RAPPORT SAE 21

ABDALLAH Johan
ANTY Anne-Juliette
DESMET Mathis

Sommaire

1. Introduction

Objectif SAÉ (suivant Programme pédagogique National) : Le professionnel R&T peut être sollicité pour construire et mettre en place le réseau informatique d'une « petite » entreprise. L'objectif est alors de répondre aux besoins de commutation, de routage, de services réseaux de base et de sécurité formulés pour la structure. Ce réseau s'appuie sur des équipements et des services informatiques incontournables mais fondamentaux pour fournir à la structure un réseau fonctionnel et structuré.

Le travail s'articule en 4 grandes étapes :

- Construction du cœur du réseau interne (commutation, VLANs, MLS)
- Intégration des services réseau internes (DHCP, DNS) et de la sécurité (pare-feu ASA)
- Mise en place de la DMZ et des mécanismes de traduction d'adresses (NAT)
- Connexion au réseau public et configuration du routage dynamique (EIGRP)

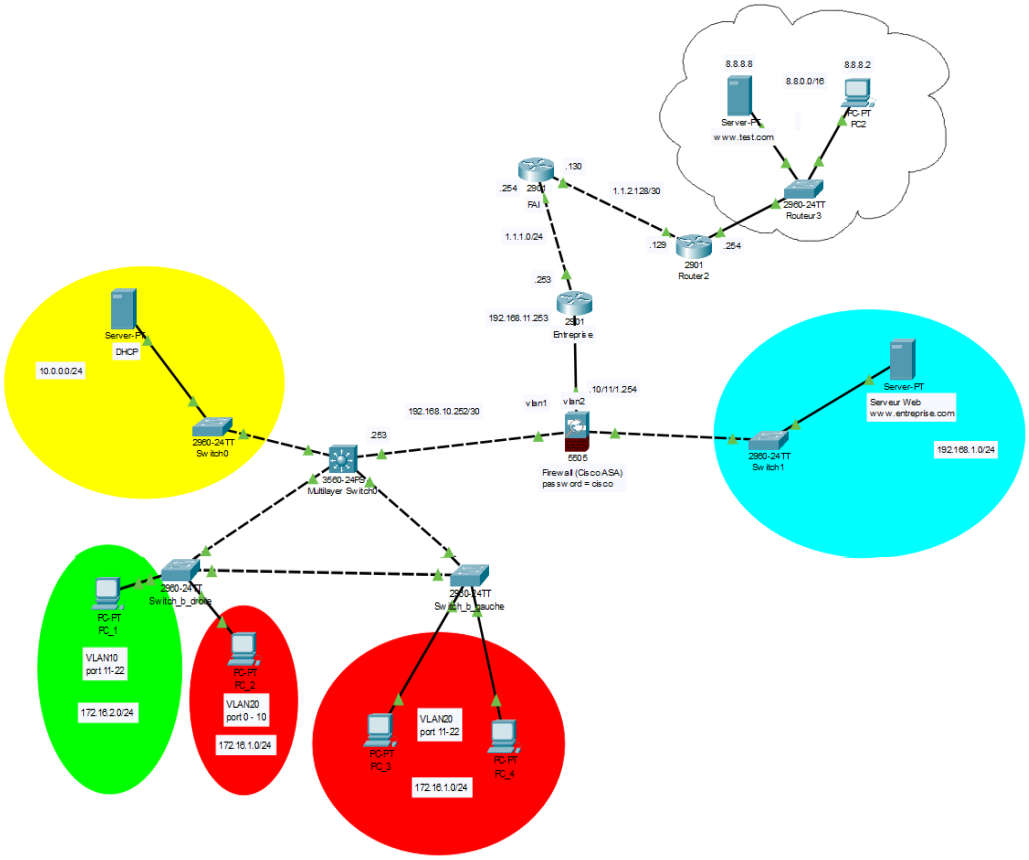
Ce rapport documente les étapes de conception, les choix d'adressage, les configurations mises en œuvre et les tests fonctionnels réalisés.

2. Cahier des charges

L'objectif est de construire un réseau d'entreprise typique d'une PME avec :

- Un cœur de réseau comportant un multi-layer switch (MLS), appelé switch de niveau 3 qui est capable de switcher ou router suivant les besoins
- Ce MLS sert plusieurs VLANs :
  - Deux VLANs correspondant à deux groupes de travail dans l'entreprise (par exemple service RH et service ingénierie)
  - Le VLAN des serveurs internes
- Ce MLS est ensuite raccordé à un pare-feu (CISCO Asa) qui offre les services ci-après :
  - Il permet les machines sur Internet d'accéder au serveur Web de la DMZ uniquement sur les ports 80 et 443 en TCP dans les deux cas
  - Il contrôle que les paquets reçus par les clients internes correspondent à des connexions initiées par les clients internes.
- Un FAI qui :
  - fournit un range d'adresse publique au routeur de bordure de l'entreprise etoffre les services de NAT :
    - NAT (overloading en langage CISCO) pour les machines des VLAN 10 et 20 lorsqu'elles accèdent à Internet
    - NAT statique pour le serveur Web de la DMZ lorsqu'on y accède depuis l'extérieur.
  - s'interconnecte avec un autre réseau dans lequel se trouvent un serveur Web, pour tester que les machines internes de l'entreprise, en adressage privé, peuvent accéder à des ressources « sur Internet » et un client pour tester l'accès au serveur Web de l'entreprise qui est dans la DMZ.

3. Schéma global du réseau



4. Plan d’adressage IP complet

Réseau / VLAN	Adresse réseau	Masque	Passerelle (MLS ou ASA)	Plage DHCP (si utilisé)	Utilisation
VLAN 10 – RH	172.16.2.0	/24	172.16.2.254	172.16.2.11-22	Postes RH
VLAN 20 – Ingénierie	172.16.1.0	/24	172.16.1.254	172.16.20.1-22	Postes Ingénierie
VLAN Serveurs	10.0.0.0	/24	10.0.0.254	Static	Serveurs internes (DNS, DHCP)
DMZ	192.168.1.0	/24	192.168.1.254 (ASA)	Staticc	Serveur Web public
MLS <-> ASA	192.168.10.252	/30	192.168.10.253 (MLS)	-	Lien interne sécurisé
ASA <-> Routeur Entreprise	192.168.11.252	/30	192.168.11.254 (ASA)	-	Vers FAI
Réseau public (FAI)	1.1.1.0	255.255.255.0	1.1.1.254 (routeur FAI)	-	NAT statique, internet coté FAI
Lien FAI <-> internet	1.1.2.128	/30	1.1.2.129	-	Interconnexion vers test.com
Réseau test.com	8.8.0.0	/16	8.8.8.254 (Routeur externe)	Static	Serveur externe + client test

Justification des choix :

- Les VLANs internes utilisent des adresses privées en 172.16.0.0/12 pour distinguer RH et Ingénierie, avec une passerelle sur le MLS et un masque /24 pour 254 hôtes possibles.
- Le VLAN serveurs utilise un bloc 10.0.0.0/8, souvent réservé aux réseaux internes critiques.
- Les liaisons point-à-point (MLS ↔ ASA et ASA ↔ FAI) utilisent des sous-réseaux en /30, parfaits pour des liens à 2 hôtes.
- La DMZ est isolée dans le réseau 192.168.1.0/24 et gérée par l’ASA, avec NAT statique vers l’IP publique 1.1.1.253.
- Le réseau public FAI simule Internet et interagit avec un réseau de test 8.8.0.0/16 pour valider les accès depuis/vers l’extérieur.

