



(FST)

Niveau : L3-FST

Réseaux 1

Soumis au chargé de cours : Ismaël SAINT AMOUR

Préparé par : Jameson DOMINIQUE

Date : 07 Mars 2025

Réseaux 1

Configuration d'un Pare-feu et d'un VPN Site-à-Site sur Cisco Packet Tracer.

TD 8

Objectif :

Ce TD offre une configuration de base de pare-feu, et les bases de la configuration d'un VPN site-à-site dans Cisco PacketTracer.

1. Configurer un pare-feu sur un routeur Cisco en utilisant des listes de contrôle d'accès (ACL).
2. Bloquer et autoriser certains types de trafic réseau.
3. Tester la connectivité et la sécurité du réseau
4. Configurer un VPN Site-à-Site entre deux routeurs Cisco.
5. Sécuriser la communication entre deux réseaux distants en utilisant **IPsec**.
6. Tester la connectivité et vérifier le bon fonctionnement du VPN.

Étapes du TD :

Configuration d'un Pare-feu

Topologie

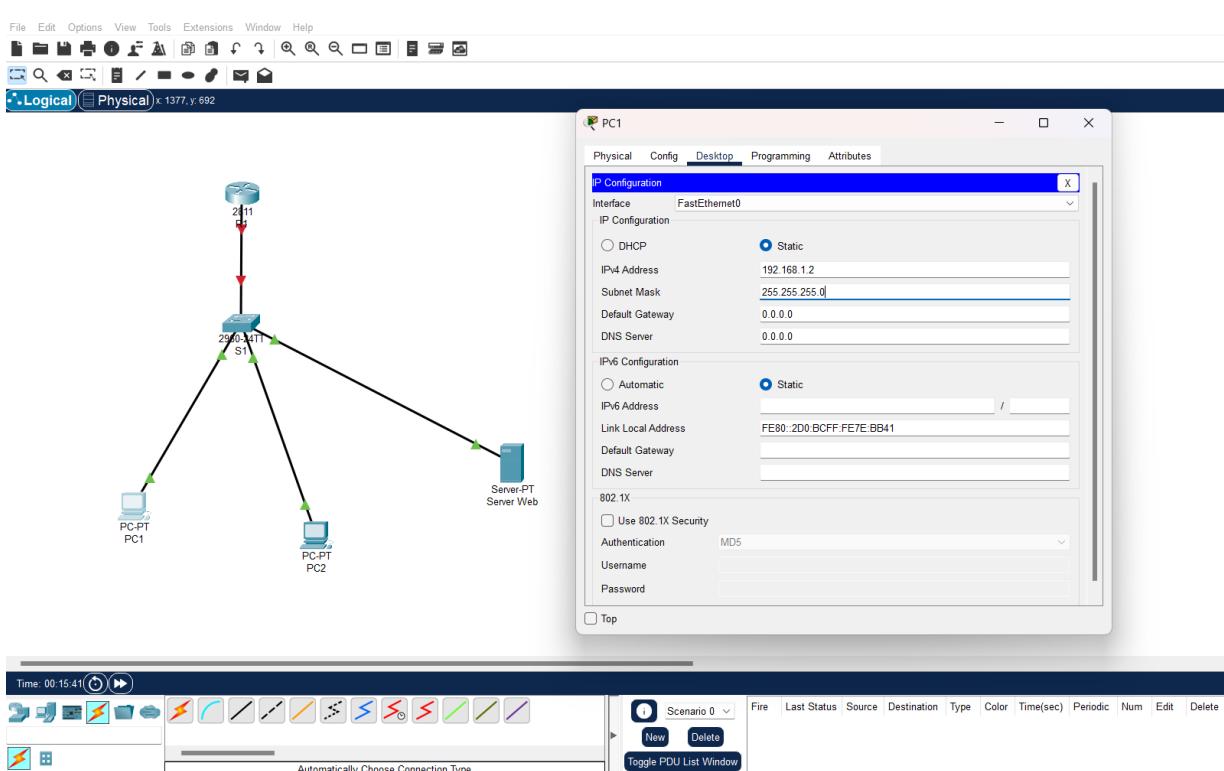
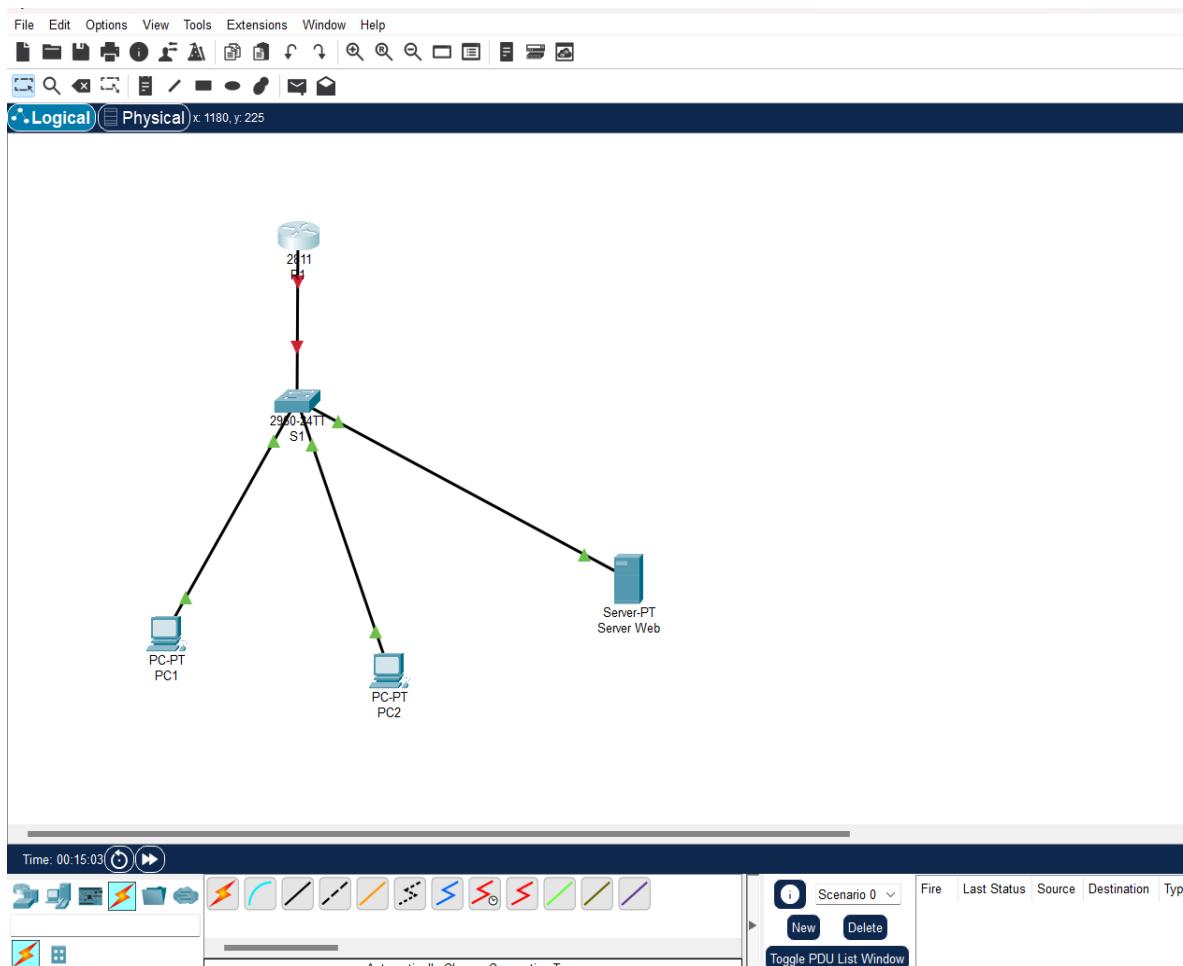
1 routeur Cisco (ex : 2811)

