TD – NAT & IPSEC

Objectif : permettre le fonctionnement d'un tunnel IPSEC avec NAT

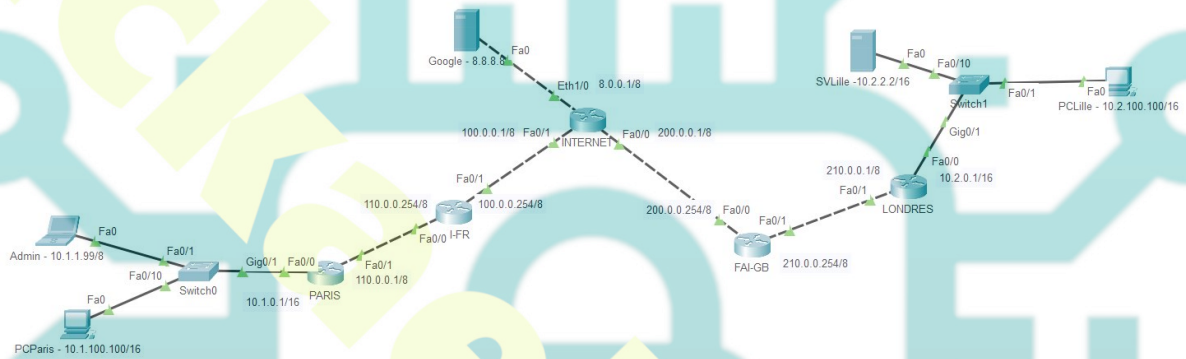

Schéma du TD

Contraintes

On souhaite utiliser le NAT pour l'accès à internet, mais on souhaite également utiliser un tunnel IPSEC entre la station admin de Paris 10.1.1.99/16 et le serveur de Londres 10.2.2.2 et inversement. Cette communication VPN ne doit pas passer par le NAT.

Paramétrage du routeur internet

```
en
conf t
no ip domain-lookup
hostname INTERNET
int fa0/1
ip address 100.0.0.1 255.0.0.0
no shut
int fa0/0
ip address 200.0.0.1 255.0.0.0
no shut
int e1/0
ip address 8.0.0.1 255.0.0.0
no shut
 end
conf t
router rip
version 2
no auto-summary
network 100.0.0.0
network 200.0.0.0
network 8.0.0.0
 end
```

Paramétrage du routeur FAI-FR

```
en
conf t
no ip domain-lookup
hostname FAI-FR
int fa0/1
ip address 100.0.0.254 255.0.0.0
no shut
int fa0/0
ip address 110.0.0.254 255.0.0.0
no shut
 end
conf t
router rip
version 2
no auto-summary
network 100.0.0.0
network 110.0.0.0
 end
```

Paramétrage du routeur FAI-GB

```
en
conf t
no ip domain-lookup
hostname FAI-GB
int fa0/0
ip address 200.0.0.254 255.0.0.0
no shut
int fa0/1
ip address 210.0.0.254 255.0.0.0
no shut
 end
conf t
router rip
version 2
no auto-summary
network 200.0.0.0
network 210.0.0.0
 end
```

Paramétrage du routeur PARIS

```
en
conf t
no ip domain-lookup
hostname Paris
ip route 0.0.0.0 0.0.0.0 110.0.0.254
int fa0/1
ip address 110.0.0.1 255.0.0.0
no shut
int fa0/0
ip address 10.1.0.1 255.255.0.0
no shut
 end

!mise en place du NAT
conf t
int fa0/0
ip nat inside
int fa0/1
ip nat outside
 end

!création d'une liste interdisant à la station admin d'utiliser
le NAT dans une communication avec le serveur de Londres.
conf t
access-list 122 deny ip host 10.1.1.99 10.2.0.0 0.0.255.255

!Le reste de la communication passera par le NAT
access-list 122 permit ip 10.1.0.0 0.0.255.255 any

!application de la règle NAT
ip nat inside source list 122 interface fa0/1 overload
end

!création du VPN entre Paris et Londres
en
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 210.0.0.1
crypto ipsec transform-set monset esp-3des esp-md5-hmac
 end
conf t
access-list 103 permit ip 10.1.0.0 0.0.255.255 10.2.0.0
0.0.255.255
crypto map mysite 20 ipsec-isakmp
set peer 210.0.0.1
set transform-set monset
match address 103
 exit
int fa0/1
crypto map mysite
 end
```

Paramétrage du routeur LONDRES

```
en
conf t
no ip domain-lookup
hostname LONDRES
ip route 0.0.0.0 0.0.0.0 210.0.0.254
int fa0/1
ip address 210.0.0.1 255.0.0.0
no shut
int fa0/0
ip address 10.2.0.1 255.255.0.0
no shut
 end

!nat
conf t
int fa0/0
ip nat inside
int fa0/1
ip nat outside
 end
!création d'une liste interdisant au serveur de Londres
d'utiliser le NAT dans une communication avec la station admin.
conf t
access-list 122 deny ip host 10.2.2.2 10.1.0.0 0.0.255.255
!Le reste de la communication passera par le NAT
access-list 122 permit ip 10.2.0.0 0.0.255.255 any
!application de la règle NAT
ip nat inside source list 122 interface fa0/1 overload
 end

!création du VPN entre Londres et Paris
en
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 110.0.0.1
crypto ipsec transform-set monset esp-3des esp-md5-hmac
 end
conf t
access-list 103 permit ip 10.2.0.0 0.0.255.255 10.1.0.0
0.0.255.255
crypto map mysite 20 ipsec-isakmp
set peer 110.0.0.1
set transform-set monset
match address 103
 exit
int fa0/1
crypto map mysite
 end
```

Tests

- **ping** entre la station admin et Google – doit être OK
- **sh ip nat translations** sur le PARIS – doit afficher la translation de la station admin vers Google
- **ping** entre la station admin et le serveur de Londres – doit être OK
- **sh ip nat translations** sur le PARIS – doit être vide
- **sh crypto isakmp sa** sur PARIS- doit faire apparaitre le vpn en active
- **ping** entre la station admin et la station de Londres – doit être NOT
- **ping** entre PCParis et Google – doit être OK
- **ping** entre PCParis et le serveur de Londres – doit être NOT