5. Etape 1 – Construction de cœur de réseau avec les switches d'accès et le Multi-layer switch

5.1. Création des VLANs

Trois VLANs ont été créés pour organiser logiquement le réseau interne :

VLAN	Nom	ID	Réseau IP	Utilisation
RH	VLAN 10	10	172.16.2.0/24	Postes RH
Ingénierie	VLAN 20	20	172.16.1.0/24	Postes Ingénierie
Serveurs	VLAN 30	30	10.0.0.0/24	Serveurs internes (DNS, DHCP)

Chaque switch d'accès a été configuré pour affecter ses ports aux VLANs correspondants :

exemple pour switch d'accès droit

```
Sbdroite>en
Sbdroite#configure terminal
Sbdroite(config)#hostname Sbdroite
Sbdroite(config)#Vlan 20
Sbdroite(config-vlan)#exit
Sbdroite(config)#interface range FastEthernet0/11 – 22
Sbdroite(config-range)#switchport mode access
Sbdroite(config-range)#switchport access vlan 20
Sbdroite(config-range)#exit
Sbdroite(config)#interface FastEthernet0/24
Sbdroite(config-if)#switchport mode trunk
Sbdroite(config-if)#switchport trunk allowed vlan 20
Sbdroite(config-if)#switchport trunk encapsulation dot1q
Sbdroite(config-if)#exit
```

Dans cette partie on a configuré des switchs, plus précisément ce sont les commandes du switch droit la commande interface range port nom_interface – nom_interface sert à mettre des vlan sur tous les ports choisis. La commande

Sbdroite(config-if)#switchport trunk allowed vlan 20, sert à fais passer le vlan 20 dans l'interface où cette commande a était mise.

