Construire un réseau informatique pour une petite structure

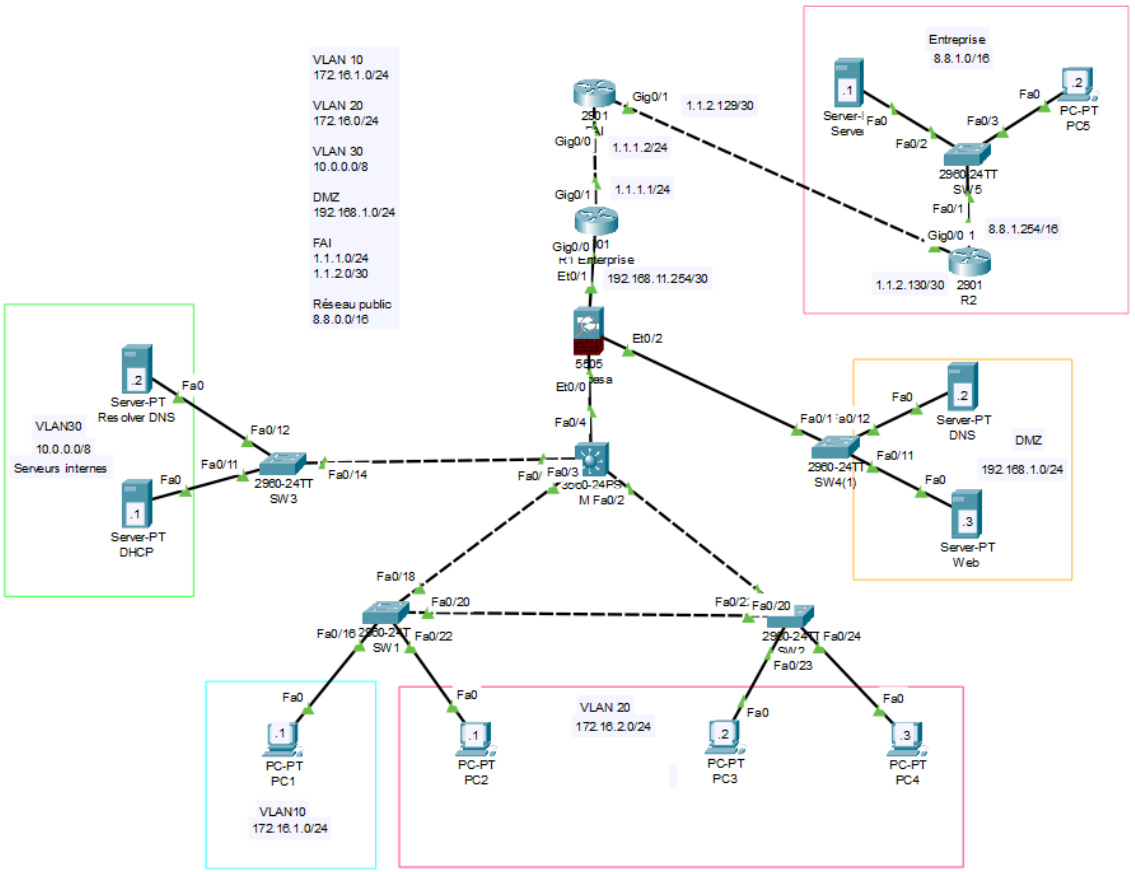
Rapport SAE 21

HERBRECHT-BOURGOIN Clément

PICOT Quentin

groupe 21

Voici notre topologie de notre réseau :



Étape 1 : Construction de coeur de réseau avec les switches d'accès et le Multilayer switch :

Configuration de SW1 :

1/ Nommer le switch SW1 :

```
SW1#conf t
SW1(config)#hostname SW1
```

2/ Création des Vlan pour SW1 :

```
SW1(config)#vlan 10
SW1(config-vlan)#name VLAN10
SW1(config)#vlan 20
SW1(config-vlan)#name VLAN20
```

- Créer les Vlan 10 et 20.

3/ Assignation des ports :

```
SW1(config)#int range Fa0/15-20
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config)#int range Fa0/20-24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
```

- Affectations des ports Fa0/15-20 pour le Vlan 10 et Fa0/20-24 pour le Van 20.

