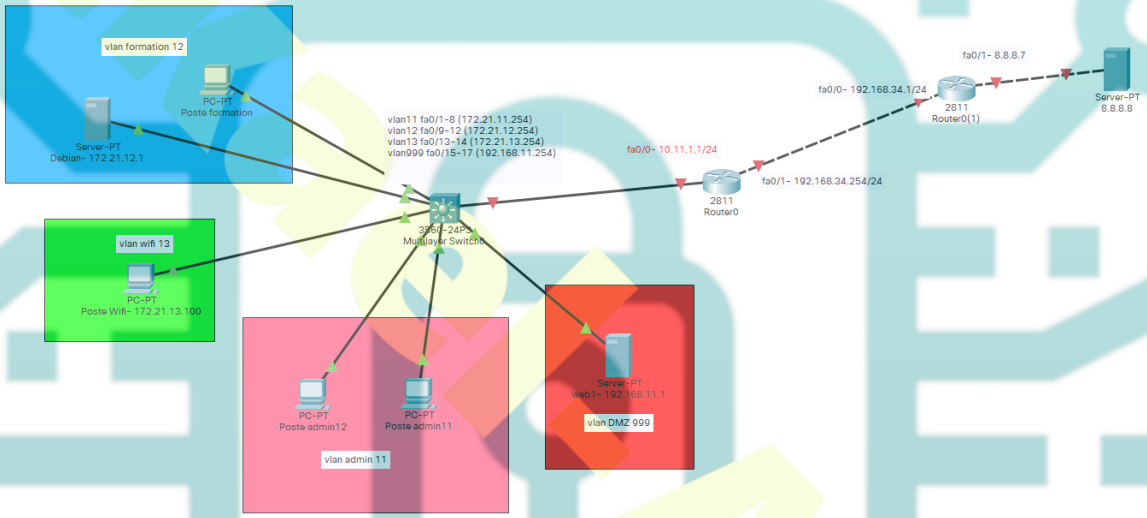
TD – ACL (2)

Objectif – Filtrer les connexions et activer le NAT via les listes de contrôle d'accès

Schéma du réseau



Étape 1

Création des vlan sur switch niveau 3

```
Switch>en
Switch#conf t
Switch(config)#vlan 11
Switch(config-vlan)#name admin
Switch(config-vlan)#vlan 12
Switch(config-vlan)#name form
Switch(config-vlan)#vlan 13
Switch(config-vlan)#name wifi
Switch(config-vlan)#vlan 999
Switch(config-vlan)#name DMZ
```

Affectation des adresses IP des vlan sur le switch

```
Vlan admin
Switch(config-vlan)#int vlan 11
Switch(config-if)#ip address 172.21.11.254 255.255.255.0
Vlan formation
Switch(config-if)#int vlan 12
Switch(config-if)#ip address 172.21.12.254 255.255.255.0
Vlan Wifi
Switch(config-if)#int vlan 13
Switch(config-if)#ip address 172.21.13.254 255.255.255.0
Vlan DMZ
Switch(config-if)#int vlan 999
Switch(config-if)#ip address 192.168.11.254 255.255.255.0
Vlan par defaut connexion vers routeur
Switch(config-if)#int vlan 1
Switch(config-if)#ip address 10.11.1.254 255.255.255.0
Switch(config-if)#no shut
Affectation de la route par défaut vers internet (routeur du site)
Switch(config-if)#ip route 0.0.0.0 0.0.0.0 10.11.1.1
```

Affectation des ports aux vlan

```
Switch>en
Switch#conf t
Vers le sw du vlan 11
Switch(config)#interface range fa0/1 - 8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 11
Vers le sw du vlan 12
Switch(config)#int interface range fa0/9 - 12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 12
Vers le vlan 13
Switch(config)# interface range fa0/13 - 14
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 13
Vers DMZ
Switch(config-if)# interface range fa0/15 - 17
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 999
```

Test de ping entre les vlan (fonctionnel)

Étape 2

Configuration du routeur du site

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 10.11.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.34.254 255.255.255.0
Router(config-if)#no shutdown

Indication de la passerelle par défaut vers internet
ip route 0.0.0.0 0.0.0.0 192.168.34.1
Indication des routes agrégées vers les vlan 11, 12 et 13
Router(config)#ip route 172.21.0.0 255.255.0.0 10.11.1.254
Indication des routes vers le vlan DMZ
Router(config)#ip route 192.168.11.0 255.255.255.0 10.11.1.254
```

Test de ping des vlan vers le routeur (fonctionnel)

Paramétrage du NAT

```
Paramétrage de base indiquant l'extérieur et l'intérieur
 Router(config)#int fa0/0
 Router(config-if)#ip nat inside
 Router(config-if)#int fa0/1
 Router(config-if)#ip nat outside

Création des règles autorisant la sortie des réseaux 172.21.11.0,
172.21.12.0 et 172.21.13.0
 Router(config)#access-list 2 permit 172.21.0.0 0.0.255.255

Création de l'affectation dynamique adresses privées/publiques
sur l'interface vers internet
 Router(config)#ip nat inside source list 2 interface fa0/1
overload
```

Test de ping des machines des vlan vers internet (fonctionnel)
Test de ping de la DMZ vers internet échec (normal) on ne veut pas et on n'a pas indiqué de règle dans les ACL

Création de la règle de redirection internet vers DMZ

```
Router(config)#ip nat inside source static 192.168.11.80
192.168.34.254
```

Test d'accès internet et de ping vers le routeur du site 192.168.34.x (fonctionnel)

Étape 3

Sécurisation des flux

Gestion de l'accès vers le vlan DMZ (ACL sur le switch de niveau 3)

```
On autorise uniquement les flux https vers la DMZ de l'extérieur
ou de l'intérieur
 Switch(config)#access-list 101 permit tcp any any eq 443
 Switch(config)#int vlan 999

Affectation de la règle en sortie du sw
 Switch(config-if)#ip access-group 101 out
```

Test d'accès depuis l'intérieur et depuis l'extérieur avec le navigateur en http simple (échec)

Test d'accès depuis l'intérieur et depuis l'extérieur avec le navigateur en https (fonctionnel)

Règles empêchant le routage entre les vlan

```
Les demandes du vlan 11 vers le 12 et 13 sont bannies mais pas
vers les autres adresses
 Switch(config)#access-list 21 deny 172.21.12.0 0.0.0.255
 Switch(config)#access-list 21 deny 172.21.13.0 0.0.0.255
 Switch(config)#access-list 21 permit any
 Switch(config)#int vlan 11
 Switch(config-if)#ip access-group 21 out

Les demandes du vlan 12 vers le 11 et 13 sont bannies mais pas
vers les autres adresses
 Switch(config)#access-list 22 deny 172.21.11.0 0.0.0.255
 Switch(config)#access-list 22 deny 172.21.13.0 0.0.0.255
 Switch(config)#access-list 22 permit any
 Switch(config-if)#int vlan 12
 Switch(config-if)#ip access-group 22 out

Les demandes du vlan 13 vers le 11 et 12 sont bannies mais pas
vers les autres adresses
 Switch(config)#access-list 23 deny 172.21.11.0 0.0.0.255
 Switch(config)#access-list 23 deny 172.21.12.0 0.0.0.255
 Switch(config)#access-list 23 permit any
 Switch(config-if)#int vlan 13
 Switch(config-if)#ip access-group 23 out
```

Test ping entre vlan (échec)
Test ping vers internet (succès)