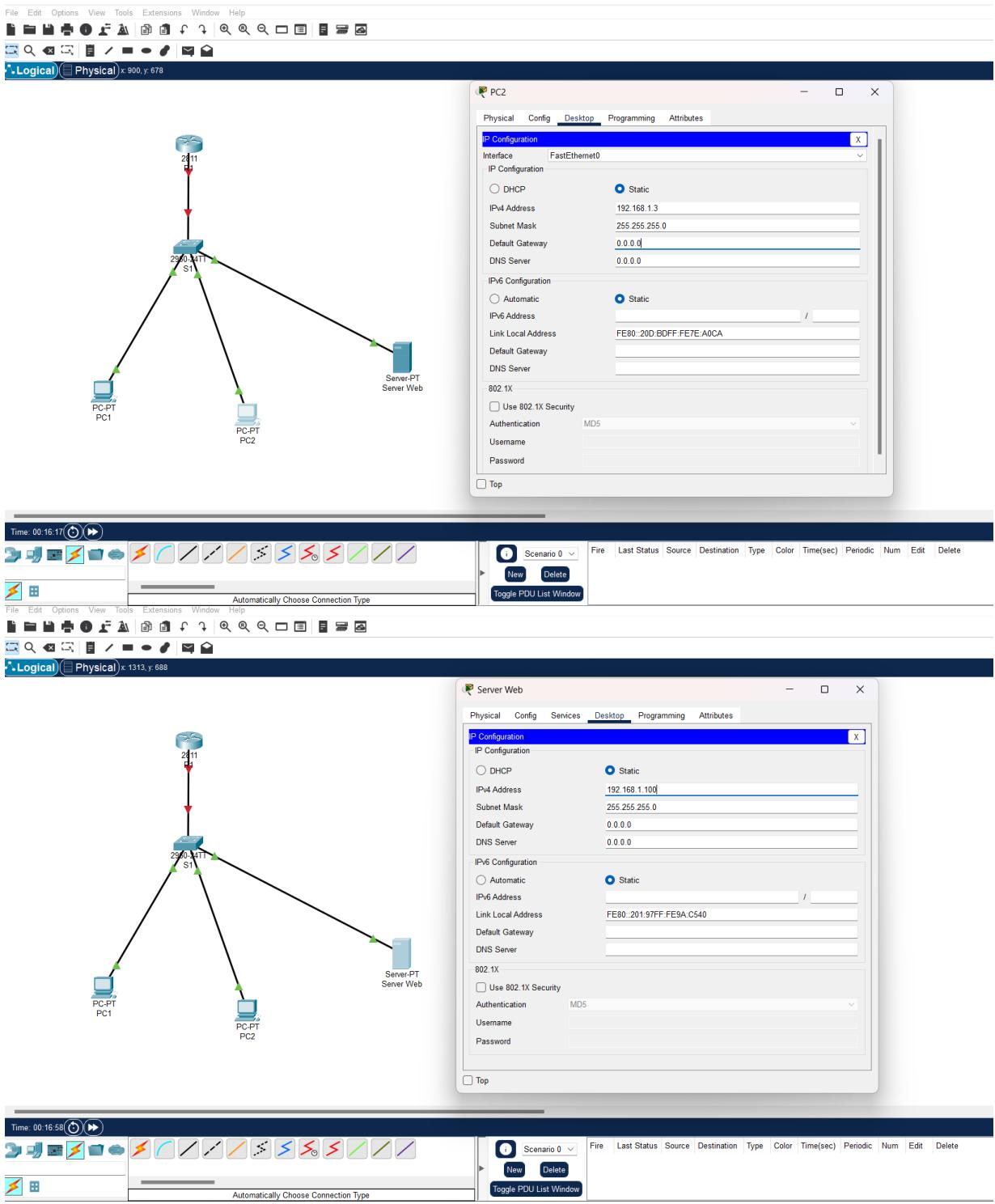
1 switch Cisco (ex : 2960)

3 PC (PC1, PC2, Serveur Web)

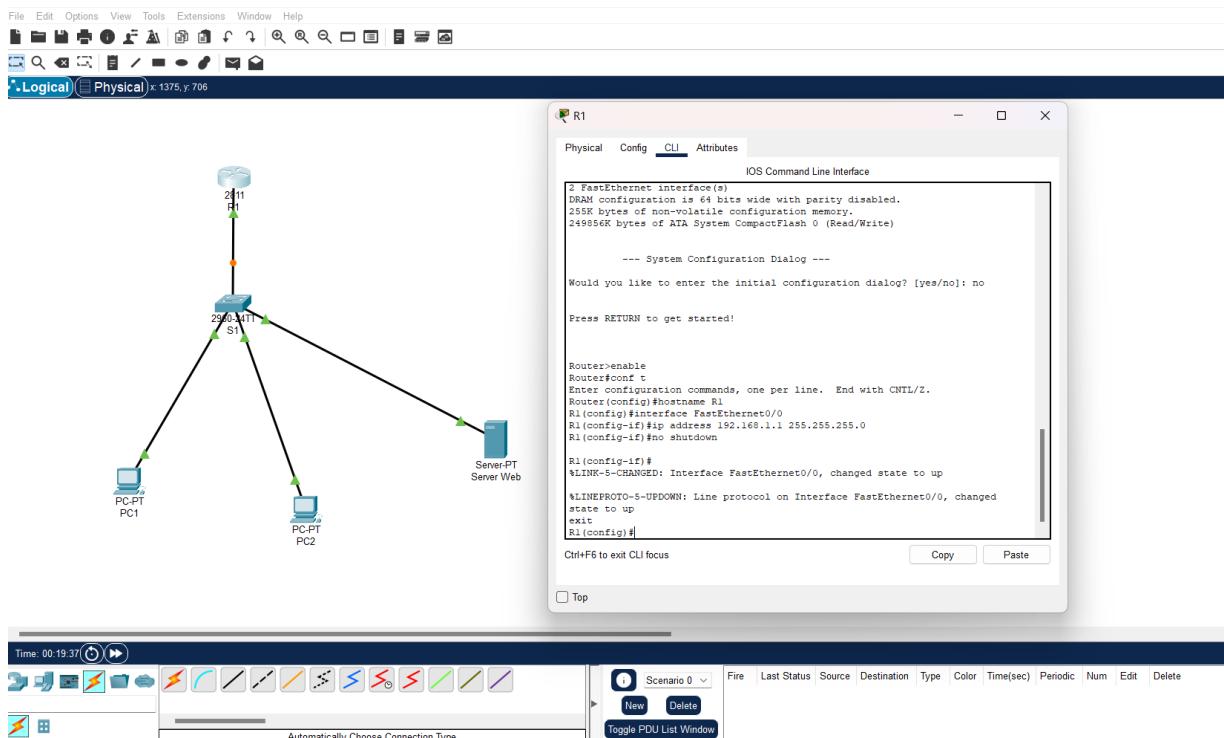
1. Architecture du Réseau

Périphérique	Adresse IP	Rôle
PC1	192.168.1.2	Client (Autorisé)
PC2	192.168.1.3	Client (Bloqué)
Serveur Web	192.168.1.100	Serveur Web (HTTP)
Routeur (R1)	192.168.1.1	Passerelle pare-feu
		-