5.2. Configuration du MLS

Le MLS agit en **switch de niveau 3**, avec des **interfaces virtuelles (SVI)** configurées pour chaque VLAN, assurant le routage inter-VLAN via la commande ip routing.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname MLS
MLS(config)#spanning-tree vlan 1 root primary
MLS(config)#Vlan 20
MLS(config-vlan)#exit
MLS(config)#Vlan 10
MLS(config-vlan)#exit
MLS(config)#interface FastEthernet0/1
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
MLS(config-if)#switchport trunk allowed vlan 10-20
MLS(config-if)#exit
MLS(config)#interface FastEthernet0/2
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
MLS(config-if)#switchport trunk allowed vlan 20
MLS(config-if)#exit
MLS(config)#ip routing
MLS(config)#interface vlan 10
MLS(config-if)#ip address 172.16.2.254 255.255.255.0
MLS(config-if)#no shutdown
MLS(config-if)#exit
MLS(config)#interface vlan 20
MLS(config-if)#ip address 172.16.1.254 255.255.255.0
```

MLS(config-if)#no shutdown

MLS(config-if)#exit

MLS(config)#vlan 30

MLS(config-vlan)#exit

MLS(config)#interface vlan 30

MLS(config-if)#ip address 10.0.0.254 255.255.255.0

MLS(config-if)#no shutdown

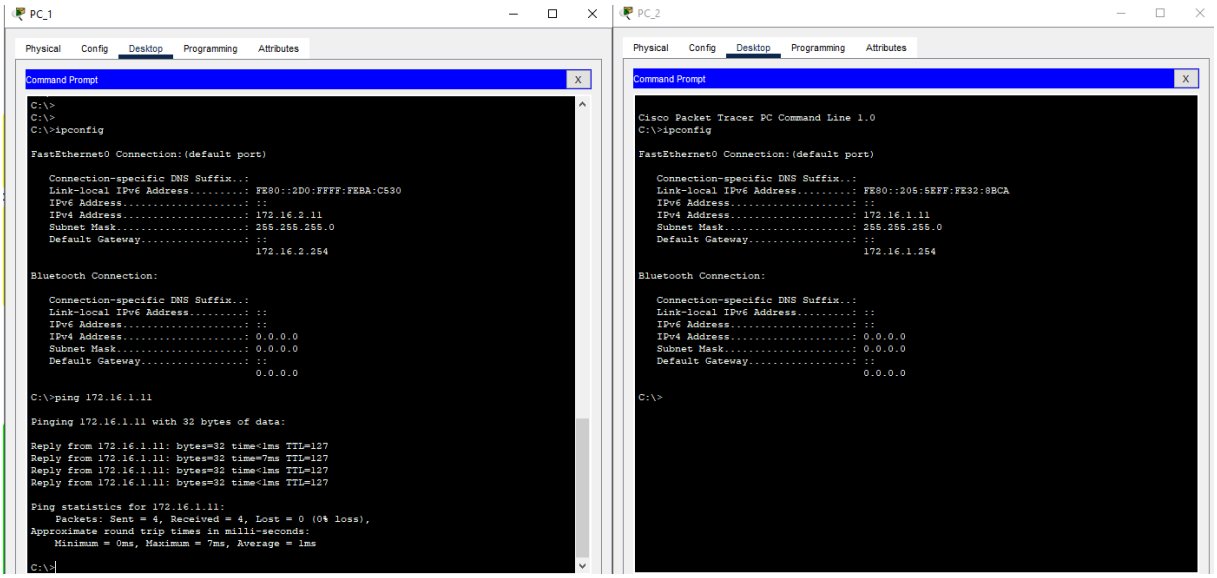
MLS(config-if)#exit

Dans cette partie on a configuré un switch Multilayer. Les adresses IP peuvent être seulement configuré sur des vlan. La commande qui permet de créer un vlan est (config)#vlan [numéro]. Pour mettre des adresses IP sur des interfaces, il faut seulement entrer dans l'interface est mettre la commande switchport access vlan [numéro]. La commande ip routing permet d'activer le routage inter vlan ce qui signifie que n'importe quelle vlan peut discuter entre elle. La commande spanningtree vlan 1 root primary, cette commande sert à mettre ce switch multilayer à activer le mode routage. Ces commandes servent MLS(config-if)#switchport trunk encapsulation dot1q, MLS(config-if)#switchport mode trunk, MLS(config-if)#switchport trunk allowed vlan 20 a faire passer la vlan à travers le réseau.

