TP n°8 : Introduction au filtrage par ACL standard et étendue sur un routeur Cisco.

Durée : 2h

Objectif principal

Reconnaître une situation courante où une **ACL Standard** (qui peut filtrer des paquets selon l'IP Source) peut être mise en place, et être capable de mettre en place cette ACL Standard.

Reconnaître une situation courante où une **ACL Étendue** (qui peut filtrer des paquets selon l'IP Source ou Destination et des messages TCP ou UDP selon les numéros de port) peut être mise en place, et être capable de mettre en place cette ACL Étendue.

MÉMOS (Cheat Sheets)

ACL (source packetlife.net)

Compte rendu individuel

Vous devez obligatoirement déposer chacun en fin de séance un compte rendu (CR) illustré de votre groupe au format **TP8.[pdf|odt|docx]** pour ce TP sur Moodle. Vous pouvez compléter ce CR après la séance en déposant un nouveau fichier **TP8v2.[pdf|odt|docx]**.

Vos **CR seront vos uniques documents autorisés en CTP**. Il est donc très important de bien y faire figurer **tous les détails** (commandes précises, notions importantes, manips importantes, ...).

Présentation

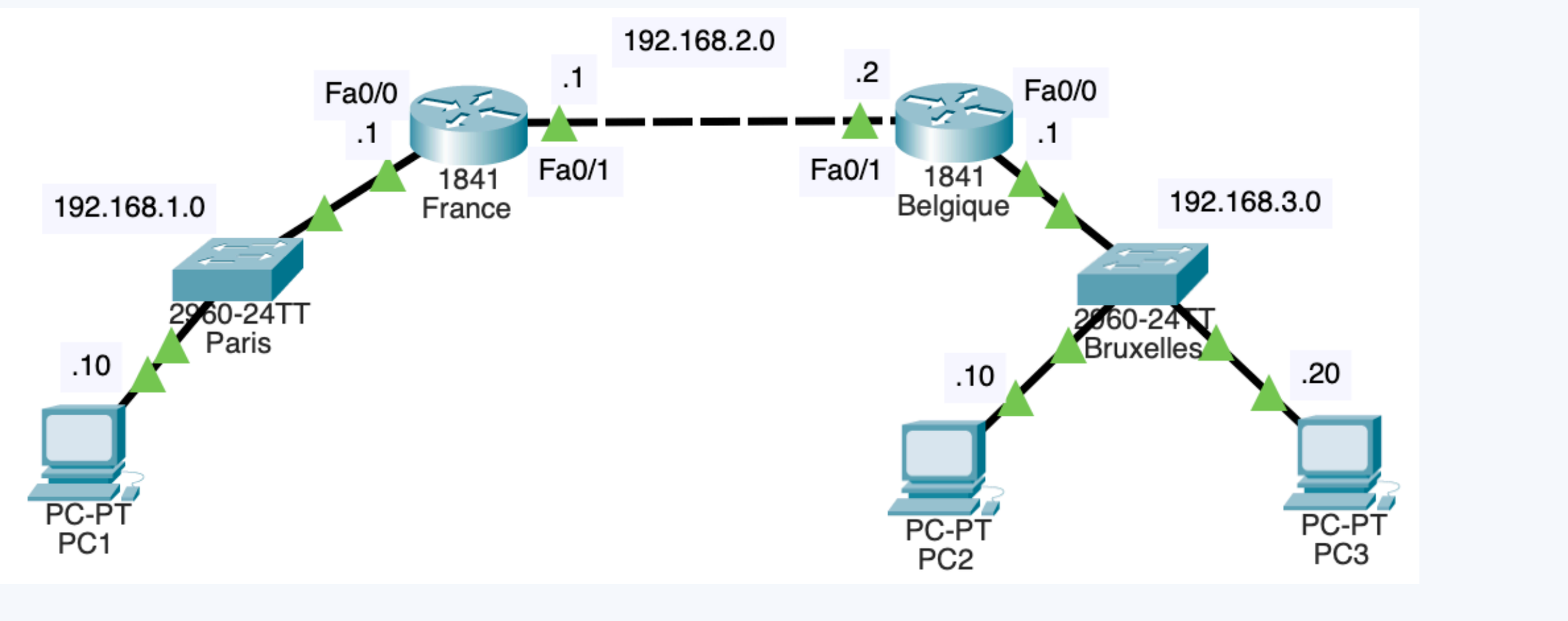
Une liste de contrôle d'accès (ACL) est constituée d'une ou plusieurs entrées de contrôle d'accès (ACE) (ou règles) qui permettent de contrôler le trafic réseau autorisé sur des équipements Cisco.

