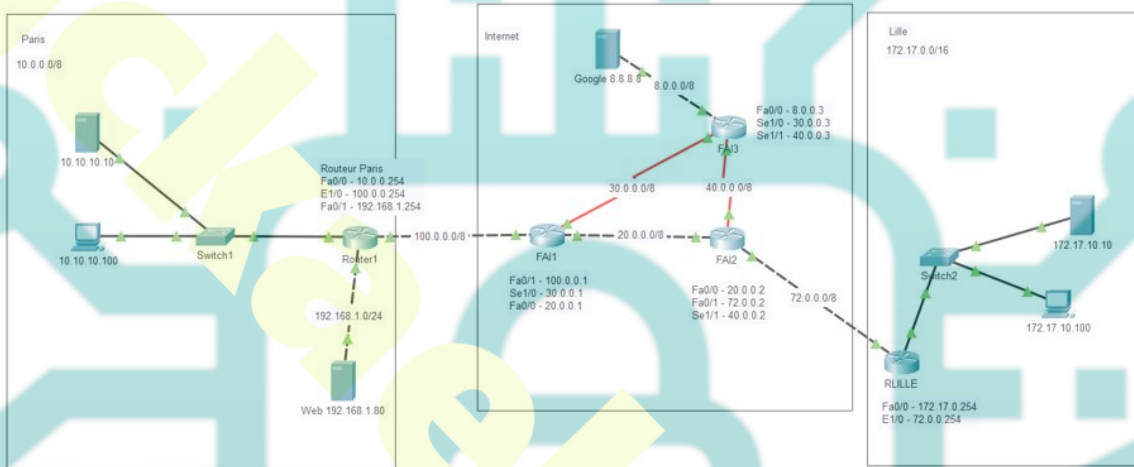


## TD – VPN IPSEC

**Objectif : mettre en œuvre un tunnel IPSEC entre 2 sites**



Construire le schéma suivant en activant le routage dynamique de votre choix.

## Configuration du VPN pour Paris

```
conf t
!on active la fonction crypto sur le routeur Paris.
crypto isakmp enable

!on paramètre la policy qui détermine chiffrement, hachage
d'authentification, etc.
crypto isakmp policy 20

!authentification = clé pré-partagée
authentication pre-share

!chiffrement 3DES
encryption 3des

!Hachage MD5
hash md5

!identifiant diffie-Hellman
group 1

!temps de validité de la connexion avant une nouvelle négociation
des clefs
lifetime 3600
exit

!configuration de la clé
crypto isakmp key Pa$$word address 72.0.0.254 (@ip routeur
distant)

!transformation des données IPSEC en utilisant ESP (utiliser les
mêmes protocoles que lors de la première étape).
crypto ipsec transform-set monset esp-3des esp-md5-hmac

!on configure la crypto map qui va associer l'access-list, le
trafic, et la destination :
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.17.0.0
0.0.255.255
```

```
crypto map mysite 20 ipsec-isakmp
set peer 72.0.0.254
set transform-set monset
match address 102
exit
```

**!on affecte la règle à l'interface wan**  
int e1/0  
crypto map *mysite*

### Configuration du VPN Lille

```
conf t
crypto isakmp enable
crypto isakmp policy 20
authentication pre-share
encryption 3des
hash md5
group 1
lifetime 3600
exit
crypto isakmp key Pa$$word address 100.0.0.254
crypto ipsec transform-set monset esp-3des esp-md5-hmac
access-list 102 permit ip 172.17.0.0 0.0.255.255 10.0.0.0
0.255.255.255
crypto map mysite 20 ipsec-isakmp
set peer 100.0.0.254
set transform-set monset
match address 102
exit
int e1/0
crypto map mysite
```

## Test de la configuration

- Faire un ping entre un PC de Paris et un PC de Lille (le premier ping va échouer, c'est le temps de négociation entre les routeurs)
- Voir la connexion VPN  
`sh crypto isakmp sa`