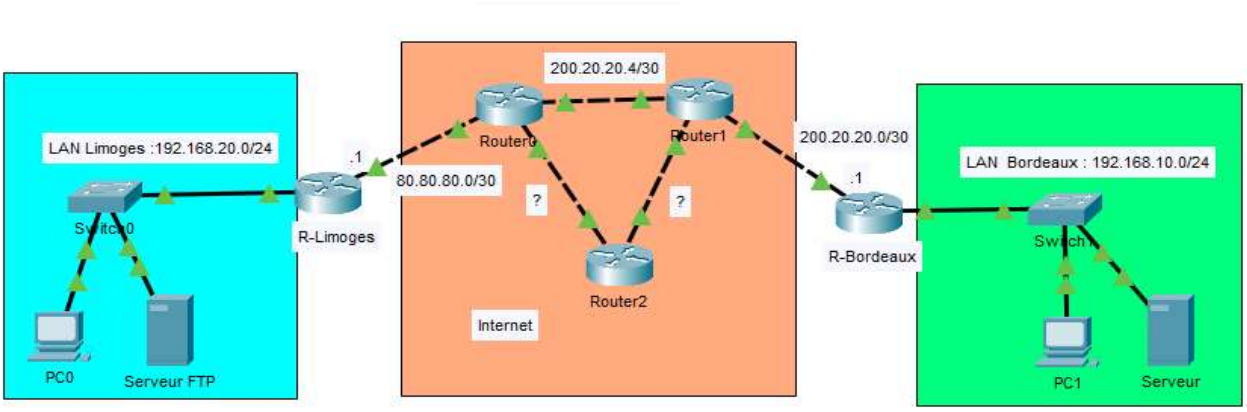
Tunnel VPN IPsec site-à-site

La mise en place d'un tunnel **IPSec** est une solution sécurisée pour interconnecter les différents sites d'une entreprise au travers d'un réseau non sécurisé comme **Internet**. Elle permet en effet d'échanger des données entre sites de manière sécurisée en mettant en œuvre les mécanismes **d'authentification**, de **chiffrement**, et **d'intégrité**.

IPSec utilise le chiffrement **asymétrique** et **symétrique** pour assurer la rapidité et la sécurité du transfert des données. Dans le cas du chiffrement asymétrique, la clé de chiffrement est rendue publique tandis que la clé de déchiffrement reste privée. IPSec établit une connexion sécurisée avec un chiffrement asymétrique et passe au chiffrement symétrique pour accélérer le transfert des données.

Maquette de l'atelier :



1. Activation du module « securityk9 »

Sous Packet tracer, il faut dans un premier temps activer le module de sécurité **securityk9** sur les routeurs 2911 de Limoges et de Bordeaux :

- Exécutez la commande ***show version*** pour vérifier que la licence du pack sécurité n'est pas activée.
- Activez le module **securityk9** avec la commande suivante :

```
R(config)#license boot module c2900 technology-package securityk9
```

- Sauvegarder la configuration puis, redémarrer le routeur :

```
R# copy run start
R# reload
```

- Vérifier l'activation du pack **securityk9** :

```
# show version
```

2. Adressage IP

Réaliser l'adressage des PC et des interfaces des routeurs.

3. Routage dynamique OSPF

- Configurer le routage dynamique sur les routeurs Internet.
- Vérifier la connectivité entre les différents réseaux.

4. Mise en place du VPN

L'objectif est de mettre en place un **tunnel VPN IPsec** reliant les routeurs R-Limoges et R-Bordeaux afin de **sécuriser** le trafic transitant entre les réseaux 192.168.20.0/24 et 192.168.10.0/24.

La configuration du **tunnel VPN IPsec** sur les routeurs Limoges et Bordeaux, consiste à définir les paramètres des 2 phases suivantes :

a. Phase 1 :

Pendant cette phase, les deux routeurs négocient les conditions requises pour établir une connexion sécurisée. Elle inclut un accord mutuel sur les paramètres de chiffrement, d'authentification et d'autres associations de sécurité (AS).