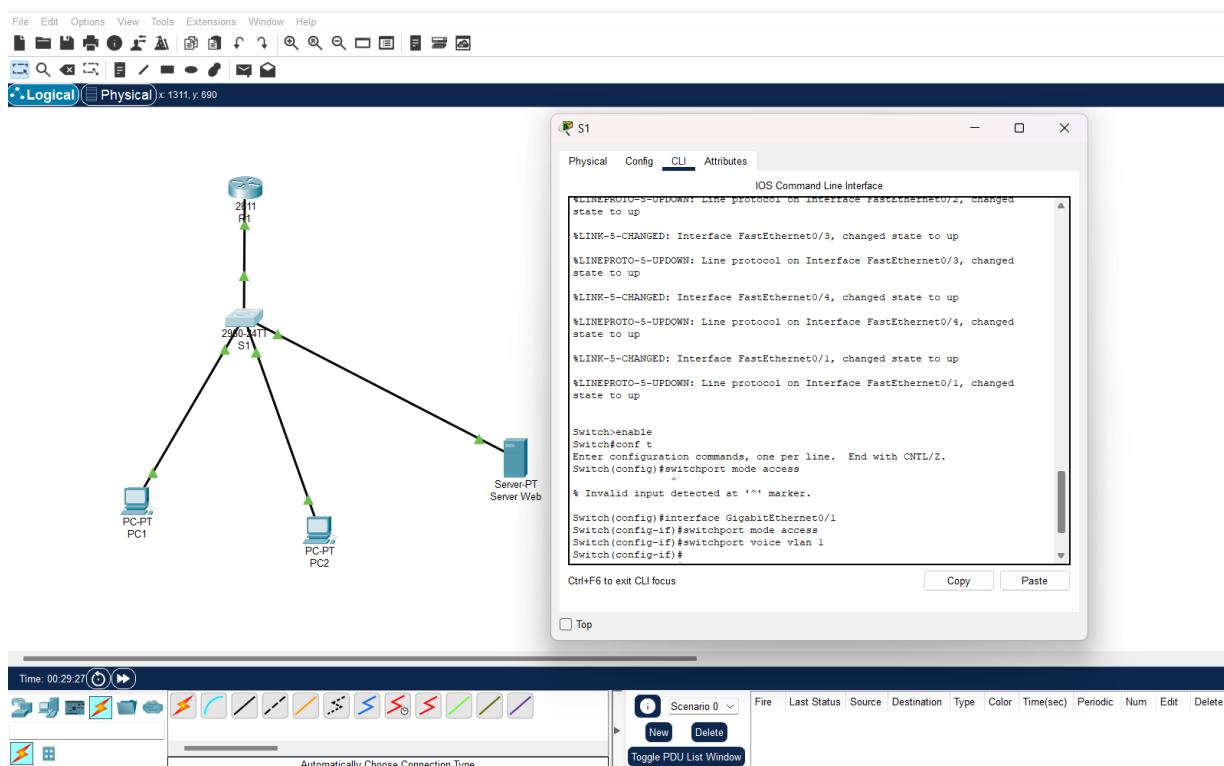




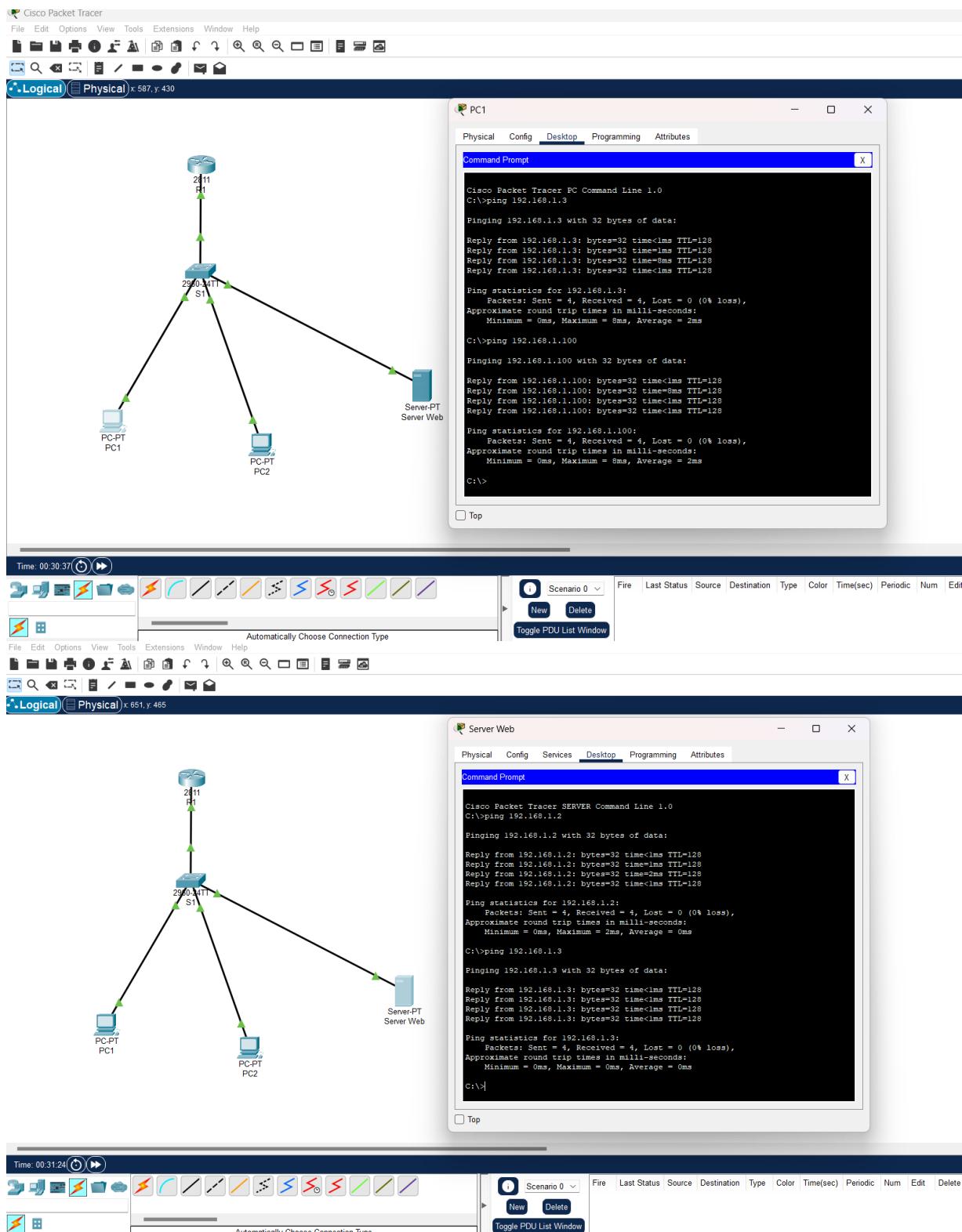
2. Configuration de Base du Routeur



3. Configuration du commutateur



4. Configurez les adresses IP des autres dispositifs et vérifiez la connectivité avec les PC.

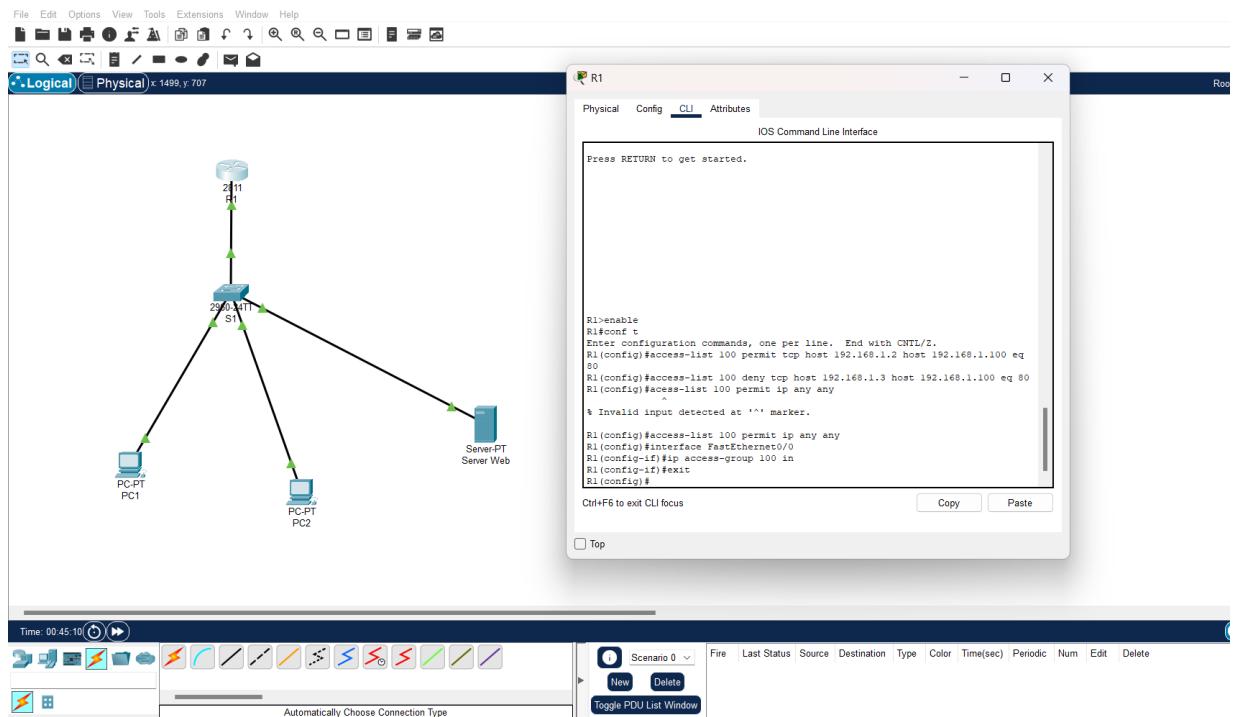


5. Configuration des Listes de Contrôle d'Accès (ACL)

Nous allons :

- ◆ Autoriser **PC1** (192.168.1.2) à accéder au **Serveur Web**.
- ◆ Bloquer **PC2** (192.168.1.3) sur le port **HTTP (80)**.
- ◆ Autoriser le reste du trafic.

