matériel

# Mettre en place une connexion VPN

Un VPN (Virtual Private Network) est un réseau privé établi sur le réseau public, généralement via Internet.

Cependant, le réseau privé est un réseau logique sans aucune ligne de réseau physique, il est donc appelé réseau privé virtuel.

La connexion directe du réseau local à Internet, bien que pouvant permettre l'échange de données, entraînerait l'exposition des données privées à tous les utilisateurs sur Internet.

## Utilisation du VPN IPSec pour accéder à votre réseau domestique

La technologie VPN (Virtual Private Network) établit un réseau privé à travers le réseau public, qui peut fournir une communication sécurisée vers un ordinateur distant ou un réseau distant, et garantir un échange de données sécurisé.

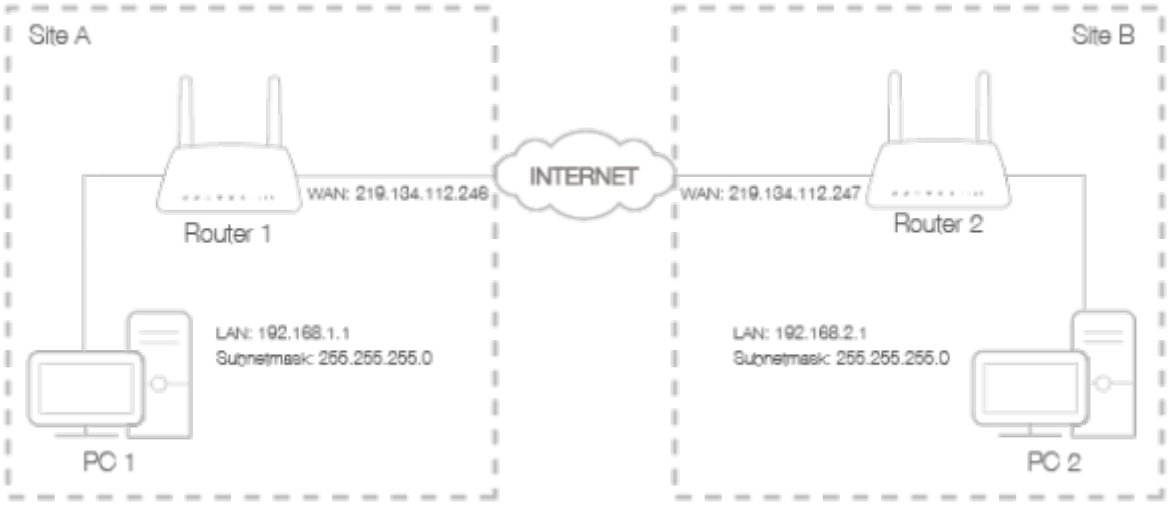
IPSec est l'une des principales implémentations des VPN.

Nous voulons établir un tunnel VPN IPSec pour connecter deux réseaux locaux via Internet afin que les hôtes de différents réseaux locaux distants puissent communiquer entre eux comme s'ils se trouvaient dans le même réseau local.

Par exemple, je suis l'administrateur réseau d'un bureau régional, je dois laisser mon personnel de bureau visiter les serveurs et les ressources du siège, et vice versa.

Je sais que le routeur de mon bureau et l'appareil du siège social prennent tous deux en charge la fonction VPN IPSec, j'ai donc décidé de configurer une connexion VPN avec le siège social.

