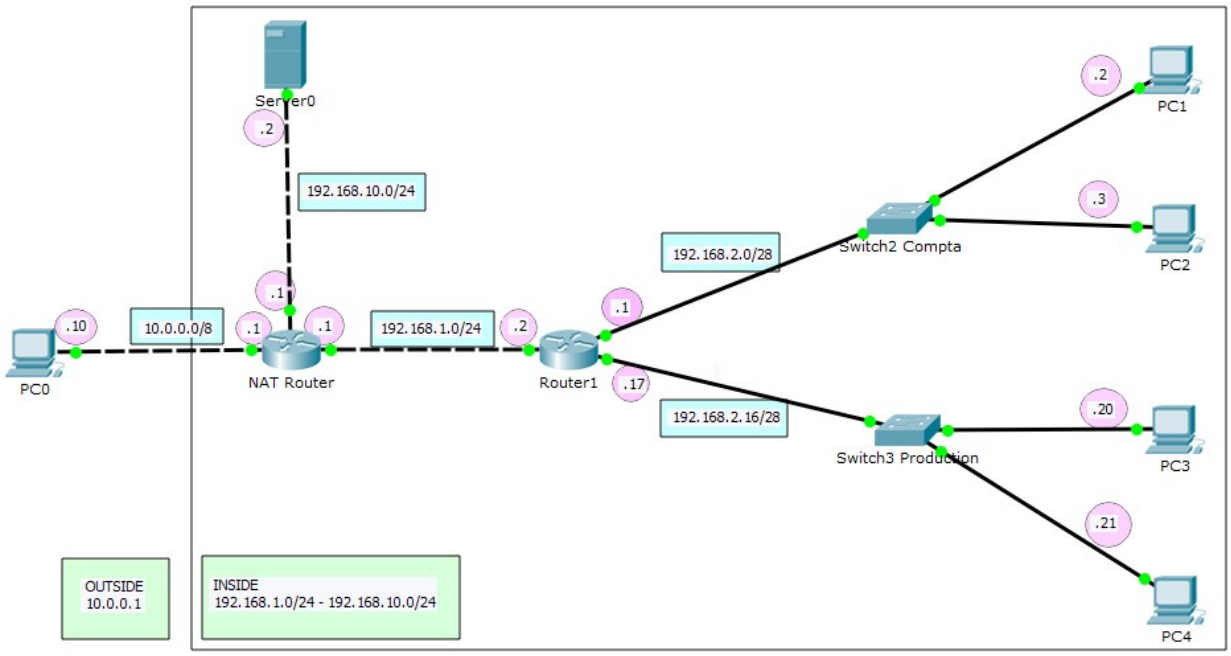
TD n° 4 : Sécurité des équipements réseau

Rappel : ce TD doit faire l'objet d'un Compte Rendu électronique à déposer sur GitLab avant le début de séance suivante, à l'attention de l'enseignant responsable de votre groupe.

Partie 1 : sécurisation d'un commutateur

En plus de configurer la sécurité d'accès aux PC et serveurs, il est important que les matériels réseaux soient également configurés avec des fonctions de sécurité. Cette première partie vise à sécuriser les accès à un commutateur et à vérifier la sécurité de ses ports.

1. Reprendre le circuit du TD3 (R3.06_TD3_exo2.pkt) :



1. *Configuration du routeur Router1 :*

a) En mode configuration, attribuer le mot de passe 'class' pour le mode d'exécution privilégié :

```
(config)# enable secret class
```

b) Configurer l'accès console distant avec le mot de passe 'cisco' :

```
(config)# line vty 0 5
(config-line)# password cisco
```

2. *Configuration du commutateur Switch2 :*

Pour améliorer la sécurité du commutateur, il est pertinent d'attribuer l'interface de gestion à un VLAN autre que le VLAN1 : on crée ici un VLAN 99 auquel on attribue une adresse IP.

a) Établir de la même manière que pour le routeur les mots de passe pour les accès au commutateur ***Switch2***.

b) Configurer une passerelle par défaut pour ***Switch2*** avec l'adresse IP de ***Router1*** :

```
Switch(config)# ip default-gateway 192.168.2.1
```

c) Créer un VLAN99 et le nommer **`Gestion`**

```
Switch2(config)# vlan 99
Switch2(config-vlan)# name Gestion
Switch2(config-vlan)# exit
Switch2(config)#
```

d) Configurer l'interface de gestion du VLAN 99 à l'adresse 192.168.2.10/28 (cf configuration d'interface 'classique').

e) Exécuter la commande **`show vlan`**, puis **`show ip interface brief`** sur Switch2.