Une **ACL standard** peut **filtrer des paquets selon l'IP Source** (détails dans la suite du TP).

Une **ACL étendue** peut **filtrer des paquets selon l'IP Source ou Destination et des messages TCP ou UDP selon les numéros de port** (détails dans la suite du TP).

Travail demandé

- Logué-e sous votre session **Linux**, créez sous Packet Tracer le schéma suivant (rappel au cas où : utilisez la commande **packettracer** dans un terminal, loguez vous en tant que guest et patientez - la connexion peut être longue).
- **Configurez les routeurs uniquement en ligne de commandes.**



Au niveau des câbles, les routeurs sont reliés entre eux par un câble croisé (Copper cross-over), les autres sont des câbles droits (Copper straight-through).

Règle : connexion entre mêmes équipements == câble croisé

Règle : connexion entre équipements différents == câble droit

Exception : Entre un PC et un routeur == câble croisé (idem entre Hub et Switch).

De nos jours, les cartes réseau s'adaptent automatiquement.

Aide/rappel configuration du PC1.

Lui donner son adresse IP et sa passerelle par défaut en graphique, puis vérifier en ligne de commande sa configuration.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::203:E4FF:FE87:EC17
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
```

Aide/rappel configuration du routeur France suivant le schéma.

Configuration du nom du routeur

```
Router>en
Router#conf t
Router(config)#hostname France
France(config)#
```

Configuration de l'interface FastEthernet0/0 suivant le schéma.

```
France(config)#int fa0/0
France(config-if)#ip address 192.168.1.1 255.255.255.0
France(config-if)#no shutdown
France(config-if)#
```

Configuration de l'interface FastEthernet0/1 suivant le schéma.

```
France(config-if)#exit
France(config)#int fa0/1
France(config-if)#ip address 192.168.2.1 255.255.255.0
France(config-if)#no shutdown
France(config-if)#
```

Affichage des configurations finales des interfaces pour vérification.

```
France(config-if)#end
France#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        192.168.2.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
France#
```

Trucs et astuces

Vous pouvez appuyer sur tabulation pour compléter le nom d'une commande (complétion automatique)

Vous pouvez utiliser le symbole ? pour avoir de l'aide sur le prochain mot clé utilisable d'une commande

```
France#show ip ?
```

- Vérifiez que les équipements présents dans un même réseau se pinguent.

```
France#ping 192.168.1.10
France#ping 192.168.2.2
Belgique#ping 192.168.2.1
Belgique#ping 192.168.3.10
Belgique#ping 192.168.3.20
```

Lors des précédents TP vous aviez mis en place un routage dynamique RIP ou OSPF, ici nous allons mettre en place un **routage statique**, pour changer et montrer comment c'est possible aussi de le faire sous des routeurs Cisco, comme nous l'avions fait avec des machines sous Linux.

Il suffit d'ajouter ici une route vers le réseau 192.168.3.0 passant par 192.168.2.2 pour le routeur France, et une route vers le réseau 192.168.1.0 passant par 192.168.2.1 pour le routeur Belgique.

- Mettez en place les routes pour que tous les PC se pinguent.

```
France(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

En affichant la table de routage, vous pouvez voir cette route mise en "static"

```
France#sh ip ro
```

- Vérifiez que PC1 pinguent PC2 et PC3.

Vous allez maintenant mettre en place une **ACL Standard** (access control list - liste de contrôle d'accès)

Une **ACL Standard** porte un numéro **entre 1 et 99**. Il peut y avoir plusieurs règles dans une ACL.

Une **ACL Standard** filtre suivant l'**adresse IP source d'un paquet**.

Une **ACL Standard** se place **au plus près de la destination du paquet à filtrer**.

La **mise en place d'un filtrage par ACL** se fait en **deux étapes** :

1. **Créer** l'ACL
2. **Appliquer** l'ACL sur une interface pour le **trafic entrant (inbound)** ou **sortant (outbound)**.

La création d'une règle d'une **ACL Standard** se fait via la commande suivante **en étant placé au niveau de la configuration terminal (après conf t)**.

```
access-list numero-de-la-liste {permit|deny} {host|source source-wildcard|any}
```

source-wildcard est le masque générique (ou masque inversé), dans le cas d'un hôte, il peut être omis.

L'application d'une **ACL Standard** à une interface se fait via la commande suivante **en étant placé au niveau de l'interface à configurer**.

```
ip access-group numero-de-la-liste {in|out}
```

On souhaite par la mise en place d'une ACL standard **couper les communications de PC3 (192.168.3.20) vers PC1 (192.168.1.10)** (par exemple un ping), uniquement de PC3 vers PC1, par exemple PC2 pourra toujours pinguer PC1.

