Date : 13/11/23

Intervenant : Cédric Surquin.

Cisco

Lab 3-3 / Travail Pratique

Filtrer le trafic avec les ACLs (Access Control List)

Date : 13/11/23 Intervenant : Cédric Surquin.

Objectifs

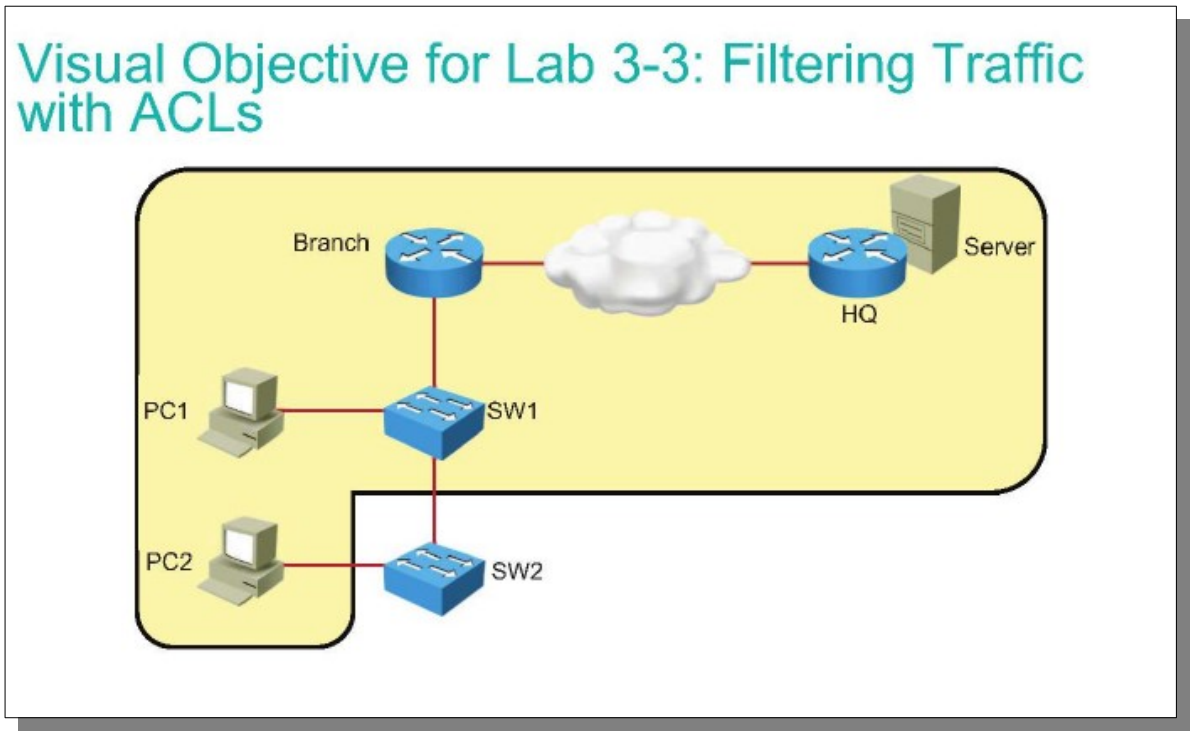
Un mécanisme commun, simple et assez basique afin de filtrer le trafic est le mécanisme dit «d'ACL », qui nous permet d'autoriser, limiter, ou restreindre l'accès à un réseau ou une ressource présente sur ce réseau.

