**Institut Universitaire des Sciences**

**Faculté des Sciences et Technologies**

**Td6 dans le cadre du cours de Réseaux 2**

**Préparé par Wendy COLAS**

**A l’attention de Monsieur Ismaël SAINT AMOUR**

**Mai 2025**

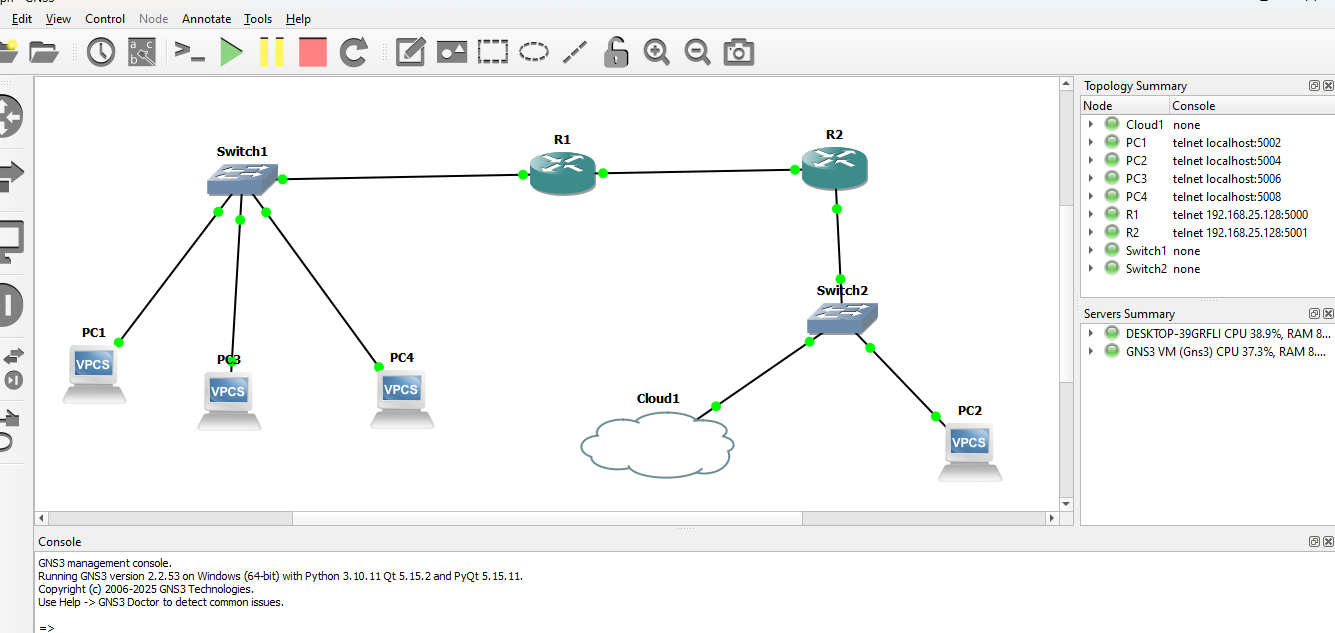
# Reproduction de la topologie en configurant un VPN site-à-site

## Introduction

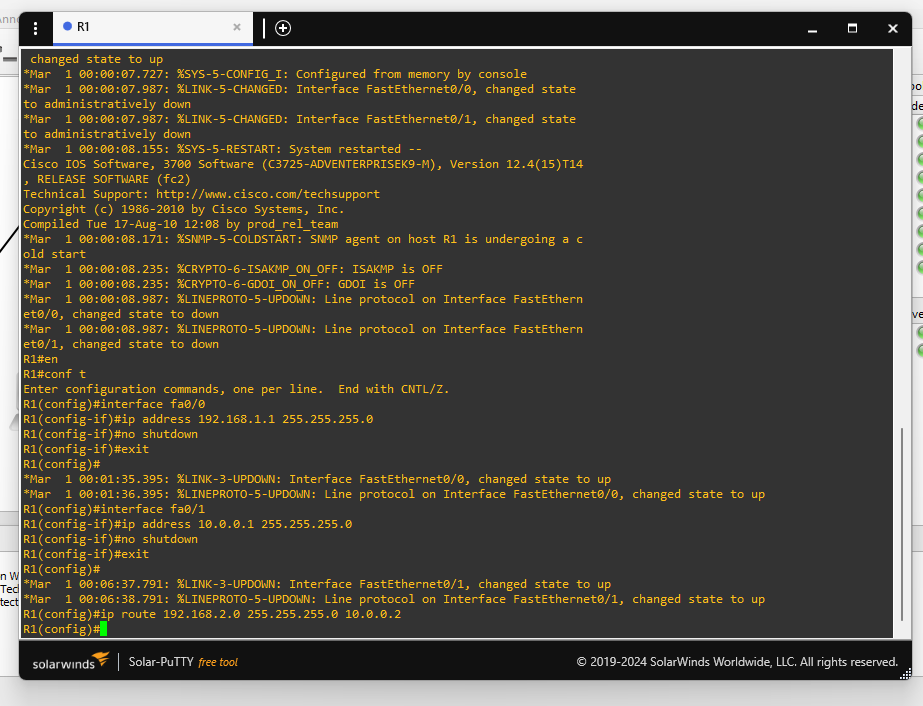
Dans ce document, nous détaillons le processus de configuration d’un VPN site-à-site afin de sécuriser les échanges entre deux réseaux. Cette configuration implique l’utilisation de routeurs, de VPCS et d’outils tels que Solar-PuTTY pour l’administration. Chaque étape est illustrée par une image accompagnée d’une explication détaillée.

