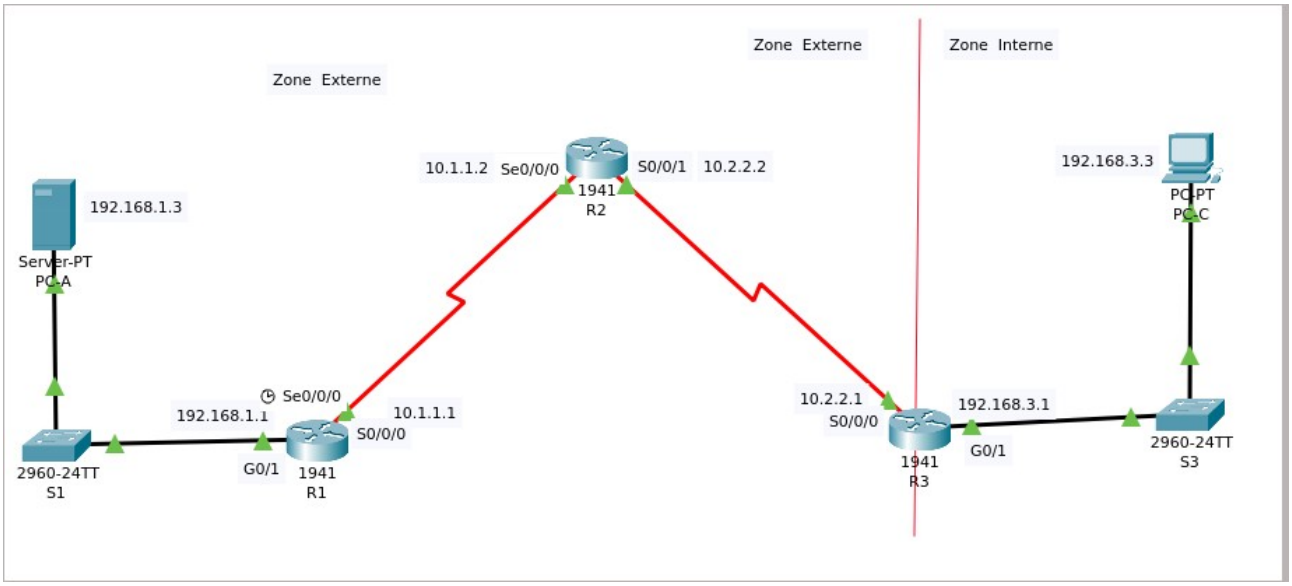
Configuration d'un Firewall ZPF

Dans ce TP, vous allez configurer un ZPF (Zone-Based Policy Firewalls) de base sur un routeur R3 qui permettra aux hôtes internes d'accéder aux ressources externes et bloquera l'accès des hôtes externes aux ressources internes. Ensuite, vous vérifierez la fonctionnalité du pare-feu à partir des hôtes internes et externes.



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Objectif :

1. Vérifiez la connectivité entre les appareils avant la configuration du pare-feu.
2. Configuration d'un pare-feu ZPF sur le routeur R3.
3. Vérifiez la fonctionnalité du pare-feu ZPF en utilisant ping, SSH et un navigateur web
4. Rédigez un compte rendu du TP en commentant les commandes associées au pare-feu ZPF et **cherchez s'il y a d'autres options à tester.**"

1. Configurer les routeurs avec les éléments suivants :

a) Mot de passe de la console : ciscoconpa55
b) Mot de passe pour les lignes vty : ciscovtypa55
c) Mot de passe d'activation : ciscoenpa55
d) Noms d'hôte et adressage IP comme dans le tableau ci-dessus.
e) Login local et mot de passe: Admin / Adminpa55
f) configuration du routage statique/RIP

2. Vérifier la connectivité entre les hôtes :

a) Depuis le prompt du PC-A, faites un ping vers PC-C à l'adresse 192.168.3.3

b) Depuis le prompt du PC-C, effectuez une connexion SSH vers l'interface S0/0/1 sur R2 à l'adresse 10.2.2.2. Utilisez le nom d'utilisateur Admin et le mot de passe Adminpa55 pour vous connecter. Puis quittez la session SSH.

c) Depuis PC-C, ouvrez un navigateur web vers le serveur PC-A (192.168.1.3) (Changer le index.html de la page web du serveur PC-A) .