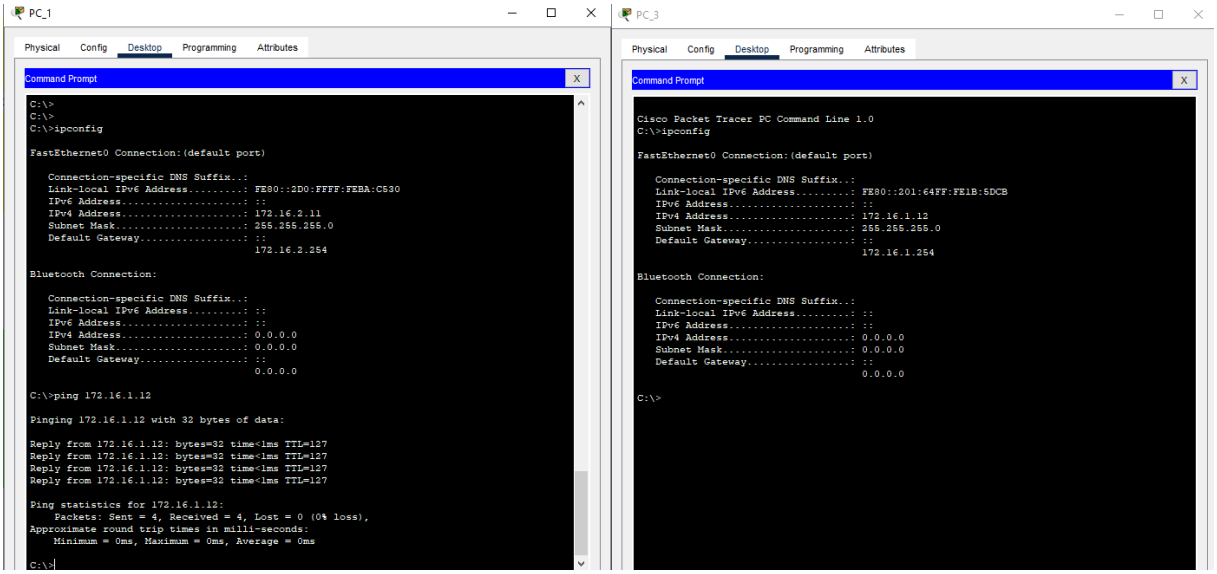
5.3. Tests de connectivité

Des tests de ping ont été réalisé pour valider la connectivité.

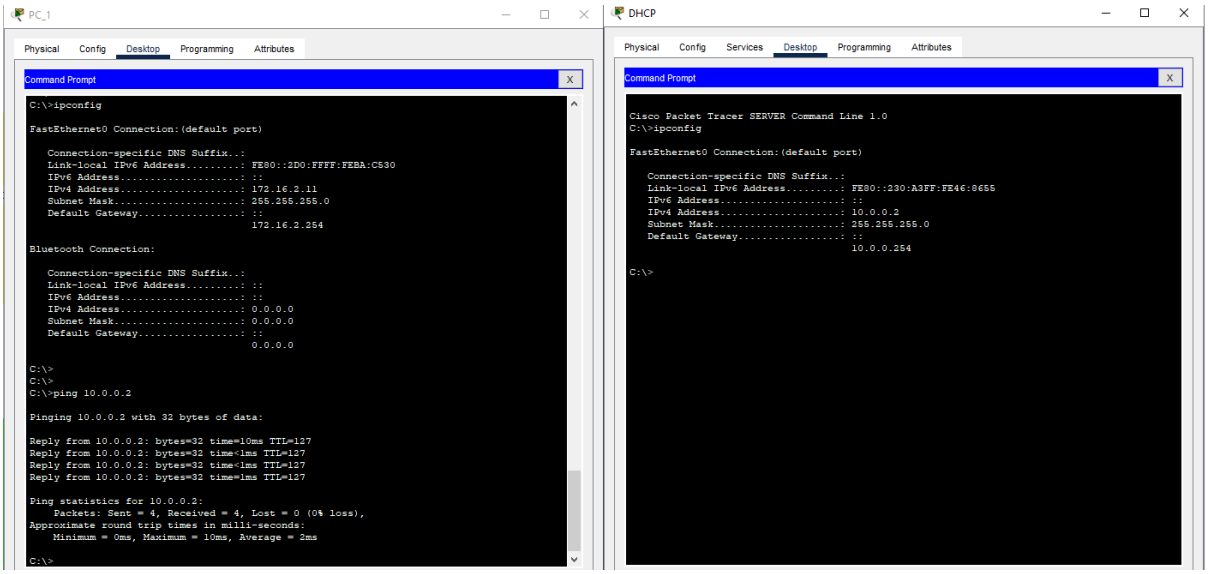
- PC1 (VLAN 10) → PC2 (VLAN 20) Ping OK (intra-VLAN) ✅



- PC1 (VLAN 10) → PC3 (VLAN 20) Ping OK (inter-VLAN) ✅



- PC1 (VLAN 10) → Serveur DHCP (VLAN 10) Ping OK (intra-VLAN) ✅



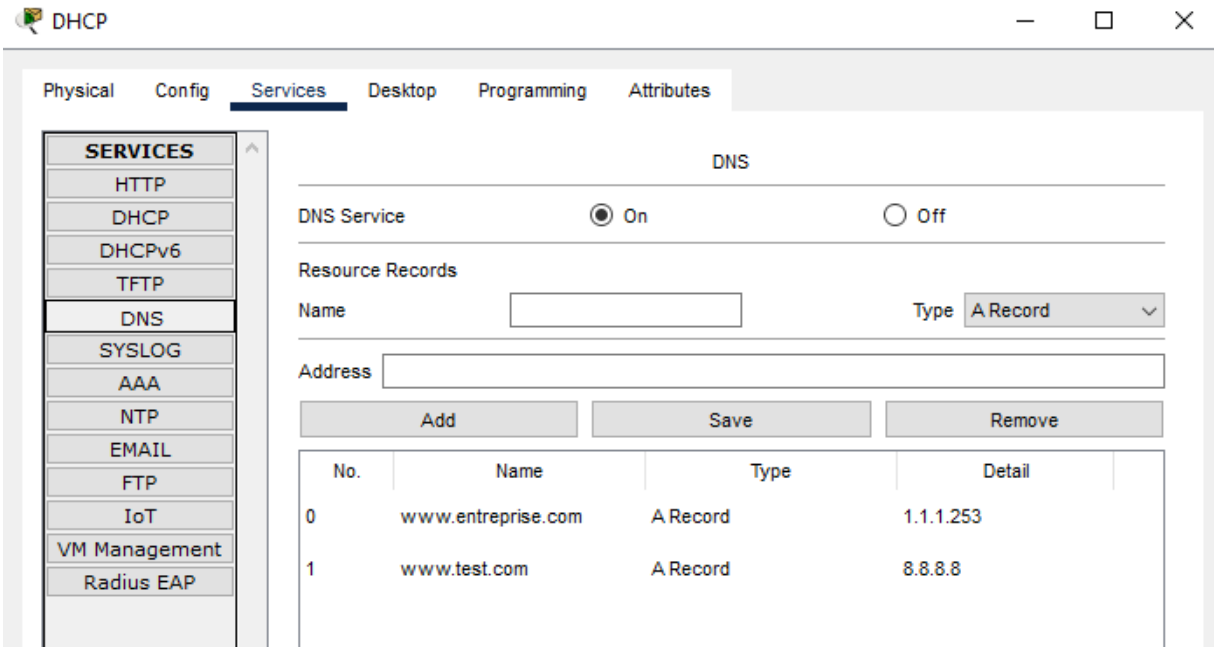
6. Etape 2 – Ajout de l'ASA et du service DHCP

6.1. Configuration du DNS interne

Le serveur DNS est placé dans le VLAN 30 (serveurs) et possède une IP statique dans la plage 10.0.0.0/24.

Deux enregistrements de type A ont été créés :

Nom de domaine	IP associée	But
www.test.com	8.8.8.8	Accès vers l'extérieur
www.entreprise.com	1.1.1.253	Accès public DMZ

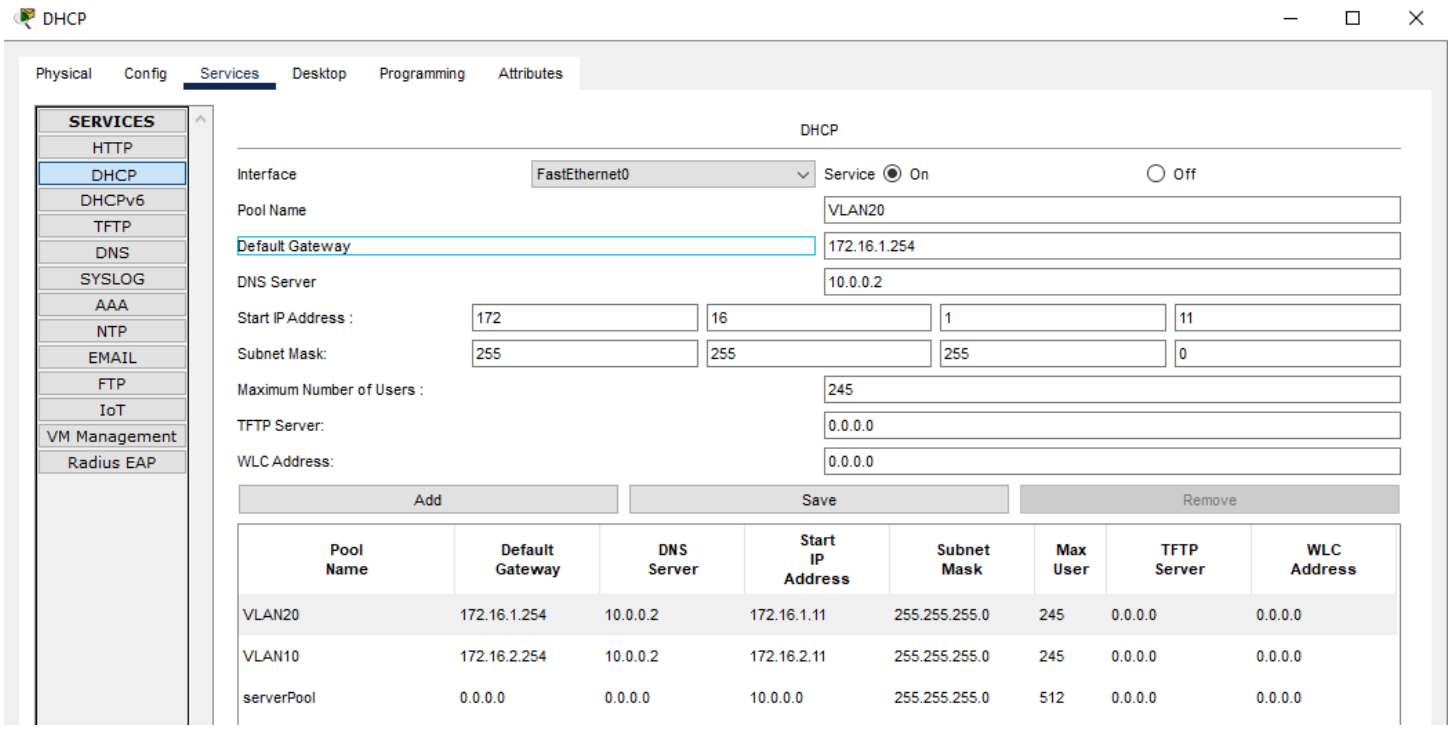


6.2. Mise en place du serveur DHCP

Le serveur DHCP est également situé dans le VLAN 30, à l'adresse 10.0.0.2.

Deux pools ont été créés, chacun dédié à un VLAN :

VLAN	Pool DHCP	Plage IP attribuée	Gateway	DNS
VLAN 10	VLAN10	172.16.2.11-22	172.16.2.254	10.0.0.2
VLAN 20	VLAN20	172.16.1.1-22	172.16.1.254	10.0.0.2



6.3. Configuration sur le nouveau switch et le MLS

Pour permettre aux clients des VLANs 10 et 20 de recevoir une IP via un serveur DHCP situé dans un autre VLAN, les interfaces VLAN sur le nouveau switch et le MLS ont été configurées avec la directive suivante :

Configuration du switch pour ces deux serveurs

Sbdroite>en

Sbdroite#configure terminal

Sbdroite(config)#Vlan 30