## Étapes de la configuration

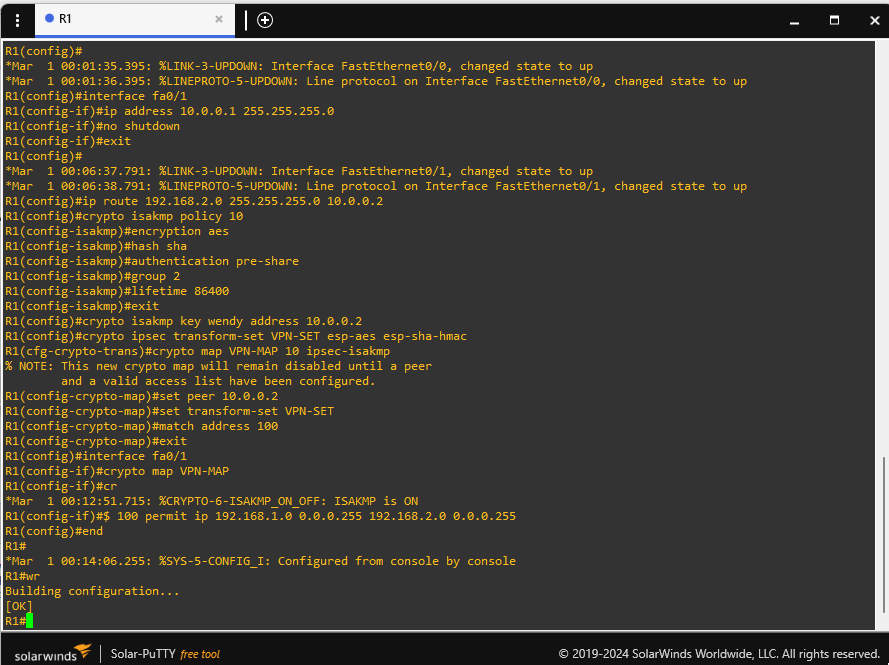
### 1. Topologie réseau initiale

  
La topologie initiale est conçue sur GNS3 et comporte des routeurs, des switchs et des PC simulés. Cette architecture permet une connexion étendue et la mise en œuvre du VPN.

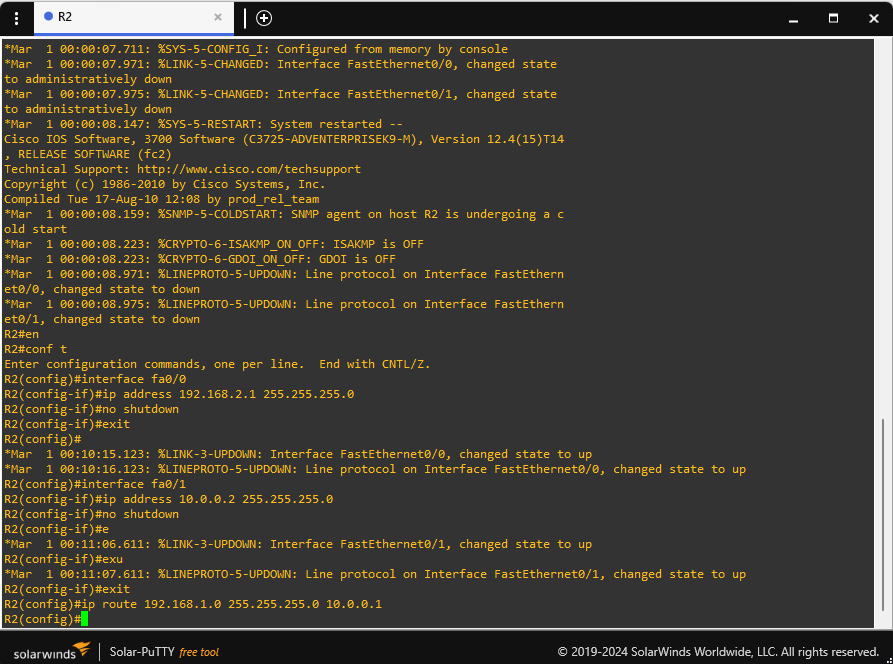
### 2. Configuration du premier routeur (R1)

  
À l’aide de Solar-PuTTY, nous configurons les interfaces de R1 et attribuons les adresses IP nécessaires à la communication entre les sous-réseaux.

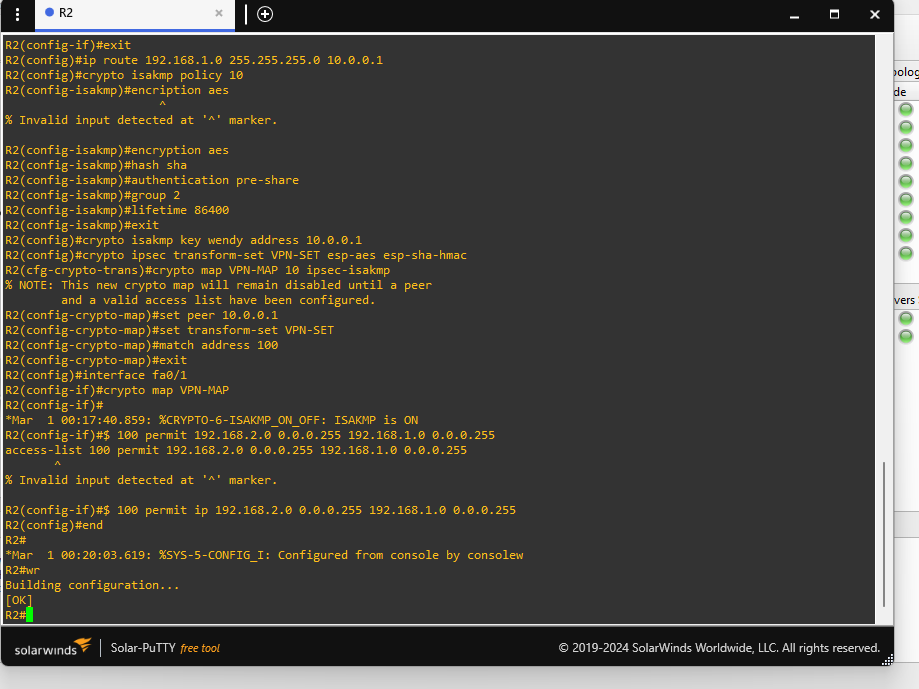
### 3. Configuration du second routeur (R2)

  
Le routeur R2 est configuré avec ses interfaces réseau et routes statiques afin d’assurer la communication avec R1 et les PC du réseau.

