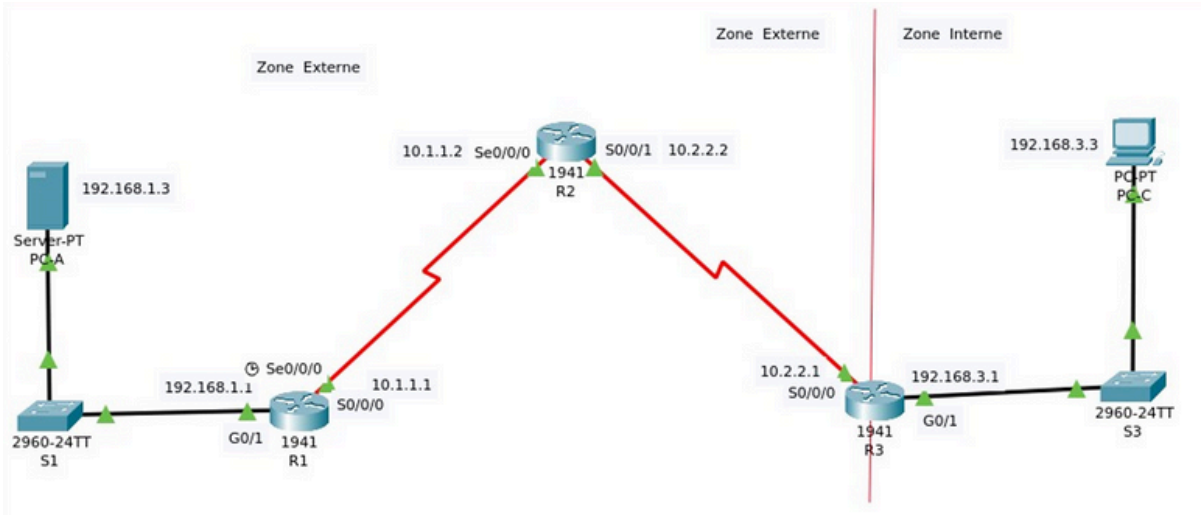
UNIVERSITÉ ABDELMALEK ESSAADI FACULTÉ DES SCIENCES ET TECHNIQUES DE TANGER
DÉPARTEMENT GÉNIE INFORMATIQUE

TP Configuration d'un Firewall ZPF



Encadré par :

- **Pr Abderrahim GHADI**

Réalisé par :

- **Chaimae Bouassab**

Module : Architecture & Technologies Big Data
Master : Sécurité IT & BigData

Objectifs du TP :

Configurer un pare-feu ZPF sur R3 pour :

- Autoriser les connexions internes (PC-C vers PC-A / Internet)
- Bloquer les connexions externes (PC-A vers PC-C)
- Vérifier avec : ping, SSH, navigateur web

Élément	Mot de passe	Quand l'utiliser
Console	ciscoconpa55	Lorsqu'on accède physiquement au routeur
VTY (accès distant)	ciscovtypa55	Pour les connexions via SSH ou Telnet
Enable (privilège)	ciscoenpa55	Pour passer de > à #
Utilisateur local Admin	Adminpa55	Utilisé pour l'authentification SSH
SSH (login remote)	Admin / Adminpa55	Pour se connecter à R2 via SSH depuis PC-C

