TD – ACL Cisco (1)

Objectif : tester le filtrage grâce aux ACL

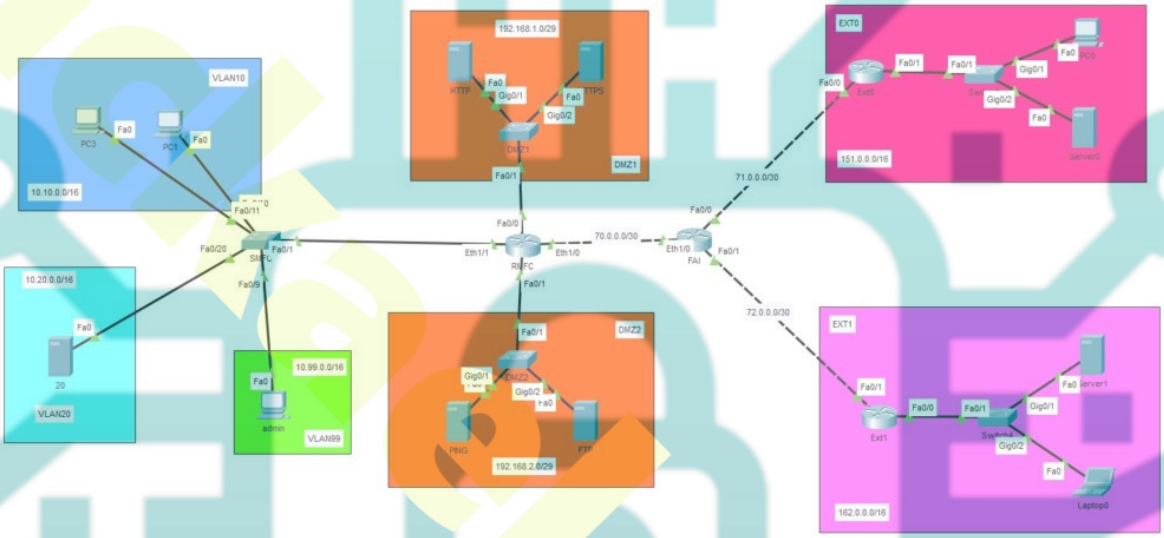

Schéma du TD

TD1 – ACL et NAT

Paramétrage du switch

```
SMFC
en
conf t
hostname smfc
vlan 10
name 10
vlan 20
name 20
vlan 99
name admin
int range fa0/10-14
switchport access vlan 10
int range fa0/20-24
switchport access vlan 20
int fa0/9
switchport access vlan 99
int vlan 99
ip address 10.99.0.1 255.255.0.0
no shut
int fa0/1
switchport mode trunk
end
```

Paramétrage routeur FAI

```
!RFAI
en
conf t
hostname fai
int e1/0
ip address 70.0.0.1 255.255.255.252
no shut
int fa0/0
ip address 71.0.0.1 255.255.255.252
no shut
int fa0/1
ip address 72.0.0.1 255.255.255.252
no shut
end
conf t
router rip
version 2
no auto-summary
network 70.0.0.0
network 71.0.0.0
network 72.0.0.0
end
```

Paramétrage routeur ext0

```
!REXT0
en
conf t
hostname ext0
int fa0/0
ip address 71.0.0.2 255.255.255.252
no shut
int fa0/1
ip address 151.0.0.254 255.255.0.0
no shut
end
conf t
router rip
version 2
no auto-summary
network 71.0.0.0
network 151.0.0.0
end
```

Paramétrage routeur ext1

```
!REXT1
en
conf t
hostname ext1
int fa0/0
ip address 162.0.0.254 255.255.0.0
no shut
int fa0/1
ip address 72.0.0.2 255.255.255.252
no shut
end
conf t
router rip
version 2
no auto-summary
network 72.0.0.0
network 162.0.0.0
end
```

Paramétrage de base routeur MFC

```
!RMFC
en
conf t
hostname rmfc
int fa0/0
ip address 192.168.1.254 255.255.255.248
ip nat inside
no shut
int fa0/1
ip address 192.168.2.254 255.255.255.248
ip nat inside
no shut
int e1/0
ip address 70.0.0.2 255.255.255.252
ip nat outside
no shut
int e1/1
no shut
int e1/1.10
encapsulation dot1q 10
ip address 10.10.0.254 255.255.0.0
ip nat inside
no shut
int e1/1.20
encapsulation dot1q 20
ip address 10.20.0.254 255.255.0.0
ip nat inside
no shut
int e1/1.99
encapsulation dot1q 99
ip address 10.99.0.254 255.255.0.0
ip nat inside
no shut
end
conf t
router rip
version 2
```

```
no auto-summary
network 70.0.0.0
end
```