Sbdroite(config-vlan)#exit

Sbdroite(config)#interface range FastEthernet0/1 – 24

Sbdroite(config-range)#switchport mode access

Sbdroite(config-range)#switchport access vlan 30

Sbdroite(config-range)#exit

Dans cette partie on a configuré un autre switch comme on fait dans l'étape 1.

Configuration du MLS

Sbdroite(config)#interface FastEthernet0/3

Sbdroite(config-range)#switchport mode access

Sbdroite(config-range)#switchport access vlan 30

Sbdroite(config-range)#exit

MLS(config)#interface vlan 20

MLS(config-if)#ip helper-address 10.0.0.2

MLS(config-if)#no shutdown

MLS(config-if)#exit

MLS(config)#interface vlan 10

MLS(config-if)#ip helper-address 10.0.0.2

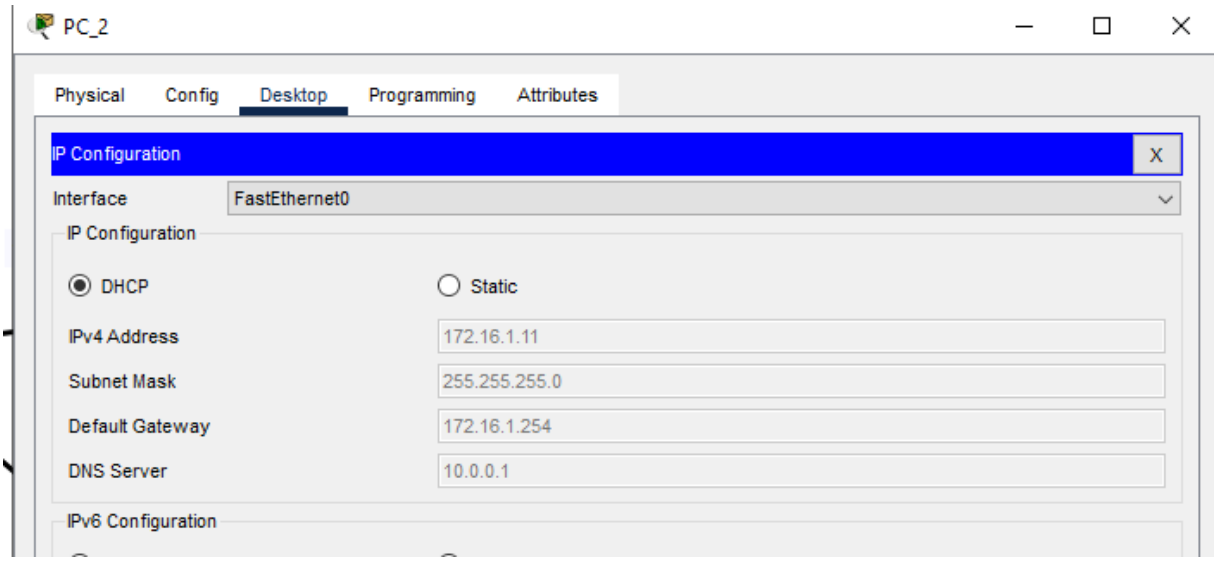
MLS(config-if)#no shutdown

MLS(config-if)#exit

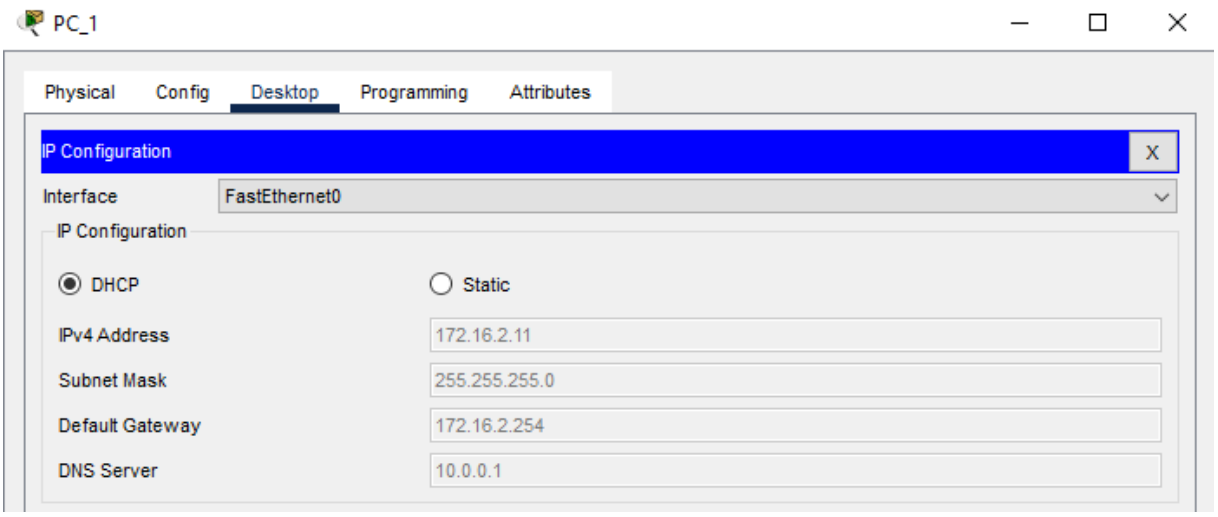
Dans cette partie on a configuré le MLS de telle sorte à faires les requêtes DHCP pour attribuer une adresse à chaque machine des vlan 10 et vlan 20. La commande ip-helper sert à rediriger le flux des requêtes DHCP vers un serveur DCHP pour que ces machines puissent avoir une machine afin qu'elle puisse discuter dans le réseau.

6.4. Configuration sur les PC

Adresse PC2 du VLAN 20 :



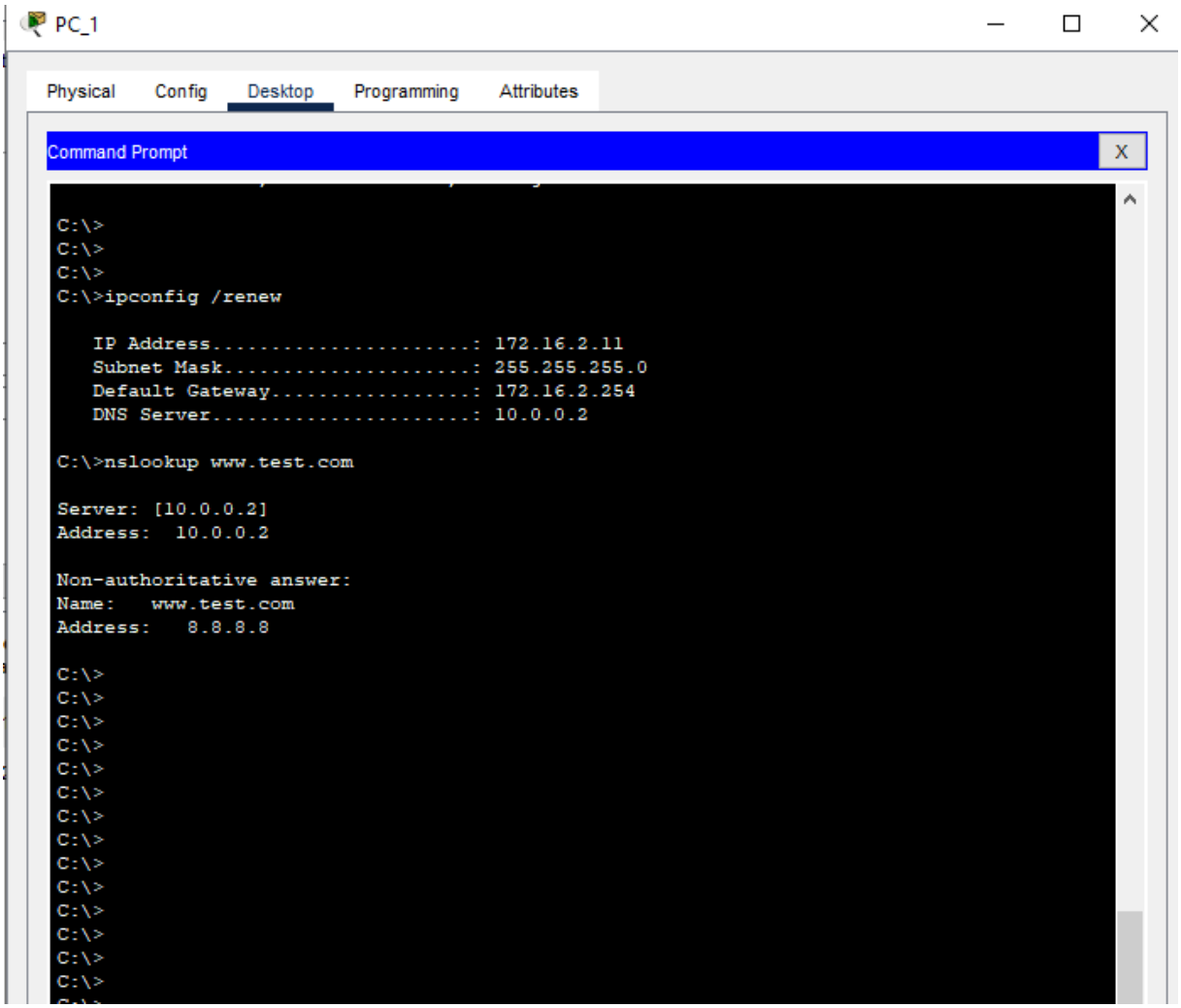
Adresse PC1 du VLAN 10 :



6.5. Tests fonctionnels

Les PC de chaque VLAN reçoivent bien leur adresse IP automatiquement.

Testons maintenant les domaines depuis le PC1 :

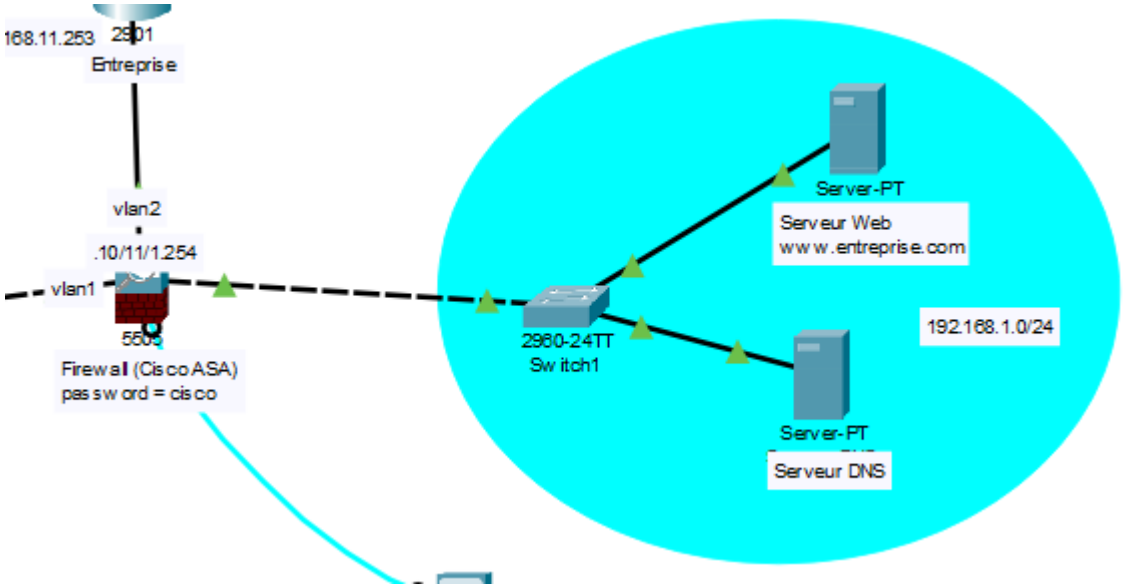


Bonnes résolutions IP.

7. Etape 3 – Ajout de la DMZ et du routeur du FAI

7.1. Mise en place de la DMZ

La DMZ est une zone tampon entre l'intérieur du réseau et Internet. Elle héberge le serveur Web public de l'entreprise.



7.2. Configuration complète de l'ASA

Configuration de l'ASA5505 :