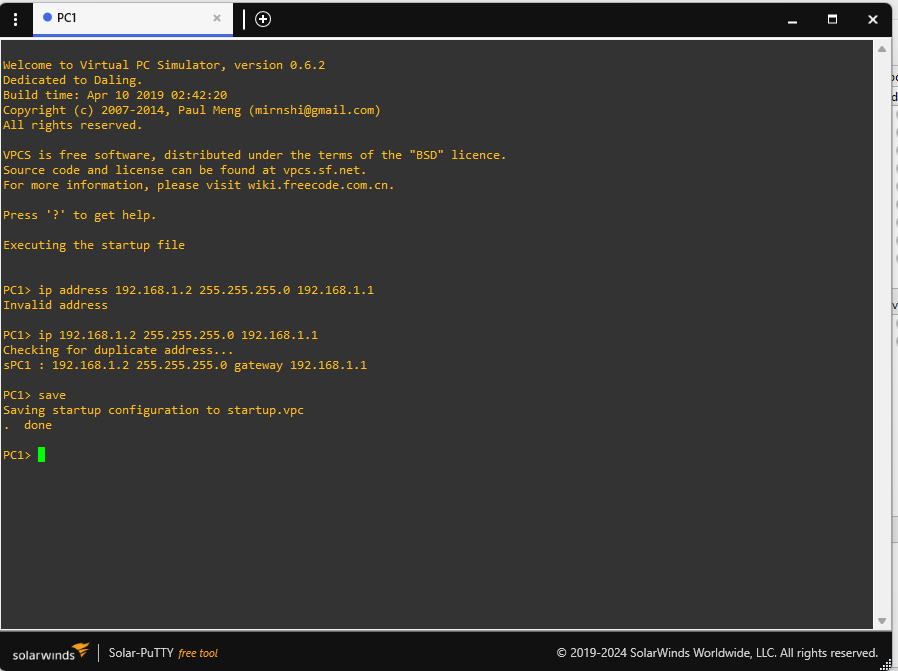
### 4. Vérification de l’état des interfaces

  
Une vérification est effectuée pour s’assurer que les interfaces sont bien actives et que les routes sont correctement définies.

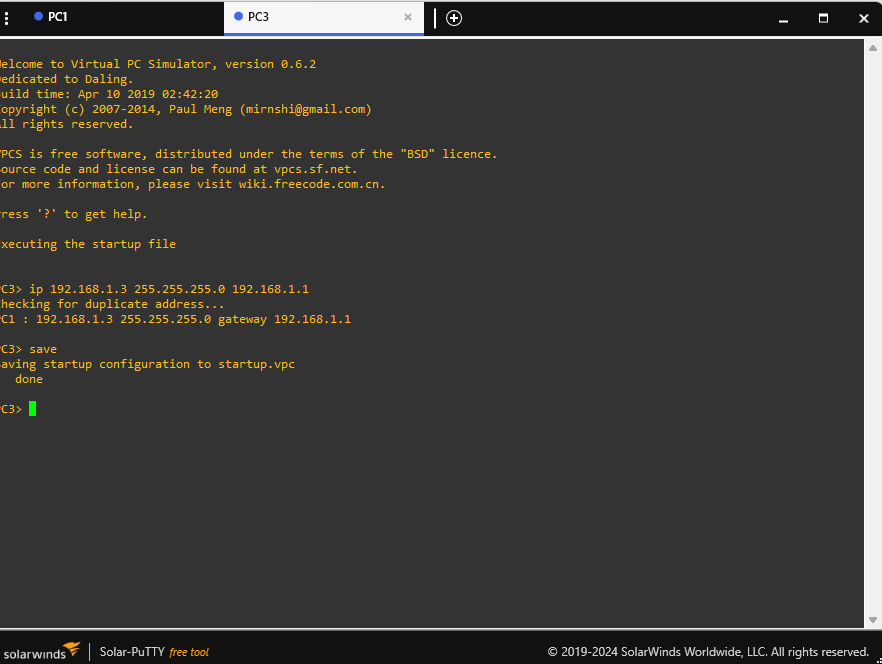
### 5. Test de communication entre les sous-réseaux

  
Un test de connectivité est réalisé entre les sous-réseaux via des commandes ping.

