ACTIVITE 6
Pare-feu par zone - ZPF

L'objectif de cette activité est de configurer un routeur ZPF.

1 – Configurer un pare-feu ZPF

Utilisez le fichier "Act 6 - Pare-feu ZPF.pkt" pour la suite de l'activité.

Votre mission

Dans cette activité, vous allez configurer un routeur ZPF de base à la périphérie R3 qui permet aux hôtes internes d'accéder aux ressources externes et empêche les hôtes externes d'accéder aux ressources internes. Vous vérifierez ensuite le fonctionnement du pare-feu à partir des hôtes internes et externes.

Les routeurs ont été préconfigurés avec les informations d'identification suivantes :

- Mot de passe de console : **ciscoconpa55**
- Mot de passe pour les lignes vty : **ciscovtypa55**
- Mot de passe d'activation : **ciscoenpa55**
- Nom d'utilisateur et mot de passe locaux : **Admin / Adminpa55**

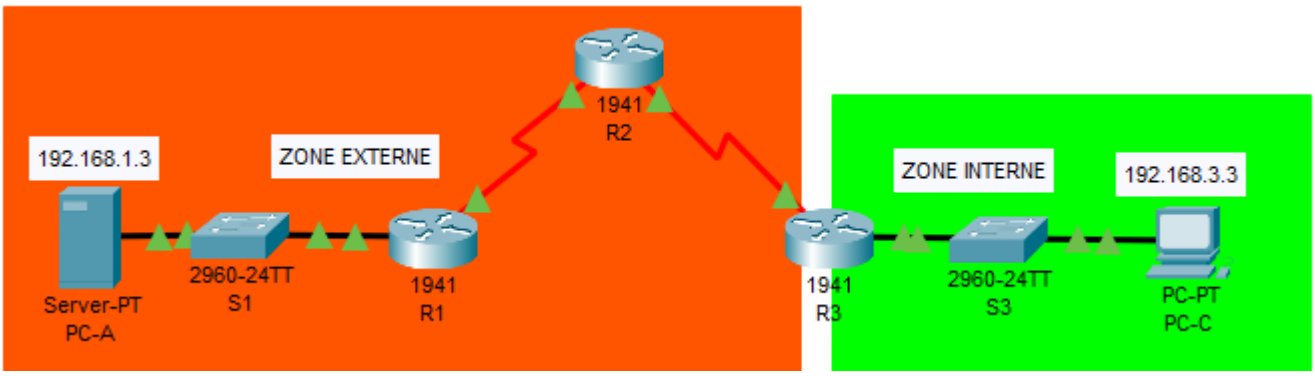

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut	Port du commutateur
R1	G0/1	192.168.1.1	255.255.255.0		S1 F0/5
	S0/0/0	10.1.1.1	255.255.255.252		
R2	S0/0/0	10.1.1.2	255.255.255.252		
	S0/0/1	10.2.2.2	255.255.255.252		
R3	G0/1	192.168.3.1	255.255.255.0		S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252		
PC-A	Carte réseau (NIC)	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	Carte réseau (NIC)	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

☞ 1 – Vérifiez la connectivité entre les périphériques avant la configuration du pare-feu :

- Faites un ping entre PC-A et PC-C puis entre PC-C et PC-A.
- Vous pouvez aussi faire un tracert entre les deux PC.
- Testez depuis le navigateur de PC-C l'accès au serveur PC-A

Il n'y a pas de pare-feu donc vous devez pouvoir communiquer.

✍ 2 – Établissez des sessions SSH sur l'interface S0/0/1 de R2 à partir des deux PC.

À partir de l'invite de commande, utilisez la ligne de commande **ssh -l [username] [ip address]** pour démarrer une session SSH.

Vous utiliserez le nom d'utilisateur et le mot de passe donné au début de l'activité.

Commande (depuis PC-C) :

```
C:\>ssh -l Admin 10.2.2.2
```

Commande (depuis PC-A) :

```
C:\>ssh -l Admin 10.2.2.2
```

Bien comprendre les étapes de la configuration d'un pare-feu à politique basée sur les zones

Etape 1 (zone security …) :
Il faut nommer les zones que l'on veut contrôler : Zone intérieure, extérieure, zone 1, 2 ou 3, …

Etape 2 (access-list 101 permit ip …) :
On définit les règles sans les associées à une interface ou à une zone : ACL 1, ACL 2, …

Etape 3 (class-map type … / match access-group …) :
Création d'une classe (mappage de classe) : On va ajouter à la classe les règles que l'on souhaite utiliser.

Etape 4 (policy-map type … / class type inspect …) :
Il faut définir la politique de sécurité entre deux zones en sélectionnant un mappage de classe (étape 3) et en précisant l'action à faire (inspect, drop, …) lorsque on aura des "match".

Etape 5 (zone-pair security …) :
Définir la paire de zone que l'on veut contrôler et préciser le sens de la communication (source / destinataire) : par exemple zone intérieure (source) et zone 2 (destinataire) forment une paire de zone.

Etape 6 (interface …/ zone-member security …) :
Associer les interfaces (G0/0, S0/1/0, …) avec les zones définies à l'étape 1.

Etape 7 (show policy-map …) :
Tester la ZPF.

Commençons …

Vous allez créer (questions 3, 4 et 5) deux zones de sécurité sur R3 : zone interne et zone externe.

✍ 3 – Commencez par activer le mode "Privilège" puis le mode de "configuration terminal" pour R3 depuis l'onglet CLI.