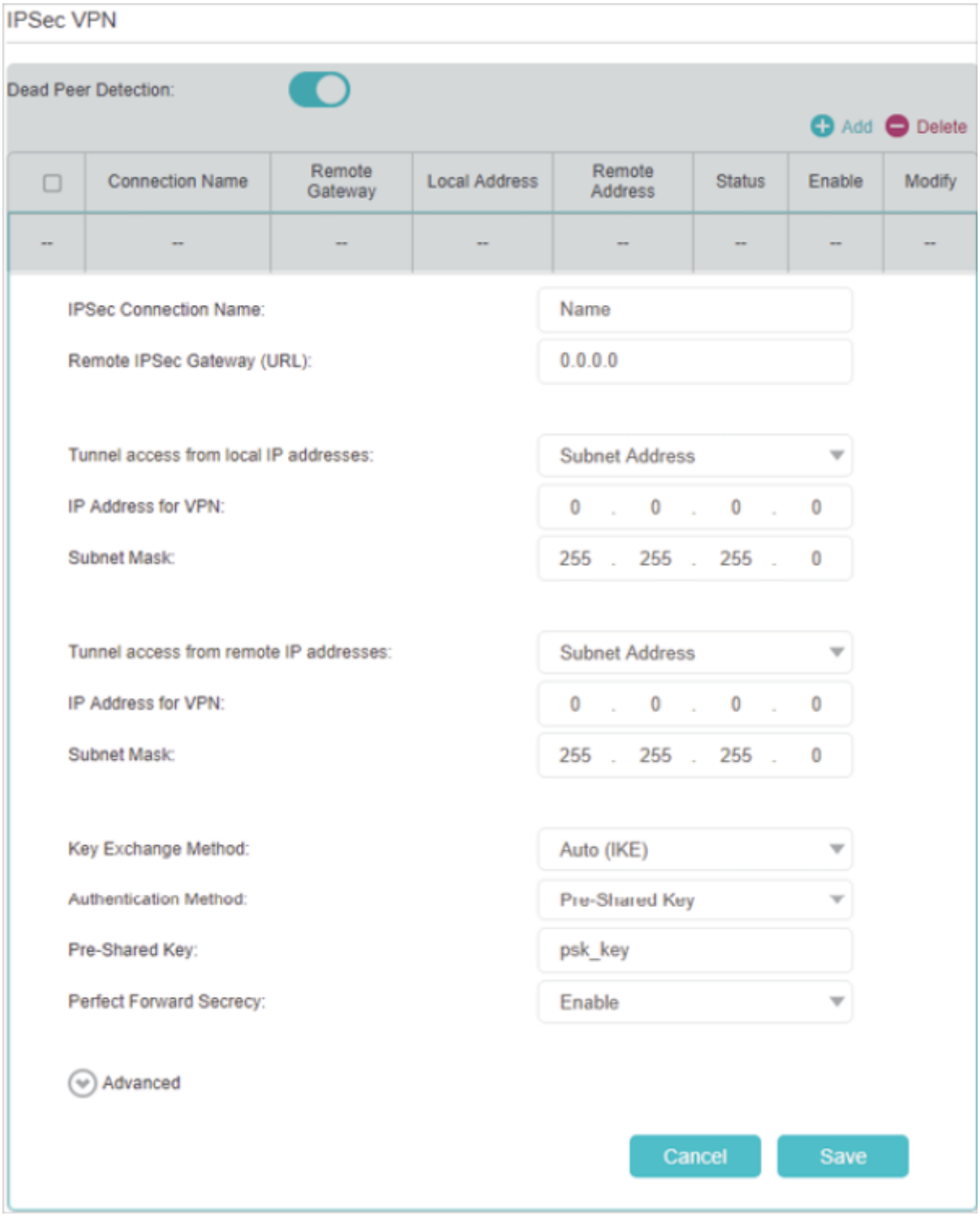
Le schéma suivant est une topologie VPN typique. Ici, le site A fait référence au réseau du bureau régional (réseau local). Et le site B fait référence au réseau du siège (réseau distant) auquel je souhaite me connecter.




**Méthode** :

**Assurez-vous de la topologie** que vous souhaitez construire et notez les IP LAN et WAN du site A (réseau local) et du site B (réseau distant).

**Configuration sur le site A** (réseau local) :
**Connectez-vous sur la page http://tplinkmodem.net** avec le mot de passe du routeur.
Allez dans **Avancée > VPN > VPN IPSec** pour ouvrir la page de configuration. Cliquez sur Ajouter pour configurer un tunnel VPN.




**IPSec Connection Name** : spécifiez un nom

**Remote IPSec Gateway (URL)** : entrez l'adresse IP WAN du site B.

Pour configurer le réseau local du site A :
**Tunnel access from local IP addresses** : nous prenons ici l'adresse de sous-réseau comme exemple.

