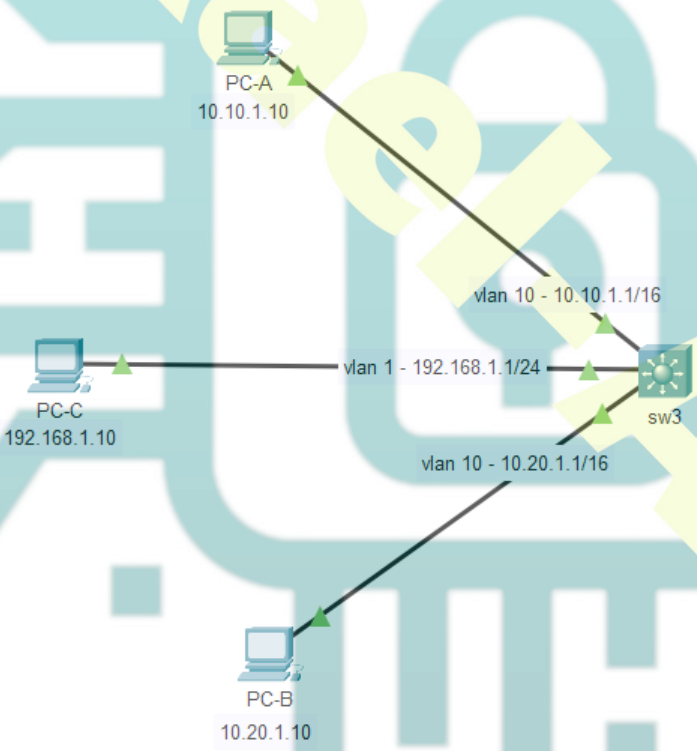
TD – Comprendre les ACL

Etape 1 – Les ACL sur un switch de niveau 3

Le choix du IN et du OUT sur une interface de vlan

Le commutateur fait son rôle de routage entre les 3 vlan (1, 10 et 20) car il n'y a pas d'ACL.



A partir du PC-A (10.10.1.10) vers le PC-B et le PC-C

C:\>ping 10.20.1.10

Reply from 10.20.1.10: bytes=32 time=1ms TTL=127

C:\>ping 192.168.1.10

Reply from 192.168.1.10: bytes=32 time=1ms TTL=127

Nous allons maintenant créer 1 ACL étendue, nommée ACL NOV20-10.

L'ACL NOV20-10 doit empêcher le vlan 20 de communiquer avec le vlan 10 mais doit permettre la communication vers les autres réseaux.

```
ip access-list extended NOV20-10
Deny ip 10.20.0.0 0.0.255.255 10.10.0.0 0.0.255.255
Permit ip 10.20.0.0 0.0.255.255 any
```

A – Nous allons tester l'ACL NOV20-10 sur l'interface de vlan 20 en IN

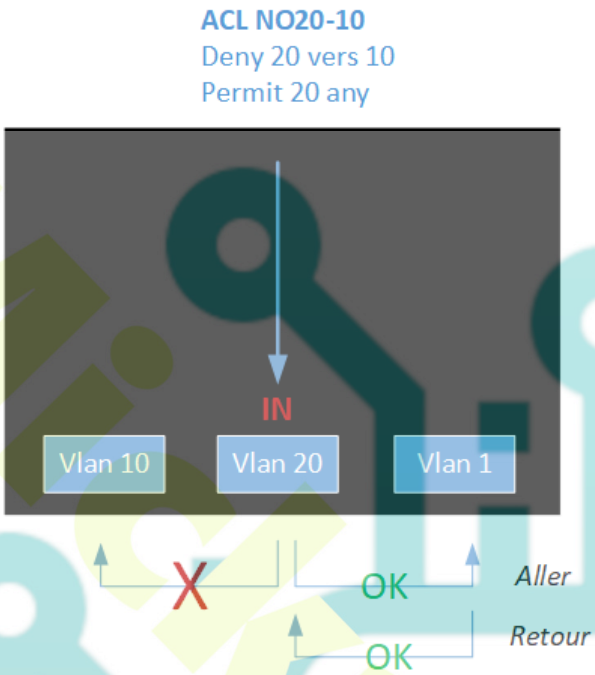
```
int vlan 20
ip access-group NOV20-10 in
```

Test du filtrage

```
A partir du PC-B
Pinging 10.10.1.10
Reply from 10.20.1.1: Destination host unreachable.

Pinging 192.168.1.10
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127
```

Cela fonctionne parfaitement, mais pourquoi ?