Quel est l'état du VLAN 99 ?
Quel sont l'état et le protocole de l'interface de gestion du VLAN 99 ?

f) Attribuer les ports Fa0/1 et Fa1/1 au VLAN 99 sur le commutateur (ports reliant le switch d'une côté au PC1 et de l'autre au routeur).

g) Exécuter à nouveau la commande **`show ip interface brief`** sur Switch2

Quel sont maintenant l'état et le protocole de l'interface de gestion du VLAN 99 ?

3. *Vérifier la communication entre les interfaces :*

a) ping de PC1 vers R1
b) ping de PC1 vers l'adresse de gestion du VLAN 99
c) ping de Switch2 vers R1
d) ping de PC2 vers l'adresse de gestion du VLAN 99

4. *Accès SSH sur Switch2 :*

a) Configuration :

```
Switch(config)#username admin password cisco
Switch(config)#
Switch(config)#hostname S2
S2(config)#
```

```
S2(config)#ip domain-name iut-reso.com
S2(config)#
S2(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S2(config)#
*mars 1 0:23:36.362:  %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#
S2(config)#line vty 0 4
S2(config-line)#transport input ssh
S2(config-line)#login local
```

b) Vérifier la configuration SSH (à vous de trouver la commande …)

Quelle est la version de SSH ? Combien de tentatives de connexions permet-il ? Quel est le délai d'attente par défaut ?

c) Modifier la configuration pour fixer un time-out de 75s et 2 essais maximum.

d) Ouvrir une connexion SSH depuis PC1 avec le login ***admin*** et mot de passe ***cisco***.

e) Faire la même tentative depuis PC2.

Quelle(s) connexion(s) a(ont) réussi ? Pourquoi ?

5. Sécurité des ports sur Switch2 :

a) Arrêter les ports non utilisés sur le commutateur en utilisant les commandes ***interface range*** et ***shutdown***.

b) Notez l'adresse MAC de ***Fa1/0*** sur ***Router1***. À partir de l'interface en ligne de commande de ***Router1***, exécutez la commande ***show interfaces fa1/0*** et notez l'adresse MAC de l'interface

```
Router#show interfaces FastEthernet 1/0
FastEthernet1/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 00e0.8fe7.0760 (bia
00e0.8fe7.0760)
  Internet address is 192.168.2.1/28
...
```

c) Envoyer un PDU de Router1 vers Switch2

d) Sur Switch2, exécutez une commande ***show mac address-table*** ;

Quelle est l'adresse qui apparaît pour le port Fa0/1 ?

e) Dans l'interface de configuration de Fa0/1, définir l'adresse MAC autorisée (celle du routeur) :

```
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address 00E0.8FE7.0760
```

f) Alternativement, on peut utiliser la commande ***switchport port-security mac-address sticky*** pour ajouter la première adresse MAC apprise dynamiquement sur le port .

g) Exécuter la commande **`show port-security interface f0/1`** pour afficher les paramètres de sécurité définis.

Quel est le statut du port ?
Quel est le nombre maximum d'adresses MAC autorisées ?

h) Reproduire la même configuration pour le port Fa1/1 qui relie le commutateur au PC1.

i) Afficher la configuration avec les commandes **`show port-security`** et **`show running-config`**.

j) Test de la sécurité : tout en gardant la console ouverte sur Switch2, modifier l'adresse MAC sur PC1, puis tenter un ping vers Router1

La requête ping a-t-elle abouti ? Pourquoi ? Qu'affiche la console de Switch2 ?

k) Rétablir adresse MAC de PC1 ; arrêter puis remettre en fonction l'interface sur le commutateur. Vérifier la communication !

Partie 2 :Configuration des accès sur un routeur

Dans cette partie, les accès au serveur vont être contrôlés : le réseau « production » par FTP uniquement et le réseau « compta » aura un accès web seulement. Les deux réseaux pourront envoyer un ping au serveur mais pas entre eux.

A chaque mot-clé saisi dans l'interface de configuration, utiliser «? » pour visualiser les options !