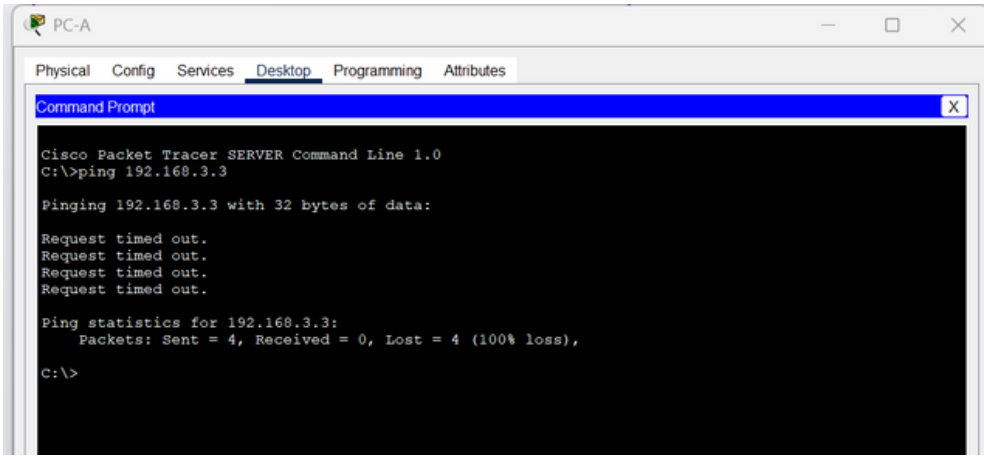
Contexte et scénario

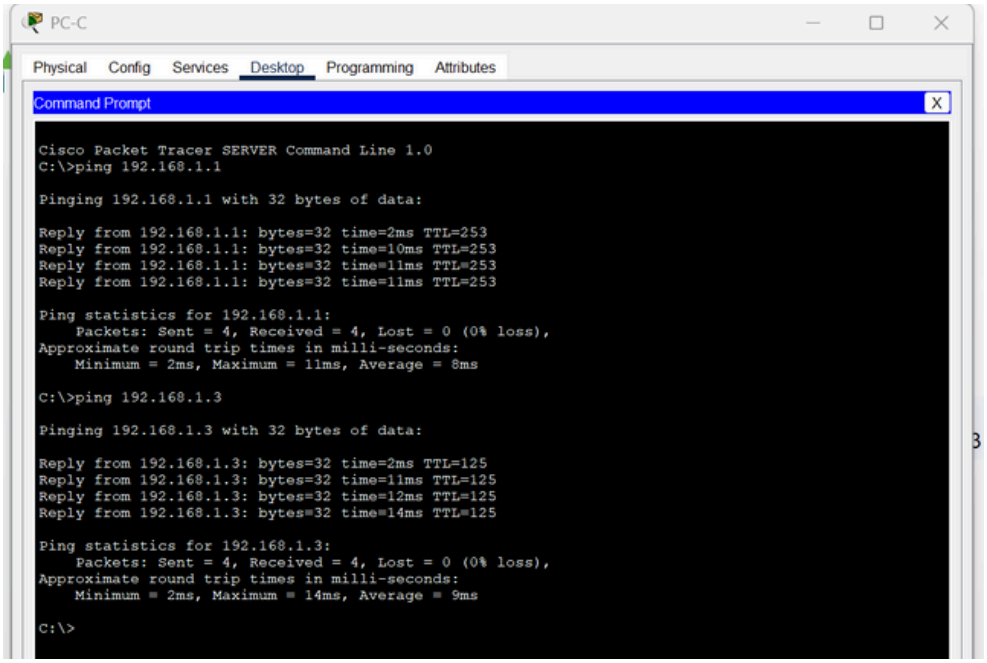
Les pare-feux ZPF représentent une évolution récente des technologies de sécurité Cisco. Dans ce TP, l'objectif est de configurer un pare-feu ZPF de base sur un routeur de périphérie (R3), afin de :

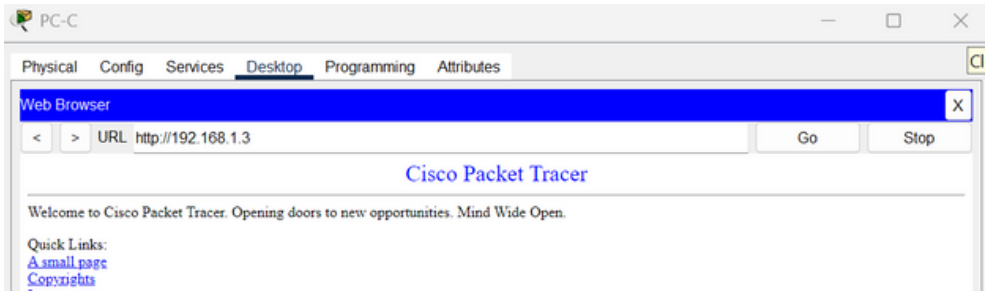
Autoriser l'accès des hôtes internes aux ressources externes ;

Bloquer toute tentative d’accès depuis l’extérieur vers le réseau interne.