Les étapes de la mise en place de cette ACL sont résumées ci-après.

- Étape 1 : Création de la liste sur le routeur le plus proche de la destination (France ici)
  - Interdire les paquets dont 192.168.3.20 est la source : `access-list 1 deny host 192.168.3.20`
  - Autoriser les autres paquets : `access-list 1 permit any`

Sans cette règle, les paquets ne passent pas par défaut : la dernière règle non écrite d'une ACL est "deny any" (filtrage/suppression du paquet).

- Étape 2 : Affectation de la liste au plus près de la destination
  - La destination est ici PC1 (192.168.1.10). L'ACL sera alors mise **sur le routeur France sur son interface Fa0/0 vers le réseau 192.168.1.0 en sortie (outbound)** car c'est l'interface d'un routeur la plus proche de la destination PC1 (trajet PC3 vers PC1).
  - La commande à utiliser sur cet interface sera alors : `ip access-group 1 out`
- Configurez l'ACL sur le routeur France coupant les communications de PC3 (192.168.3.20) vers PC1 (192.168.1.10).

Création de l'ACL Standard 1 et application de cette dernière à l'interface fa0/0

```
France(config)#access-list 1 deny host 192.168.3.20
France(config)#access-list 1 permit any
France(config)#int fa0/0
France(config-if)#ip access-group 1 out
```

Vous pouvez alors voir vos ACL grâce à la commande

```
France#show access-lists
```

ou en raccourci

```
France#sh ac
```

Vous pouvez aussi voir dans la running config l'ACL et son application à une interface.

```
France#sh run
!
[...]
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
[...]
!
access-list 1 deny host 192.168.3.20
access-list 1 permit any
!
[...]
```

- Quels PC peuvent maintenant se pinguer ?
- Quel message avez-vous quand vous pinguez PC1 depuis PC3 ? Pourquoi ?
- Quel message avez-vous quand vous pinguez PC3 depuis PC1 ? Pourquoi ?

On souhaite maintenant modifier cette ACL standard 1 pour interdire cette fois à **tout le réseau 192.168.3.0** de communiquer avec PC1 (192.168.1.10).

Cela veut dire qu'on voudrait modifier la règle `access-list 1 deny host 192.168.3.20` en `access-list 1 deny 192.168.3.0 0.0.0.255`

Pour ce faire vous pouvez modifier chaque règle d'une ACL en utilisant son numéro que vous pouvez voir en l'affichant :

```
France#show access-lists
Standard IP access list 1
    10 deny host 192.168.3.20
    20 permit any
```

Dans notre cas, nous souhaitons donc modifier la règle 10.

Accédez alors aux règles de l'ACL standard 1 ainsi

```
France(config)#ip access-list standard 1
```

Puis, supprimez la règle 10 :

```
France(config-std-nacl)#no 10
```

Pour la mettre à jour comme ceci :

```
France(config-std-nacl)#10 deny 192.168.3.0 0.0.0.255
```

Affichez alors les ACL pour voir si la modification a bien été effectuée

```
France#show access-lists
Standard IP access list 1
    10 deny 192.168.3.0 0.0.0.255
    20 permit any
```

Vérifiez que maintenant ni PC2 ni PC3 ne peuvent pinguer PC1.

Remarque, nous aurions pu supprimer l'ACL 1 pour la recréer :

```
France(config)#no access-list 1
```

Si vous vouliez ne plus l'utiliser, il faudrait aussi ne plus l'appliquer à l'interface où elle était appliquée.

```
France(config-if)#no ip access-group 1 out
```

La suppression d'une ACL n'entraine pas la suppression de son application à une interface, et s'il reste une ACL vide appliquée à une interface, comme par défaut la dernière règle non écrite d'une ACL est de tout filtrer ("deny any"), alors tout le trafic sera coupé sur cette interface.

On va maintenant mettre en place une **ACL Étendue** pouvant filtrer des paquets plus finement qu'une ACL Standard.

Une **ACL Étendue** porte un numéro **entre 100 et 199**. Idem, il peut y avoir plusieurs règles dans une ACL.

Une **ACL Étendue** peut filtrer suivant l'**adresse IP source** ou **destination** d'un paquet, et également suivant les **numéros de ports**.

Une **ACL Étendue** se place **au plus près de la source du paquet à filtrer** (rappel, pour les ACL standards c'était au plus près de la destination).