Créer l'ACL

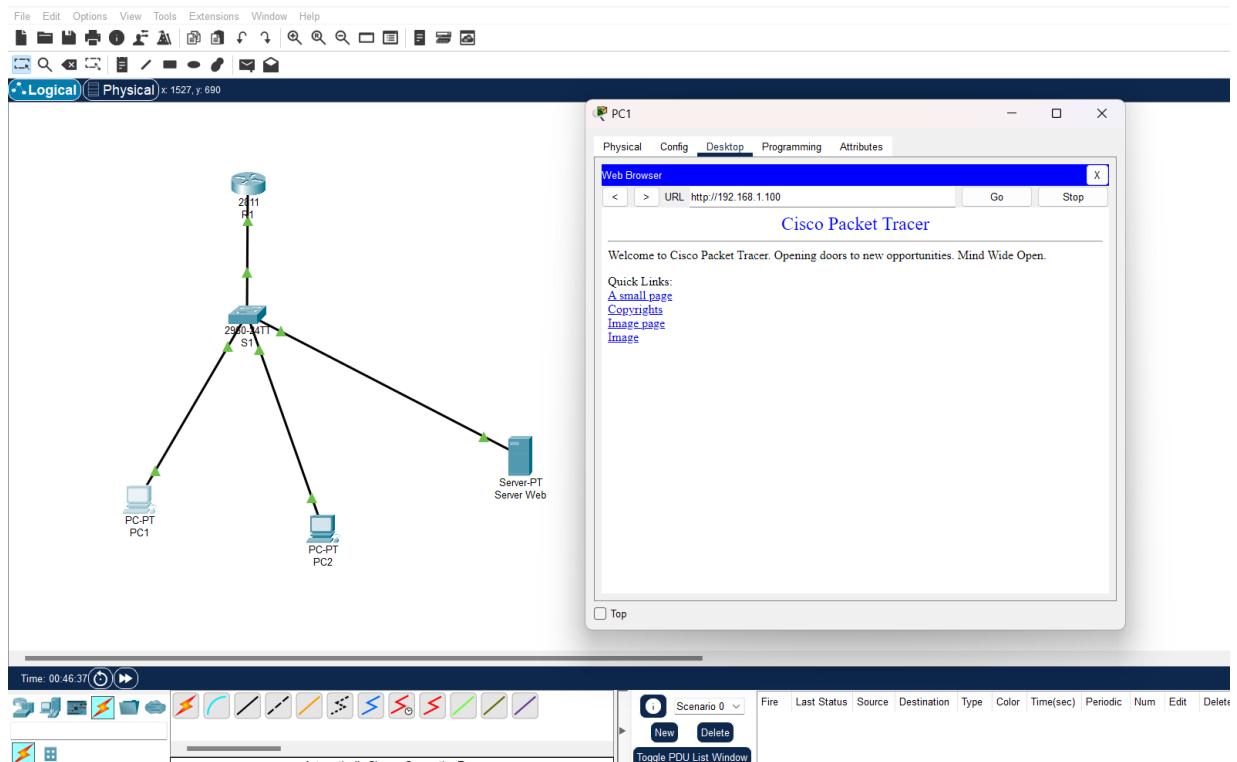


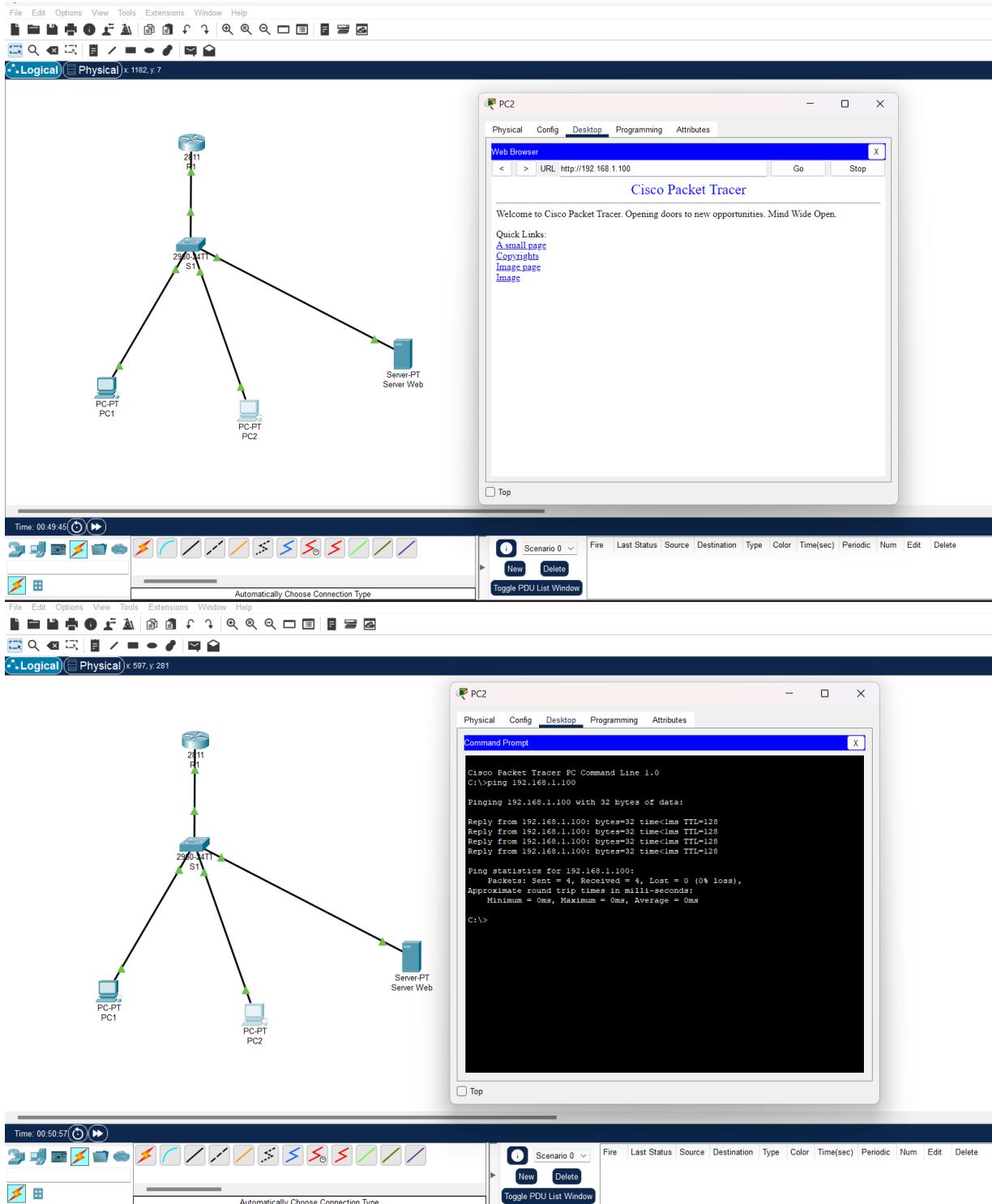
6. Tester la Configuration

Sur **PC1**, ouvrez un navigateur et essayez d'accéder à <http://192.168.1.100> → **Ça doit fonctionner**

Sur **PC2**, essayez d'accéder à <http://192.168.1.100> → **Accès refusé**

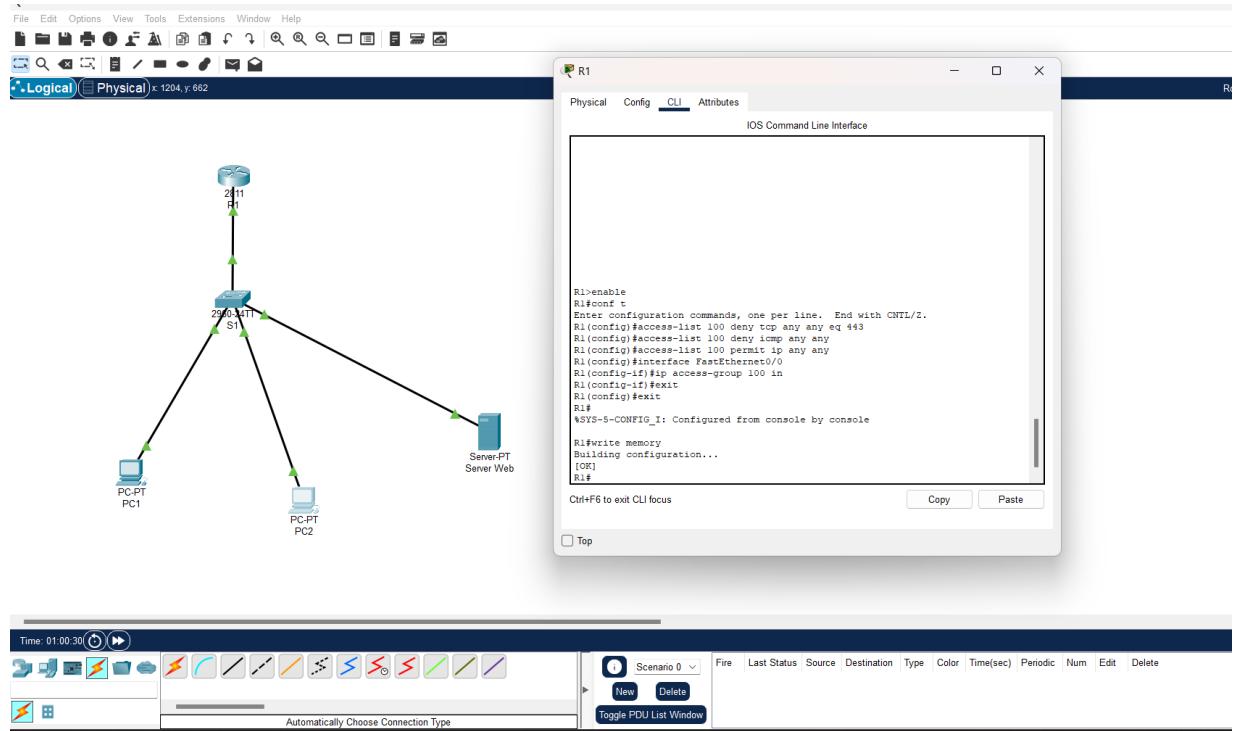
Testez avec la commande ping :