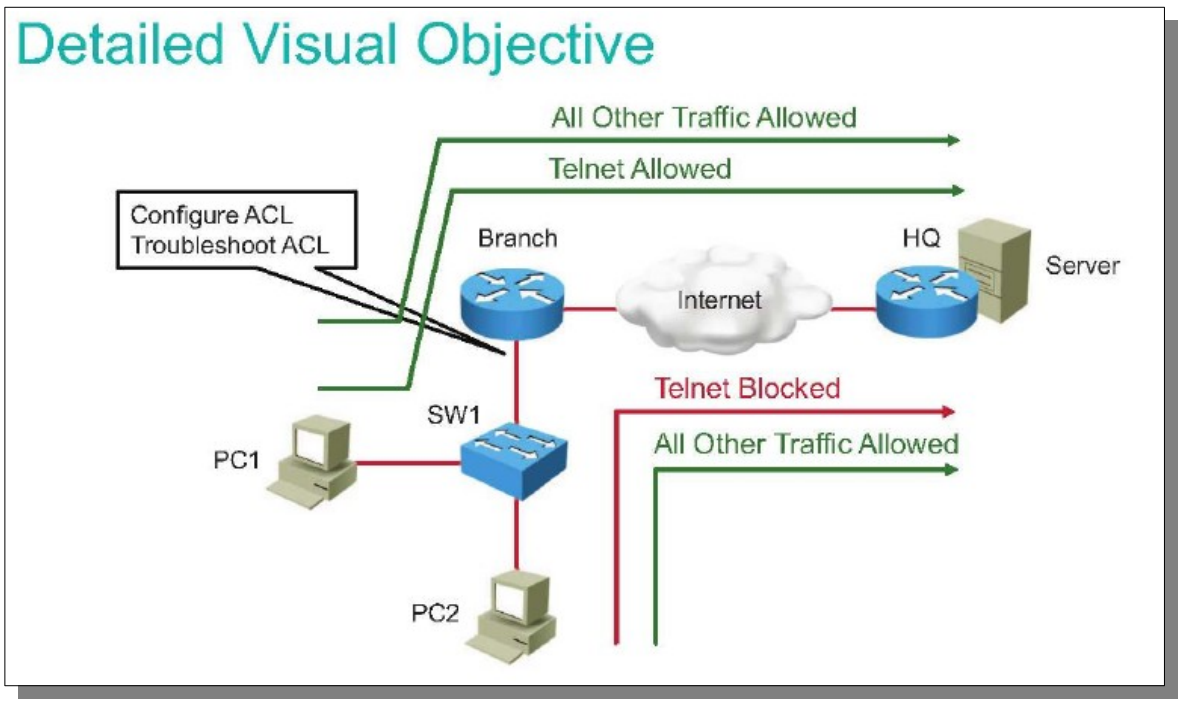
Vous aurez terminé cette activité lorsque vous aurez atteint les objectifs suivants :

1. Configurer des ACLs étendues, des ACLs nommées
2. Dépanner un problème de configuration ACL

Date : 13/11/23 Intervenant : Cédric Surquin.

Visualisation des objectifs :





Date : 13/11/23 Intervenant : Cédric Surquin.

Ressources Requises :

Ci-joint les ressources requises pour ce TP

Liste de commandes :

Le tableau décrit les commandes utilisées dans cette activité et sont classées alphabétiquement afin que vous puissiez facilement localiser les informations dont vous avez besoin. Reportez-vous à cette liste si vous avez besoin d'aide lors de la configuration et la poursuite de cette activité.

Commandes	Descriptions
configure terminal	Activates the configuration mode from the terminal
interface *interface*	Entrer dans l'interface mentionnée pour effectuer sa configuration propre.
ip access-group *ACL_name* **{in|out}**	Active et applique une ACL à une interface précise
ip access-list extended *ACL_name*	Définis une ACL et entre en mode de configuration de celle-ci.
{**permit** | **deny**} {test conditions}	Définis la politique à appliquer pour une ACL précise.
show access-lists *ACL_name*	Affiche le contenu de toutes les ACLs
show ip interface *interface-type interface number*	Affiche des informations IP spécifiques à propos d'une interface précise, y compris les ACLs appliquées à cette interface !