Une **ACL Étendue** finit comme une ACL standard par une règle implicite non écrite deny any (politique par défaut à rejet).

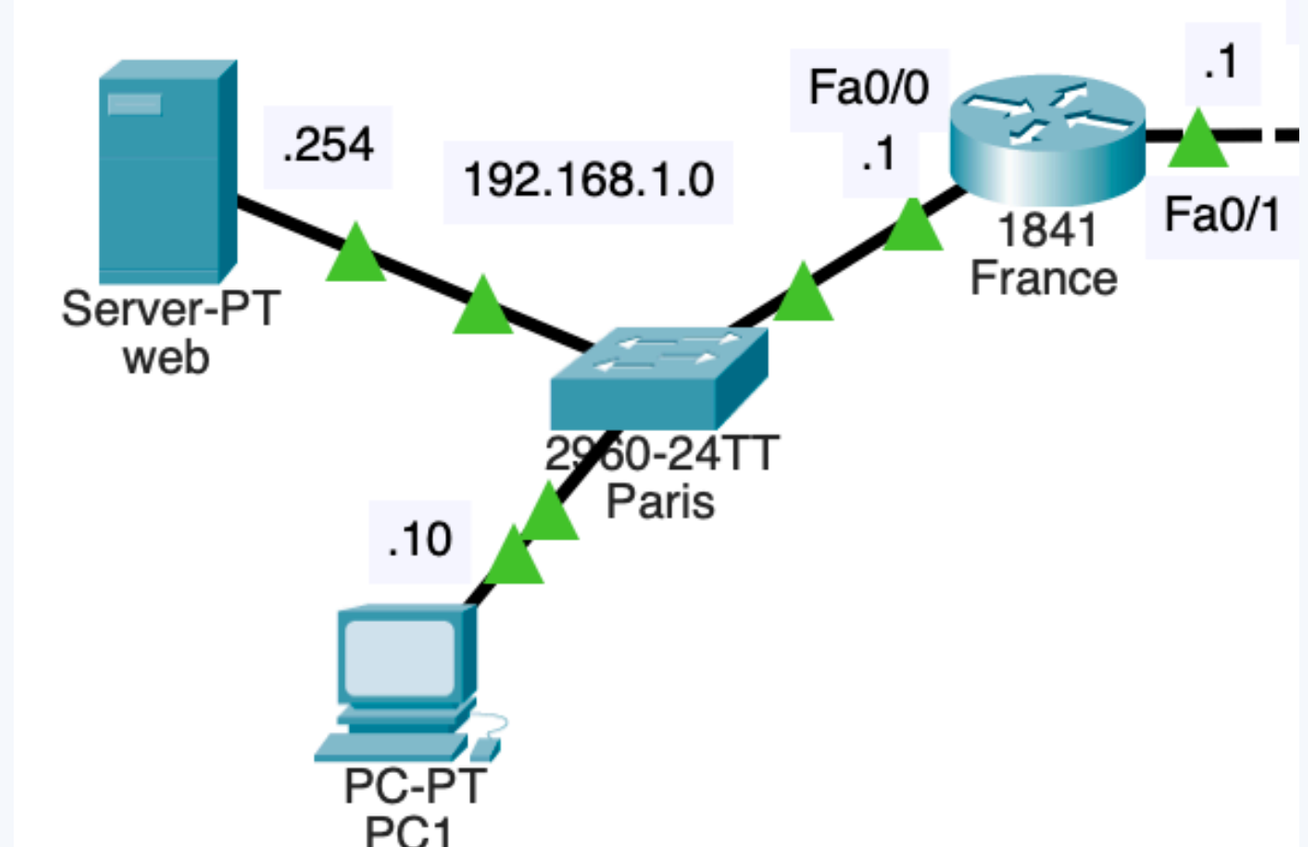
La création d'une règle d'une **ACL Étendue** se fait via la même commande **access-list** avec différentes options en fonction du protocole filtré (Pour plus détails voir la documentation Cisco par exemple).

```
access-list numero-de-la-liste {deny|permit} protocole source source-wildcard destination destination-wildcard
[plus d'autres options dépendantes du protocole]
```