A faire :

- Stratégie ISAKMP numérotée 10 :

```
R-Limoges(config)#crypto isakmp policy 10
```

- Chiffrement : AES

```
R-Limoges(config-isakmp)#encryption aes
```

- Authentification par clé pré-partagée ;
- Groupe Diffie-Hellman : 5 ;
- Renégociation : toutes les 15 minutes ;

```
R-Limoges(config-isakmp)#authentication pre-share
R-Limoges(config-isakmp)#group 5
R-Limoges(config-isakmp)#lifetime 900
R-Limoges(config-isakmp)#exit
```

- Définition de la clé pré-partagée « cisco1234 » et l'adresse du routeur homologue :

```
R-Limoges(config)#crypto isakmp key cisco1234 address @ip-R-Bordeaux
```

Explications :

Ces premières commandes permettent la définition d'une **stratégie IKE** (Internet Key Exchange) portant le n° 10. Cette stratégie utilise le protocole de chiffrement AES (Advanced Encryption standard), une méthode d'authentification basée sur une clé pré-partagée spécifiée, un échange de clé Diffie-Hellman de groupe 5 et une renégociation toutes les 15 minutes (soit 900 secondes). Il s'agit de la phase 1.

Les deux routeurs VPN devront avoir une **stratégie IKE commune** et avoir **validé** entièrement **la phase 1** avant de pouvoir passer à l'étape suivante, c'est-à-dire la phase 2.

b. Phase 2 :

- IPsec SA (Security Association) numérotée **50** avec authentification AH/SHA et chiffrement ESP/3DES :

```
R-Limoges(config)#crypto ipsec transform-set 50 ah-sha-hmac esp-3des
```

- Crypto map : **MYMAP** associée à la stratégie IKE n° 10 et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes :

```
R-Limoges(config)# crypto map MYMAP 10 ipsec-isakmp
R-Limoges(config-crypto-map)#set peer @ip-R-Bordeaux
R-Limoges(config-crypto-map)#set security-association lifetime seconds
                              1800
R-Limoges(config-crypto-map)#set transform-set 50
R-Limoges(config-crypto-map)#match address 101
R-Limoges(config-crypto-map)#exit
```

- Application de la crypto map à l'interface gig0/1 :

```
R-Limoges(config)#interface gig0/1
R-Limoges(config-if)#crypto map MYMAP
```

- Création de l'ACL n° **101** (192.168.20.0 /24 > 192.168.10.0 /24).

```
R-Limoges(config)#access-list 101 permit ip 192.168.20.0 0.0.0.255
192.168.10.0 0.0.0.255
```

Explications :

Les commandes ci-dessus indiquent les modifications (transformations) à appliquer aux paquets IP en termes de chiffrement et hachage (ESP-AES, AH-SHA-HMAC).

Elles permettent également de définir le routeur homologue, la durée de vie de l'association de sécurité, la stratégie de transformation à utiliser (ici 50), ainsi qu'une ACL (ici 101) pour définir quel trafic sera soumis au tunnel. Il s'agit de la phase 2.

Pour terminer, les paramètres du tunnel IPsec sont associés à **l'interface gig0/1.**

5. Configuration du 2ème routeur : R-Bordeaux

La configuration du routeur de Bordeaux est quasi identique à celle du routeur de Limoges (hormis bien sûr, **l'homologue** et **l'ACL** qui diffèrent).

Reprenez les mêmes commandes en faisant attention aux points suivants :

```
R-Bordeaux(config)#crypto isakmp key cisco1234 address ????
```

```
R-Bordeaux(config-crypto-map)#set peer ????
```

```
R-Bordeaux(config)#interface ???
```

```
R-Bordeaux(config)#access-list 101 permit ip ????
```

6. Tests

- **Tracert**
  Vérifiez le routage des paquets IP au travers du tunnel IPsec en testant avec la commande **`tracert`** entre les hôtes distants. **Que remarquez-vous ?**
- En mode simulation, analyser le contenu des paquets IP échangés via le VPN. **Réaliser des copies d'écran.**

7. Diagnostic des routeurs VPN

- **IKE**

  #show crypto isakmp policy

  #show crypto isakmp sa

  #show crypto isakmp peers

- **IPSEC**

  #show crypto ipsec ?