1. *Liste de contrôle d'accès numérotée pour FTP et ICMP*

a) En mode de configuration sur Router1, créer une liste d'accès (ACL) numérotée étendue (n° supérieur à 100) en utilisant la commande access-list :

```
access-list access-list-number {permit | deny} protocol
    source source-wildcard [operator port] destination
    destination-wildcard [operator port] [established]
    [log]
```

`access-list-number`	Le n° identifiant la liste (entre 100 et 199)
`{permit | deny}`	Indique si la liste autorise ou bloque les adresses spécifiées
`protocol`	IP, TCP, UDP, ICMP, GRE, ou IGRP.
`source et destination`	Adresses IP source et destination (hôtes ou réseaux)

`source-wildcard`
`destination-wildcard`
	Masque générique : inverse binaire du masque réseau !
	Exemple :
	`11111111.11111111.11111111.11100000 = 255.255.255.224`
	`00000000.00000000.00000000.00011111 = 0.0.0.31`

`[operator port]`	Optionnel : `operator` peut être `lt` (less than), `gt` (greater than), `eq` (equal to), or `neq` (not equal to) `port` : n° de port TCP (p.ex. 23 pour telnet, 21 pour ftp ...)

La liste à créer (n°100) doit autoriser le protocole TCP provenant du réseau « production » à destination du serveur (mot-clé ***host*** avant l'adresse IP du serveur), en précisant le protocole ftp par l'option ***eq ftp*** (ftp étant un trafic tcp spécifique, correspondant au port 21).

Par défaut, tout autre trafic est refusé.

b) Créer une deuxième instruction de liste pour autoriser le trafic ICMP entre le réseau « production » et le serveur. Le n° de liste reste identique, il n'y a pas de trafic spécifique.

c) Appliquer la liste sur l'interface entrante du réseau « production » :

```
Router(config)#interface fa2/0
Router(config-if)#ip access-group 100 in
```

d) Vérifier l'implémentation de la liste en envoyant une requête ***ping*** vers le serveur puis une connexion ***ftp*** depuis l'un des PC « production ».

Une connexion avec un autre protocole (http p.ex) fonctionne-t-elle ? Relever dans votre compte-rendu les commandes utilisées.

2. Liste de contrôle d'accès nommée pour HTTP et ICMP

A chaque mot-clé saisi dans l'interface de configuration, utiliser «? » pour visualiser les options !

Une ACL numérotée peut être composée de nombreuses règles, mais la seule façon de la modifier est de la supprimer (***no access-list <nb>***) et de la redéfinir … Avec les ACL nommées, il est possible de ne supprimer qu'une règle, en utilisant le mot-clé ***no*** devant une règle donnée.

a) En mode de configuration sur Router1, créer une liste d'accès nommée étendue, en utilisant la commande ***ip access-list*** :

ip access-list extended *name* ↵
{permit|deny} protocol source source-wildcard [operator [port]]
destination destination-wildcard **[operator [***port***]]**

`extended`	Pour créer une liste étendue (existe aussi en standard)
`name`	Le nom de la liste
`{permit|deny}`	Indique si la liste autorise ou bloque les adresses spécifiées
`protocol`	IP, TCP, UDP, ICMP, GRE, ou IGRP.
`source destination`	Adresses IP source et destination (hôtes ou réseaux)
`[operator [port]]`	`operator` peut être `lt` (less than), `gt` (greater than), `eq` (equal to), or `neq` (not equal to) `port` : n° de port TCP (p.ex. 80 pour http) ou un mot-clé comme `www` ...
`source-wildcard` `destination-wildcard`	Masque générique : inverse binaire du masque réseau

On crée une liste étendue, car elle doit gérer les adresses IP source et destination. A la différence des listes numérotées, on entre en mode de configuration de liste, ce qui se traduit par une invite telle que :

```
R1(config-ext-nacl)#permit tcp ...
```

La liste à créer, nommée ***HTTP_SEUL***, autorise le trafic ***tcp*** depuis le réseau « compta » à destination du serveur (mot-clé ***host*** avant l'adresse IP du serveur), en précisant le protocole ftp par l'option ***eq www*** (www étant un trafic tcp spécifique, correspondant au port 80).

Par défaut, tout autre trafic est refusé.

b) Créer une deuxième instruction de liste pour autoriser le trafic ICMP entre le réseau « compta » et le serveur ; il n'y a pas de trafic spécifique à préciser.

c) Appliquer la liste sur l'interface entrante du réseau « compta » :

```
Router(config)#interface fa1/0
Router(config-if)#ip access-group HTTP_SEUL in
```

d) Vérifier l'implémentation de la liste en envoyant une requête ***ping*** vers le serveur puis une connexion ***web*** depuis le navigateur web de l'un des PC « compta ».

e) Établir une connexion ftp vers le serveur.

Une connexion avec un autre protocole fonctionne-t-elle ?
Relever dans votre compte-rendu les commandes utilisées.