```
ASA#sh run
: Saved
:
ASA Version 8.4(2)
!
hostname ASA
domain-name ciscosecurity.com
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
switchport access vlan 3
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
```

```
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.10.254 255.255.255.252
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.11.254 255.255.255.252
!
interface Vlan3
no forward interface Vlan1
nameif DMZ
security-level 50
ip address 192.168.1.254 255.255.255.0
!
webvpn
object network obj_any_inside
subnet 172.16.0.0 255.240.0.0
nat (inside,outside) dynamic interface
object network obj_web_dmz
host 192.168.1.10
nat (DMZ,outside) static 1.1.1.253
!
route inside 172.16.2.0 255.255.255.0 192.168.10.253 1
route inside 172.16.1.0 255.255.255.0 192.168.10.253 1
route outside 0.0.0.0 0.0.0.0 192.168.11.253 1
!
access-list trafic1 extended permit tcp any host 192.168.1.80 eq www
access-list trafic1 extended permit tcp any host 192.168.1.80 eq 443
access-list trafic1 extended permit tcp any host 192.168.1.20 eq domain
access-list OUTSIDE_IN extended permit tcp any host 192.168.1.10 eq www
access-list OUTSIDE_IN extended permit tcp any host 192.168.1.10 eq 443
!
!
access-group OUTSIDE_IN in interface outside
!
!
class-map maps
class-map inside
class-map Bonjour
match default-inspection-traffic
class-map Aurevoir
!
policy-map Aurevoir
class Bonjour
inspect http
inspect icmp
policy-map type inspect dns sip-high
parameters
policy-map Rebonjour
class Bonjour
```

