TP4 BONUS - DMZ Firewall sur routeurs CiscoAccess Control Lists (ACL)

Abdel-malik FOFANA, Ivan KRIVOKUCA

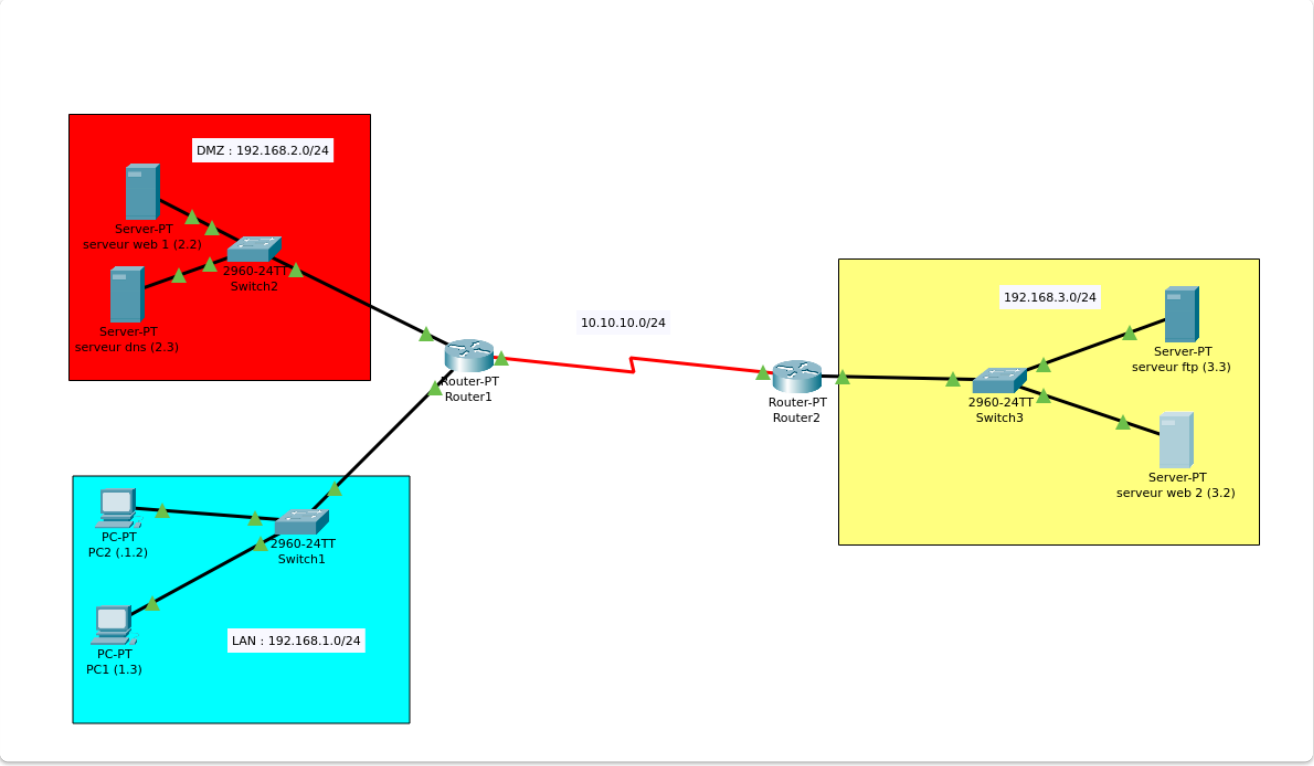
1. Objectif et présentation de la plateforme

2. Configuration de LAN, DMZ et Routeur sans filtrage

2.1. Configuration du réseau

1. Construire le réseau ci-dessus avec les paramètres réseaux indiqués.

Voici le réseau construit sur *cisco packet tracer*



2. Configurer les interfaces des Routeurs cotés LAN, DMZ et WAN.

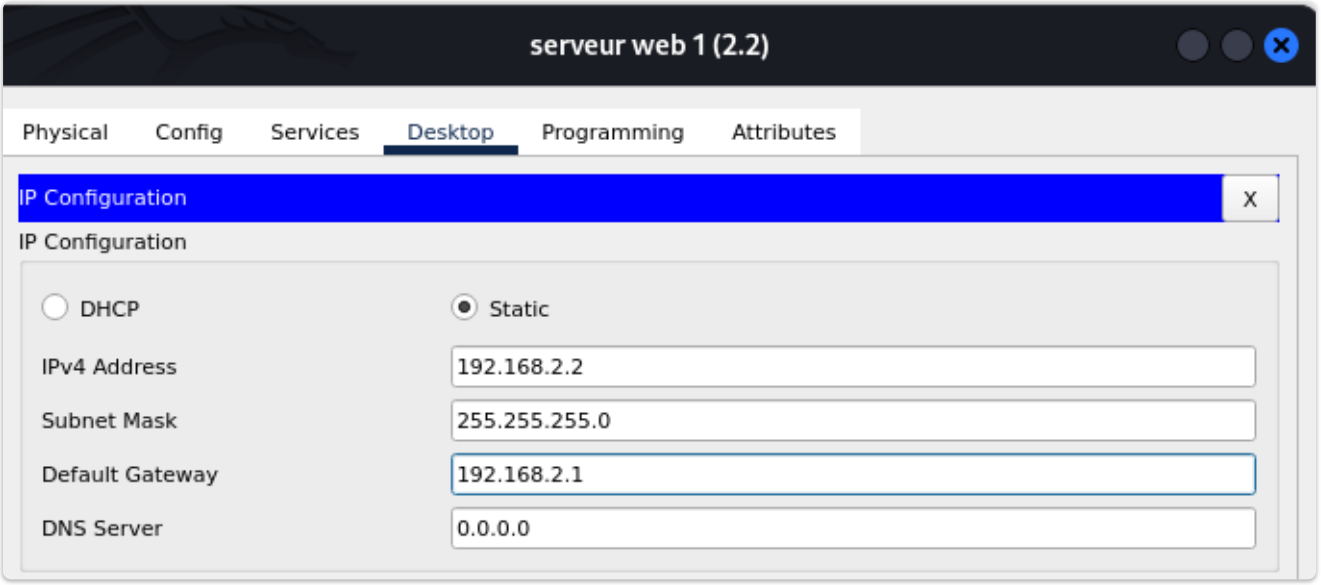
interface Routeur 1 ⟶ LAN : *192.168.1.1*
interface Routeur 1 ⟶ DMZ : *192.168.2.1*
interface Routeur 1 ⟶ Routeur 2 : *10.10.10.1*
interface Routeur 2 ⟶ DMZ : *192.168.3.1*
interface Routeur 2 ⟶ Routeur 1 : *10.10.10.2*