Partie 1 : Vérification de la connectivité réseau

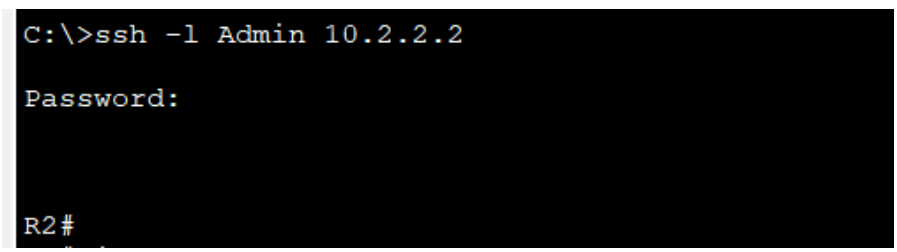






Depuis PC-C, ouvrir un navigateur et saisir 192.168.1.3 (serveur web de PC-A) dans la barre d'URL → la page d'accueil doit s'afficher.

Depuis PC-C, se connecter à R2 via SSH :



Activer le package sécurité :

Vérifier via show version

```
R3>
R3>show ver
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 15:41 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2811 uptime is 18 minutes, 49 seconds
System returned to ROM by power-on
System image file is "flash0:c2800nm-advipservicesk9-mz.151-4.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
```

🔧 Partie 2 : Création des zones de pare-feu sur R3

S'il est inactif :

Créer les zones :

```
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#license boot module c1900 technology-package securityk9
                  ^
```

📄 Partie 3 : Identification du trafic autorisé via une class-map

Créer une ACL pour le trafic interne :

Créer une class-map liée à cette ACL :

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

🔐 Partie 4 : Définition des règles de pare-feu (policy-map)

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
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
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be
inspected
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#
R3(config)#
R3(config)#
```

Créer un pair de zones :

🔗 Partie 5 : Application des règles de sécurité ZPF

Appliquer la policy-map au pair de zones :

```
R3(config)#
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#interface g0/1
```

```
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.3.1     YES manual up                    up
Serial0/3/0            unassigned      YES unset  administratively down down
Serial0/3/1            10.2.2.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R3#
```

Copy Paste

Assigner les interfaces aux zones (exemple adapté à Mon routeur) :

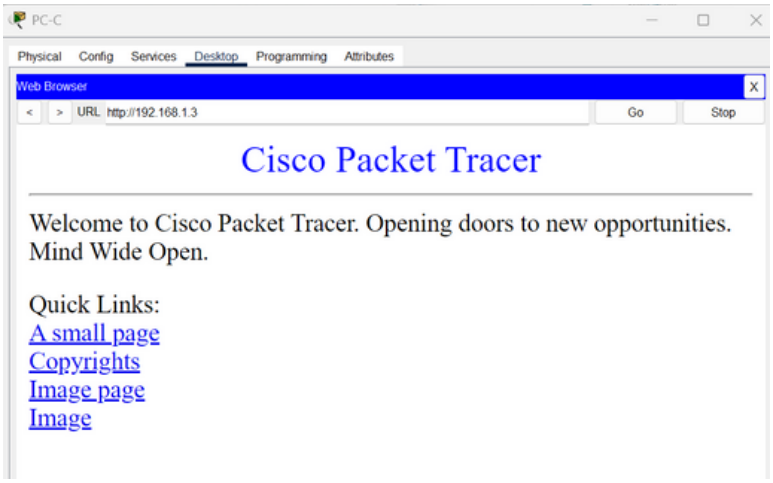
- **Pour le LAN (réseau interne / zone IN-ZONE) :**