7. Bloquer le Trafic HTTPS et ICMP

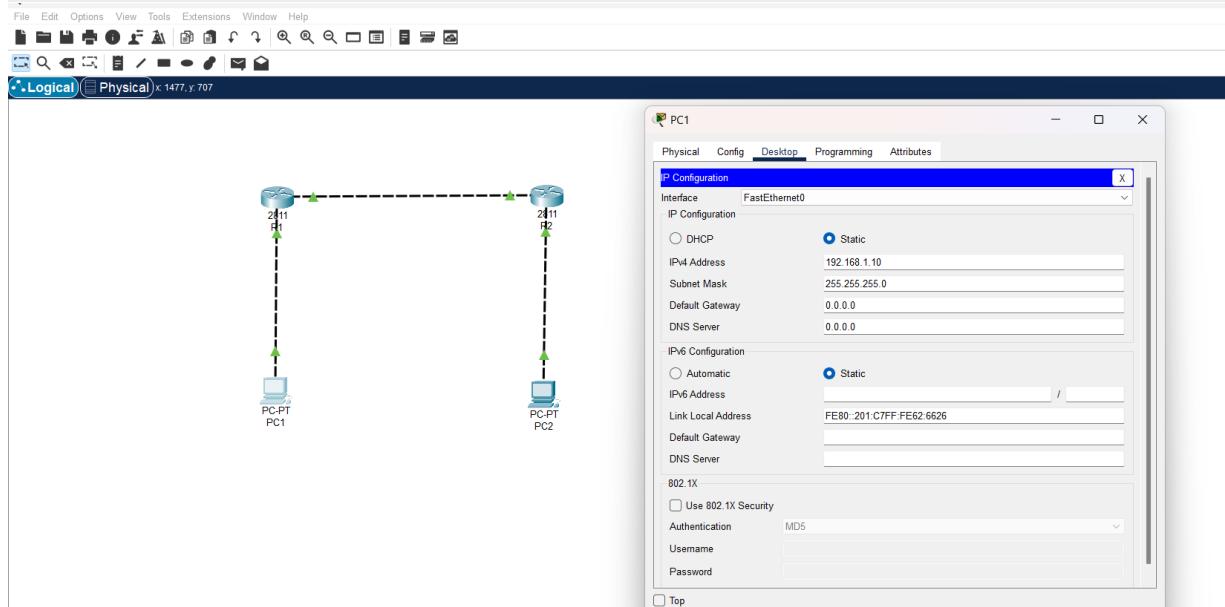
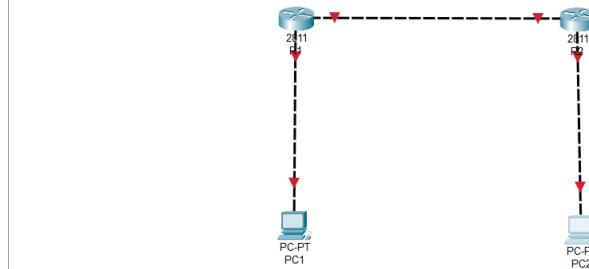
8. Sauvegarde de la Configuration

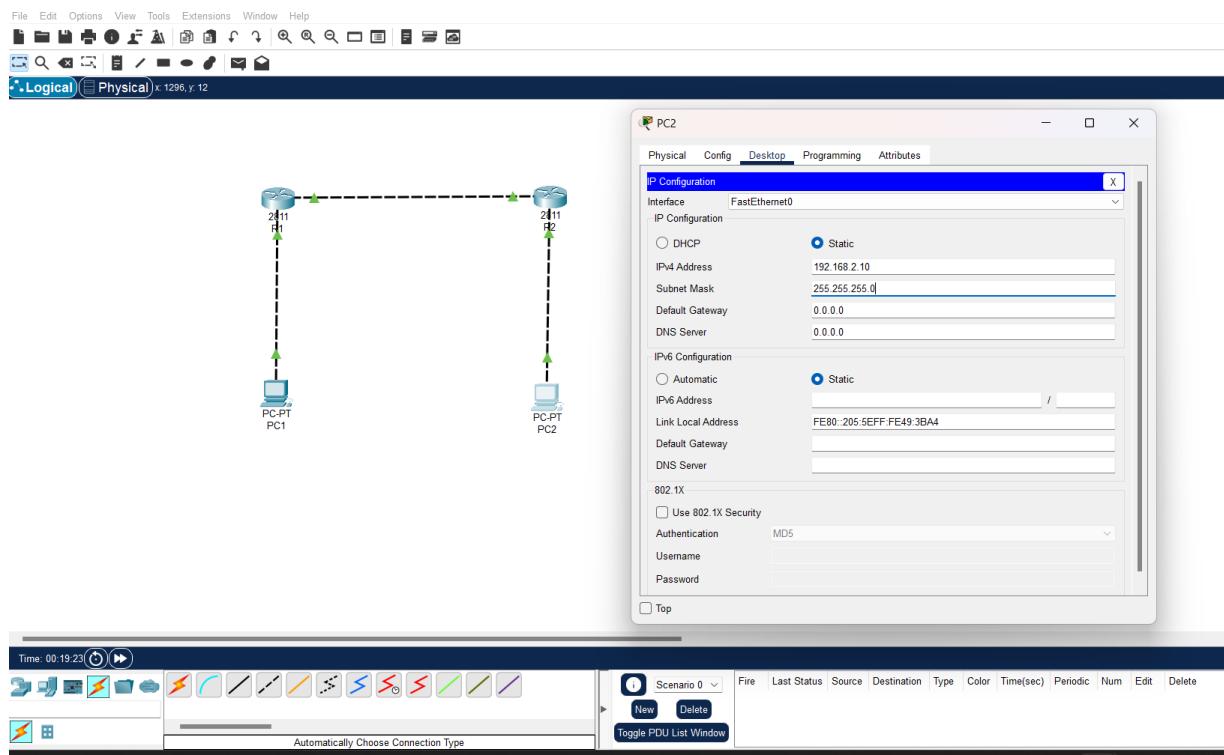


Configuration d'un VPN Site-à-Site

1. Architecture du Réseau

Péphérique	Adresse IP	Rôle
PC1	192.168.1.10	Client Site 1
Routeur R1	192.168.1.0 (LAN) 10.0.0.1 (WAN)	Routeur Site 1
Routeur R2	192.168.2.0 (LAN) 10.0.0.2 (WAN)	Routeur Site 2
PC2	192.168.2.10	Client Site 2

