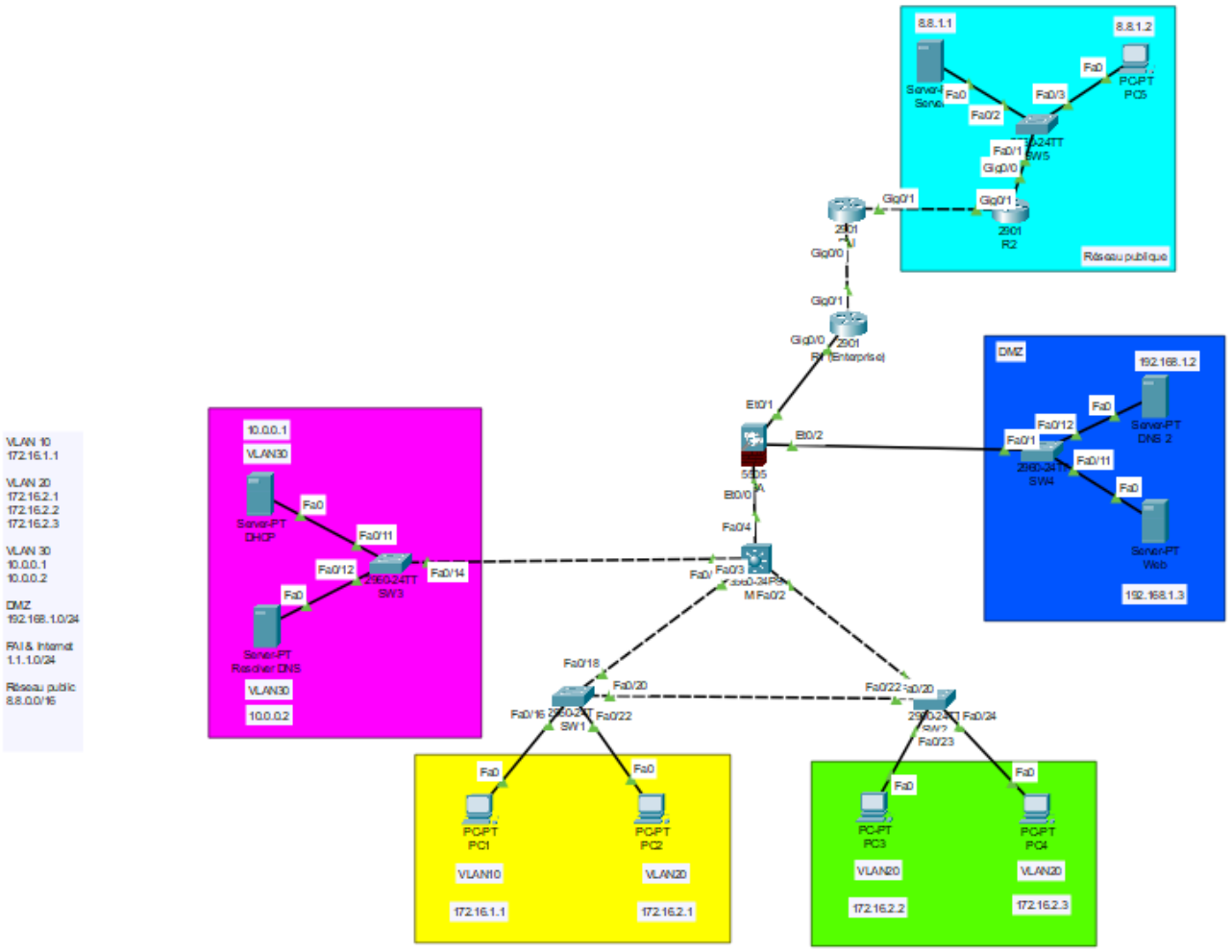
DYSHLEVYY Bohdan
TIBERDANI Nasser
Groupe : 9

SAÉ 21

Construire un réseau informatique pour petite structure

Compte-rendu

Notre topologie:



ETAPE 1 : Construction de coeur de réseau avec les switches d'accès et le Multi-Layer switch

Pour SW1 :

1. 2.Sur le premier switch on passe en mode de configuration globale, puis on renomme ce switch en SW1

SW1#conf t
SW1(config)#hostname SW1

2. On crée les VLANs 10 et 20 et les nomme respectivement VLAN10 et VLAN20, puis on assigne les ports Fa0/15-20 pour le VLAN 10 et Fa0/20-24 pour le VLAN 20 en mode accès.