Mise en place du NAT et des ACL

```
conf t
access-list 2 permit 10.0.0.0 0.255.255.255
access-list 2 permit 192.168.1.0 0.255.255.255
ip nat inside source list 2 interface E1/0 overload
end
```

Test NAT

- Faire test de ping LAN vers DMZ
- Faire test de ping LAN vers WAN
- Faire test de ping WAN vers DMZ
- Faire test de ping WAN vers LAN

Mise en place de la redirection vers DMZ

```
conf t
!regles de redirection vers les serveurs de la DMZ1 et la DMZ2
ip nat inside source static tcp 192.168.2.253 21 70.0.0.2 21
ip nat inside source static tcp 192.168.1.252 443 70.0.0.2 443
ip nat inside source static tcp 192.168.1.253 80 70.0.0.2 80
end
```

Test règle de DMZ

- Faire test de connexion WAN vers DMZ pour vérifier les règles

TD 2 ACL sans NAT

```
Suppression règles sur RMFC
en
reload
```

Reconfiguration du routeur MFC

```
!RMFC
en
conf t
hostname rmfc
int fa0/0
ip address 192.168.1.254 255.255.255.248
no shut
int fa0/1
ip address 192.168.2.254 255.255.255.248
no shut
int e1/0
ip address 70.0.0.2 255.255.255.252
no shut
int e1/1
no shut
int e1/1.10
encapsulation dot1q 10
ip address 10.10.0.254 255.255.0.0
no shut
int e1/1.20
encapsulation dot1q 20
ip address 10.20.0.254 255.255.0.0
no shut
int e1/1.99
encapsulation dot1q 99
ip address 10.99.0.254 255.255.0.0
no shut
end
conf t
router rip
version 2
no auto-summary
network 70.0.0.0
network 192.168.1.0
network 192.168.2.0
network 10.10.0.0
network 10.20.0.0
```

```
network 10.99.0.0
end
```

Mise en place des ACL WAN DMZ1

```
conf t
ip access-list extended WAN-DMZ1
!autoriser le HTTP vers le HTTP 192.168.1.253
permit tcp any host 192.168.1.253 eq 80
!autoriser le HTTPS vers le HTTPS 192.168.1.252
permit tcp any host 192.168.1.252 eq 443
!Affectation des règles sur l'interface DMZ1
int fa0/0
ip access-group WAN-DMZ1 out
end
```

- Tester les règles d'accès de et vers la DMZ1

Mise en place des ACL WAN DMZ2

```
Conf t
ip access-list extended WAN-DMZ2
!autoriser le ping vers le serveur PING 192.168.2.253
permit icmp any host 192.168.2.253
!autoriser le FTP vers le serveur FTP 192.168.2.252
permit tcp any host 192.168.2.252 eq 21
!Affectation des règles sur l'interface DMZ1
int fa0/1
ip access-group WAN-DMZ2 out
end
```

- Tester les règles accès de et vers la DMZ2

Mise en place ACL du VLAN10 vers EXT

```
conf t
ip access-list extended lan10-ext
!autoriser le http et https pour le vlan 10 10 10.10.0.0 vers
l'extérieur
permit tcp 10.10.0.0 0.0.255.255 any eq 80
permit tcp 10.10.0.0 0.0.255.255 any eq 443
!Affectation des règles sur la sous interface du vlan10
int e1/1.10
ip access-group lan10-ext in
end
```

- Tester les règles accès du vlan 10 et vers les autres réseaux lan et wan

Mise en place ACL du VLAN20 vers EXT

```
conf t
ip access-list extended lan20-ext
!Autoriser uniquement le ping du serveur 20 10.20.20.20 vers
l'extérieur
permit icmp host 10.20.20.20 any
int e1/1.20
ip access-group lan20-ext in
end
```

- Tester les règles accès du serveur de la DMZ2 vers autres réseaux lan et wan