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#
```

```
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
ip address 10.10.10.2 255.255.255.0
Router(config-if)#ip address 10.10.10.2 255.255.255.0
Router(config-if)#
```

3. Configurer les interfaces des PCs LAN et DMZ avec les valeurs des adresses IP indiqués ci-dessus.

Voici un exemple de comment on a donner une IP statique au serveur web, nous avons procéder de la même manière pour les autres PCs:



DMZ (gateway : 192.168.2.1):

- Web Server 1 : 192.168.2.2
- Internal DNS Server : 192.168.2.3

LAN (gateway 192.168.1.1):

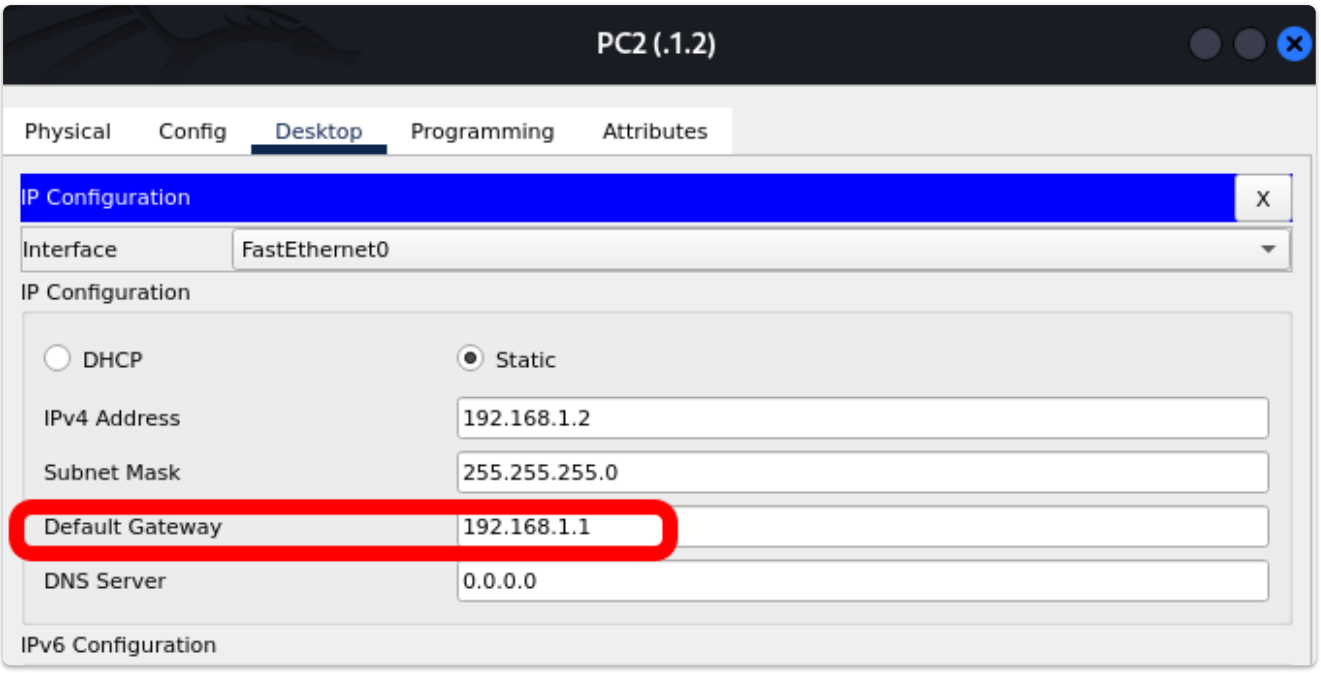
- PC2 : 192.168.1.2
- PC1 : 192.168.1.3

Routeur sans filtrage (gateway : 192.168.3.1):

- Web Server 1 : 192.168.3.2
- FTP Server : 192.168.3.3

4. Configurer le routage dynamique et les passerelles par défaut dans les PCs et les serveurs.

Toutes les machines ont leur propre passerelle par défaut configurée de cette manière (ici un exemple avec le *PC2* du LAN et la passerelle *192.168.1.1*).



Pour le routage dynamique nous avons utilisé le routage OSPF (simple et rapide)

Pour le ROUTER 1 (connecté au LAN et DMZ) voici les commandes:

```
Router1(config)# router ospf 1
Router1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

```
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet1/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
O    192.168.3.0/24 [110/65] via 10.10.10.2, 00:01:40, Serial2/0
```

Pour le ROUTER 2 (représentant internet 192.168.3.0/24)

```
Router2(config)# router ospf 1
```

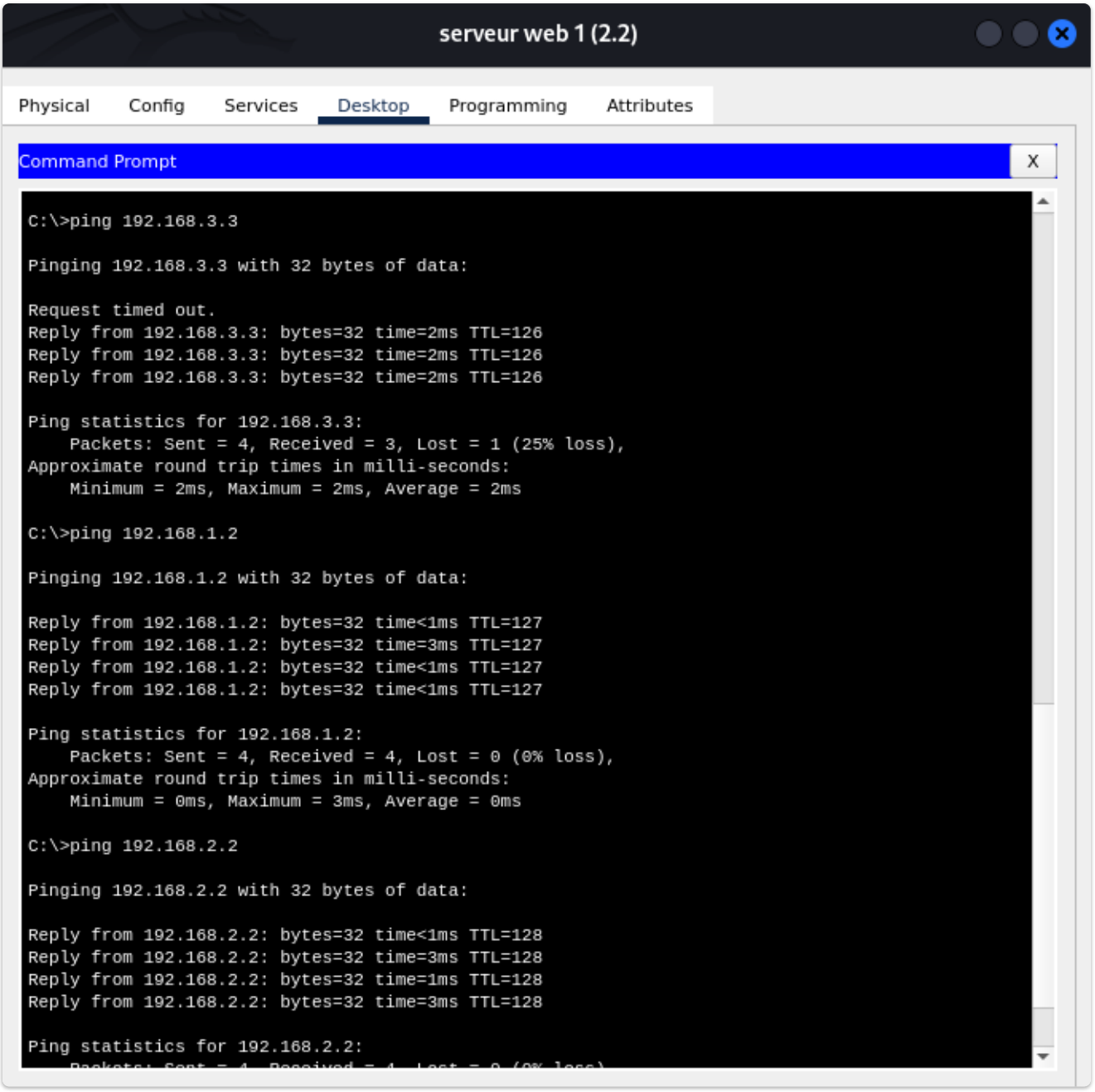
```
Router2(config-router)# network 192.168.3.0 0.0.0.255 area 0
```