SW1(config)#vlan 10
SW1((config-vlan)#name VLAN10
SW2(config)#vlan 20
SW1(config-vlan)#name VLAN20
SW1(config)#int range Fa0/15-20
SW1(conf-if-range)#switchport mode access
SW1(conf-if-range)#switchport access vlan 10
SW1(config)#int range Fa0/20-24
SW1(conf-if-range)#switchport mode access
SW1(conf-if-range)#switchport access vlan 20

Pour SW2 :

1. Sur le deuxième switch on passe en mode de configuration globale, puis on renomme ce switch en SW2.

SW2#conf t
SW2(config)#hostname SW2

2. On crée le VLAN 20 et le nomme VLAN20, puis on assigne les ports Fa0/20-24 pour le VLAN 20 en mode accès.

SW2(config)#vlan 20
SW2(config-vlan)#name VLAN20
SW2(config)#int range Fa0/20-24
SW2(conf-if-range)#switchport mode access
SW2(conf-if-range)#switchport access vlan 20

Pour SW3 :

1. Sur le troisième switch on passe en mode de configuration globale, puis on renomme ce switch en SW3.

```
SW3#conf t
SW3(config)#hostname SW3
```

2. On crée le VLAN 30 et le nomme VLAN30, puis on assigne les ports Fa0/10-14 pour le VLAN 30 en mode accès.

```
SW3(config)#vlan 30
SW3(config-vlan)#name VLAN30
SW3(config)#int range Fa0/10-14
SW3(conf-if-range)#switchport mode access
SW3(conf-if-range)#switchport access vlan 30
```

MLS (Multi-Layer Switch) :

1. Sur le quatrième switch on passe en mode de configuration globale, puis on renomme ce switch en MLS.

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

2. On configure le mode STP en PVST (Per-VLAN Spanning Tree) et on définit la priorité pour les VLANs 10, 20 et 30 respectivement.

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

3. On assigne les adresses IP aux interfaces VLANs 10, 20 et 30 respectivement, puis on les active.

```
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
```

4. On active le routage IP sur MLS.

MLS(config)#ip routing

5. On assigne les ports Fa0/1 pour VLAN10 en mode accès ; Fa0/2 pour VLAN20 en mode accès ; Fa0/3 pour VLAN30 en mode accès.

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

6. Après cela on configure Fa0/4 comme un port avec une adresse IP.

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

7. Ensuite on crée ip route vers le réseau entre MLS et ASA.

MLS(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1

Pour SW1 et SW2 (En mode Trunk) :

1. On configure Fa0/20 sur SW1 en mode trunk et on permet les VLANs 10 et 20.

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

2. On configure Fa0/20 sur SW2 en mode trunk et on permet les VLANs 10 et 20.

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

ETAPE 2 : Ajout de l'ASA et du service DHCP

Pour Resolver DNS :

1. On a ajouté deux enregistrements de type A au Resolver DNS et lui avons donné comme nom : « www.test.com » et « www.entreprise.com ».

No.	Name	Type	Detail
0	www.entreprise.com	A Record	192.168.1.3
1	www.test.com	A Record	8.8.8.1

Pour Serveur DHCP :

1. Sur le serveur DHCP on a créé deux pools d'adresse IP, le premier est pour le sous-réseau du Vlan10 et le second pour le Vlan20.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan10	192.168.1...	10.0.0.2	172.16.1.0	255.255.2...	256	0.0.0.0	0.0.0.0
vlan20	192.168.1...	10.0.0.2	172.16.2.0	255.255.2...	256	0.0.0.0	0.0.0.0

Pour ASA :

1. Sur l'ASA on passe en mode de configuration globale, puis on renomme ce firewall en ASA.

ASA#conf t
ASA(config)#hostname ASA

2. On configure le VLAN 1 (inside) et le VLAN 2 (outside) avec les niveaux de sécurité 100 pour VLAN 1 et 0 pour VLAN 2 et on leur attribue les adresses IP respectives.