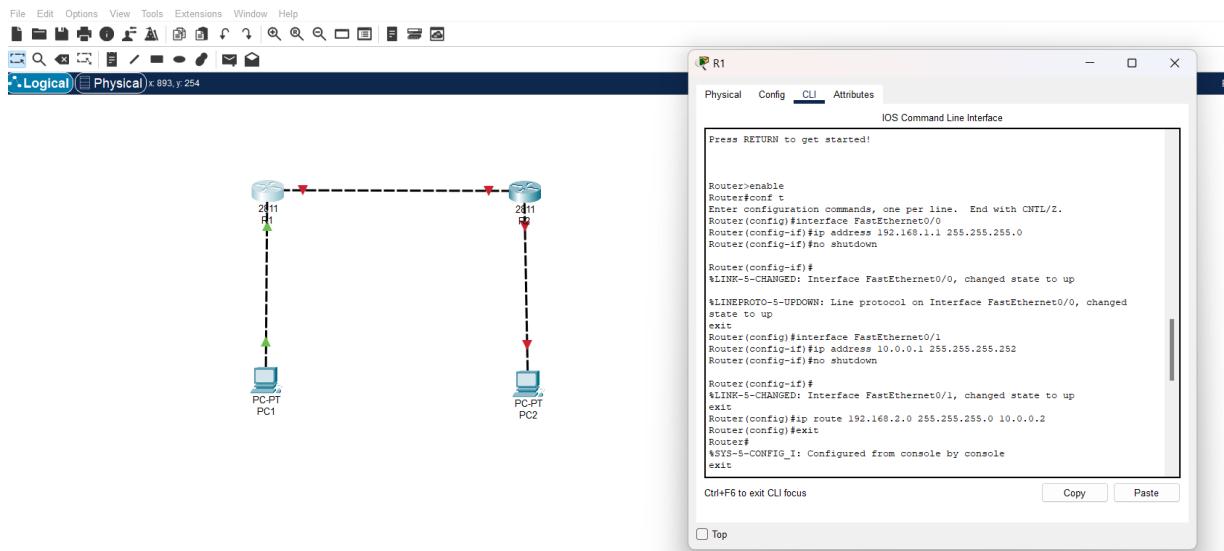


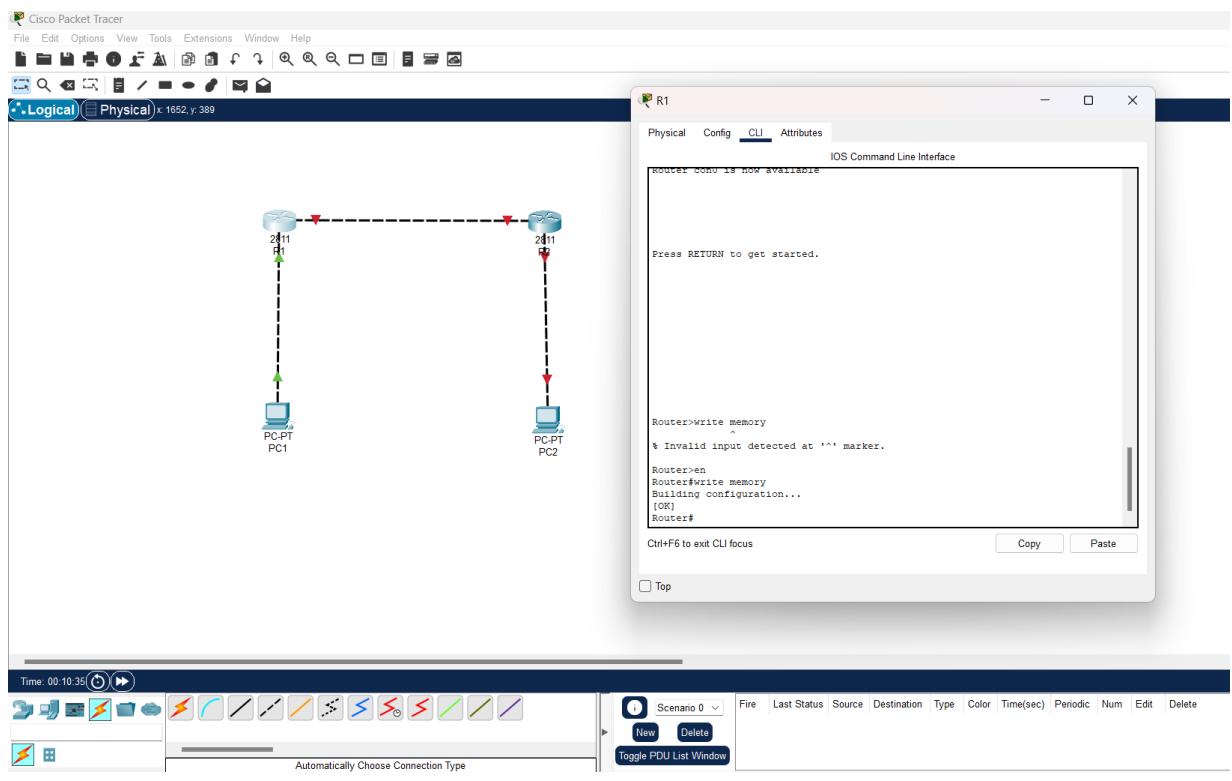


Configuration des Adresses IP

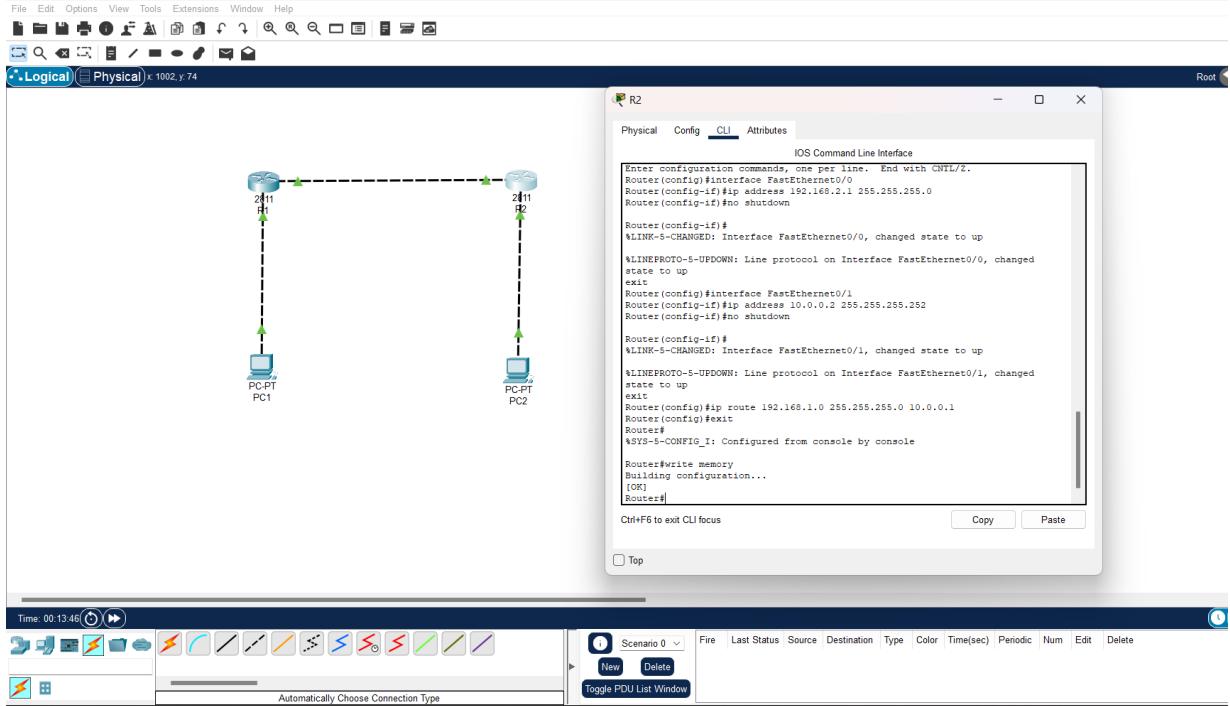
Avant de configurer le VPN, nous devons configurer les **interfaces réseau** de chaque routeur.

Sur R1 (Site 1)





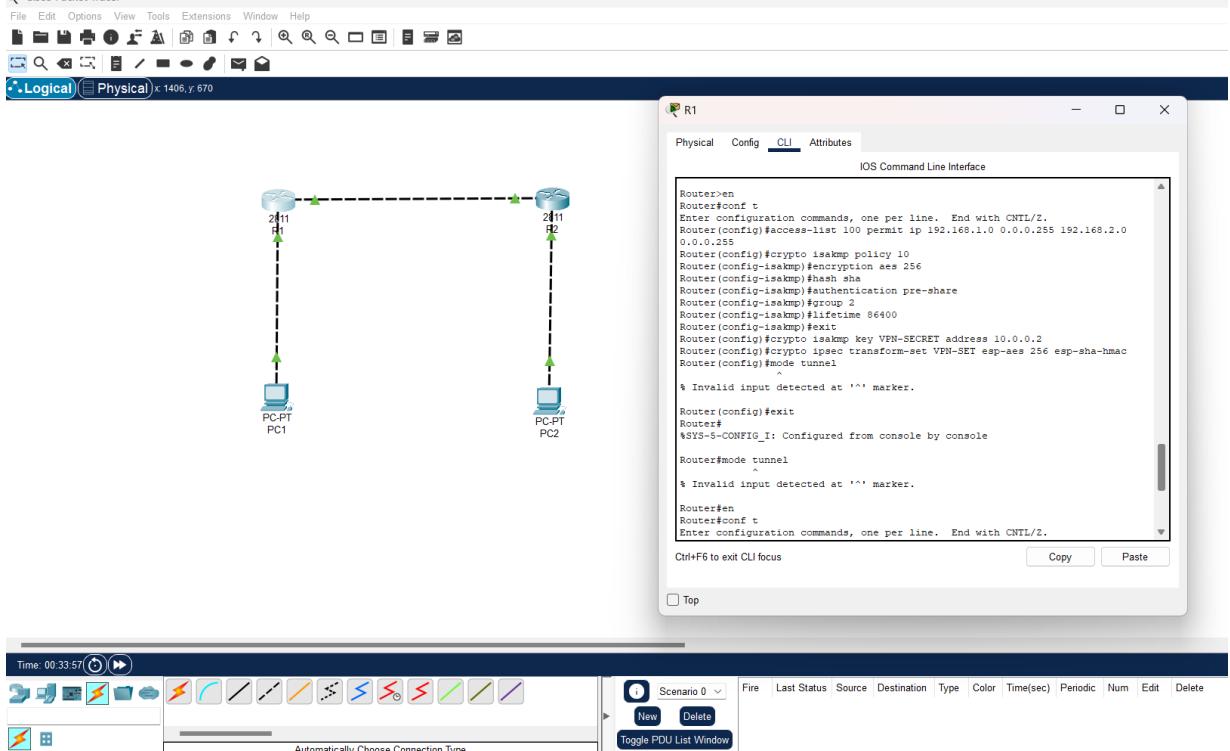
Sur R2 (Site 2)