Router**(config)#hostname R2**
Référencez un nom de domaine : **R2(config)#ip domain-name lsi.com**
Activez le cryptage avec les paires de clé RSA
R2(config)#crypto key generate rsa
How many bits in the modulus [512]: **2048**
Passez à la version 2 : R2**(config)#ip ssh version 2**
Configurez login, mot de passe (admin, cisco) : R2**(config)#username admin password Adminpa55**
Configuration des lines pour déclarer que seul le protocole SSH sera disponible avec l'utilisateur que nous venons de créer : **R2(config)#line vty 0 15**
R2(config-line)#login local
R2(config-line)#transport input ssh
→ Ces 3 dernière commandes permettent de désactiver telnet et activer ssh sur tous les VTY (Virtual Terminal Lines)

Nous pouvons à présent tester la connexion sur le poste client avec la commande suivante :
C:\> ssh -l admin 10.2.2.2

Remarque :
Pour désactiver toutes les formes d'accès à distance (Telnet et SSH) :
R2 (config) # line vty 0 15
R2(config-line) # transport input none
Pour réactiver de nouveau SSH :
R2 (config) # line vty 0 15
R2(config-line)#login local
R2 (config-line) # transport input telnet ssh

3. Création des zones Firewall sur le Routeur 3 :

a) Vérification du package de sécurité dans le routeur R3 (securityk9).

b) Si le package de technologie de sécurité n'a pas été activé, activez-le. (accepté la licence, sauvegarder (NVRAM)l a configuration puis recharger le routeur.

a) **R3 # sh version**
b) **R3(config)# license boot module c1900 technology-package securityk9**
R3# copy running-config startup-config
R3# write memory
R3# reload

4. création des deux zones (interne et externe)

R3(config)# zone security IN-ZONE
R3(config-sec-zone) exit
R3(config-sec-zone)# zone security OUT-ZONE
R3(config-sec-zone)# exit

```
R4# copy running-config startup-config
R4# copy run start
```

5. Identification du trafic à l'aide d'une class-map

a) Créez une ACL définissant le trafic interne. Utilisez la commande access-list pour créer une ACL étendue 101 permettant tous les protocoles IP depuis le réseau source 192.168.3.0/24 vers n'importe quelle destination.

b) Créez une classe d'identification faisant référence à l'ACL du trafic interne.

- Utilisez la commande class-map de type inspect avec l'option match-all pour créer une classe d'identification nommée IN-NET-CLASS-MAP.
- Utilisez la commande match access-group pour faire correspondre l'ACL 101.

```
a)  R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
b)  R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
    R3(config-cmap)# match access-group 101
    R3(config-cmap)# exit
```

6. Spécification des politiques du pare-feu

a) Créez une map de politique pour déterminer quoi faire avec le trafic correspondant. Utilisez la commande policy-map de type inspect pour créer une map de politique nommée IN-2-OUT-PMAP."

b) Spécifiez un type de classe 'inspect' et faites référence à la classe d'identification IN-NET-CLASS-MAP

c) Spécifiez l'action d'inspection pour cette map de politique via la commande inspect.

d) Quittez les deux modes config-pmap-c et config-pmap.

```
    R3(config)# policy-map type inspect IN-2-OUT-PMAP
    R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
    R3(config-pmap-c)# inspect
    R3(config-pmap-c)# exit
    R3(config-pmap)# exit
```

7. Application des politiques du pare-feu

a) À l'aide de la commande zone-pair security, créez une zone-pair nommée IN-2-OUT-ZPAIR. Spécifiez les zones source et destination qui ont été créées précédemment."