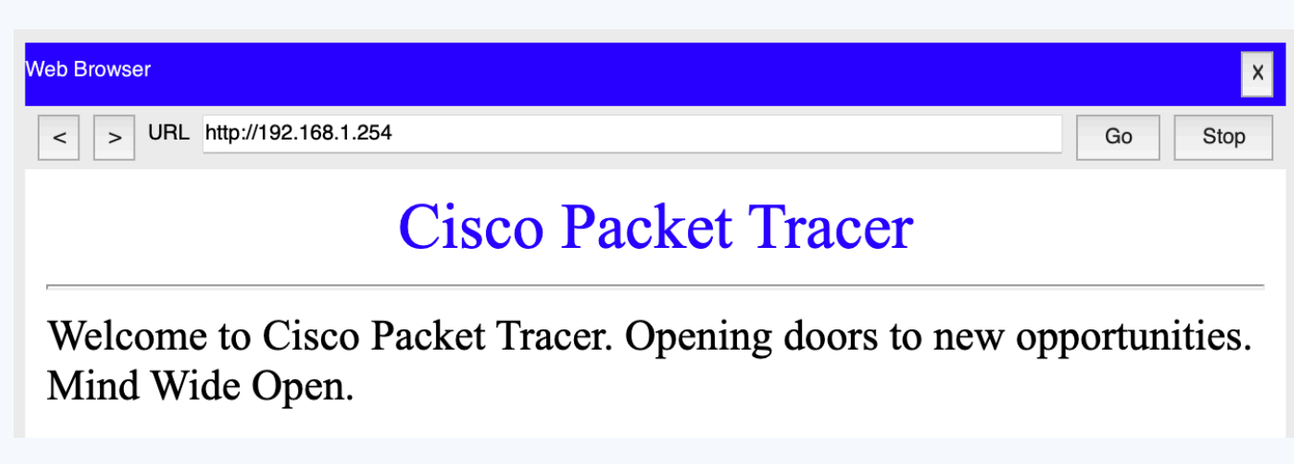
De même, l'application d'une **ACL Étendue** à une interface se fait avec la commande suivante :

```
ip access-group numero-de-la-liste {in|out}
```

- Commencez par enlever l'ACL standard créée précédemment.
- Vérifiez que PC3 et PC2 pingent PC1.
- Ajoutez maintenant un serveur Web d'adresse IP 192.168.1.254 dans le réseau 192.168.1.0.



- Vérifiez que vous pouvez consulter le site depuis PC2 et PC3.
  - **PC2 | Desktop | Web Browser**



- Faites en sorte maintenant que PC2 et PC3 :
  - puissent accéder au site web (service web port tcp 80) sur 192.168.1.254
  - puissent pinguer 192.168.1.254
  - ne puissent pas pinguer les autres machines.

On peut prendre par exemple le numéro 100.

L'ACL doit se placer au plus près du filtrage donc sur le trafic entrant (inbound) de l'interface fa0/1 192.168.3.1

```
Belgique(config)#int fa0/0
Belgique(config-if)#ip access-group 100 in
```

Création de l'ACL étendue

- Permettre le trafic tcp vers le port 80 de 192.168.3.0 vers 192.168.1.254

```
access-list 100 permit tcp 192.168.3.0 0.0.0.255 host 192.168.1.254 eq 80
```

- Permettre les pings de 192.168.3.0 vers 192.168.1.254

```
access-list 100 permit icmp 192.168.3.0 0.0.0.255 host 192.168.1.254 echo
```

- Le reste est par défaut interdit.

- Depuis PC2 et PC3, vérifiez que vous pouvez accédez au site web et pinguez le serveur web, mais que vous ne pouvez pas pinguez PC1.
- Vérifiez le cheminement des paquets en mode simulation.

S'il vous restait du temps, voyez avec l'enseignant pour mettre en place en réel ce shéma en groupes.

N'oubliez pas de déposer votre compte rendu.

SYNTHÈSE

À l'issue de ce TP :

- Vous êtes capable de reconnaître une situation courante où une **ACL Standard** (qui peut filtrer des paquets selon l'IP Source) peut être mise en place, et êtes capable de mettre en place cette ACL Standard.
  - Les **ACL standards** se placent au plus près possible de la **destination** du trafic à filtrer, car elles ne peuvent pas spécifier cette destination. Si une ACL standard était placée à la source du trafic, elle influerait sur toutes les destinations du trafic : soit que des `deny` soit que des `permit`.
- Vous êtes capable de reconnaître une situation courante où une **ACL Étendue** (qui peut filtrer des paquets selon l'IP Source ou Destination et des messages TCP ou UDP selon les numéros de port) peut être mise en place, et êtes capable de mettre en place cette ACL Étendue.
  - Les **ACL étendues** se placent au plus près possible de la **source** du trafic à filtrer. De cette façon, le trafic indésirable est refusé à proximité du réseau source sans traverser l'infrastructure du réseau.

(Les commandes font également l'objet de questions aux DS et évaluations écrites)