Configuration de SW2 :

1/ Création des Vlan pour SW2:

```
SW2(config)#vlan 20
SW2(config-vlan)#name VLAN20
```

2/ Assignation des ports :

```
SW2(config)#int range Fa0/20-24
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
```

- Configuration des ports Fa0/20-24 pour le Vlan 20.

Configuration de SW3 :

1/ Création des Vlan pour SW3 :

```
SW3(config)#vlan 30
SW3(config-vlan)#name VLAN30
```

2/ Assignation des ports :

```
SW3(config)#int range Fa0/10-14
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 30
```

- Configuration des ports Fa0/10-14 pour le Vlan 30 en mode accès.

STP et Trunk sur MLS (Multi-Layer Switch) :

1/ Configuration du protocole STP (Spanning Tree Protocol) :

```
MLS(config)#spanning-tree mode pvst
MLS(config)#spanning-tree vlan 10,20,30 priority 0
```

- Configuration du mode STP en PVST (Per-Vlan Spanning Tree) et définit la priorité pour les Vlan 10, 20 et 30.

2/ Configuration des interfaces pour les Vlan :

```
MLS(config)#int vlan 10
MLS(conf-if)#ip add 172.16.1.254 255.255.255.0
MLS(conf-if)#ip helper-address 10.0.0.1
MLS(conf-if)#no shut
MLS(config)#int vlan 20
MLS(conf-if)#ip add 172.16.2.254 255.255.255.0
MLS(conf-if)#ip helper-address 10.0.0.1
MLS(conf-if)#no shut
MLS(config)#int vlan 30
MLS(conf-if)#ip add 10.0.0.254 255.0.0.0
MLS(conf-if)#no shut
```

- Assigne des adresses IP aux interfaces Vlan 10, 20 et 30.

3/ Activer le routage IP :

```
MLS(config)#ip routing
```

4/ Configuration des interfaces physiques pour avoir accès aux Vlan :

```
MLS(config)#int Fa0/1
MLS(conf-if)#switchport mode access
MLS(conf-if)#switchport access vlan 10
MLS(config-if)#no shut
MLS(config)#int Fa0/2
MLS(conf-if)#switchport mode access
MLS(conf-if)#switchport access vlan 20
MLS(config-if)#no shut
MLS(config)#int Fa0/3
MLS(conf-if)#switchport mode access
MLS(conf-if)#switchport access vlan 30
MLS(config-if)#no shut
MLS(config)#int Fa0/4
MLS(config)#no switchport
MLS(config-if)#ip add 192.168.10.2 255.255.255.0
MLS(config-if)#no shut
```

- Configuration des ports Fa0/1, Fa0/2 et Fa0/3 en mode accès pour les Vlan 10, 20 et 30. Configuration du port Fa0/4 comme port routeur.

5/ Configuration d'une ip route vers le MLS et ciscoasa :

```
MLS(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

Configuration des trunks entre SW1 et SW2 :

1/ Pour SW1 en mode trunk :

```
SW1#conf t
SW1(config)#int Fa0/20
SW1(conf-if)#switchport mode trunk
SW1(conf-if)#switchport trunk allowed vlan 10, 20

SW2#conf t
SW2(config)#int Fa0/20
SW2(conf-if)#switchport mode trunk
SW2(conf-if)#switchport trunk allowed vlan 10,20
```

- Configuration de Fa0/20 en mode trunk et permet les Vlan 10 et 20.

Étape 2 : Ajout de l'ASA et du DHCP :

1/ Configuration des interfaces des Vlan :