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

Pour R1 :

1. Sur le premier routeur on passe en mode de configuration globale, puis on renomme ce routeur en R1.

```
R1#conf t
R1(config)#hostname R1
```

2. On configure l'adresse IP sur l'interface Gig0/0 et on l'active

```
R1(config)#int Gig0/0
R1(config-if)#ip add 192.168.11.254 255.255.255.252
R1(config-if)#no shut
```

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

Pour ASA :

1. On passe en mode configuration globale.

```
ASA#conf t
```

2. On configure le VLAN 3, puis on le nomme DMZ et on lui attribue un niveau de sécurité de 50.

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

3. On configure l'adresse IP pour l'interface VLAN 3 (DMZ).

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

4. On configure l'interface e0/2 en mode accès et l'assigne au VLAN 3.

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

5. On indique les routes de l'inside par l'interface Fa0/4 du MLS.

ASA(config)#route inside 172.16.1.0 255.255.255.0 192.168.10.2
ASA(config)#route inside 172.16.2.0 255.255.255.0 192.168.10.2
ASA(config)#route inside 10.0.0.0 255.0.0.0 192.168.10.2

6. On indique les routes de l'outside par l'interface Gig0/0 du R1.

ASA(config)#route outside 0.0.0.0 0.0.0.0 192.168.11.254

7. On crée des listes d'accès pour permettre le trafic HTTP, HTTPS et les réponses ICMP vers la DMZ, puis on applique cette liste à l'interface DMZ.

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

8. On ajoute une ACL à l'interface extérieure pour autoriser le trafic ICMP vers le serveur web.

ASA(config)#access-list outside_access_in extended permit icmp any host 1.1.1.253
ASA(config)#access-group outside_access_in in interface outside

9. On crée l'inspection ICMP, FTP, TFTP et DNS pour qu'on puisse pinger les machines externes quand on passe par l'ASA.

ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#policy-map inspection_default
ASA(config-pmap)#exit

ASA(config)#policy-map type inspect dns preset_dns_map
ASA(config-pmap)#parameters
ASA(config-pmap-p)#message-length maximum 512

ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#inspect ftp
ASA(config-pmap-c)#inspect tftp
ASA(config-pmap-c)#inspect dns preset_dns_map

ASA(config)#service-policy global_policy global

10. On s'assure que les règles NAT pour la traduction des adresses internes et DMZ vers l'extérieur sont correctes.

ASA(config)#object network webserver
ASA(config-network-object)# host 192.168.1.3
ASA(config-network-object)# nat (DMZ,outside) static 1.1.1.253

Pour R1 :

1. On passe en mode configuration globale.

R1#conf t

2. On configure l'interface Gig0/0 avec une adresse IP et comme un interface de NAT inside.

R1(config)#int Gig0/0
R1(config-if)#ip add 192.168.11.254 255.255.255.252
R1(config-if)#ip nat inside
R1(config-if)#no shut

3. On configure l'interface Gig0/1 avec une adresse IP et comme un interface de NAT outside.

R1(config)#int Gig0/1
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#no shut

4. On crée une liste d'accès permettant tout le trafic.

R1(config)#access-list 1 permit any

5. On crée un pool NAT (POOLNAT) pour les adresses IP et on configure la translation d'adresses IP source à partir de la liste d'accès 1 avec overload (NAT masquerading).

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
R1(config)#ip route 8.8.0.0 255.255.0.0 GigabitEthernet0/1
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
R1(config)#ip route 192.168.10.0 255.255.255.0 192.168.11.253
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.253

Pour FAI :

1. Sur le deuxième routeur on passe en mode de configuration globale, puis on renomme ce routeur en FAI.

FAI#conf t
FAI(config)#hostname FAI

2. On configure les adresses IP des interfaces Gig0/0 et Gig0/1.

FAI(config)#int Gig0/0
FAI(config-if)#ip add 1.1.1.2 255.255.255.0
FAI(config-if)#no shut
FAI(config)#int Gig0/1
FAI(config-if)#ip add 1.1.2.129 255.255.255.252
FAI(config-if)#no shut

3. Ensuite on crée ip route vers le réseau entre l'ASA et 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

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

Pour R2 :

1. Sur le troisième routeur on passe en mode de configuration globale, puis on renomme ce routeur en R2.

R2#conf t
R2(config)#hostname R2

2. On configure les adresses IP des interfaces Gig0/0 et Gig0/1.

R2(config)#int Gig0/0
R2(config-if)#ip add 8.8.1.254 255.255.0.0
R2(config-if)#no shut
R2(config)#int Gig0/1
R2(config-if)#ip add 1.1.2.130 255.255.255.252
R2(config-if)#no shut

3. On active le routage EIGRP et configure les réseaux locaux à annoncer.

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

Pour FAI :

1. On active le routage EIGRP et configure les réseaux locaux à annoncer.

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