ACL – TP récapitulatif

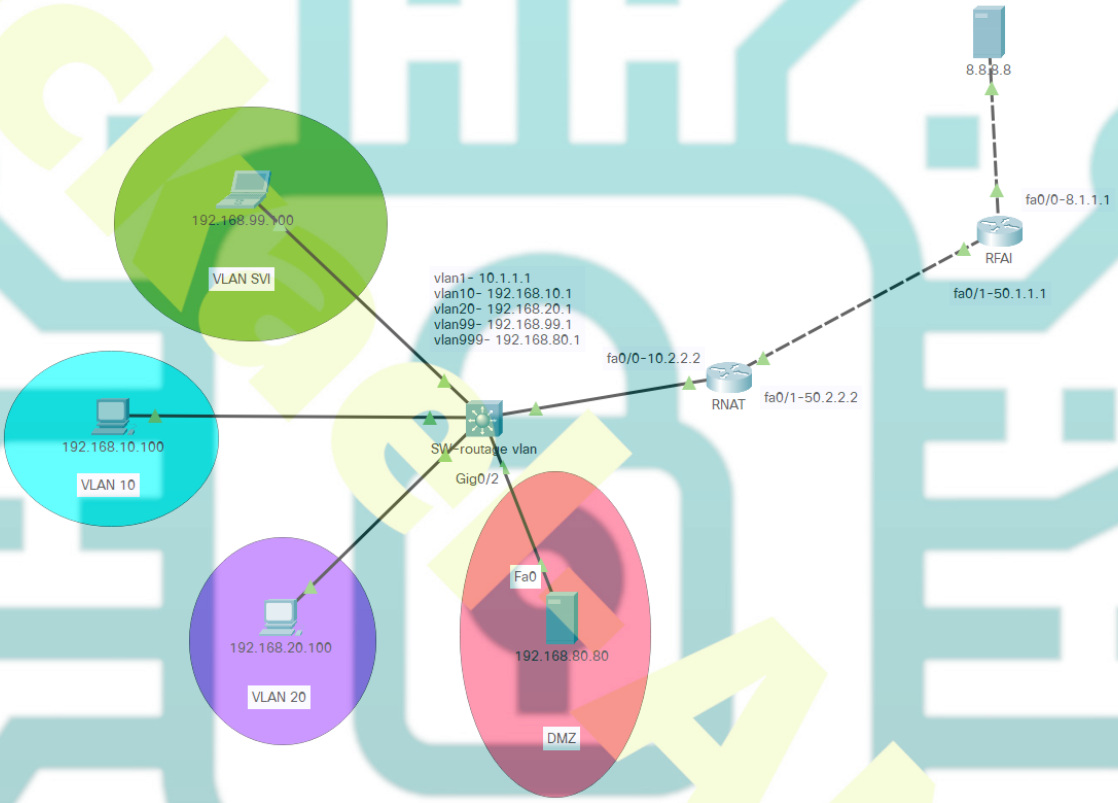

Schéma du TP

Consignes du TD

Le RNAT déclare RIP sur le réseau 50.0.0.0 uniquement et le RFAI déclare RIP sur le réseau 50.0.0.0 et le réseau 8.0.0.0

Le serveur 8.8.8.8 fait office de serveur web et DNS pour tout le TP sur le nom www.google.fr – 8.8.8.8

Paramétrage du switch

- Nommer le switch en SW
- Créer les vlan 10, 20, 99 (SVI), 999 (DMZ)
- Affecter le port 10 au vlan 10
- Affecter le port 20 au vlan 20
- Affecter le port 9 au vlan 99
- Affecter le port gi0/2 au vlan 999
- Affecter les adresse IP aux interfaces de vlan comme dans le schéma
- Activer SSH

ACL du switch

- **Créer l'ACL interdisant l'accès SSH** vers le switch en dehors du PC admin
- **Créer l'ACL interdisant au vlan 10 de communiquer avec les vlan 20** et en lui permettant l'accès aux autres réseaux
- **Créer l'ACL interdisant au vlan 20 de communiquer avec les vlan 10** et la DMZ mais en lui permettant l'accès aux autres réseaux
- **Créer l'ACL de protection du PC de l'administrateur** selon les règles suivantes :
  le PC admin doit pouvoir utiliser tous les protocoles mais on ne peut pas le joindre en dehors des réponses à ses requêtes sur le PING, TCP et DNS
- **Créer l'ACL de protection du VLAN DMZ** selon les règles suivantes :
  On autorise le flux https vers le serveur WEB de la DMZ depuis les autres réseaux.
  On autorise tous les protocoles vers le serveur WEB de la DMZ depuis le PC ADMIN

Paramétrage du routeur NAT

- Nommer le routeur en RNAT
- Activer SSH

- Activer le NAT

ACL du routeur

- **Créer l'ACL interdisant l'accès SSH** vers le routeur en dehors du PC admin
- **Créer l'ACL NAT** selon les règles suivantes :
  On permet aux vlan de sortir en TCP 80 (http) et 443 (https)
  On permet aux clients (vlan 10, vlan 20) de lancer des requêtes DNS vers le DNS de Google
  On permet au poste de l'administrateur l'accès vers le WAN avec tous les protocoles
- On créer la règle de redirection **WAN-DMZ** en autorisant le https uniquement

Tests à effectuer

- Les communications entre le vlan 10 et 20 ne doivent pas passer
- Les vlan 10 et 20 ont accès au serveur web 8.8.8.8 par son nom et son adresse IP en http et https uniquement
- Le vlan 10 accède à la DMZ en https uniquement mais le vlan 20 ne peut pas accéder à la DMZ
- Les communications des vlan 10 et 20 ne doivent pas passer vers le PC admin
- Seul le PC admin peut exécuter SSH sur le switch et le routeur
- Le PC admin accèdent à toutes les zones (vlan, DMZ et internet)
- Le serveur 8.8.8.8 peut accéder au serveur web de la DMZ en https uniquement