```
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#no ip address
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasaASA(config-if)#int e/0
ciscoasa(config-if)#switchport mode access
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#no shut
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#int e0/1
ciscoasa(config-if)#switchport mode access
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#no shut
ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip add 192.168.10.1 255.255.255.0
ciscoasa(config-if)#no shut
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip add 192.168.11.253 255.255.255.252
ciscoasa(config-if)#no shut
```

- Configuration du Vlan 1 en inside et du Vlan 2 en outside avec pour chacun, des différents niveaux de sécurité.

Configuration du Routeur (R1)

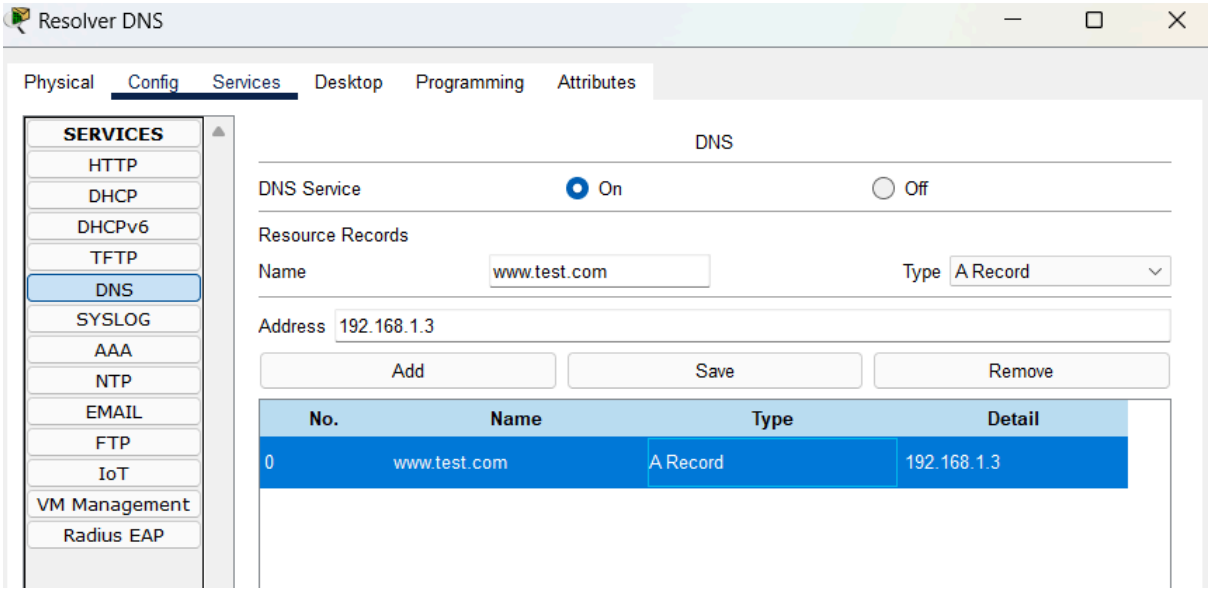
1/ Configurer l'interface de R1 :