**IP Address for VPN** : plage IP LAN du site A

**Subnet Mask** : masque de sous-réseau du site A.

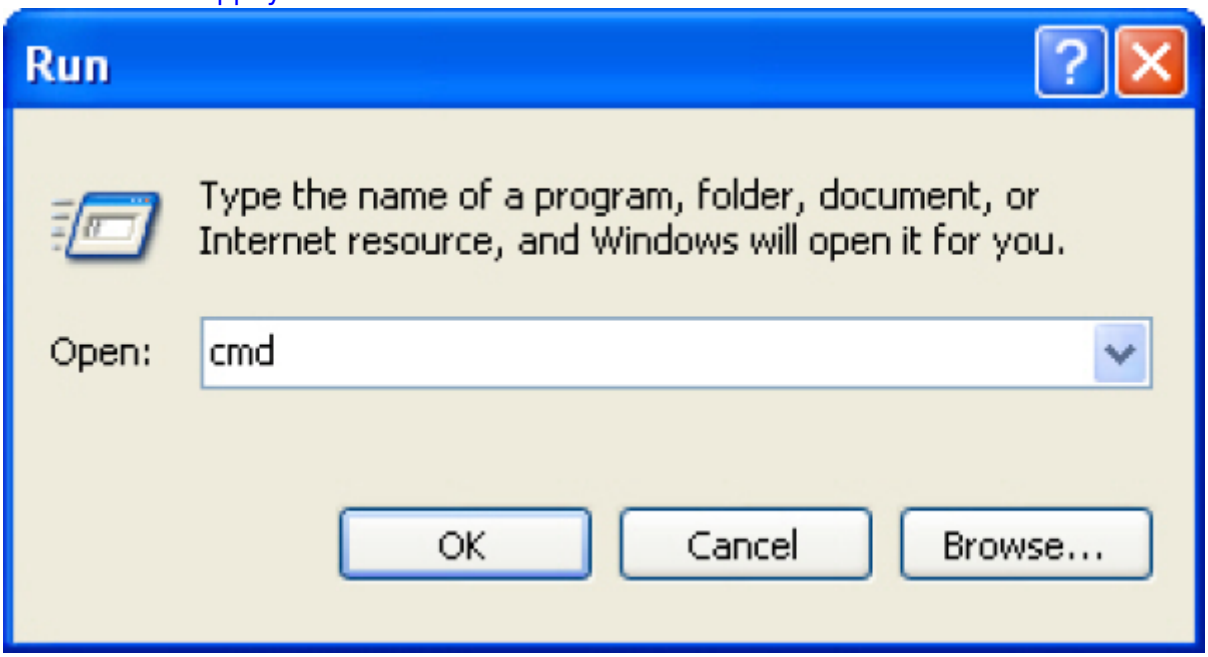
4. Pour configurer le réseau local du site B :
   **Tunnel access from local IP addresses** : nous prenons ici l'exemple de l'adresse de sous-réseau.

