mon Routeur).

Configurez une route statique sur le routeur « Internet » pour qu'il puisse joindre vos réseaux (Local et DMZ).

MonRouteur :

Network Address
192.168.3.0/24 via 10.1.1.2

Routeur1 :

Network Address
192.168.1.0/24 via 10.1.1.1
192.168.2.0/24 via 10.1.1.1

Donnez un extrait pertinent du résultat du sh run sur les deux routeurs

MonRouteur :

```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.2.254 255.255.255.0
duplex auto
speed auto
!
interface Ethernet0/0/0
ip address 10.1.1.1 255.255.255.252
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.3.0 255.255.255.0 10.1.1.2
!
ip flow-export version 9
```

Routeur1 :

```
interface FastEthernet0/0
ip address 192.168.3.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.1.2 255.255.255.252
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.1.1.1
ip route 192.168.2.0 255.255.255.0 10.1.1.1
!
ip flow-export version 9
```

Donnez la table de routage des deux routeurs.

MonRouteur :

```
Gateway of last resort is not set

10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Ethernet0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 [1/0] via 10.1.1.2
```

Routeur1 :

```
Gateway of last resort is not set

10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.1.1
S    192.168.2.0/24 [1/0] via 10.1.1.1
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Testez la connectivité sur chacun des liens. Testez la connectivité de bout en bout : entre les machines et les serveurs.

PC0 -> Serveur JAUNE (192.168.1.1 -> 192.168.3.2) -> Validé

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC0 -> Serveur ROUGE (192.168.1.1 -> 192.168.2.1) -> Validé

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC0 -> Serveur VERT (192.168.1.1 -> 192.168.1.2) -> Validé

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC1 -> Serveur VERT (192.168.3.1 -> 192.168.1.2) -> Validé

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1 -> Serveur ROUGE (192.168.3.1 -> 192.168.2.1) -> Validé

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
Reply from 192.168.2.1: bytes=32 time=31ms TTL=126
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 7ms
```

PC1 -> Serveur JAUNE (192.168.3.1 -> 192.168.3.2) -> Validé

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Donnez le résultat d'un ping entre le PC0 et le PC1.

La connexion entre le PC0 et le PC1 (**192.168.3.1**) marche bien.

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126
Reply from 192.168.3.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

II. Exercice 1 : Mise en place du pare-feu

Configurez une « access list » qui autorise le trafic TCP destiné au serveur HTTP quelle que soit la source de ce trafic. Le serveur WEB doit être joignable par http et HTTPS (http sécurisé).

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 permit tcp any host 192.168.2.1 eq 80
Router(config)#access-list 100 permit tcp any host 192.168.2.1 eq 443

Router(config)#access-list 100 deny ip any 192.168.1.0 0.0.0.255
Router(config)#access-list 100 deny icmp any any
Router(config)#access-list 100 permit ip any any
Router(config)#exit
```

Appliquez cette « access list » au routeur local.

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit

Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
```

Faites les tests suivants :

- vérifiez que le réseau 192.168.1.0/24 n'est plus visible depuis Internet

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.254: Destination host unreachable.
Reply from 192.168.2.254: Destination host unreachable.
Reply from 192.168.2.254: Destination host unreachable.
Reply from 192.168.2.254: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- vérifiez que l'ICMP (Ping) ne traverse pas le Pare-feu

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- vérifiez que le serveur WEB de la DMZ est visible depuis Internet (et aussi depuis le réseau local)

```
C:\>telnet 192.168.2.1 80
Trying 192.168.2.1 ...Open

[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1 443
Trying 192.168.2.1 ...Open
```

- vérifiez que le serveur WEB local n'est pas accessible depuis Internet

```
C:\>telnet 192.168.2.1 80
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.2.1 443
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding
```

Voici un autre élément de votre cahier de charges :

- le pare-feu ne doit pas interdire aux PCs du réseau local d'accéder à Internet (par exemple, le serveur WEB du réseau Jaune)

Faites le test pour vérifier cet accès. Normalement, cela ne doit pas fonctionner.

Expliquer pourquoi. Passez en mode simulation et filtrez sur TCP pour comprendre

```
C:\>telnet 192.168.3.2 443
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.3.2 80
Trying 192.168.2.1 ...
% Connection timed out; remote host not responding
```

Cela ne fonctionne pas car l'acl ne permet pas d'accéder à ce serveur web.

Pour résoudre ce problème et répondre au dernier élément du cahier de charges, autorisez le trafic venant de n'importe quel serveur Web (en HTTP et en HTTPS) à atteindre le réseau 192.168.1.0/24. Donnez la règle ajoutée.

```
Router(config)#access-list 100 permit tcp any 192.168.1.0 0.0.0.255 eq 80
Router(config)#access-list 100 permit tcp any 192.168.1.0 0.0.0.255 eq 443
```