```
R1(config)#int Gi0/0
R1(config-if)#ip add 192.168.11.254 255.255.255.252
R1(config-if)#no shut
```

- Configure l'adresse IP.

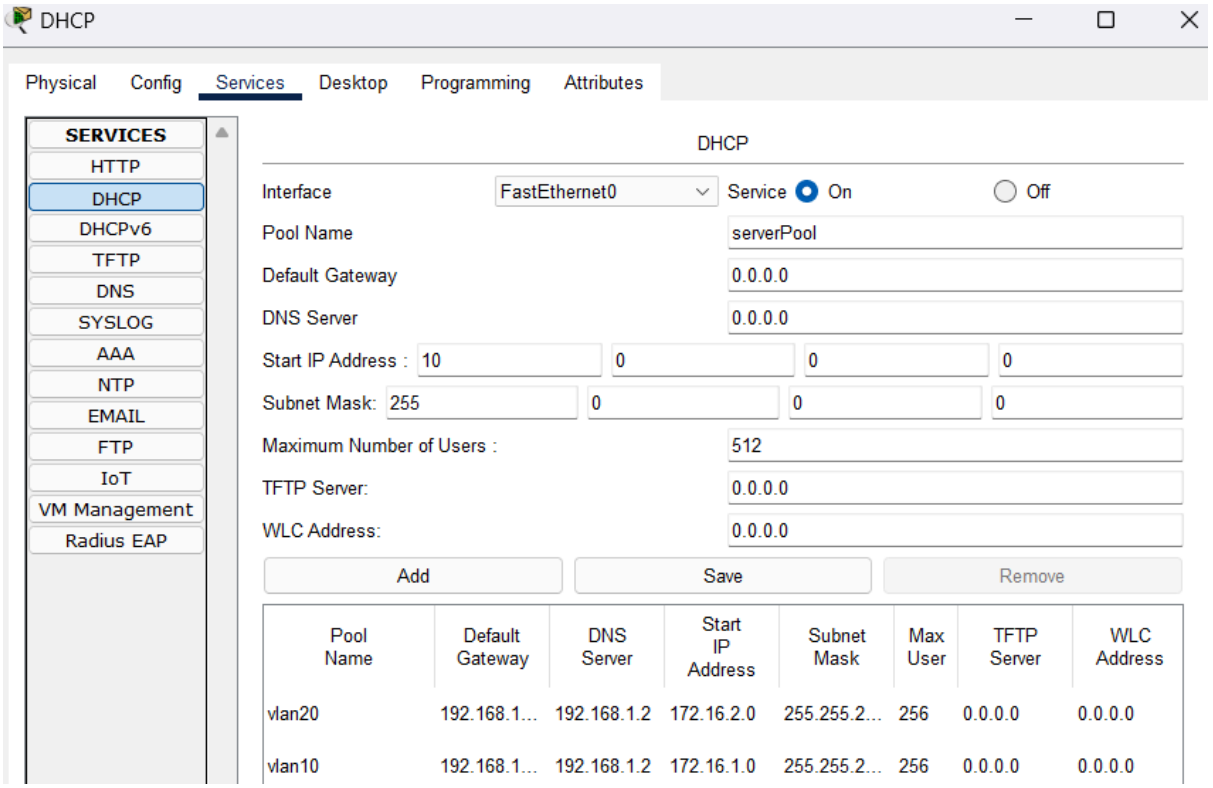
Pour le Resolver DNS :

Nous avons ajouter un enregistrement de type A au Resolver DNS “www.test.com” .



Pour le Serveur DHCP :

Pour le DHCP nous avons créé deux pools, le premier est pour le sous-réseau du Vlan 10 et le second pour Vlan 20.



Étape 3 : Ajout de la DMZ et du routeur du FAI :

Configuration de l'ASA

1/ Configurer les Vlan pour la DMZ :

```
ciscoasa#conf t
ciscoasa(config)#int vlan 3
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif DMZ
ciscoasa(config-if)#security-level 50
```

- Configuration du Vlan 3 avec un niveau de sécurité de 50.

2/ Configuration de l'interface physique pour la DMZ :

```
ciscoasa(config-if)#int e0/2
ciscoasa(config-if)#switchport mode access
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#no shut
```

- Configuration de l'interface e0/2 en mode accès et l'assigne au Vlan 3.

3/ Adresse IP à l'interface Vlan :

```
ciscoasa(config)#int vlan 3
ciscoasa(config-if)#ip add 192.168.1.1 255.255.255.0
ciscoasa(config-if)#no shut
```

- Configuration de l'adresse IP pour l'interface Vlan 3.

4/ Configuration des routes statiques :

```
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.168.11.254
ciscoasa(config)#route inside 172.16.1.0 255.255.255.0 192.168.10.2
ciscoasa(config)#route inside 172.16.2.0 255.255.255.0 192.168.10.2
ciscoasa(config)#route inside 10.0.0.0 255.0.0.0 192.168.10.2
```

- Configuration des routes statiques pour diriger le trafic.

5/ Listes d'accès :

```
ciscoasa(config)#access-list accessDMZ extended permit tcp any host 192.168.1.3 eq www
ciscoasa(config)#access-list accessDMZ extended permit tcp any host 192.168.1.3 eq
443
ciscoasa(config)#access-list accessDMZ extended permit icmp any any echo-reply
ciscoasa(config)#access-list accessDMZ extended permit udp any host 192.168.1.2 eq
domain
ciscoasa(config)#access-group accessDMZ out interface DMZ
```

- Création de ligne d'accès pour permettre le trafic HTTP, HTTPS et les réponses ICMP vers la DMZ, puis appliquer cette liste à l'interface DMZ.

6/ Inspection ICMP, FTP, TFTP et DNS afin de pinger vers l'asa :