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial2/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

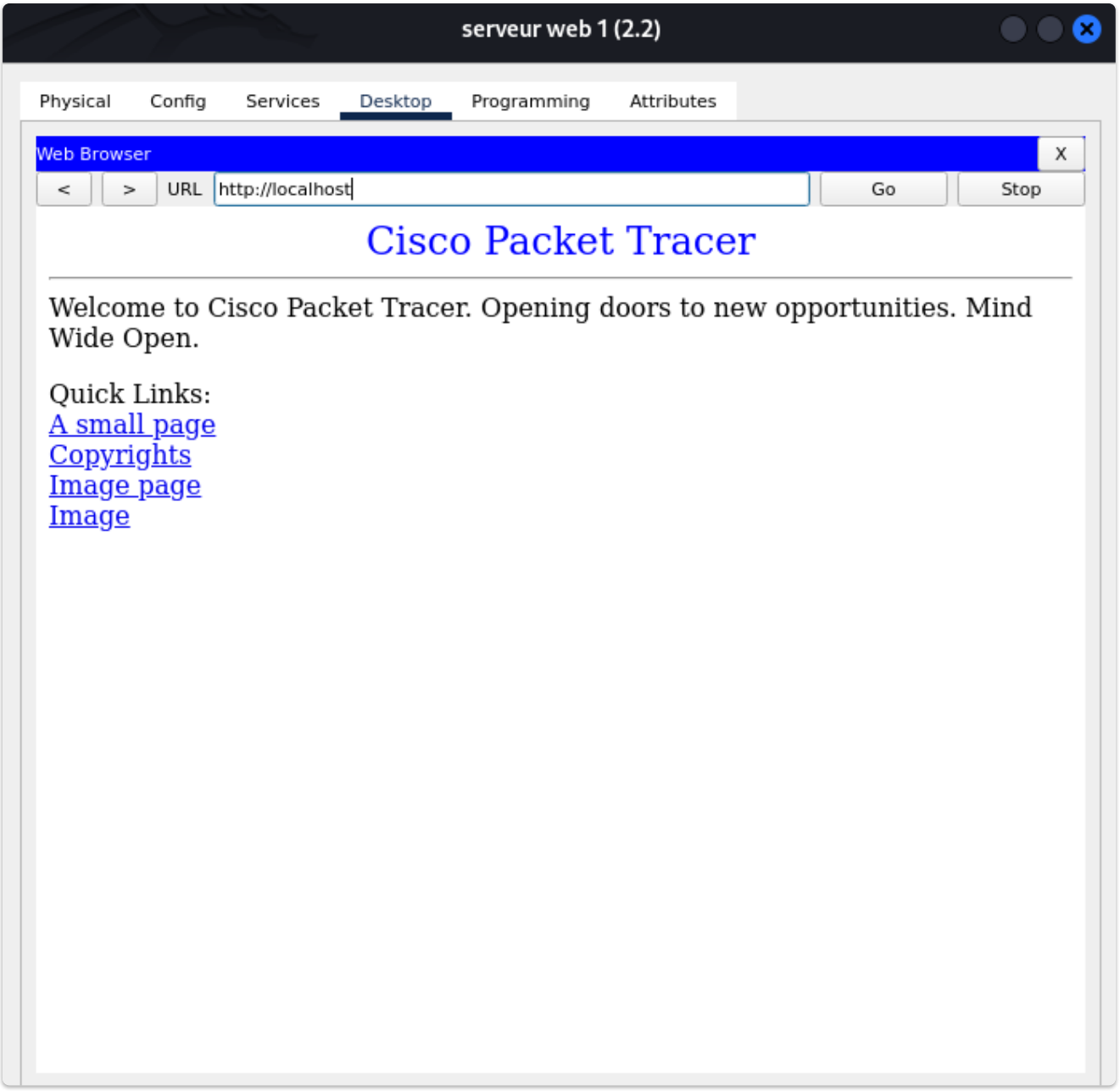
Le serveur web peut ping tout le monde, donc la configuration est à jour et fonctionnelle



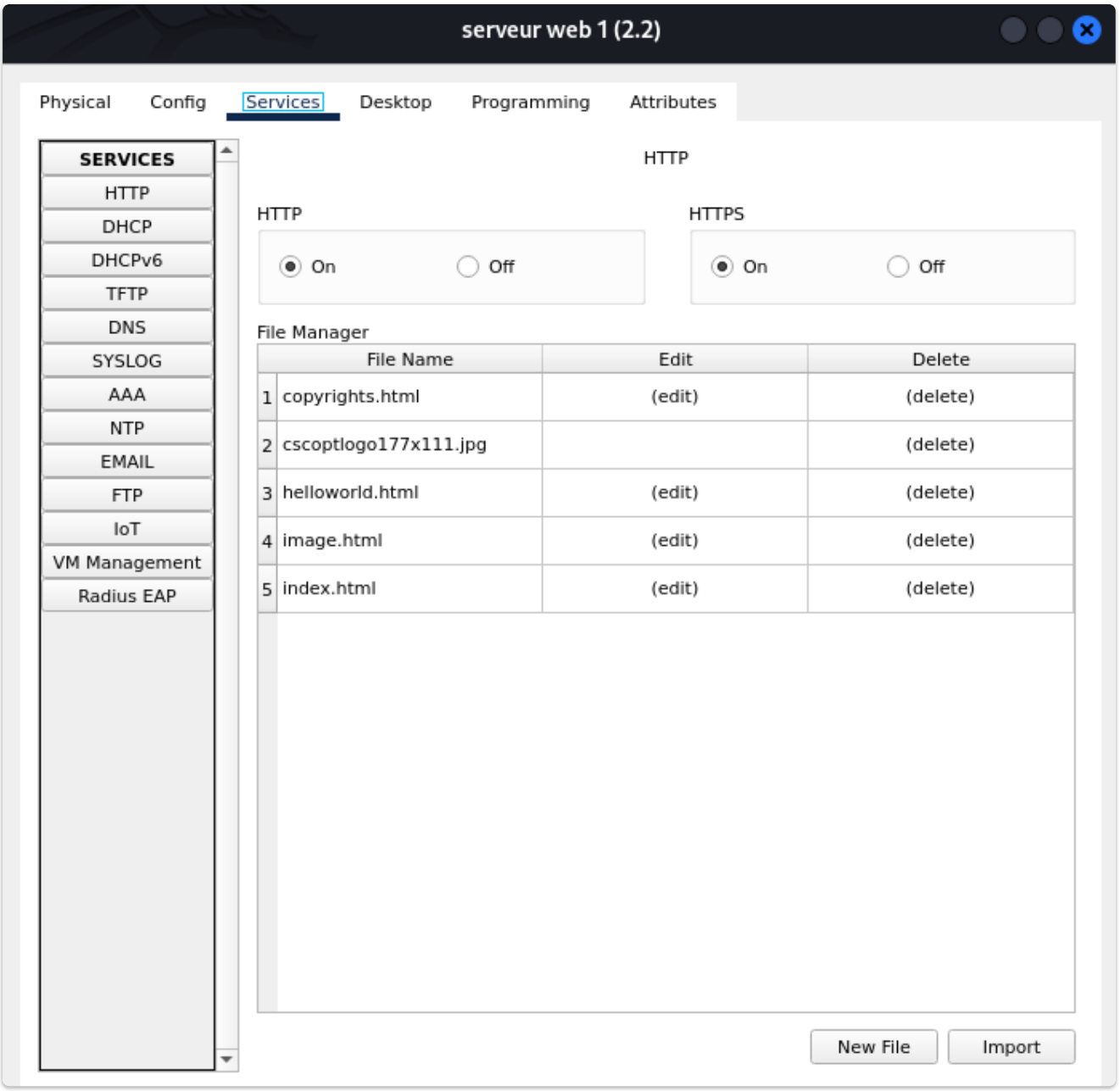
2.2. Serveur HTTP

1. Sur DMZ, vérifier que le serveur web est actif.

Le serveur web est effectivement actif, comme on peut le voir sur ces captures d'écran.