Dans notre cas, la règle est interprétée dès l'arrivée sur le port depuis l'intérieur. On lit la règle le réseau 20 ne peut pas communiquer avec le réseau 10 (interdiction) mais peut communiquer avec les autres réseaux (autorisé)



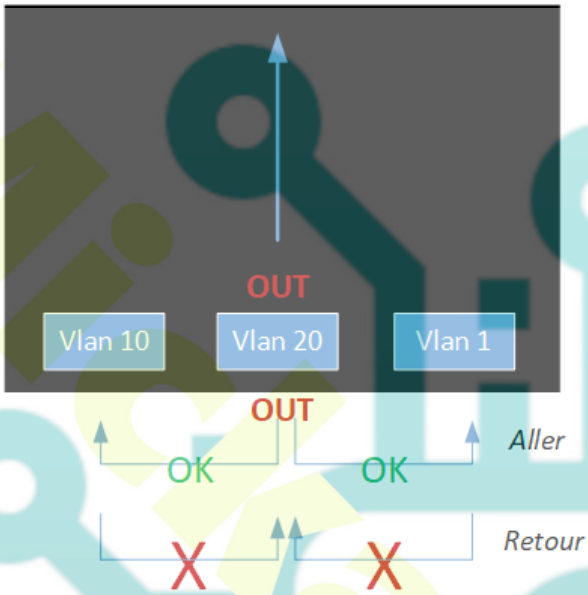
B – Nous allons tester l'ACL NOV20-10 sur l'interface de vlan 20 en OUT

```
int vlan 20
ip access-group NOV20-10 out

Pinging 10.10.1.10
Request timed out.

Pinging 192.168.1.10
Request timed out.
```

Problème de communication. Comment l'interpréter ?

Dans ce cas là, le datagramme IP passe on analyse la règle au retour dans le port comme venant de l'extérieur et là aucune des règles ne correspond et on utilise la règle par défaut **DENY ANY ANY**

ACL NO20-10
Deny 20 vers 10
Permit 20 any



C – Nous allons tenter d'inverser les règles de l'ACL NOV20-10 en gardant le OUT sur l'interface de vlan 20

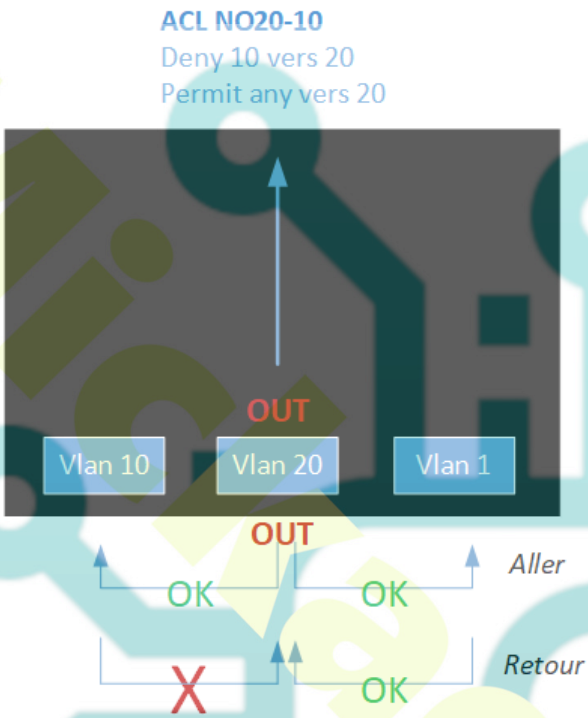
On supprime la règle NOV20-10
no ip access-list extended NOV20-10

on la recréée
ip access-list extended NOV20-10
Deny ip 10.10.0.0 0.0.255.255 10.20.0.0 0.0.255.255
Permit ip any 10.20.0.0 0.0.255.255

NB. on ne supprime pas l'affectation de la règle sur l'interface vlan 20 (ip access-group) puisque qu'on veut toujours utiliser le même nom d'ACL

Pinging 10.10.1.10
Request timed out.
Pinging 192.168.1.10
Reply from 192.168.1.10: bytes=32 time<1ms TTL=127

C’est fonctionnel, mais vraiment ?



Dans ce cas là, le datagramme IP passe on analyse la règle au retour dans le port comme venant de l’extérieur et là les règles sont fonctionnelles. Cependant, la trame est sortie et peut donc être capturée et analysée, ce qui est très mauvais pour la sécurité.

En conclusion, on utilise des règles IN sur les switches pour gérer les filtres et par sécurité, on affecte les règles pour chaque vlan, c’est à dire dans notre cas les règles suivantes en IN.