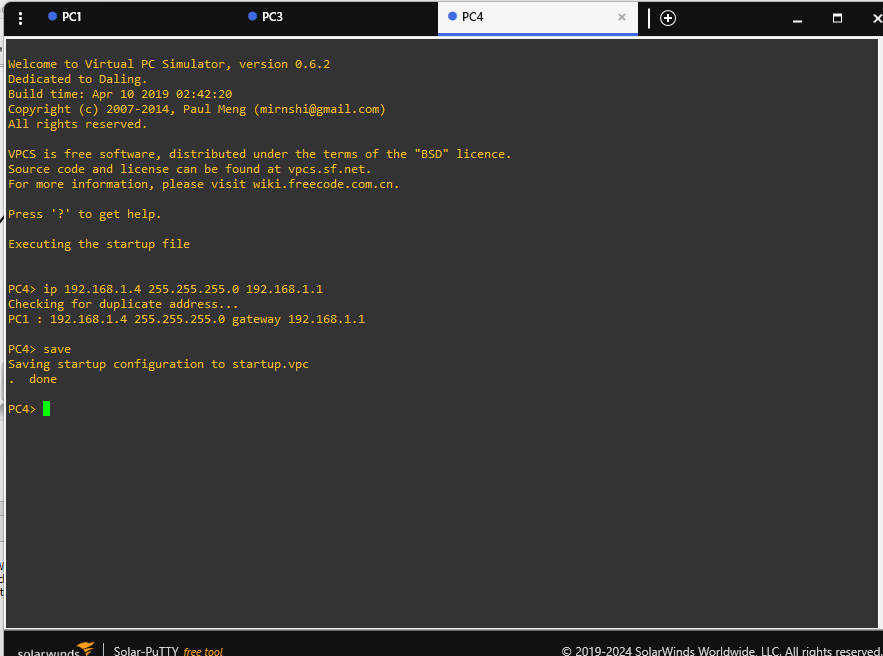
### 6. Configuration des routes statiques

  
Les routes statiques sont mises en place sur R2 pour garantir l’acheminement du trafic entre les réseaux.

### 7. Mise en place de la sécurité avec IPsec et ISAKMP

  
La configuration VPN débute avec l’établissement des règles de sécurité IPsec et des paramètres ISAKMP.

### 8. Vérification des associations de sécurité

  
Un état des associations de sécurité IPsec et ISAKMP est vérifié pour s’assurer que le tunnel VPN est bien actif.

### 9. Débogage des configurations VPN

  
Une analyse des logs est effectuée pour identifier d’éventuels problèmes de connexion et d’authentification.

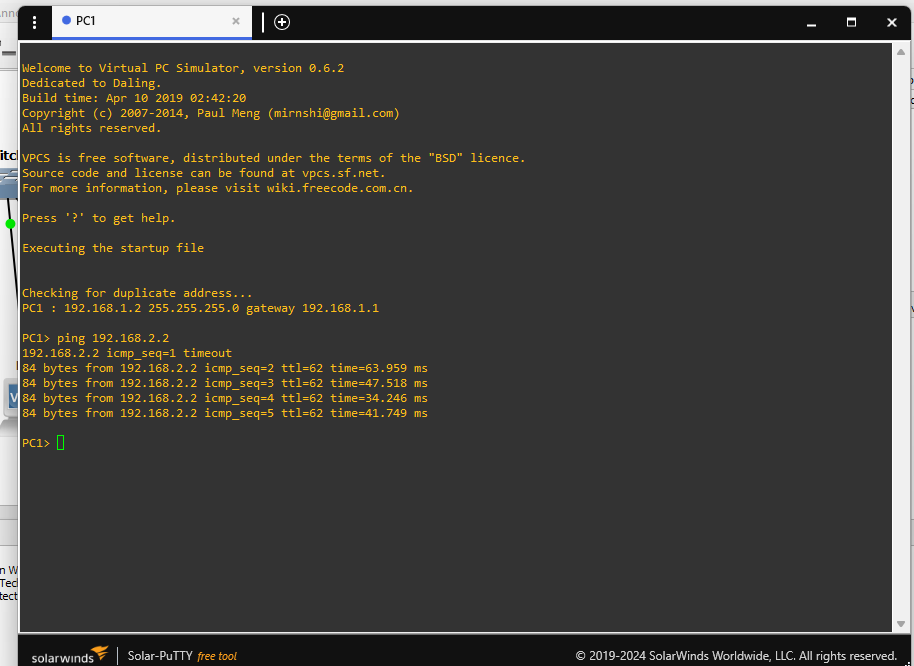
### 10. Simulation du trafic via VPCS

  
Les tests de communication entre les machines via VPCS confirment la fonctionnalité du VPN.

### 11. Correction et validation finale

  
Des ajustements sont apportés aux configurations pour garantir un tunnel sécurisé et efficace.

### 12. Vérification finale de la communication VPN

  
Un dernier test est effectué pour valider le bon fonctionnement du VPN site-à-site avant sa mise en production.

## Conclusion

La configuration d’un VPN site-à-site permet de sécuriser les communications entre deux réseaux distants. Grâce à l’utilisation d’IPsec, ISAKMP et des routes statiques, les échanges sont protégés et le trafic est correctement acheminé entre les sous-réseaux. Ce document détaille chaque étape du processus avec des explications et des illustrations pour une compréhension approfondie.