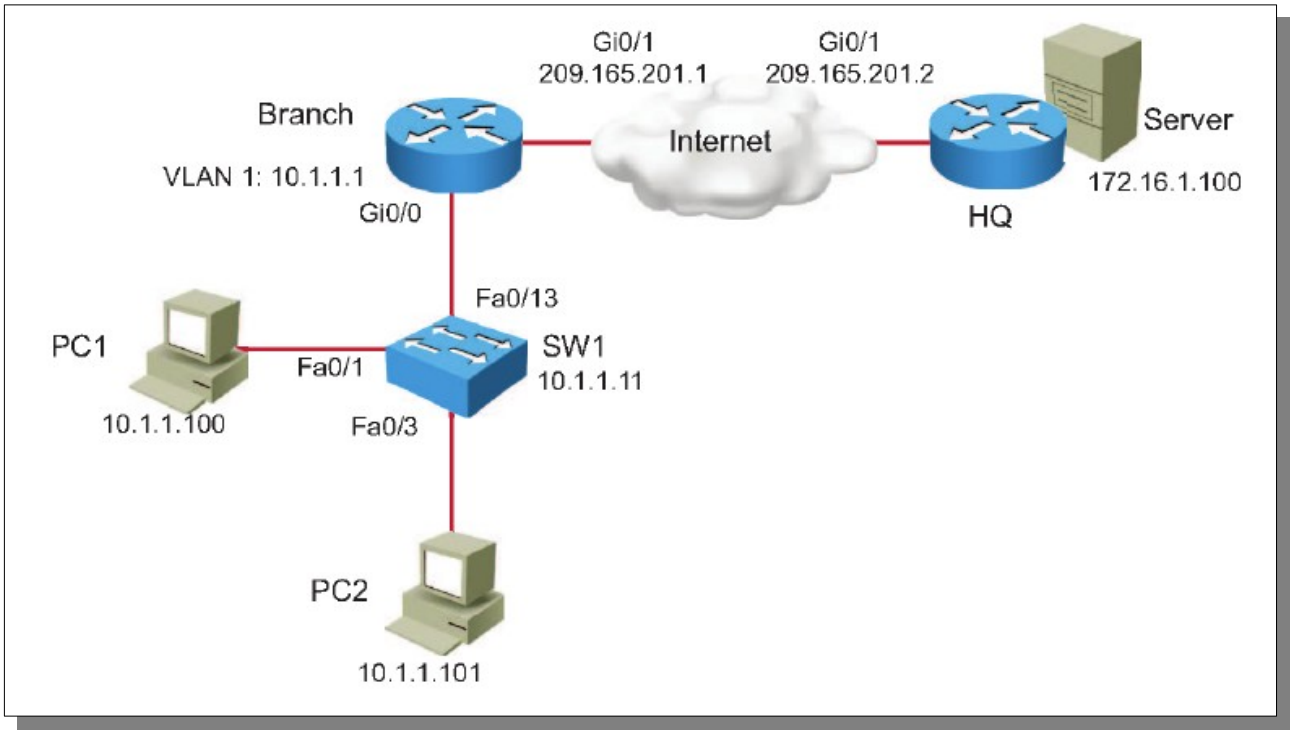
Aide à la mise en place :

Appareil	Périphériques
Branch	Cisco 2901 ISR
Headquarters	Cisco 2901 ISR
SW1	Catalyst 2960 Series Switch
PC1	N'importe quel PC
PC2	N'importe quel PC

Date : 13/11/23 Intervenant : Cédric Surquin.

Topologie et Adressage IP

Les appareils sont connectés par le biais de leurs interfaces Ethernet. La capture ci-dessous illustre la topologie, les noms et les types d'interfaces, ainsi que les adresses IP qui sont utilisées dans ce lab.



Appareils	Interfaces	Adresses IP
Branch	Gi0/1	209.165.201.1/27
Branch	Gi0/0	10.1.1.1/24
HeadQuarters	Gi0/1	209.165.201.2/27
HeadQuarters	Loopback0	172.16.1.100/24
SW1	VLAN 1	10.1.1.11/24
PC1	Connection réseau local par interface Ethernet	10.1.1.100/24
PC2	Connection réseau local par interface Ethernet	10.1.1.101/24

Tâche 1 : Configurer une ACL

Les ACLs vous permettent de filtrer l'accès au réseau au niveau 3 de la couche OSI, en se basant sur l'entête des paquets IP. Dans cette tâche, vous allez configurer une ACL qui empêche une connectivité en Telnet depuis le PC2 vers le serveur. Tout autre trafic IP sera autorisé.