```
inspect icmp
policy-map map
class inside
policy-map aurevoir
class Bonjour
inspect icmp
!
service-policy Rebonjour interface outside
service-policy Aurevoir interface DMZ
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
!
!
!
!
```

Explications du show run :

Le nom du pare-feu est défini (ASA) ainsi qu'un domaine local fictif. Un mot de passe chiffré protège l'accès privilégié au système (MDP = cisco).

- Trois interfaces VLAN sont configurées pour représenter les différentes zones :

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.254 255.255.255.252
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.11.254 255.255.255.252
interface Vlan3
 nameif DMZ
 no forward interface Vlan1
 security-level 50
 ip address 192.168.1.254 255.255.255.0
```

- inside : réseau interne de l'entreprise, niveau de confiance maximum (**100**).

- outside : lien vers Internet ou le routeur du FAI, niveau de confiance minimum (**0**).

- DMZ : zone tampon contenant le serveur web, sécurité intermédiaire (**50**) avec la directive no forward pour interdire la communication directe avec l'interface inside.

- Affectation des ports physiques :

```
interface Ethernet0/0
 switchport access vlan 2
interface Eth0/1
BUG
interface Ethernet0/2
 switchport access vlan 3
```

Les ports Eth0/0 et 0/2 sont respectivement associés a outside et DMZ via les VLANs 2 et 3.

- Routage :

```
route outside 0.0.0.0 0.0.0.0 192.168.11.253
```

- Le trafic à destination des VLANs internes passe par le **MLS** (192.168.10.253).

- La route par défaut vers Internet passe par le **routeur du FAI** (192.168.11.253).

- Règles de filtrage (ACL) :

```
access-list ALLOW_ALL extended permit ip any any
access-list OUTSIDE_IN extended permit tcp any host 192.168.1.10 eq www
access-list OUTSIDE_IN extended permit tcp any host 192.168.1.10 eq 443
!
!
access-group ALLOW_ALL in interface inside

access-group OUTSIDE_IN in interface outside
```

Cette **liste de contrôle d'accès (ACL)** autorise uniquement :

- Le trafic HTTP (port 80) et HTTPS (port 443) **vers le serveur Web** DMZ (192.168.1.80)
- Le trafic DNS (port 53) vers le **serveur DNS interne** (192.168.1.20)

Tout autre trafic entrant non explicitement autorisé est **bloqué par défaut**.

Nous n'avons pas réussi à configurer cet aspect

- Traduction d'adresses (NAT) :

Nous n'avons pas reussi a configurer le NAT

7.3. Configuration complète du routeur FAI et ENTREPRISE

Configuration de le routeur FAI :

```
Router#sh run
Building configuration...

Current configuration : 861 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
```

```
!
license udi pid CISCO2901/K9 sn FTX15248036
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 1.1.1.254 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 1.1.2.130 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 1.1.2.128 0.0.0.3
network 1.1.1.0 0.0.0.255
!
ip nat inside source static tcp 192.168.1.80 80 1.1.1.253 80
ip nat inside source static tcp 192.168.1.80 443 1.1.1.253 443
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
```

```
!
line vty 0 4
login
!
!
!
end


Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.10.0 255.255.255.252 192.168.11.254
Router(config)#ip route 172.16.10.0 255.255.255.0 192.168.11.254
Router(config)#ip route 172.16.20.0 255.255.255.0 192.168.11.254
Router(config)#ip route 10.0.0.0 255.255.255.0 192.168.11.254
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.254
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#sh run
Building configuration...

Current configuration : 1116 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX15248036
!
!
!
!
!
!
!
!
```

```
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 1.1.1.254 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 1.1.2.130 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 1.1.2.128 0.0.0.3
network 1.1.1.0 0.0.0.255
!
ip nat inside source static tcp 192.168.1.80 80 1.1.1.253 80
ip nat inside source static tcp 192.168.1.80 443 1.1.1.253 443
ip classless
ip route 192.168.10.0 255.255.255.252 192.168.11.254
ip route 172.16.10.0 255.255.255.0 192.168.11.254
ip route 172.16.20.0 255.255.255.0 192.168.11.254
ip route 10.0.0.0 255.255.255.0 192.168.11.254
ip route 192.168.1.0 255.255.255.0 192.168.11.254
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
```

!

- Interface reseau

```
interface GigabitEthernet0/0
 ip address 1.1.1.254 255.255.255.0
 ip nat outside
interface GigabitEthernet0/1
 ip address 1.1.2.130 255.255.255.252
 ip nat inside
```

- **G0/0 (1.1.1.254)** : Connectée à l'**ASA**, déclarée comme zone **NAT externe**.

- **G0/1 (1.1.2.130)** : Reliée au réseau **test.com / 8.8.0.0**, représenté dans Packet Tracer par un autre routeur ou un serveur.

- Routage dynamique avec EIGRP

```
router eigrp 100
 network 1.1.2.128 0.0.0.3
 network 1.1.1.0 0.0.0.255
```

Le protocole **EIGRP AS 100** est utilisé pour propager les routes :

- **Vers le réseau Internet fictif** (1.1.2.128/30)
- **Vers l'ASA et le réseau public 1.1.1.0/24**

Cela permet une **interconnexion dynamique** avec le réseau externe simulé.

- NAT

```
object network obj_any_inside
 subnet 172.16.0.0 255.240.0.0
 nat (inside,outside) dynamic interface
```

Cette règle permet aux machines des VLAN internes (RH, Ingé, Admin) d'accéder à l'extérieur via l'interface outside.

```
object network obj_web_dmz
 host 192.168.1.10
 nat (dmz,outside) static 1.1.1.253
```

Cela permet aux clients Internet (par exemple 8.8.8.254) d'accéder au serveur en HTTP/HTTPS.