   **IP Address for VPN** : plage IP LAN du site B

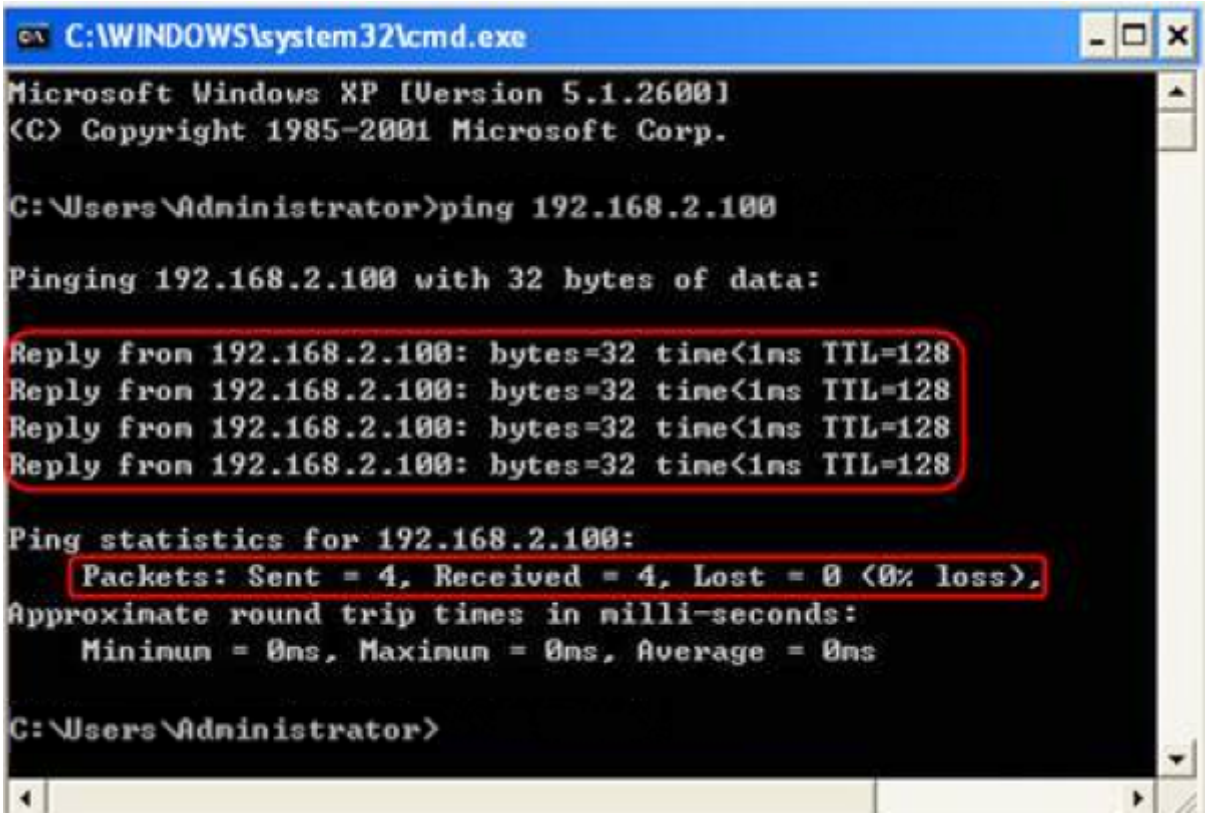
   **Subnet Mask** : masque de sous-réseau du site B.

5. **Key Exchange Method** : méthode d'échange de clés pour la stratégie. Nous sélectionnons ici Auto(IKE).
6. **Authentication method** : Pre-Shared Key
7. **Pre-Shared Key**
8. keep **Perfect Forward Secrecy** enabled. **Note**:Make sure Site A and Site B use the same key.
9. **paramètres avancés** Laissez les valeurs par défaut.
10. Cliquez ensuite sur save pour enregistrer.

3. Configuration sur le Site B (réseau distant). Reportez-vous à la configuration de l'étape 2 sur le site A et assurez-vous que le site A et le site B utilisent les mêmes clés pré-partagées et paramètres Perfect Forward Secrecy.
4. La colonne État deviendra Up si la connexion VPN a été configurée avec succès.
5. Vérifiez la connexion VPN. Vous pouvez envoyer un ping à l'adresse IP LAN du site B depuis votre ordinateur pour vérifier que la connexion VPN IPSec est correctement configurée. Pour vérifier la connexion VPN, vous pouvez procéder comme suit.
   Sur l'hôte du site A, appuyez sur [Logo Windows] + [R] pour ouvrir la boîte de dialogue Exécuter. Saisissez « cmd » et appuyez sur OK.




   Dans la fenêtre CLI, saisissez « ping 192.168.2.x » (« 192.168.2.x » peut être l'adresse IP de n'importe quel hôte du site B). Appuyez ensuite sur [Entrée].




Si Ping se déroule avec succès (obtient des réponses de l'hôte du site B), la connexion IPSec fonctionne correctement maintenant.

Terminé!

Maintenant, le VPN IPSec est implémenté pour établir une connexion.

Le produit prend en charge un maximum de dix connexions simultanées.