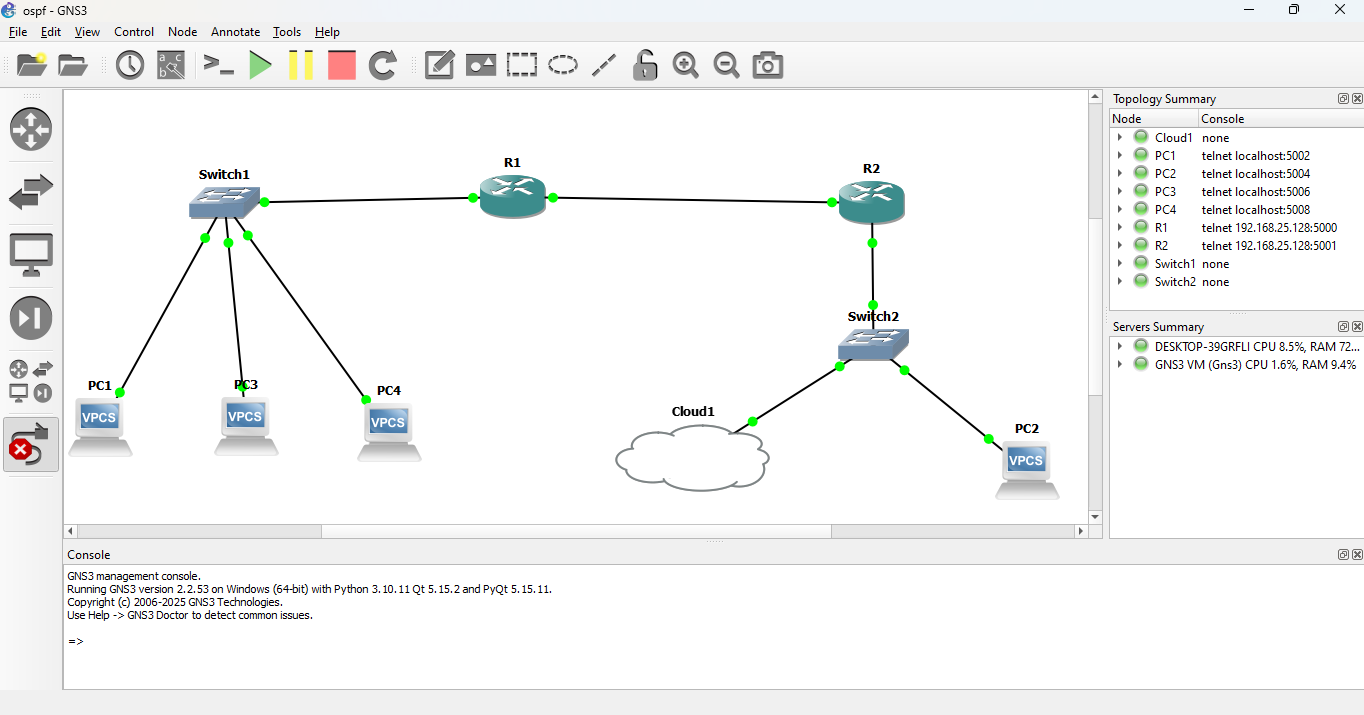
# Reproduction de la topologie en configurant un VPN GRE over IPSec avec Routage Dynamique (OSPF)

## Introduction

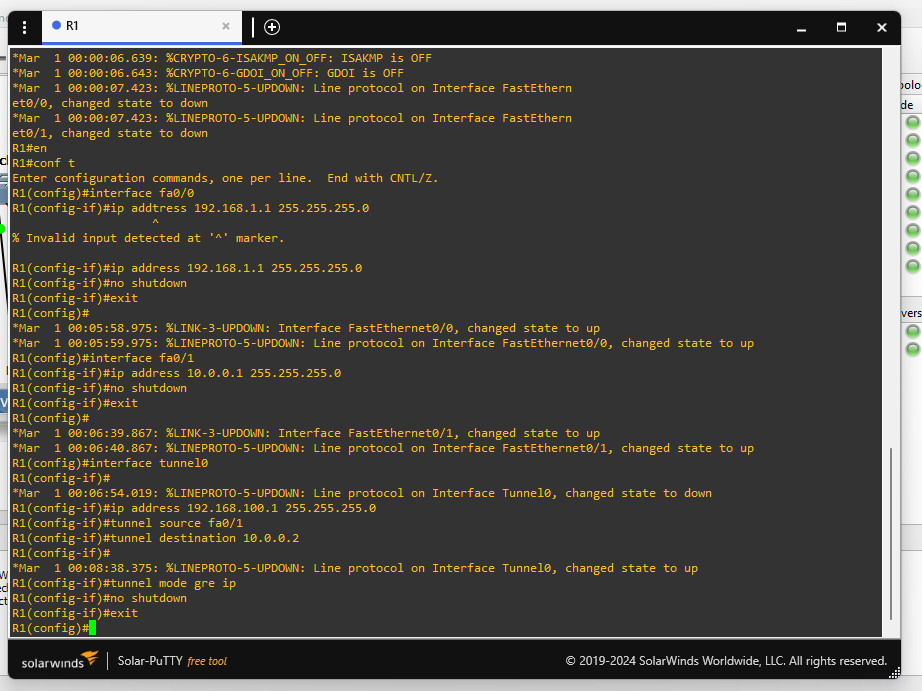
Dans ce document, nous détaillons le processus de configuration d’un **VPN GRE over IPSec** avec **routage dynamique OSPF**. Cette approche permet d’assurer la sécurité des échanges entre sites tout en bénéficiant de la flexibilité du routage dynamique. Nous utilisons **GNS3, Solar-PuTTY et Virtual PC Simulator (VPCS)** pour simuler l’environnement. Chaque étape est illustrée avec des images et des explications détaillées.