```
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#policy-map inspection_default
ciscoasa(config-pmap)#exit
ciscoasa(config)#policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum 512
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#inspect ftp
ciscoasa(config-pmap-c)#inspect  tftp
ciscoasa(config-pmap-c)#inspect dns preset_dns_map
ciscoasa(config)#service-policy global_policy global
```

Configuration du Routeur R1 :

1/ Configurer les interfaces pour le NAT :

```
R1#conf
R1(config)#int Gi0/0
R1(config-if)#ip add 192.168.11.254 255.255.255.252
R1(config-if)#ip nat inside
R1(config-if)#no shut
R1(config)#int Gi0/1
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#no shut
```

- Configuration de l'interface Gi0/1 avec une interface NAT extérieure.

2/ Configuration du pool NAT :

```
R1(config)#ip nat pool POOLNAT 1.1.1.3 1.1.1.253 netmask 255.255.255.0
R1(config)#ip nat inside source list 1 pool POOLNAT overload
```

- Création d’ un pool NAT et configuration de la translation d'adresses IP source à partir de la liste d'accès 1.

3/ Configuration des routes statiques :

```
R1(config)#ip route 8.8.0.0 255.255.0.0 Gi0/1
R1(config)#ip route 172.16.1.0 255.255.255.0 192.168.10.2
R1(config)#ip route 172.16.2.0 255.255.255.0 192.168.10.2
R1(config)#ip route 10.0.0.0 255.0.0.0 192.168.10.2
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R1(config)#ip route 1.1.2.128 255.255.255.252 1.1.1.2
```

- Configuration les routes statiques pour le trafic vers les réseaux spécifiés via les interfaces et adresses IP correspondantes.

4/ Configurer la liste d'accès pour NAT :

```
R1(config)#access-list 1 permit any
```

- Création d’une liste d'accès permettant tout le trafic.

Étape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI :

Configuration du Routeur (R2) :

1/ Configuration des interfaces :

```
R2(config)#int Gi0/0
R2(config-if)#ip add 8.8.1.254 255.255.0.0
R2(config-if)#no shut
R2(config)#int Gi0/1
R2(config-if)#ip add 1.1.2.130 255.255.255.252
R2(config-if)#no shut
```

- Configuration des adresses IP des interfaces Gi0/0 et Gi0/1.

2/ Configuration du protocole de routage EIGRP :

```
R2(config)#router eigrp 100
R2(config-router)#network 1.1.1.0 0.0.0.255
R2(config-router)#network 1.1.2.128 0.0.0.3
R2(config-router)#network 8.8.0.0 0.0.255.255
```

- Active le routage EIGRP pour l'AS 100 et configure les réseaux à annoncer.

Configuration du FAI :

1/ Configuration des interfaces :

```
FAI(config)#int Gi0/0
FAI(config-if)#ip add 1.1.1.2 255.255.255.0
FAI(config-if)#no shut
FAI(config)#int Gi0/1
FAI(config-if)#ip add 1.1.2.129 255.255.255.252
FAI(config-if)#no shut
```

- Configuration des adresses IP des interfaces Gi0/0 et Gi0/1.

2/ Configuration pour le protocole EIGRP :

```
FAI(config)#router eigrp 100
FAI(config-router)#network 1.1.1.0 0.0.0.255
FAI(config-router)#network 1.1.2.128 0.0.0.3
FAI(config-router)#network 8.8.0.0 0.0.255.255
FAI(config-router)#redistribute static
```

- Activation du routage EIGRP pour l'AS 100 et configuration des réseaux à annoncer.

3/ IP route vers l'ASA, R1 et DMZ :

```
FAI(config)#ip route 192.168.1.0 255.255.255.0 1.1.1.1
FAI(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

Ces configurations mettent en place un réseau comprenant des VLANs, du routage inter-VLAN, un pare-feu ASA avec des configurations NAT et des routes statiques, ainsi que du routage EIGRP pour l'interconnexion entre les routeurs et le fournisseur d'accès Internet (FAI).