On peut également modifier les pages HTML depuis ce menu

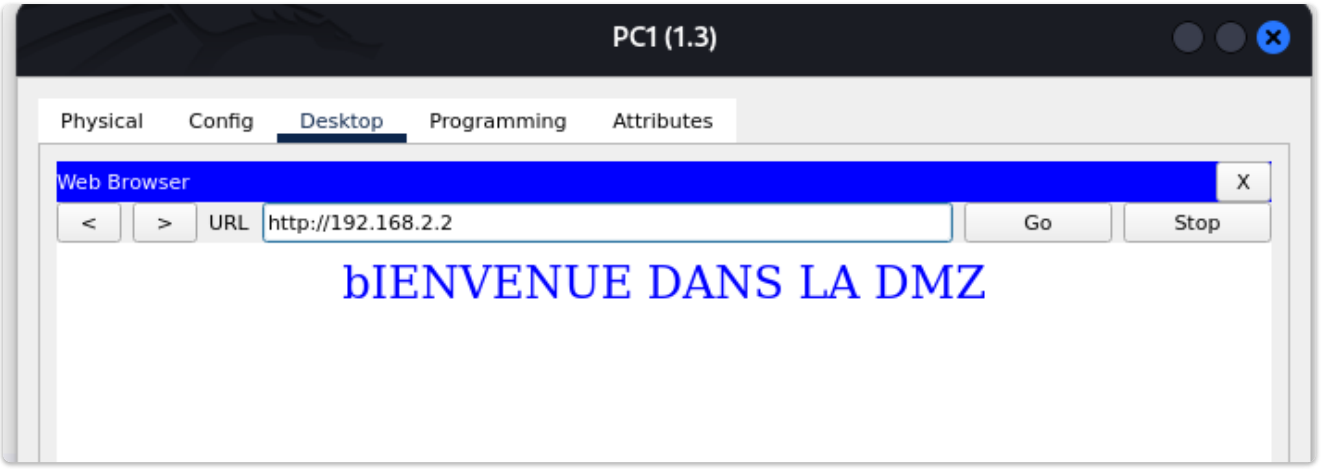


2. Editer les pages HTML d'accueils par défaut pour personnaliser le contenu

La page d'accueil par défaut a été modifiée en "Bienvenue dans la DMZ".
Nous avons modifié la page "*index.html*".

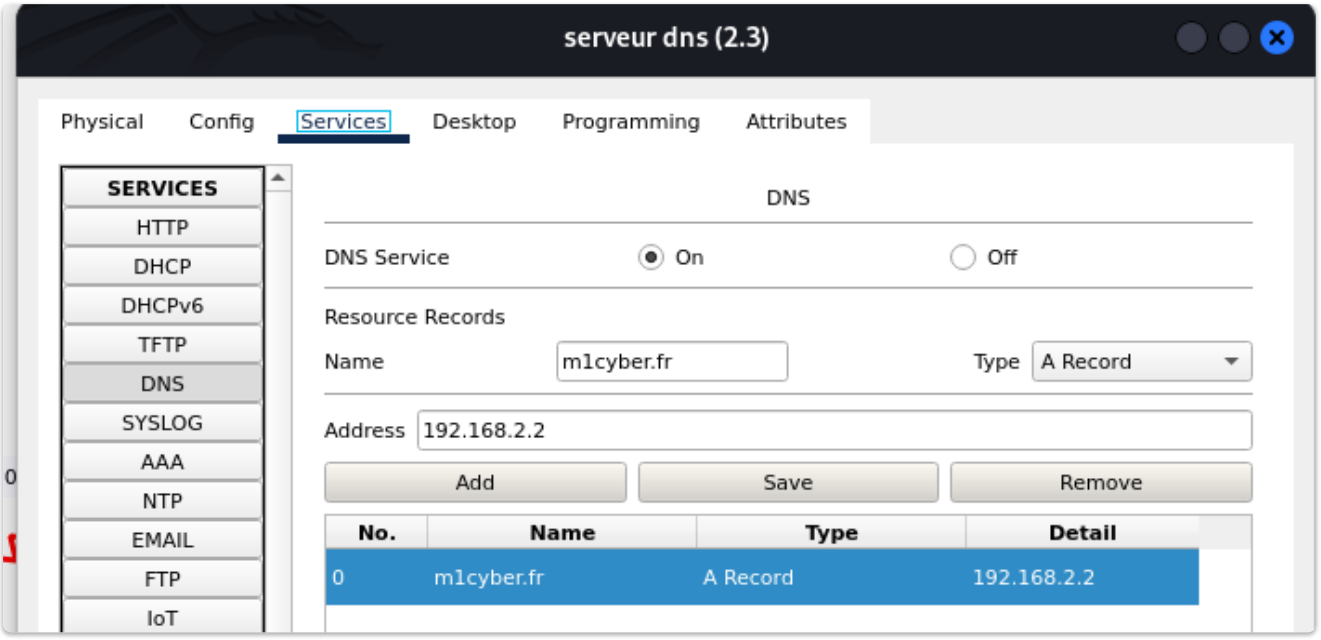
3. Sur LAN, lancer un browser web et accéder à http ://192.168.2.2.

Comme on peut le voir sur le LAN (PC1) on a accès à la page web depuis *http ://192.168.2.2*

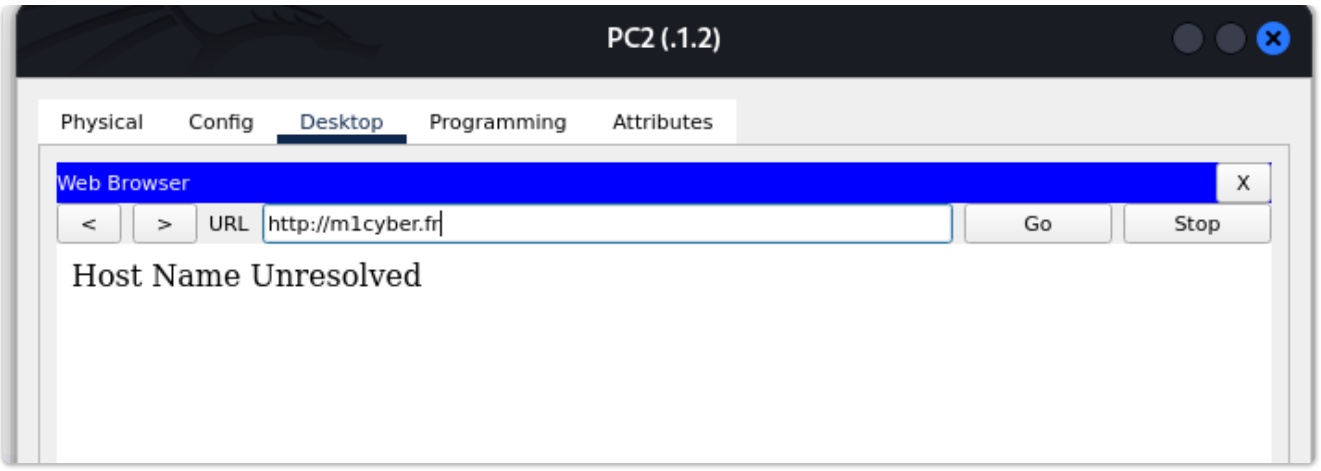


4. Changer le nom du serveur webserver1 par www.m1cyber.fr et lancer un browser web sur le LAN et accéder à http://www.m1cyber.fr. Pourquoi le browser affiche cette réponse ?