```
R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.3.1     YES manual up                    up
Serial0/3/0            unassigned      YES unset  administratively down down
Serial0/3/1            10.2.2.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface FastEthernet0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)#exit
```

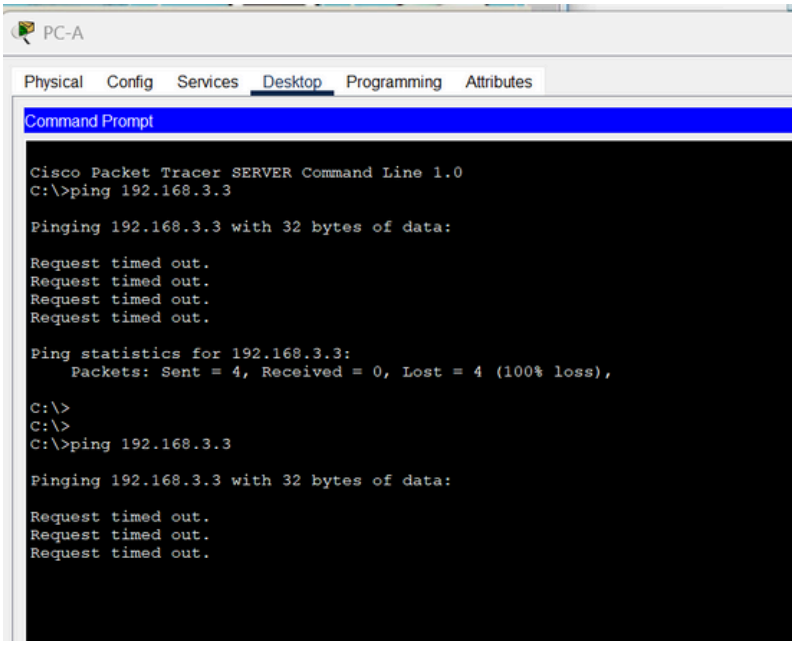
- **Pour le WAN (vers R2 / zone OUT-ZONE) :**

```
R3(config)#interface Serial0/3/1
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
```

```
R2#exit

[Connection to 10.2.2.2 closed by foreign host]
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=12ms TTL=125
Reply from 192.168.1.3: bytes=32 time=12ms TTL=125
Reply from 192.168.1.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 41ms, Average = 16ms
```

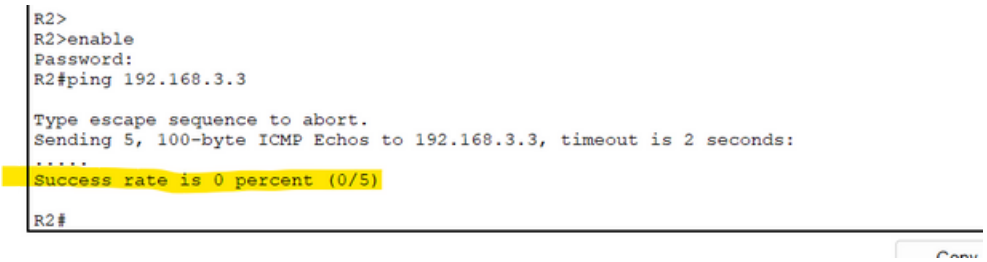


🧪 Partie 6 : Test de fonctionnement – du réseau interne vers externe



Équipement	Interface	Adresse IP	Rôle	Zone ZPF
R3	Fa0/1	192.168.3.1	Vers PC-C	IN-ZONE
R3	S0/3/1	10.2.2.1	Vers R2	OUT-ZONE

🔒 Partie 7 : Test du blocage – du réseau externe vers interne



Conclusion

- Ce TP nous a permis de comprendre et de mettre en œuvre un pare-feu basé sur des zones (Zone-Based Policy Firewall - ZPF) sur un routeur Cisco. Grâce à cette approche, nous avons pu établir des politiques de sécurité précises en définissant clairement les zones de confiance (IN-ZONE) et non de confiance (OUT-ZONE), puis en contrôlant finement le trafic autorisé entre elles.

La configuration a démontré que :

- Les hôtes internes pouvaient accéder en toute sécurité aux ressources externes via des services comme SSH ou HTTP.
- Toute tentative d'accès depuis l'extérieur vers le réseau interne a été bloquée, comme prévu dans la politique de sécurité.
- Cette architecture renforce la sécurité réseau en segmentant les flux et en appliquant des règles contextualisées sur les connexions. Elle constitue une base solide pour la mise en place de politiques de sécurité plus avancées dans des environnements professionnels réels.