Pour l’interdiction du vlan 20 vers le 10 mais pas vers les autres

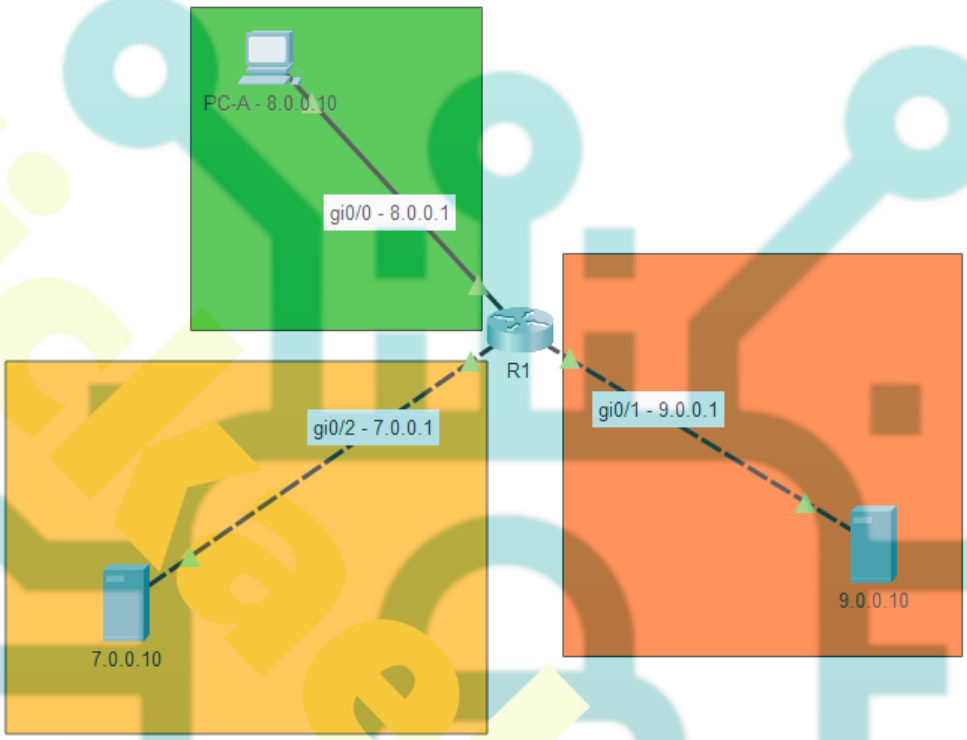
```
ip access-list extended NOV20-10
Deny ip 10.20.0.0 0.0.255.255 10.10.0.0 0.0.255.255
Permit ip 10.20.0.0 0.0.255.255 any
```

```
int vlan 20
ip access-group NOV20-10 in
```

Pour l'interdiction du vlan 10 vers le 20 mais pas vers les autres

```
ip access-list extended NOV10-20
Deny ip 10.10.0.0 0.0.255.255 10.20.0.0 0.0.255.255
Permit ip 10.10.0.0 0.0.255.255 any


int vlan 10
ip access-group NOV10-20 in
```

Etape 2 – les ACL sur un routeur



Nous allons créer une ACL interdisant le ping de la zone verte vers la zone rouge.

```
ip access-list extended ZV-R
Deny icmp 8.0.0.0 0.0.0.255 9.0.0.0 0.0.0.255
Permit ip 8.0.0.0 0.0.0.255 any
```

Test 1 – Affectation de cette règle sur l'interface verte du routeur en IN

```
int gi0/0
ip access-group ZV-R in
```

A partir du PC vert

Pinging 9.0.0.10

Reply from 8.0.0.1: Destination host unreachable.

Pinging 7.0.0.10

Reply from 7.0.0.10: bytes=32 time<1ms TTL=127

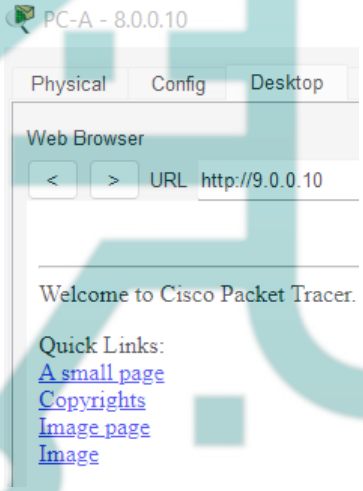
Ca fonctionne pour l'instant

A partir du Serveur rouge

Pinging 8.0.0.10

Request timed out.

La trame est partie mais pas revenu (pas terrible pour la sécurité)



L'accès http du PC vert vers le serveur rouge fonctionne ce qui est normal

A partir du Serveur orange

Pinging 8.0.0.10

Reply from 8.0.0.10: bytes=32 time<1ms TTL=127

Fonctionnement normal

Test 2 – Affectation de cette règle sur l'interface verte du routeur en OUT

```
int gi0/0
no ip access-group ZV-R in
ip access-group ZV-R out
```

A partir du PC vert

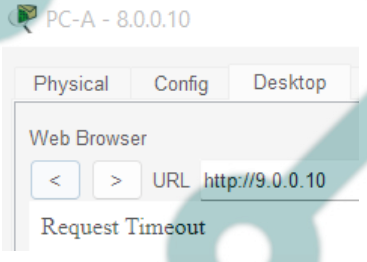
```
Pinging 9.0.0.10
Request timed out.

Pinging 7.0.0.10
Request timed out.
```