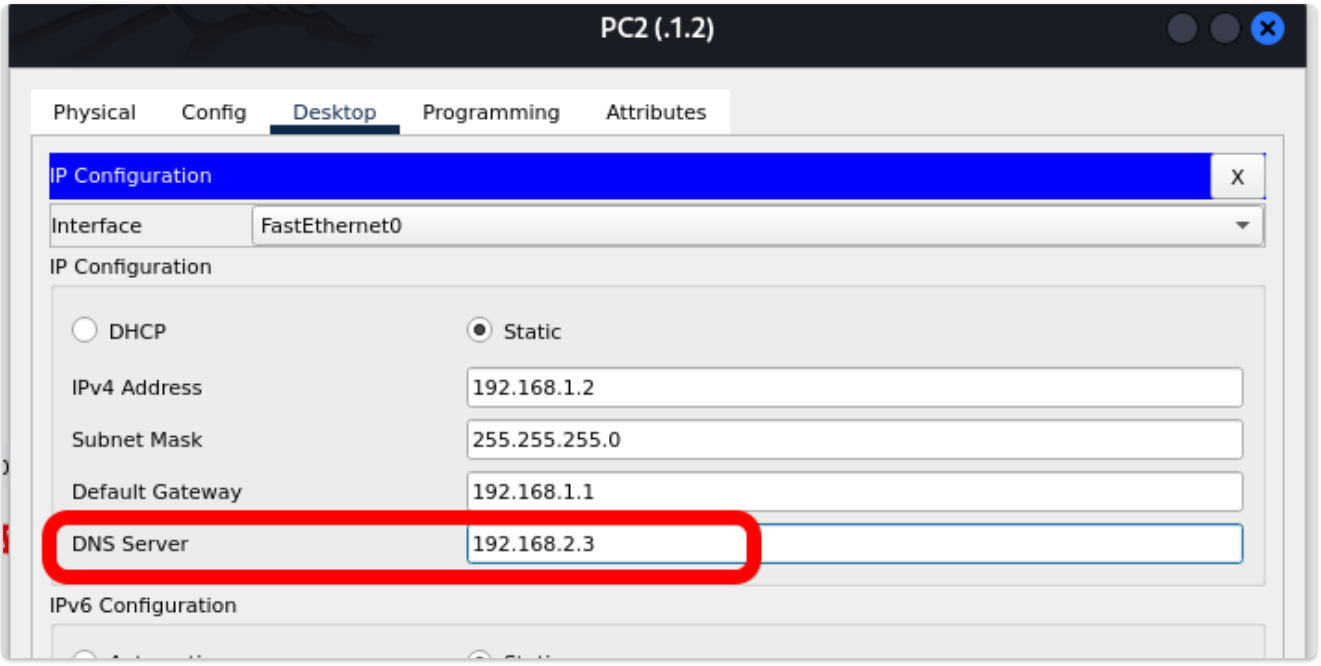
J'ai changer le nom du serveur dans le serveur DNS de la DMZ :



Mais on n'a toujours pas accès à la page web depuis le LAN, car en effet, nous n'avons pas encore spécifié de DNS pour les PC du LAN.



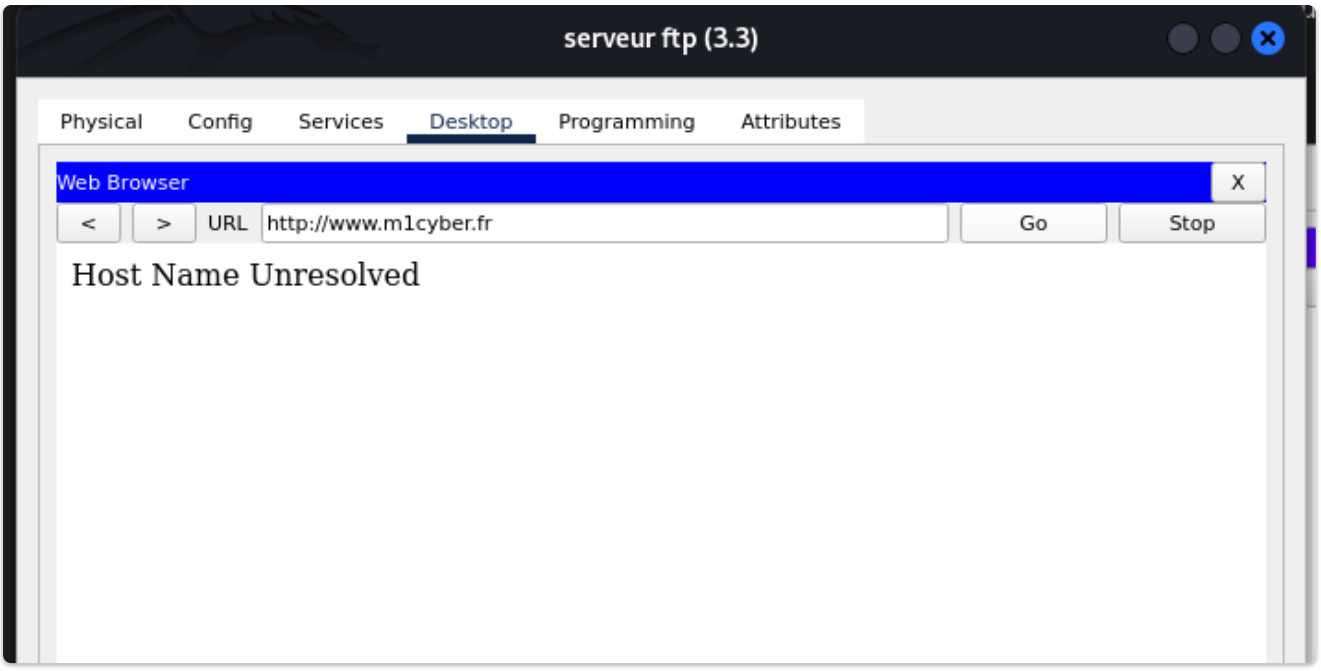
Cela est dû au fait que les PC ne sont pas configurés, en effet, nous n'avons pas encore spécifié de serveur DNS.
Une fois configurés de la manière suivante, on a accès au site web depuis l'URL http://www.m1cyber.fr/