Étape 1 :

Accédez au routeur Branch via sa ligne de commande / connexion console.

Étape 2 :

Configurez une ACL étendue nommée « Telnet » qui va empêcher la connexion depuis le PC2 vers le serveur utilisant le protocole Telnet. Tout autre trafic IP sera autorisé.

Étape 3 :

Vérifiez le contenu de l'ACL :

```
Branch#show access-lists Telnet
Extended IP access list Telnet
    10 deny tcp host 10.1.1.101 host 172.16.1.100 eq telnet
    20 permit ip any any
```

Étape 4 :

Appliquez cet ACL et sa configuration à l'interface GigabitEthernet0/0, dans la bonne direction.

Étape 5 :

Vérifiez que la configuration a bien été appliquée à la bonne interface et dans le bon sens.

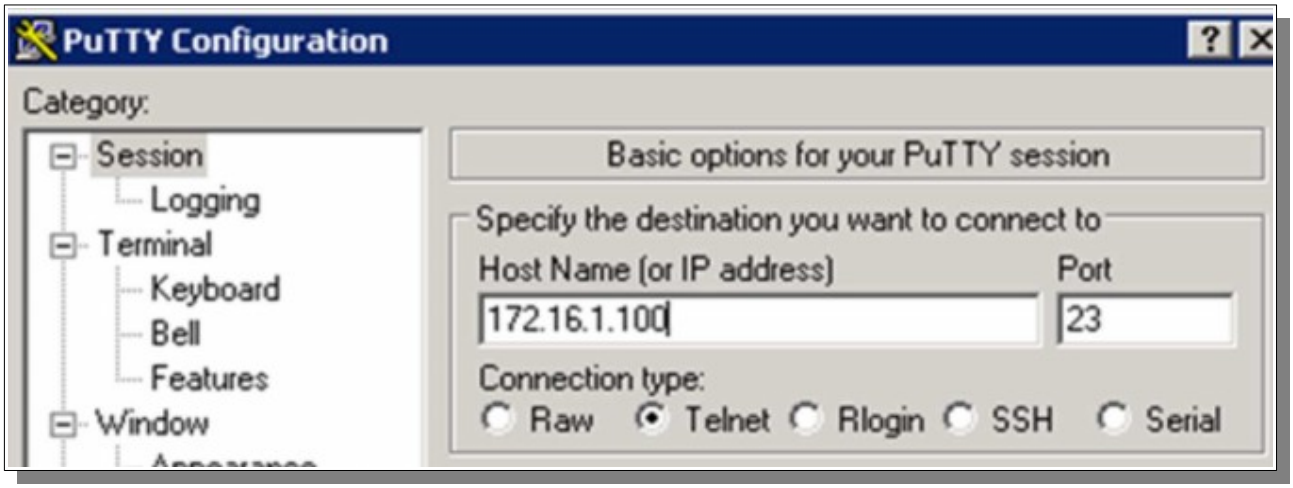
```
Branch#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is Telnet
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  <...output omitted...>
```

Étape 6 :

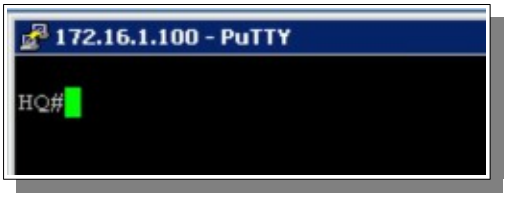
Sauvegardez la configuration courante vers la configuration à appliquer au démarrage.

Étape 7 :

Accédez au PC1, depuis son client Telnet, tentez d'établir une connexion Telnet jusqu'au serveur se trouvant à 172.16.1.100



La connexion doit être fonctionnelle, à ce stade :



Étape 8 :

Vérifiez que le compteur de « concordance de règles » à bien été incrémenté suite à notre connexion en Telnet.

```
Branch#show access-lists Telnet
Extended IP access list Telnet
    10 deny tcp host 10.1.1.101 host 172.16.1.100 eq telnet
    20 permit ip any any (10 matches)
```

Ici, on a eu 10 correspondances d'entête de paquet avec l'ACL, ayant été autorisé à passer l'interface/l'appareil.