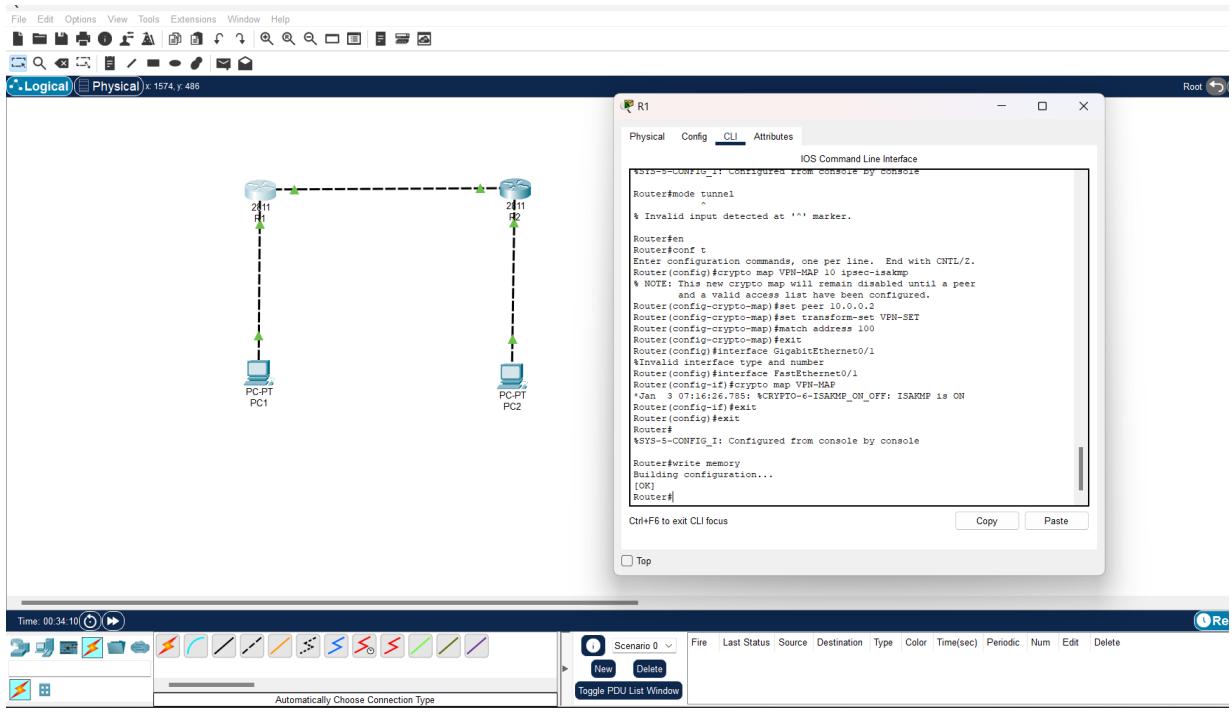


Configuration du VPN IPsec

Le **VPN IPsec** va chiffrer les communications entre **R1** et **R2**.

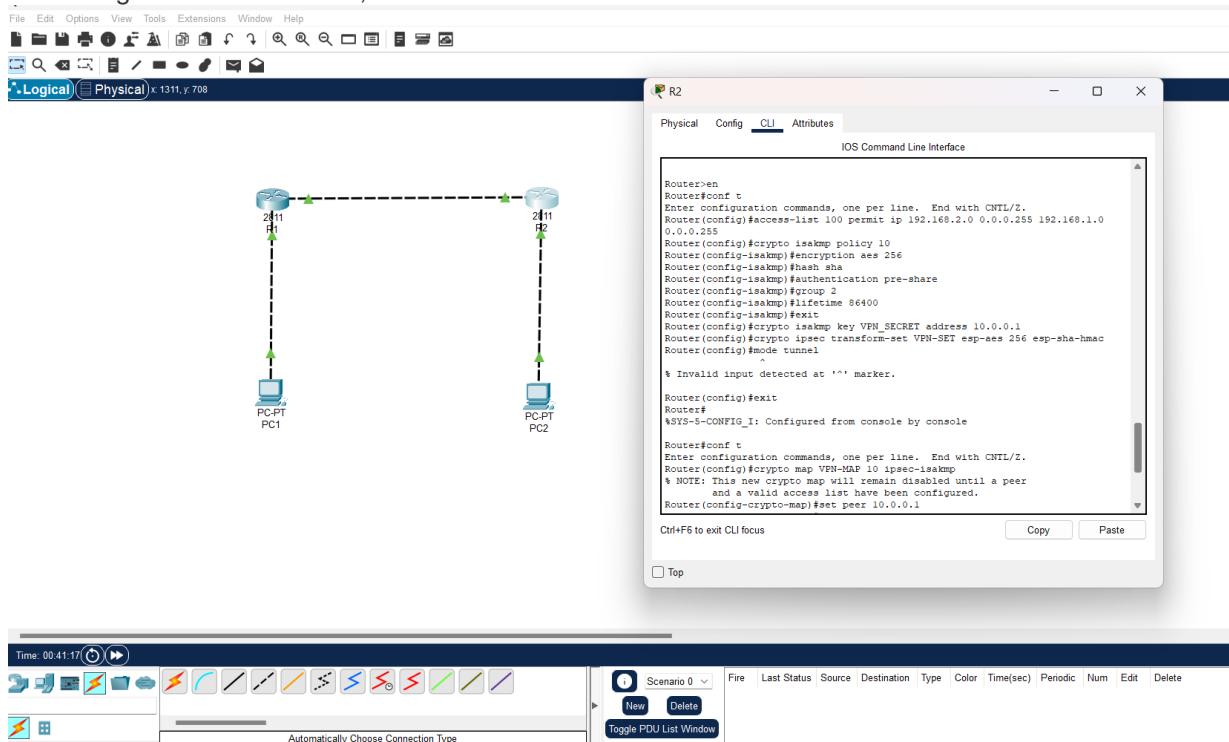
Sur R1 (Site 1)

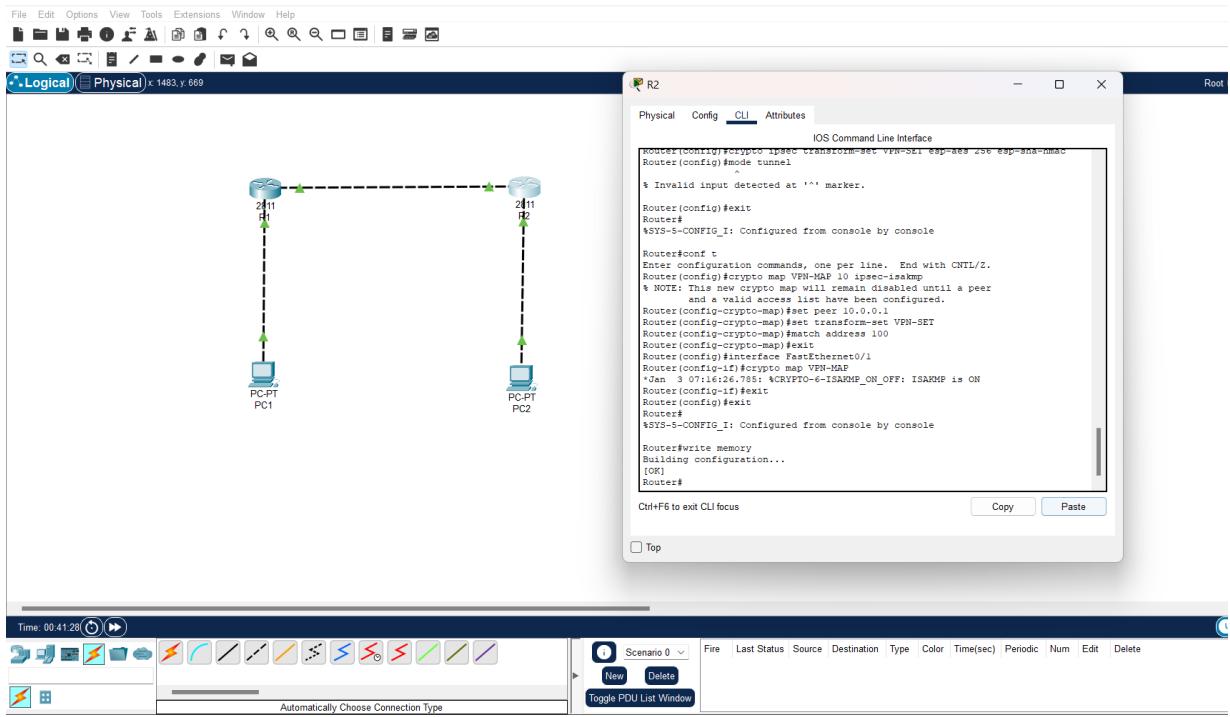




Sur R2 (Site 2)