Et maintenant on a bien accès depuis le LAN au site web

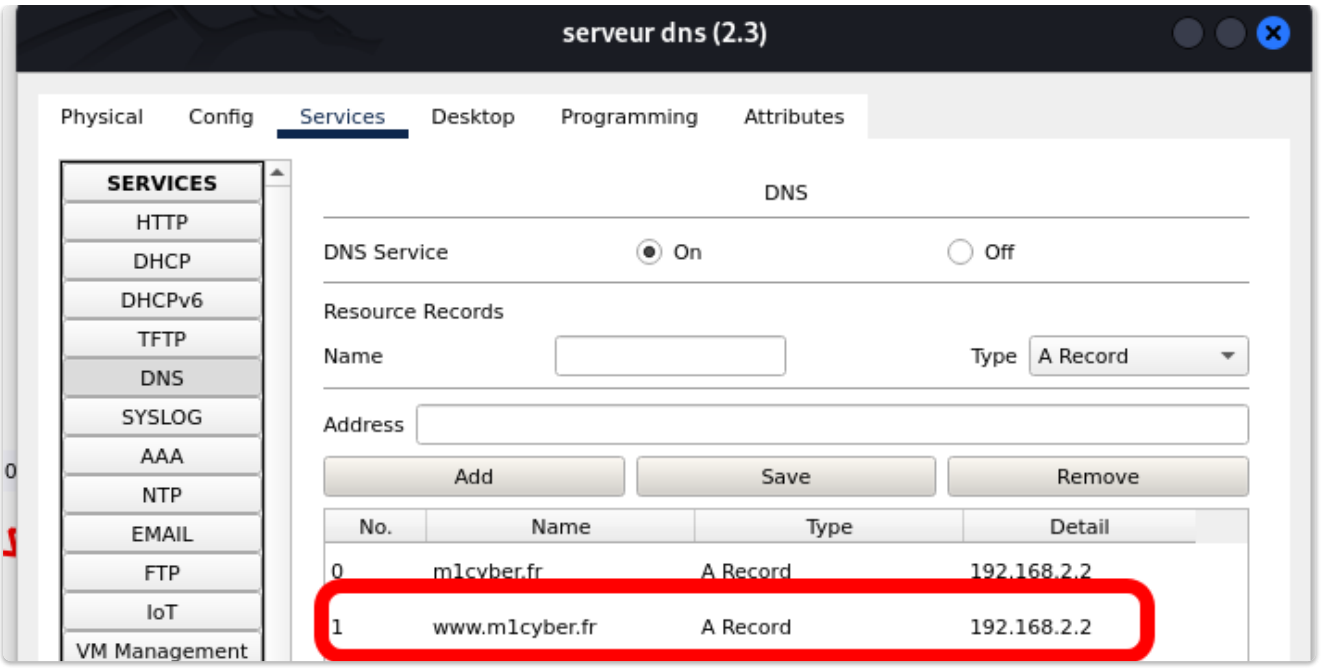
On a également accès au site web depuis le deuxième serveur web une fois configuré de la même manière.

Cependant, on n'a pas accès à http://www.m1cyber.fr/, car en effet, nous ne l'avons pas ajouté au DNS.



5. Configurez le service DNS sur le deuxième serveur afin que les ordinateurs puissent accéder à la page web http://www.m1cyber.fr en tapant une URL plutôt qu'en tapant son adresse IP.

Une fois ajouté au DNS on peut accéder à la page web en tapant http://www.m1cyber.fr


serveur dns (2.3)
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
m1cyber.fr
A Record
192.168.2.2
1
www.m1cyber.fr
A Record
192.168.2.2


serveur ftp (3.3)
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://www.m1cyber.fr
Go
Stop
bIENVENUE DANS LA DMZ

3. Configuration du filtrage

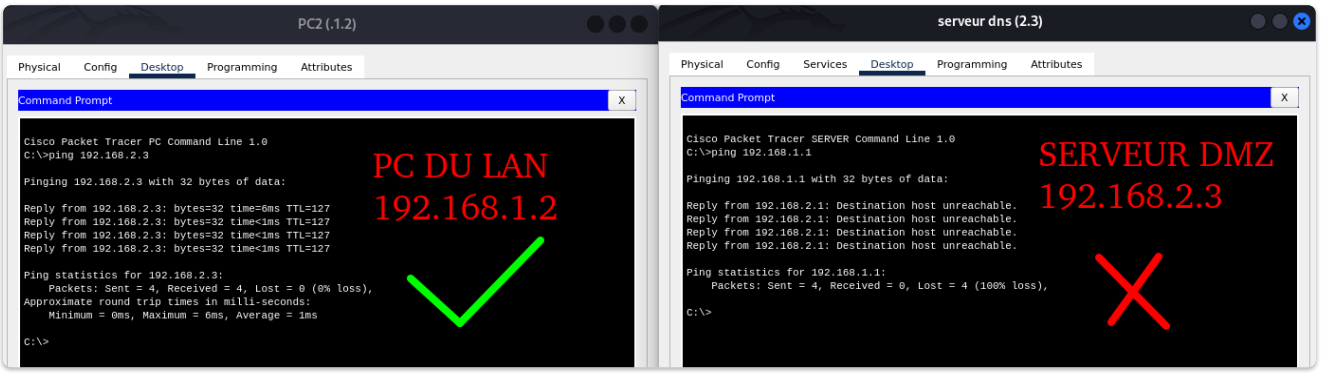
3.4. Configuration du filtrage LAN / DMZ

1. Configurer les ACL pour permettre aux machines du LAN de pinger celles de la DMZ (mais pas l'inverse)

Voici les commandes que nous avons mises dans le routeur 1 pour configurer les ACL afin de permettre aux machines du LAN de pinger celles de la DMZ (mais pas l'inverse).
nb : FastEthernet0/0 = interface DM.

```
Router(config)# access-list 101 deny icmp any 192.168.1.0 0.0.0.255 echo
Router(config)# access-list 101 permit ip any any
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 101 out
```

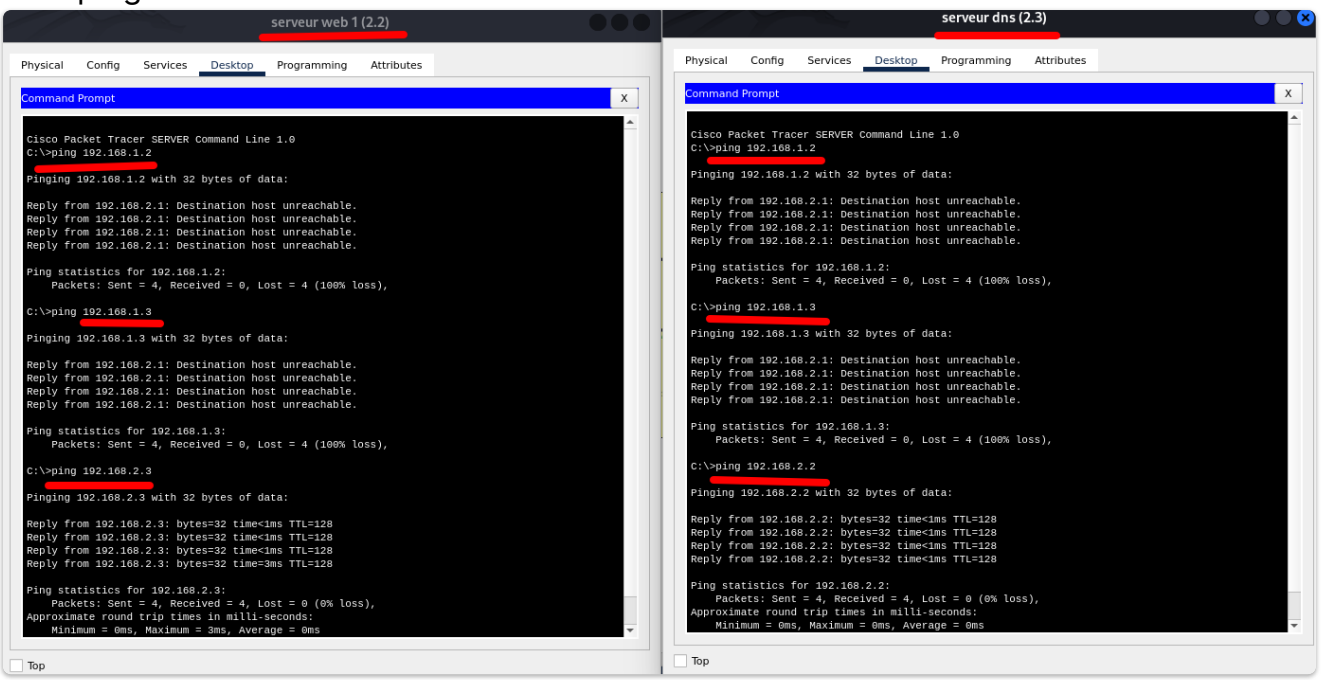
Nous empêchons tous les pings de sortir de la DMZ, mais on peut toujours pinger depuis le LAN