b) Spécifiez la map de politique pour gérer le trafic entre les deux zones : Attachez une policy-map et ses actions associées à la zone-pair via la commande « *service-policy type inspect »* et faites référence à la map de politique précédemment créée, « *IN-2-OUT-PMAP* »

c) Affectez les interfaces aux zones de sécurité appropriées :

Utilisez la commande « *zone-member security* » en mode de configuration d'interface pour assigner G0/1 à IN-ZONE et S0/0/1 à OUT-ZONE

d) Copiez la configuration en cours dans la configuration de démarrage.

```
a)  R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE

b)  R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
    R3(config-sec-zone-pair)# exit

c)  R3(config)# interface g0/1
    R3(config-if)# zone-member security IN-ZONE
    R3(config-if)# exit
    R3(config)# interface s0/0/1
    R3(config-if)# zone-member security OUT-ZONE
    R3(config-if)# exit
d)  R4# copy running-config startup-config
    R4# copy run start
```

8. **Test de fonctionnalité du pare-feu de la zone IN-ZONE vers OUT-ZONE.**

Vérifiez que les hôtes internes peuvent toujours accéder aux ressources externes après avoir configuré le pare-feu de zone :

a) Depuis le prompt de l'ordinateur interne PC-C, faites un ping le serveur externe PC-A(192.168.1.3).

b) Depuis le prompt du PC-C, effectuez une connexion SSH vers R2 à l'adresse 10.2.2.2. Utilisez le nom d'utilisateur Admin et le mot de passe Adminpa55 pour accéder à R2. La session SSH devrait réussir (ne quittez pas la session ssh).
Pendant que la session SSH est active, lancez la commande *«show policy-map type inspect zone-pair sessions»* sur R3 pour afficher les sessions établies :

- Quelle est l'adresse IP source et le numéro de port ?
- Quelle est l'adresse IP de destination et le numéro de port ?"

Depuis PC-C, quittez la session SSH sur R2 et fermez la fenêtre du prompt.
c) Depuis l'ordinateur interne PC-C, ouvrez un navigateur Web vers la page Web du serveur PC-A. Saisissez l'adresse IP du serveur 192.168.1.3 dans le champ URL du navigateur, puis cliquez sur '*GO*'.
La session HTTP devrait réussir. Pendant que la session HTTP est active, exécutez la commande « s*how policy-map type inspect zone-pair sessions* » sur R3 pour voir les sessions établies. Remarque : Si la session HTTP expire avant que vous n'exécutiez la commande sur R3, vous devrez cliquer sur le bouton 'GO' sur PC-C pour générer une session entre PC-C et PC-A." :

- Quelle est l'adresse IP source et le numéro de port ?
- Quelle est l'adresse IP de destination et le numéro de port ?"

Quittez le navigateur du PC-C

9. Test de fonctionnalité du pare-feu de la zone OUT-ZONE vers IN-ZONE.

- Depuis le prompt du PC-A, faites un ping vers la machine PC-C à l'adresse 192.168.3.3. Le ping devrait échouer.
- Depuis le routeur R2, faites un ping vers PC-C à l'adresse 192.168.3.3. Le ping devrait échouer.

==========

Sécurité routeur :

Mot de passe de la console : ciscoconpa55 :

```
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password ciscoconpa55
Router(config-line)# login   (Activez l'authentification pour la console)
Router(config-line)# exit
Router# write memory
```

Mot de passe pour les lignes vty : ciscovtypa55 :

```
Router# configure terminal
Router(config)# line vty 0 15
Router(config-line)# password ciscoconpa55
Router(config-line)# login
Router(config-line)# exit
Router# write memory
```

Mot de passe d'activation ou de privilège : ciscoenpa55 :

```
Router# configure terminal
Router(config)# enable secret ciscoenpa55
Router(config)# end
Router# write memory
```

Configurez login, mot de passe (admin, cisco) :

Router(config)#username admin password cisco

Sauvegardez la configuration actuelle dans la mémoire persistante (NVRAM) :

```
Router# copy running-config startup-config  ou Router# write memory
Router# reload
```