Commandes :

```
R3>en
Password:
R3#conf t
```

✍ 4 – Créez une zone interne que vous nommerez **IN-ZONE**

Commande :

```
R3(config)#zone security IN-ZONE
```

✍ 5 – Créez une zone externe que vous nommerez **OUT-ZONE**

Commande :

R3(config)#**zone security OUT-ZONE**

Vous allez maintenant configurer un mappage de classes (questions 6, 7 et 8) pour toutes les adresses IP du réseau interne. Tout d'abord, vous allez créer une liste de contrôle d'accès qui définit le réseau interne sur R3. Vous allez également créer un mappage de classe pour inspecter le trafic interne.

✍ 6 – Créez une liste de contrôle d'accès (ACL – numérotée 101) sur R3 qui autorise tout le trafic "réseau interne" vers toutes les destinations.

Commande :

R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any

✍ 7 – Créez un mappage de classe qui inspecte tout le trafic interne en référençant la liste de contrôle d'accès (ACL). Vous nommerez le mappage **IN-NET-CLASS-MAP.**

Commande :

R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP

✍ 8 – Utilisez la liste de contrôle d'accès (ACL - 101) précédemment créée comme critère de classification correspondant dans le mappage de classe.

Commande :

R3(config-cmap)# match access-group 101
R3(config-cmap)# **exit**

Vous avez défini les zones de sécurité et configuré les mappages de classes sur R3. Maintenant, vous allez configurer et appliquer (questions 9 et 10) les politiques de pare-feu.

✍ 9 – Créez un mappage de politiques qui inspecte le trafic en fonction du mappage de classes que vous avez précédemment configuré. Vous utiliserez le nom : **IN-2-OUT-PMAP**.

Commande :

R3(config)#policy-map type inspect IN-2-OUT-PMAP

✍ 10 – Spécifiez l'action de mappage de politiques **inspect** et faites référence au mappage de classes que vous avez créé à l'étape précédente.

Commandes :

R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect

Définissez la paire de zones avec les zones source et de destination spécifiques qui ont été créées précédemment. La zone de sécurité interne que vous avez définie plus tôt dans cette activité sera la zone de sécurité source, tandis que la zone de sécurité externe sera la zone de sécurité de destination.

✍ 11 – Créez une paire de zones (nom : **IN-2-OUT-ZPAIR**) avec les zones source et de destination créées à l'étape précédente.

Commande :

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

✍ 12 – Attachez un mappage de politiques et ses actions associées à la paire de zones configurées.

Commandes :

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

Vous allez attribuer les interfaces appropriées (questions 13, 14, 15 et 16) aux zones de sécurité que vous avez créées précédemment sur R3.

✍ 13 – Quelle interface R3 doit être attribuée à la zone de sécurité interne ?

C'est l'interface coté réseau interne : G0/1

✍ 14 – Utiliser **IN-ZONE** comme exemple de nom de zone. Pour être correct, le nom de la zone doit correspondre au nom de la zone que vous avez créée précédemment (question 4).

Commandes :

R3(config)#interface g0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit

✍ 15 – Quelle interface R3 doit être attribuée à la zone de sécurité externe ?

C'est l'interface coté réseau interne : S0/0/1

✍ 16 – Utiliser **OUT-ZONE** comme exemple de nom de zone. Pour être correct, le nom de la zone doit correspondre au nom de la zone que vous avez créée précédemment (question 5).

Commandes :

R3(config)#interface S0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit

Utilisez la commande "**show policy-map type inspect zone-pair sessions**" pour répondre aux questions suivantes.

✍ 17 – Maintenant que vous avez configuré le ZPF, quelles connexions devraient aboutir ou non ?

Toutes les connexions du réseau interne sur R3 G0/1 (le réseau interne) vers le réseau externe doivent réussir.
Toutes les connexions provenant du réseau externe, telles que tout ce qui accède à R3 via l'interface S0/0/1, doivent échouer.

✍ 18 – À partir de PC-C, établissez une session SSH vers l'interface R2 S0/0/1 (10.2.2.2) comme vous l'avez fait au début de cette activité. La connexion a-t-elle réussi ? En cas de réussite, quels sont l'adresse IP source et le numéro de port ? Quelle est l'adresse IP et le numéro de port de destination ?
Source 192.168.3.3 : port aléatoire et destination 10.2.2.2:22
Exemple de sortie de la commande show :
Nombre de sessions établies = 1
Sessions établies Session 652013648 (192.168.3.3:1035) => (10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
C'est normal puisqu'on est dans le sens zone interne vers externe.

✍ 19 – Depuis PC-C, accédez au serveur web (192.168.1.3). La connexion a-t-elle réussi ? En cas de réussite, quels sont l'adresse IP source et le numéro de port ? Quelle est l'adresse IP et le numéro de port de destination ?

Source 192.168.3.3 : port aléatoire et destination 192.168.1.3:80
Exemple de sortie de commande show : Nombre de sessions établies = 1
Session établie Session 652039936 (192.168.3.3:1034) => (192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
C'est normal, puisqu'on est dans le sens zone interne vers externe.

✍ 20 – À partir de PC-A l'invite de commande, exécutez une commande ping PC-C sur 192.168.3.3. La connexion a-t-elle réussi ? En cas de réussite, quels sont l'adresse IP source et le numéro de port ? Quelle est l'adresse IP et le numéro de port de destination ?
Echec du ping. C'est normal, puisqu'on est dans le sens zone externe vers interne => filtrage Pare-feu ZPF.

✍ 21 – Depuis R2, envoyez un ping PC-C à 192.168.3.3. La connexion a-t-elle réussi ? En cas de réussite, quels sont l'adresse IP source et le numéro de port ? Quelle est l'adresse IP et le numéro de port de destination ?

Echec du ping. C'est normal, puisqu'on est dans le sens zone externe vers interne => filtrage Pare-feu ZPF.