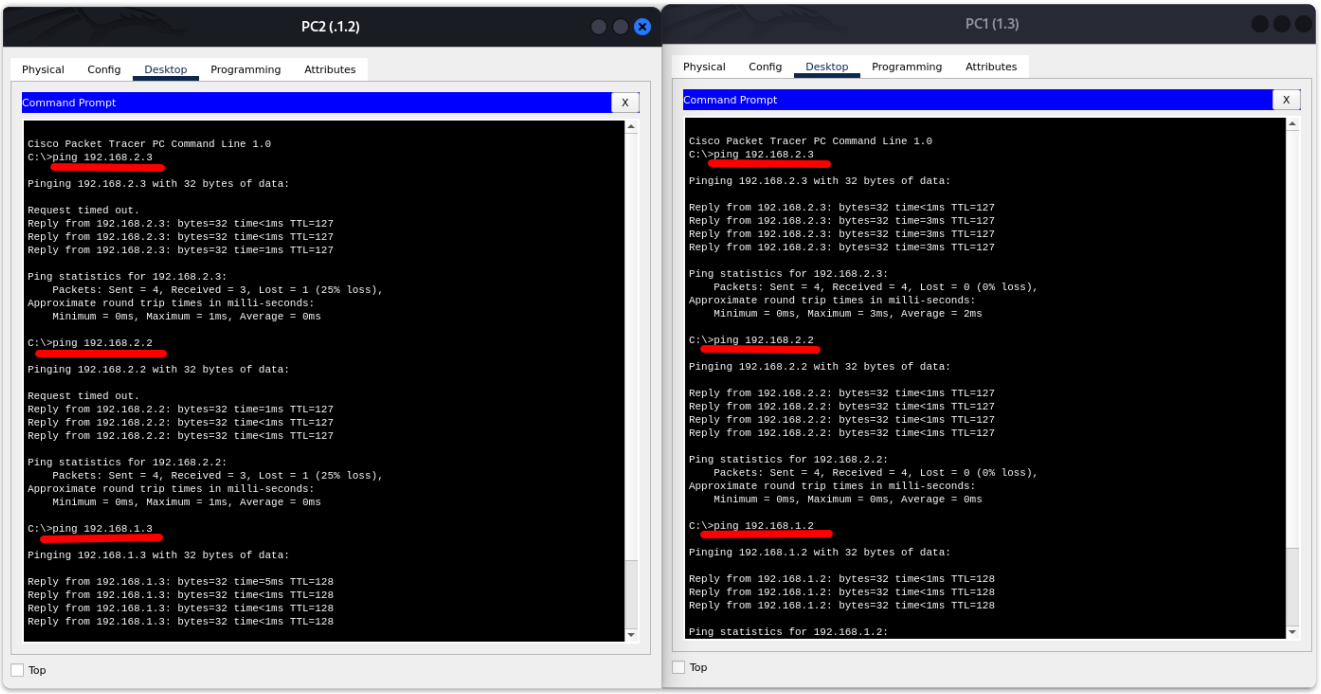
2. Valider par ping entre LAN, DMZ et Routeur, quelles sont les machines qui peuvent se pinger ou pas ?Vous pouvez représenter ceci par une matrice de flux que vous ferez évoluer en fonction du filtrage réalisé.

Comme on peut le voir, le *PC1* et le *PC2* du LAN (*192.168.1.0/24*) peuvent communiquer avec tout le monde, y compris du côté de la DMZ.

Test ping DMZ :



Test ping LAN:



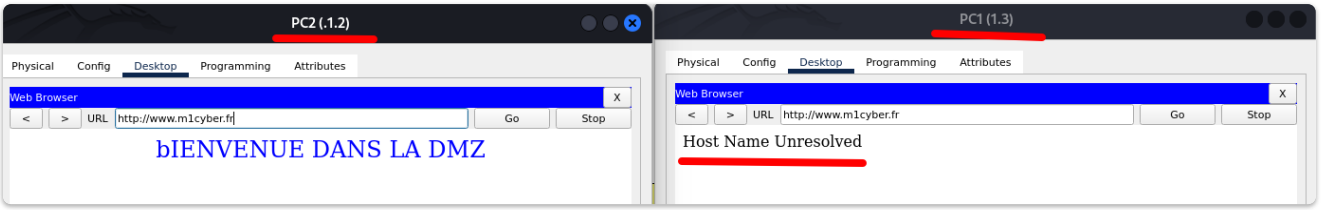
	LAN	DMZ
PC1 (*192.168.1.2*) LAN	Autorisé	Autorisé
PC1 (*192.168.1.3*) LAN	Autorisé	Autorisé
Serveur Web (*192.168.2.2*) DMZ	Refusé	Autorisé
Serveur DNS (*192.168.2.3*) DMZ	Refusé	Autorisé

3. Configurer des ACL pour empêcher les machines du LAN dont l'adresse ip est impaire de faire une résolution DNS.

Voici les commandes que l'on a fait :

```
Router(config)#access-list 100 deny udp 192.168.1.1 0.0.0.254 host
192.168.2.3 eq domain
Router(config)#access-list 100 permit ip any any
Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 100 in
```

Comme on peut le voir le PC0 (*192.168.1.2*) peut accéder au site grace au DNS, mais pas le PC1 (*192.168.1.3*)



Explication:

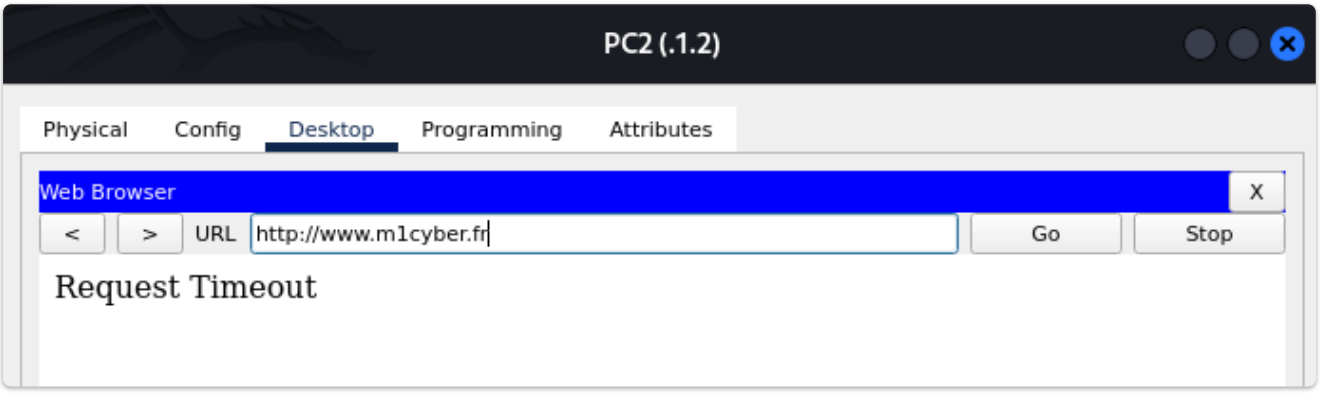
- `access-list 100 deny udp 192.168.1.1 0.0.0.254 host 192.168.2.3 eq domain`
  Cette commande bloque les requêtes DNS (192.168.2.3) sortantes provenant des adresses IP impaires du LAN vers le serveur DNS de la DMZ.
- `access-list 100 permit ip any any`
  Cette commande autorise tout autre trafic IP entre les réseaux.