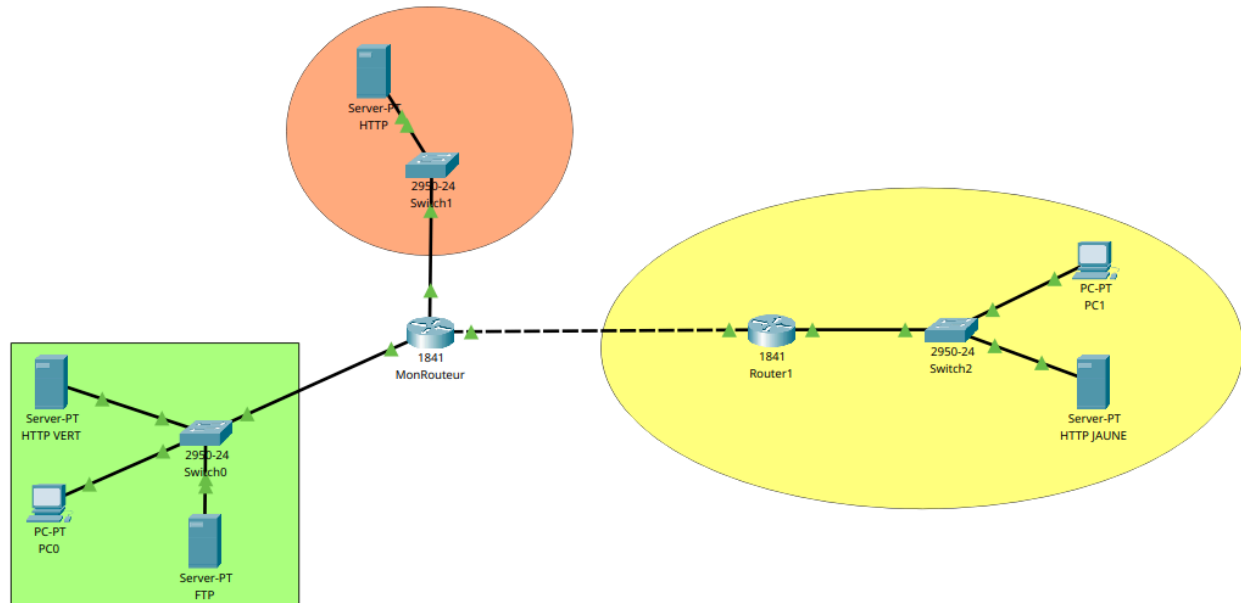
Refaites le test précédent et donnez son résultat.

```
C:\>telnet 192.168.3.2 80
Trying 192.168.3.2 ...Open

[Connection to 192.168.3.2 closed by foreign host]
C:\>telnet 192.168.3.2 443
Trying 192.168.3.2 ...Open
```

III. Exercice 2 : Attaque du réseau local

Configurez un serveur FTP dans le réseau local comme indiqué sur la figure ci-dessous



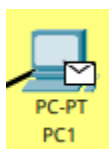
Vous allez maintenant simuler une attaque sur le serveur FTP se trouvant dans le réseau local. Le problème est que votre réseau local est ouvert sur le port 80 et le port 443.

Pour simuler cette attaque :

cliquez sur l'icône « Complexe PDU »



cliquez avec la croix sur le PC du réseau Internet (ce PC sera le PC pirate)



une fenêtre s'ouvre. configurer les paramètres

Create Complex PDU

Source Settings

Source Device: PC1

Outgoing Port: FastEthernet0 ☒ Auto Select Port

PDU Settings

Select Application: FTP

Destination IP Address: 192.168.1.3

Source IP Address: 192.168.3.1

TTL: 32

TOS: 0

Starting Source Port: 443

Destination Port: 21

Size: 1000

Simulation Settings

☒ One Shot Time: 4 Seconds

☐ Periodic Interval: Seconds

Create PDU

Enfin, cliquez sur « Create PDU ». Comme les ports 443 et 80 sont ouverts, tout le monde peut entrer dans le réseau

Successful PC1 192.168.1.3 TCP 4.000 N 1

IV. Exercice 3 : Amélioration du pare-feu (StateFull)

Effacez les règles de l'ACL créée précédemment en utilisant la commande suivante

```
Router(config)#no access-list 100
```

Tapez la commande suivante

```
Router(config)#access-list 100 permit tcp any eq 80 192.168.1.0 0.0.0.255 ?
dscp      Match packets with given dscp value
eq        Match only packets on a given port number
established established
gt        Match only packets with a greater port number
lt        Match only packets with a lower port number
neq       Match only packets not on a given port number
precedence Match packets with given precedence value
range     Match only packets in the range of port numbers
```

Plusieurs propositions sont données. Quelle est la proposition qui répond à notre problème ?

La meilleure proposition est “established” car elle permet d'autoriser uniquement les réponses HTTP et HTTPS des requêtes des PC du réseau local.


Configurez votre pare-feu pour résoudre le problème identifié. Donnez la règle ajoutée et testez votre configuration afin de prouver sa résistance à l'attaque identifiée dans le précédent exercice.

Configuration :

```
Router(config)#access-list 100 permit tcp any eq 80 192.168.1.0 0.0.0.255 established
Router(config)#access-list 100 permit tcp any eq 443 192.168.1.0 0.0.0.255 established

Router(config)#access-list 100 deny ip any 192.168.1.0 0.0.0.255
Router(config)#access-list 100 permit ip any any
```

Test :

	Failed	PC1	192.168.1.3	TCP		4.000	N	1
---	--------	-----	-------------	-----	---	-------	---	---

Grâce à l'ACL l'attaque a pu être arrêtée.

V. Exercice 4 : Amélioration du pare-feu (StateFull - CBAC)

Effacez les règles de l'ACL créée précédemment en utilisant la commande suivante :

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no access-list 100
```

Sur le routeur local, créez une règle d'inspection en utilisant la commande suivante :

```
Router(config)#ip inspect name INSPECT#1 http audit-trail on
```

Activez la règle sur l'interface située du côté de la DMZ :

```
Router(config)#interface FastEthernet0/1
Router(config-if)#ip inspect INSPECT#1 out
```

Sur le PC1, lancez le navigateur Web et accédez à l'URL suivante : http://192.168.2.1



Vérifiez les traces au niveau de la session CLI avec la commande suivante

```
Router#show ip inspect sessions
Established Sessions
Session 358007760 (192.168.3.1:1030)=>(192.168.2.1:80) http SIS_OPENING
```