## Étapes de la configuration

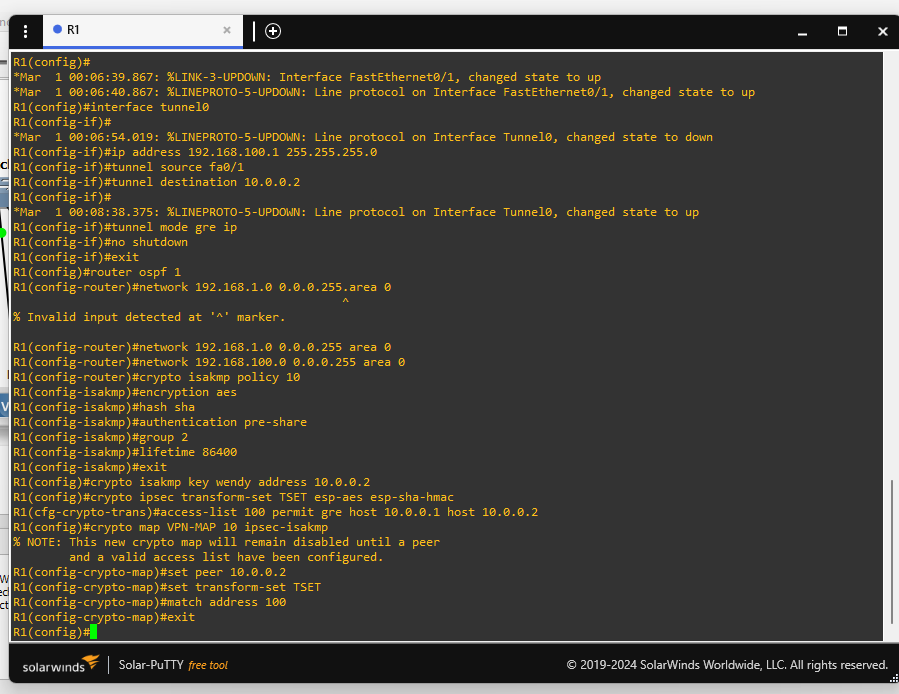
### 1. Conception de la topologie réseau

  
La topologie est construite sous **GNS3**, incluant **routeurs, switches, PC, et connexions vers le cloud**, créant un environnement de simulation réaliste.

### 2. Configuration du premier routeur (R1)

  
R1 est configuré avec **interfaces IP, tunnel GRE, et routage OSPF**. Les paramètres ISAKMP et IPsec sont définis pour chiffrer les échanges via le VPN.

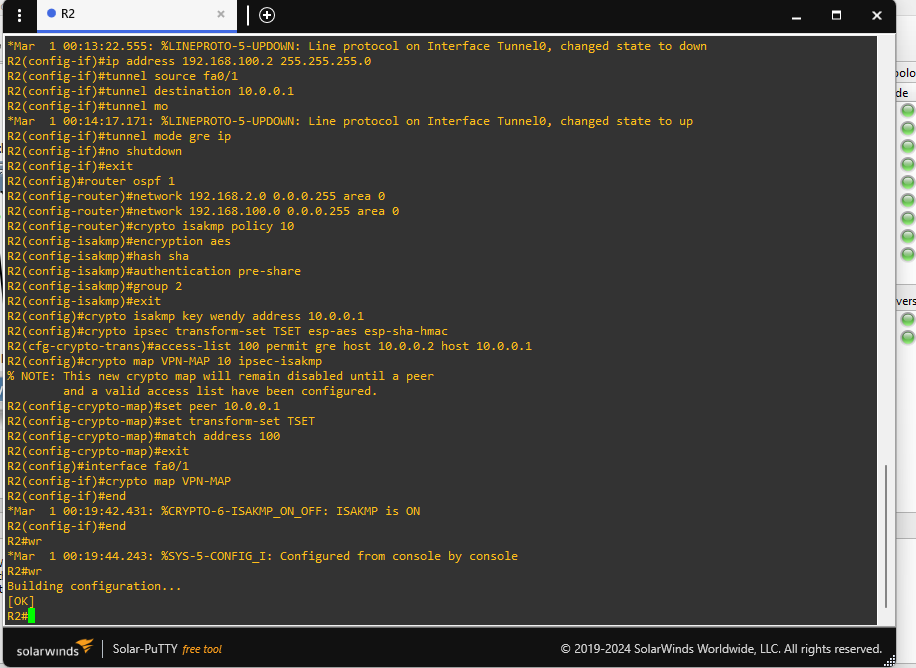
### 3. Configuration du second routeur (R2)

  
R2 est configuré avec ses **interfaces réseau, tunnel GRE et routage OSPF**, garantissant l’interconnexion sécurisée entre les sites.

### 4. Configuration de PC1 dans Virtual PC Simulator

  
PC1 est attribué l’adresse **192.168.1.2**, avec **192.168.1.1** comme passerelle.

### 5. Configuration de PC2 dans Virtual PC Simulator

  
PC2 est configuré avec **192.168.2.2** et la passerelle **192.168.2.1**.