Étape 9 :

Accédez à PC2, depuis son client Telnet, tentez une connexion à ce même serveur via le protocole Telnet, comme à l'étape 7.

Si votre ACL a été correctement définie et appliquée, sur la bonne interface et dans le bon sens, la connexion ne doit pas se faire et vous devriez rester sur un invité de commande vide comme sur la capture ci-dessous et/ou équivalent :

Étape 10 :

Vérifiez que le compteur de correspondance a encore subis une incrémentation, mais cette fois à la règle interdisant le Telnet depuis cette machine précise.

```
Branch#show access-lists Telnet
Extended IP access list Telnet
    10 deny tcp host 10.1.1.101 host 172.16.1.100 eq telnet (9 matches)
    20 permit ip any any (10 matches)
```

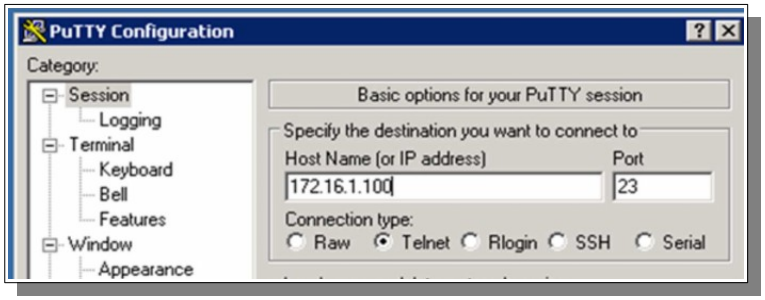
Date : 13/11/23 Intervenant : Cédric Surquin.

Tâche 2 : Dépannez une ACL

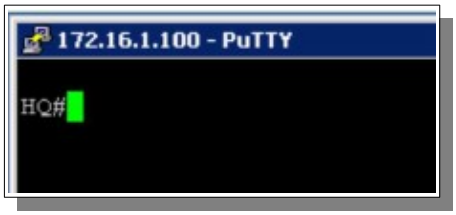
Il est primordial d'être capable d'analyser le comportement d'une ACL configurée par un tiers et de savoir les dépanner. Dans cette tâche, vous allez dépanner une ACL problématique. Vous devrez rectifier les ACLs de façon à ce que la connexion Telnet depuis PC2 vers le serveur ne soit admise, tout en autorisant toute autre forme de trafic vers le serveur.

Étape 1 :

Depuis le PC2, vérifiez que malgré notre volonté de base (interdire le Telnet depuis ce PC vers le serveur), la connexion Telnet vers le serveur soit belle et bien possible



Vous êtes censé voir le prompt du routeur HQ, comme sur la capture ci-contre.



Étape 2 :

Accédez au routeur Branch.

Étape 3 :

Vérifiez l'ACL, notamment qu'elle soit appliquée à l'interface GigabitEthernet0/0, et dans la bonne direction.

```
Branch#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.1.1.1/24
  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 Telnet
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  <...output omitted...>
```

Étape 4 :

Appliquez l'ACL de l'interface GigabitEthenet0/0 à la bonne direction.

Étape 5 :

Vérifiez le contenu de l'ACL

```
Branch#show access-lists Telnet
Extended IP access list Telnet
    10 permit ip any any (338 matches)
    20 deny ip any any
    30 deny tcp host 10.1.1.101 host 172.16.1.100 eq telnet
```

Étape 6 :

Changez l'ACL pour qu'elle empêche les connexions depuis PC2 vers le serveur. Tout autre trafic IP doit être autorisé.

Étape 7 :

Sauvegardez la configuration courante vers la configuration à appliquer au démarrage.

Étape 8 :

Tentez à nouveau une connexion Telnet depuis PC2. Si votre ACL est correcte, alors la connexion ne devrait pouvoir se faire.