4. Configurer les ACL pour que les machines du LAN puissent accéder à la DMZ uniquement en http. Qu'observez-vous ?

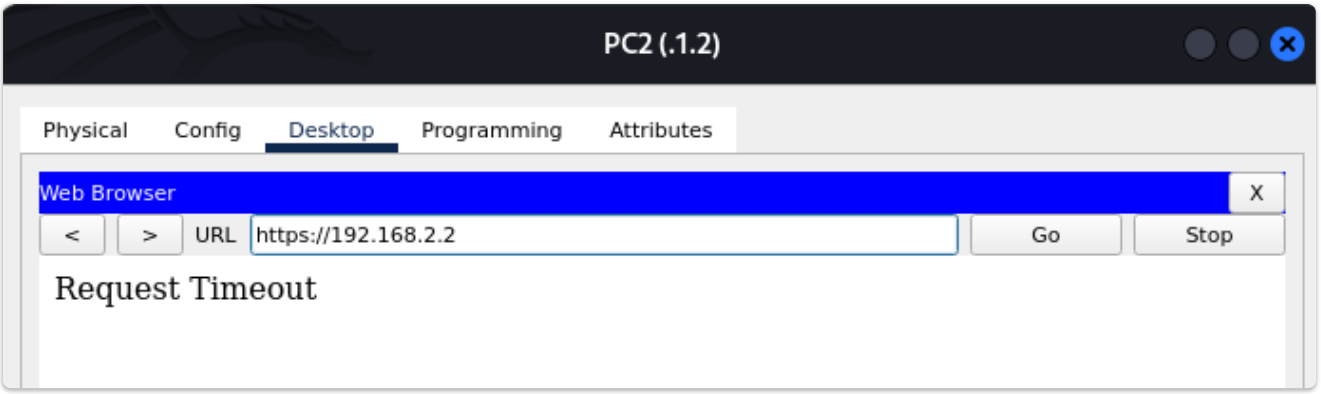
FastEthernet1/0 correspond à l'interface du LAN (*192.168.1.1*)

```
Router(config)#access-list 103 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255 eq 80
Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 103 in
```

On remarque que l'on n'a plus accès au DNS et que la seule manière d'accéder au site web est via IP, ce qui est logique car on a bloqué tout sauf HTTP (DNS bloqué également).



On a accès au site web via l'IP en HTTP mais pas en HTTPS.



5. Trouvez une ACL standard qui produit le même effet.

On obtient exactement le même résultat avec ces commandes :

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 deny any

Router(config)#interface FastEthernet1/0
Router(config-if)#ip access-group 1 in
```

6. Les machines de la DMZ ne doivent pouvoir initier aucune connexion

7. Valider avec le browser sur LAN

4. NAT / PAT

4.2. NAT et Filtrage du LAN vers Internet

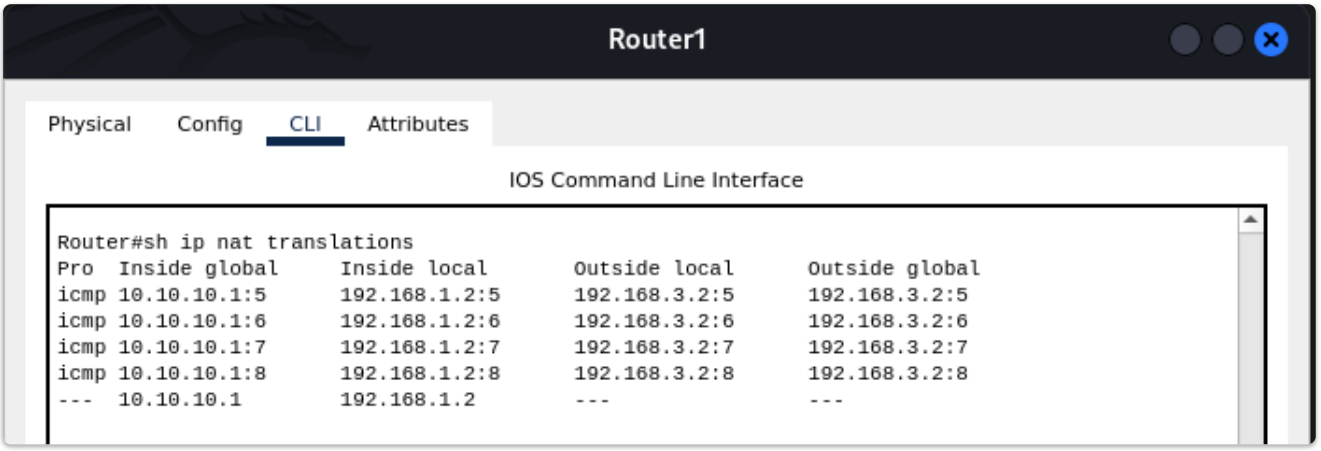
1. Donner la configuration du NAT pour que les machines du LAN puissent accéder à Internet

On va configurer le NAT manuellement pour le PC2 (*192.168.2.1*)

```
Router(config)#ip nat inside source static 192.168.1.2 10.10.10.1
...
Router(config)#interface FastEthernet1/0
Router(config-if)#ip nat inside
...
Router(config)#interface Serial2/0
Router(config-if)#ip nat outside
```

2. Valider par ping adresse IP de serveur web 2 sur le réseau Internet depuis le LAN et interpréter les échanges NAT en cours.

Lorsque l'on fait un ping du PC2 au Serveur Web 2, on peut voir que le passage de l'IP 192.168.1.2 à 10.10.10.1 a bien eu lieu, avec la commande `sh ip nat translations`



Ces résultats montrent les traductions NAT en cours sur le routeur. Ils indiquent que les paquets ICMP provenant de l'hôte interne *192.168.1.2* sont traduits en utilisant l'adresse IP *10.10.10.1* lorsqu'ils sortent du réseau local vers l'extérieur.

3. Donner la configuration de NAT pour transférer les requêtes HTTP qui arrivent sur le port 81 de l'interface du Routeur 2 vers le port 80 de serveur web 2 sur le réseau Internet.

4. Pour valider cette configuration lancer sur LAN un browser web et accéder à http://192.168.3.2:81.

On configure le NAT en précisant les interfaces :

```
Router(config)#interface FastEthernet0/0
Router(config-if)# ip nat inside

....
Router(config)#interface Serial2/0
Router(config-if)# ip nat outside

....

ip nat inside source static tcp 192.168.3.2 80 192.168.3.2 81
```

Le port forwarding fonctionne :

5. Configurer les ACL pour empêcher les machines du réseau LAN de droite d'utiliser ftp sur le réseau Internet. Tester et valider cette configuration.

Voici les commande pour empêcher les machines du réseau LAN de droite d'utiliser FTP (*FastEthernet1/0 = 192.168.1.1*)

```
Router(config)#access-list 104 deny tcp 192.168.1.0 0.0.0.255 any eq ftp
Router(config)#access-list 104 permit tcp any any

...

Router(config)#interface FastEthernet1/0

Router(config-if)#ip access-group 104 in

Router(config-if)#
```

Et comme on peut voir on ne peut plus accéder depuis le PC2 LAN (*192.168.1.2*) au serveur FTP *192.168.3.2*