### 6. Vérification du tunnel GRE sur R1

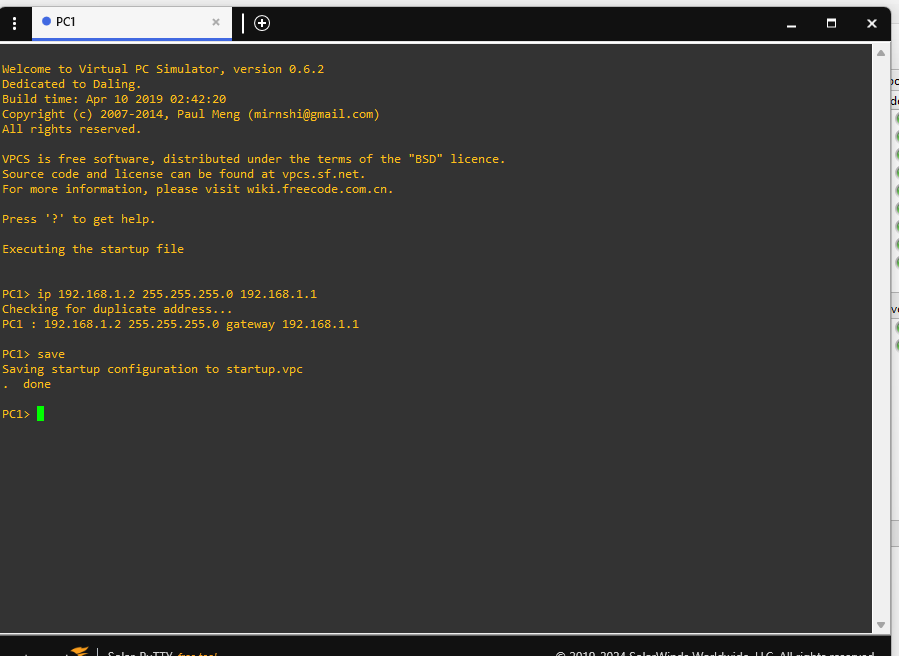


Image 18

### 7. Vérification des associations IPsec et ISAKMP

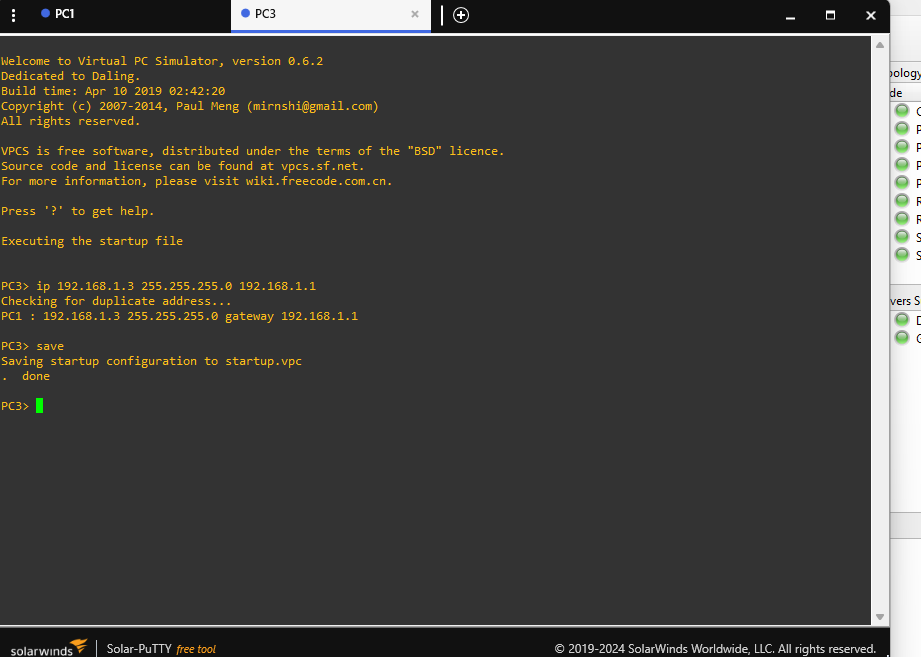


Image 19

### 8. Débogage de la connectivité tunnel



Image 20

### 9. Test de communication avec PC1

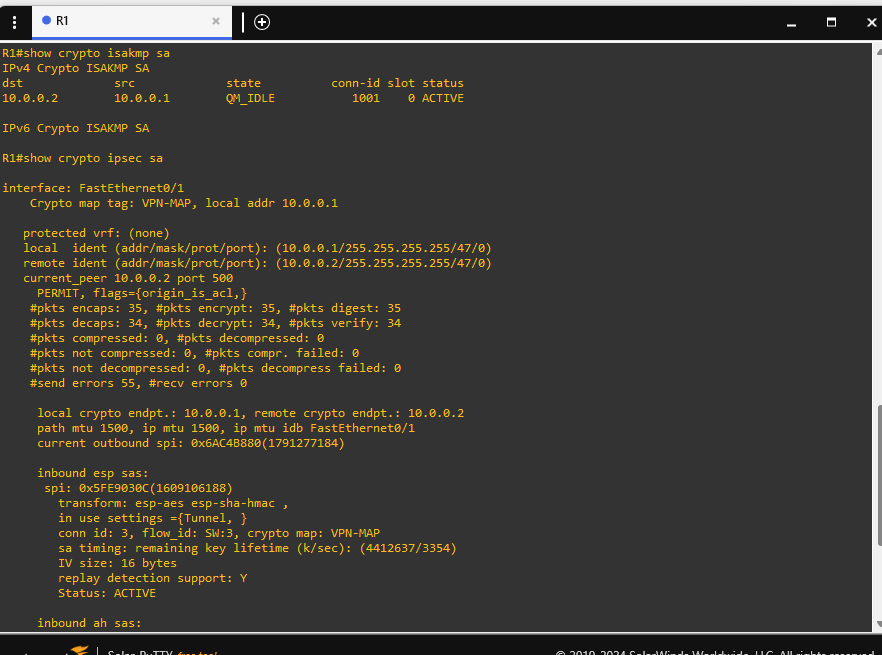


Image 21

### 10. Vérification finale du routage dynamique OSPF

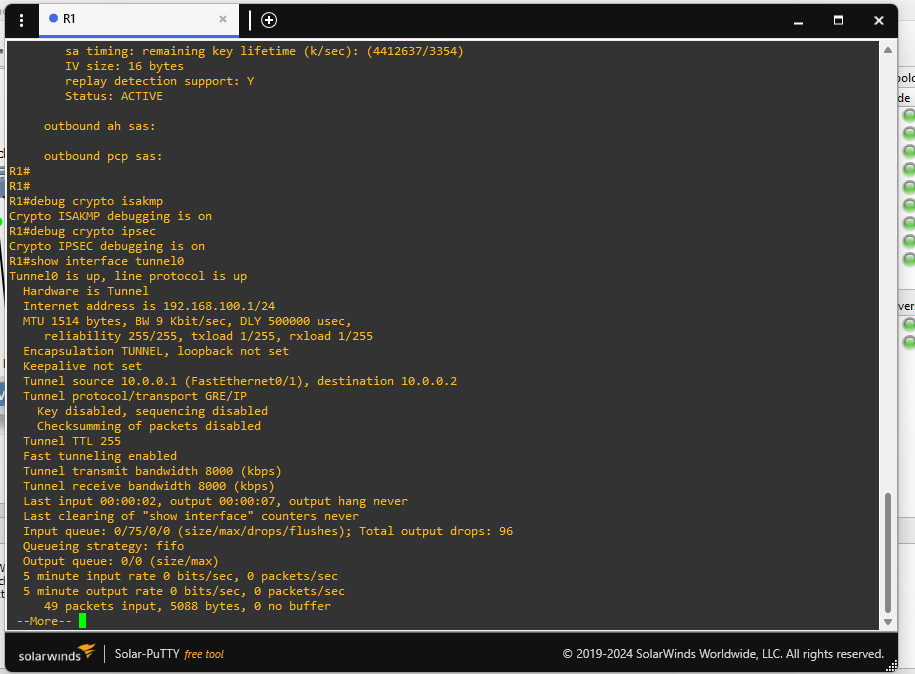
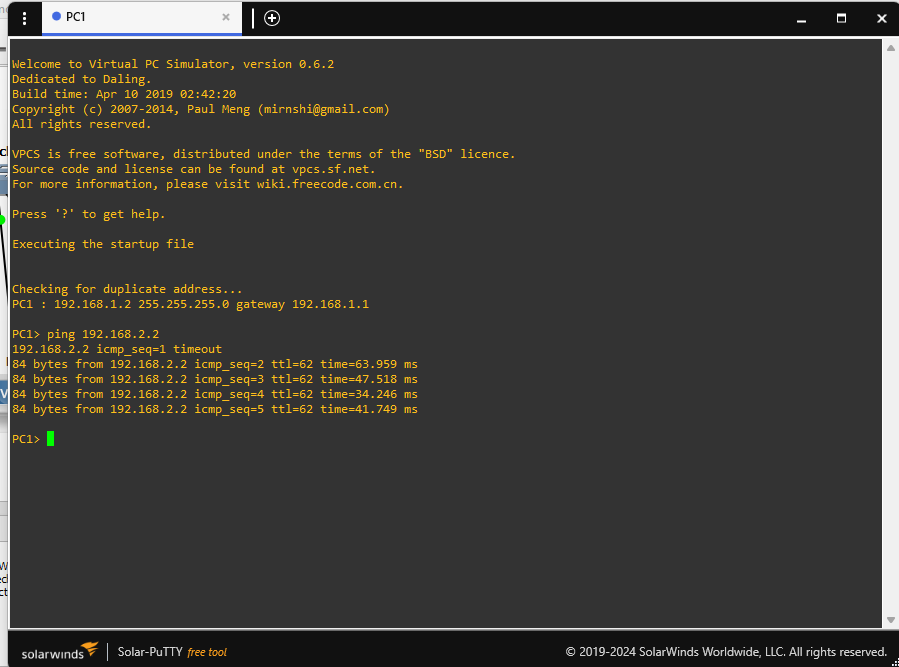
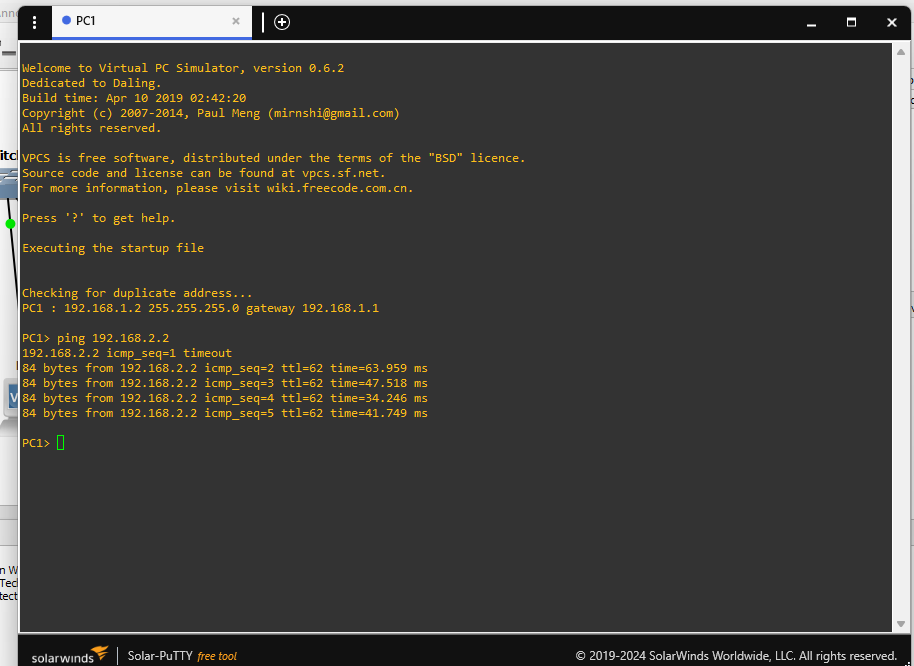


Image 22

### 11. Optimisation des configurations VPN et routage

  
Des ajustements sont apportés aux **paramètres GRE, IPsec et ISAKMP** pour assurer une fluidité des échanges sécurisés.

### 12. Test de performance et validation finale

  
Une dernière série de tests est réalisée pour valider le bon fonctionnement du **VPN GRE over IPSec avec OSPF**, confirmant que le trafic passe correctement.

## Conclusion

La mise en place d’un **VPN GRE over IPSec** avec **routage dynamique OSPF** offre une solution sécurisée et flexible pour l’interconnexion des sites distants.