Configuration routeur ENTREPRISE :

```
Router(config)#do sh run
Building configuration...

Current configuration : 1555 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX15241B34
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
```

```
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 1.1.1.1 255.255.255.0
ip access-group traffic1 in
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.11.253 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
redistribute static
network 1.1.1.0 0.0.0.255
network 192.168.12.252 0.0.0.3
!
ip nat pool DYN 1.1.1.1 1.1.1.1 netmask 255.255.255.0
ip nat inside source list 2 pool DYN overload
ip nat inside source list ACL_INT interface GigabitEthernet0/0 overload
ip nat inside source static tcp 192.168.1.80 443 1.1.1.253 80
ip nat inside source static tcp 192.168.1.80 443 1.1.1.253 443
ip nat inside source static 192.168.1.10 1.1.1.253
ip classless
!
ip flow-export version 9
!
!
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 permit 172.16.2.0 0.0.0.255
access-list 2 deny any
ip access-list extended trafic1
permit tcp any 172.16.0.0 0.0.255.255 established
permit icmp any 172.16.0.0 0.0.255.255 echo-reply
deny ip any any
ip access-list extended traffic1
ip access-list standard ACL_INT
permit 172.16.10.0 0.0.0.255
permit 172.16.20.0 0.0.0.255
permit 10.0.0.0 0.0.0.255
!
!
!
!
```

```
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

- NAT

```
ip access-list standard ACL_INT
 permit 172.16.10.0 0.0.0.255
 permit 172.16.20.0 0.0.0.255
 permit 10.0.0.0 0.0.0.255
ip nat inside source list ACL_INT interface GigabitEthernet0/0 overload
```

Interface G0/0 = vers FAI (ext)
Interface G0/1 = vers ASA (int)

```
ip nat inside source static 192.168.1.10 1.1.1.253
```

Permet au serveur web (dans la DMZ derrière l'ASA) d'être joignable avec l'adresse publique 1.1.1.253.

7.4. Tests fonctionnels

Le ping du PC1 vers 8.8.8.8 (l'internet) ne fonctionne pas.

8. Etape 4 – Ajout du réseau public 8.8.0.0/16 et interconnexion avec le FAI

Nouvelle configuration du routeur entreprise :

```
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
 ip nat outside
 no shutdown

interface GigabitEthernet0/1
 ip address 192.168.11.253 255.255.255.252
 ip nat inside
 no shutdown

access-list ACL_INT permit 172.16.0.0 0.15.255.255
access-list ACL_INT permit 10.0.0.0 0.0.0.255
ip nat inside source list ACL_INT interface GigabitEthernet0/0 overload

ip nat inside source static 192.168.1.10 1.1.1.253

ip route 0.0.0.0 0.0.0.0 1.1.1.1

end
```

La nouvelle configuration du routeur Entreprise met en œuvre deux types de NAT :

- NAT dynamique overload : permet aux utilisateurs internes (réseaux 172.16.X.X et 10.0.0.X) d'accéder à Internet avec une seule adresse publique (1.1.1.2) en utilisant l'interface GigabitEthernet0/0 comme point de sortie.
- NAT statique : permet aux utilisateurs extérieurs d'accéder au serveur web dans la DMZ via l'adresse publique 1.1.1.253, redirigée vers 192.168.1.10.

La configuration assure également les routes statiques nécessaires pour atteindre les réseaux internes via l'ASA.

Config du routeur TEST exterieur :

```
interface GigabitEthernet0/0
 ip address 8.8.8.254 255.255.0.0

interface GigabitEthernet0/1
 ip address 1.1.2.129 255.255.255.252

ip route 1.1.1.0 255.255.255.0 1.1.2.130
ip route 0.0.0.0 0.0.0.0 1.1.2.130
```

Le routeur test extérieur est configuré pour **simuler un utilisateur externe** accédant à l'infrastructure via Internet. Il possède :

- Une route par défaut vers le FAI (1.1.2.130)
- Une route spécifique pour accéder au sous-réseau public 1.1.1.0, permettant de tester l'accès NAT statique au serveur DMZ

Il permet de valider les services exposés (HTTP/HTTPS) depuis l'extérieur et de vérifier que le NAT fonctionne correctement côté entreprise.

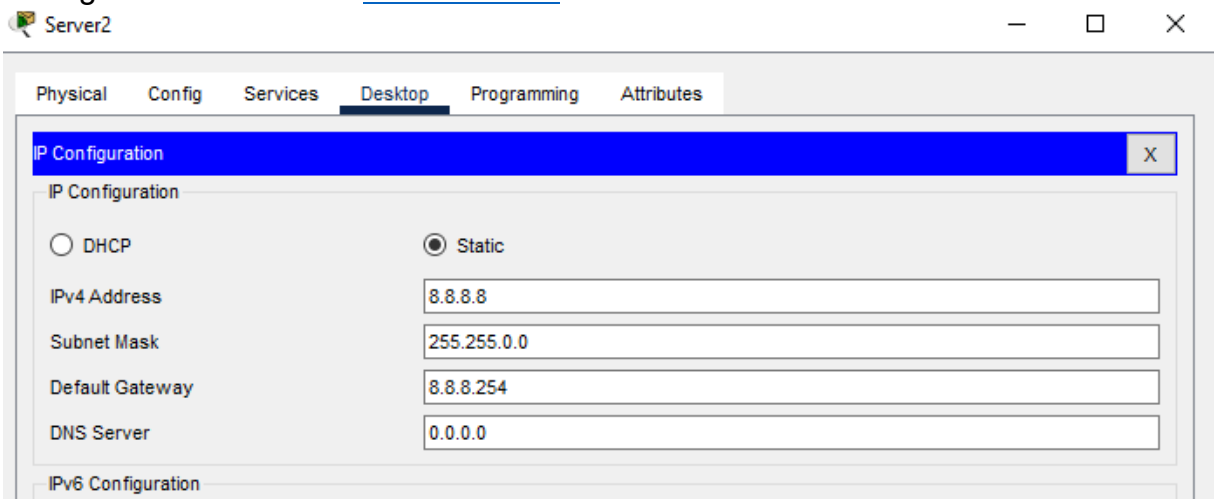
Sur le routeur entreprise :

```
Router>en
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  1.1.1.253         192.168.1.10       ---                ---
```

Confirmation du NAT

L'étape 4 consiste à rendre accessible le serveur web DMZ depuis Internet via l'adresse publique 1.1.1.253. Cela passe par un NAT statique sur le routeur Entreprise, des règles d'autorisation sur l'ASA, et des routes adaptées sur tous les routeurs. Des tests depuis le routeur test extérieur permettent de valider cette publication.

Configuration du serveur www.test.com



9. Conclusion

Malgré la mise en place générale de l'architecture réseau, certaines configurations comme le NAT et le filtrage ASA n'ont pas fonctionné correctement. En conséquence, certaines communications échouent, notamment le ping depuis le PC1 vers Internet. Ces erreurs soulignent l'importance de tester chaque étape en détail et de vérifier les liaisons et règles de traduction d'adresses.