  #show crypto ipsec sa

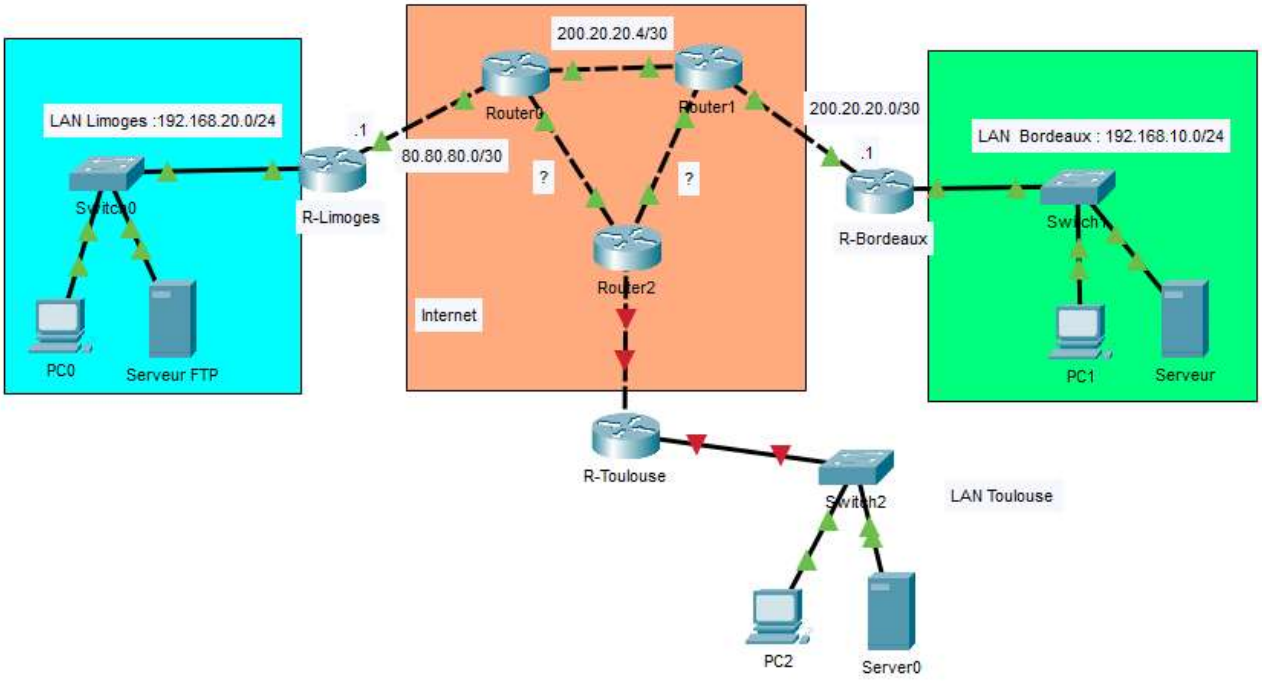
#show crypto ipsec transform-set

- **DEBUG**

#debug crypto isakmp

#debug crypto ipsec

8. Ajout d'un autre réseau distant



- Ajouter le réseau de Toulouse comme indiqué sur la maquette.
- Etablir un plan d'adressage cohérent pour interconnecter ce réseau aux autres sites.
- Configurer le routage statique.
- Mettre en place un VPN entre le site de Toulouse et celui de Bordeaux.
- Mettre en place un VPN entre le site de Toulouse et celui de Limoges.
- Tester le fonctionnement des VPN.