A partir du Serveur rouge

```
Pinging 8.0.0.10
Destination host unreachable.
```

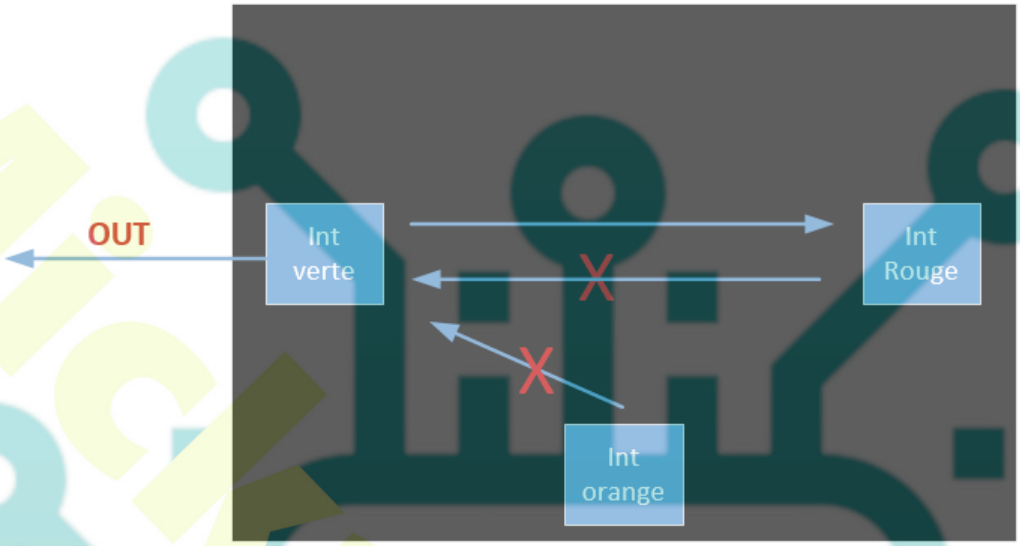
A partir du Serveur orange

```
Pinging 8.0.0.10
Destination host unreachable.
```



Rien ne fonctionne, pourquoi ?

Deny icmp 8.0.0.0 0.0.0.255 9.0.0.0 0.0.0.255
Permit ip 8.0.0.0 0.0.255.255 any



Le OUT indique vers le réseau 8.0.0.0 et comme aucune des règles ne correspond car les adresses sources ne sont pas 8.0.0.0/8, la règle utilisée est **DENY ANY ANY**

Test 3 – Affectation de cette règle sur l'interface rouge du routeur en IN

```
int gi0/1
ip access-group ZV-R in
```

A partir du PC vert
Pinging 9.0.0.10
Request timed out.

A partir du Serveur rouge
Pinging 8.0.0.10
Destination host unreachable.

Test 4 – Affectation de cette règle sur l'interface rouge du routeur en OUT

```
int gi0/1
ip access-group ZV-R out
```

A partir du PC vert
Pinging 9.0.0.10
Destination host unreachable.

A partir du Serveur rouge
Pinging 8.0.0.10
Request timed out.

Tout ça n'est pas terrible, alors nous allons suivre les conseils de Cisco.

On met toujours les règles au plus proche de la machine à protéger.

Liste des règles demandées

1. le PC vert ne doit pas pouvoir faire de ping vers le serveur rouge, mais les autres protocoles sont acceptées vers la zone rouge et orange.
2. le serveur orange ne peut accepter que les requêtes en https venant du PC vert.
3. Le serveur rouge ne doit avoir aucune contrainte d'accès.

Mise en œuvre de la règle 1

Pour répondre à la demande 1, il faut se poser la question (doit-on protéger le serveur rouge du ping du PC vert ou doit-on empêcher le PC vert de communiquer avec le rouge ?)

En fait la règle 3 n'impose aucune contrainte, donc il faut effectuer le filtre au plus près du PC vert (interface verte – gi0/0)

ACL pour la demande 1

```
ip access-list extended PC-VERT
Deny icmp 8.0.0.0 0.0.0.255 9.0.0.0 0.0.0.255
Permit ip 8.0.0.0 0.0.0.255 any
```

Affectation de l'ACL sur l'interface gi0/0 (verte)

```
int gi0/0
ip access-group PC-VERT in
```

Mise en œuvre de la règle 2

Cette fois-ci, c'est le serveur qui doit être protégé. On va donc affecter la règle sur l'interface orange (gi0/2) en out.

ACL pour la demande 2

```
ip access-list extended SV-ORANGE
Permit tcp host 8.0.0.10 host 7.0.0.10 eq 443
```

```
int gi0/2
ip access-group SV-ORANGE out
```