La configuration est similaire, en inversant les adresses IP :

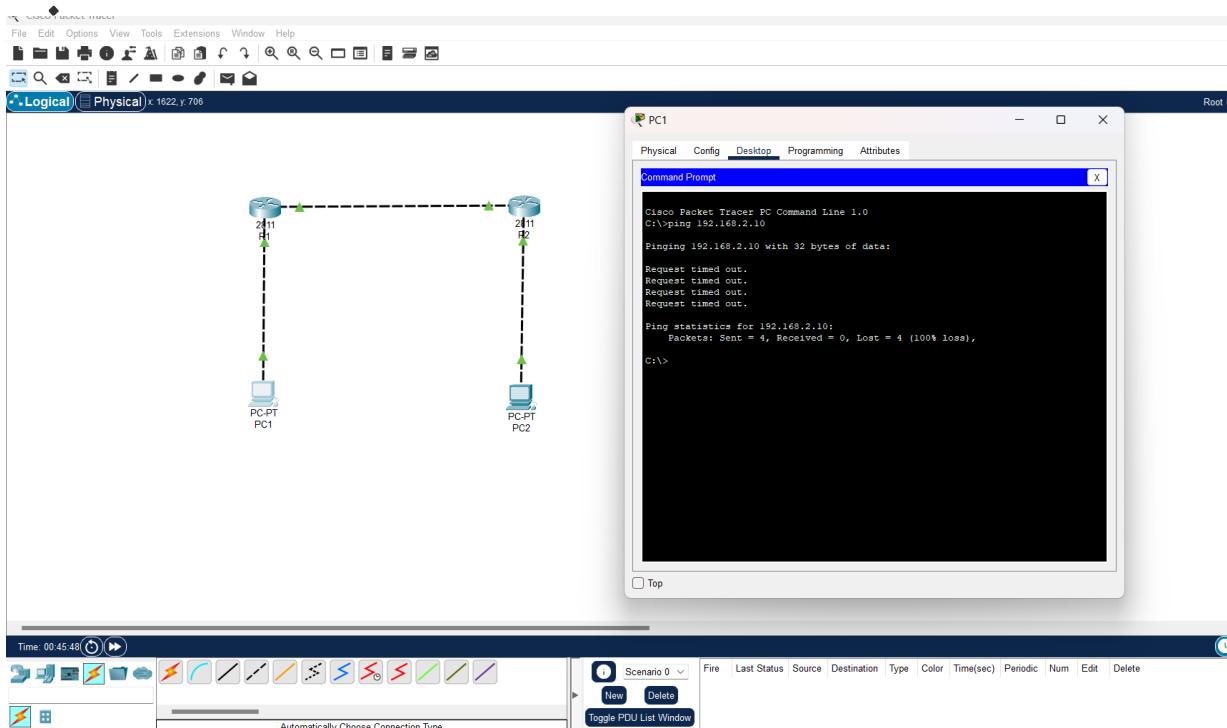




Vérification du VPN

Tester la connectivité

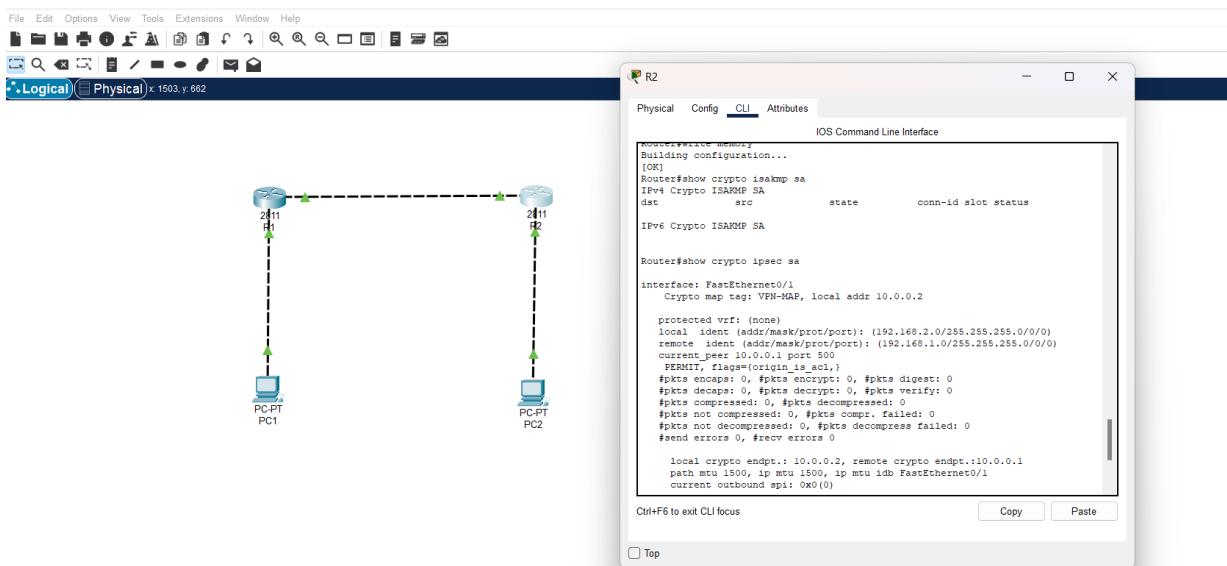
Depuis un PC du **Site 1** (192.168.1.10), essayez de **pinguer** un PC du **Site 2** (192.168.2.10) :

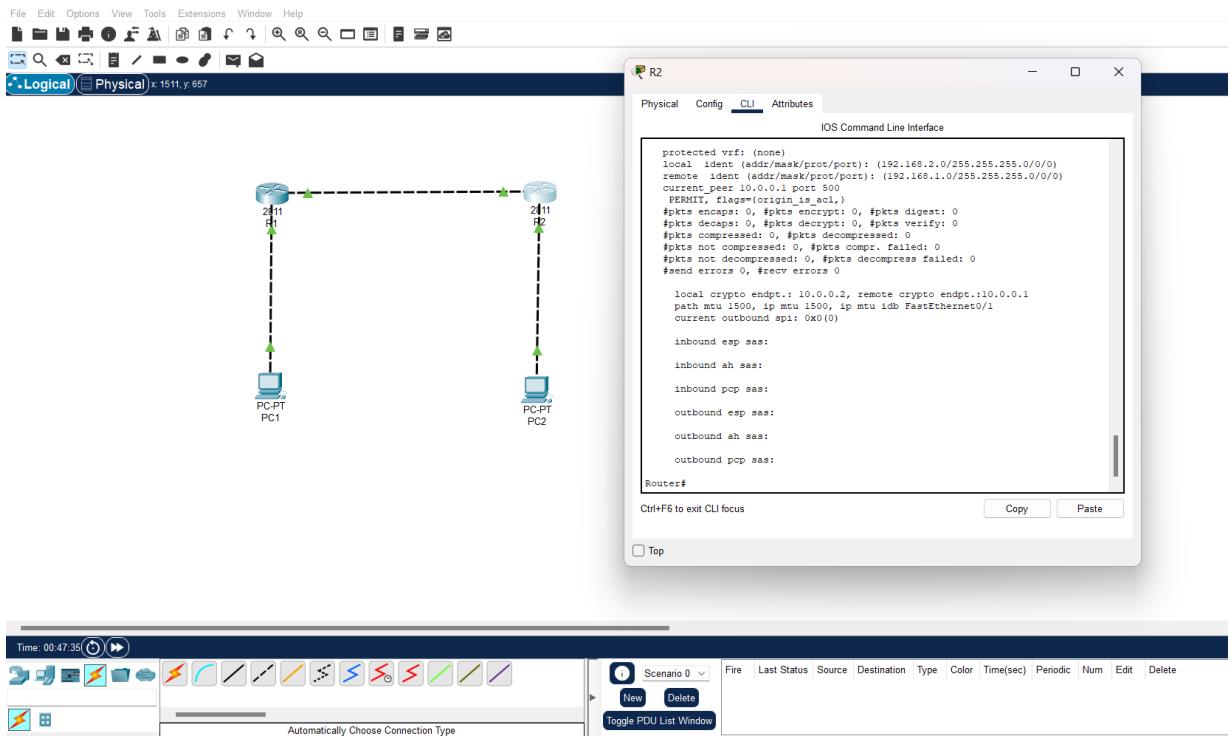


Si le **VPN fonctionne**, les paquets seront chiffrés et passés à travers le tunnel.

Vérifier l'établissement du VPN

Sur **R1 ou R2**, utilisez la commande :





CONCLUSION

Ce TD a permis de :

- Comprendre l'importance des ACL pour la sécurité réseau.
- Maîtriser les étapes critiques de configuration d'un VPN site-à-site (IKE/IPsec).
- Valider les configurations via des tests pratiques et des outils de diagnostic.
- Préparer à la mise en œuvre de solutions sécurisées dans des environnements professionnels.