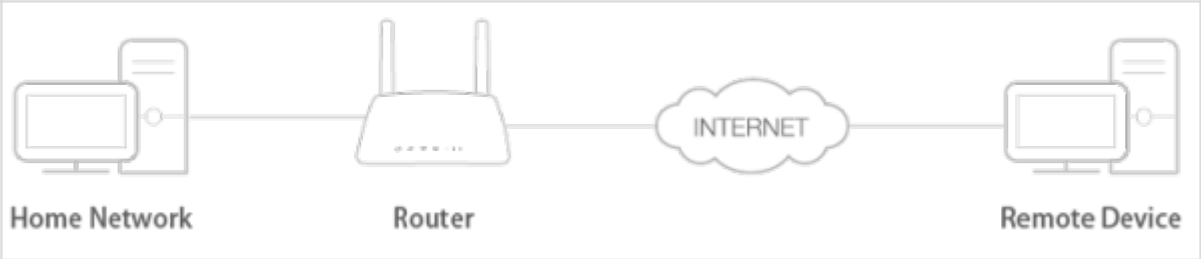
Si l'un des sites a été hors ligne pendant un certain temps, par exemple, si le site A a été déconnecté, sur le site B vous devez cliquer sur Désactiver puis sur Activer après la remise en ligne du site A afin de rétablir l'IPSec tunnel.

## Utilisation de OpenVPN pour accéder à votre réseau domestique

Dans la connexion OpenVPN, le réseau domestique peut agir comme un serveur et l'appareil distant peut accéder au serveur via le routeur qui agit comme une passerelle OpenVPN Server.

Pour utiliser la fonction VPN, vous devez activer OpenVPN Server sur votre routeur et installer et exécuter le logiciel client VPN sur l'appareil distant.

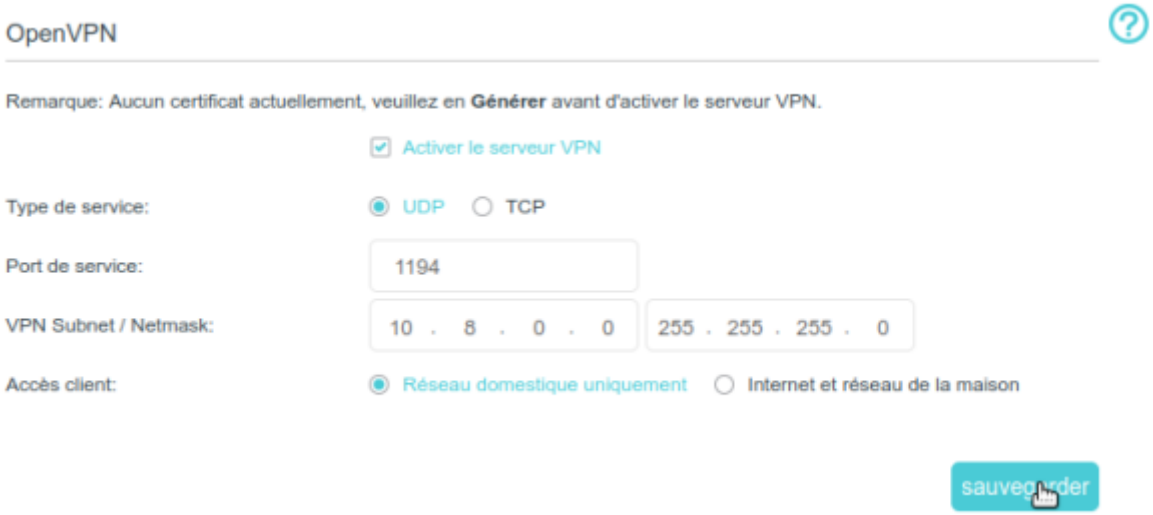
Veuillez suivre les étapes ci-dessous pour configurer une connexion OpenVPN.




## Étape 1. Configurer le serveur OpenVPN sur votre routeur

**Connectez-vous sur la page http://tplinkmodem.net** avec le mot de passe du routeur.

Accédez à **Avancée > VPN > OpenVPN** et sélectionnez **Activer le serveur VPN**.




**Note** :

- Avant d'activer le serveur VPN, nous vous recommandons de configurer le service DNS dynamique (recommandé) ou d'attribuer une adresse IP statique au port WAN du routeur et de synchroniser votre heure système avec Internet.
- La première fois que vous configurez le serveur OpenVPN, vous devrez peut-être générer un certificat avant d'activer le serveur VPN.

**Type de service** : protocole de communication pour OpenVPN Server (UDP, TCP).

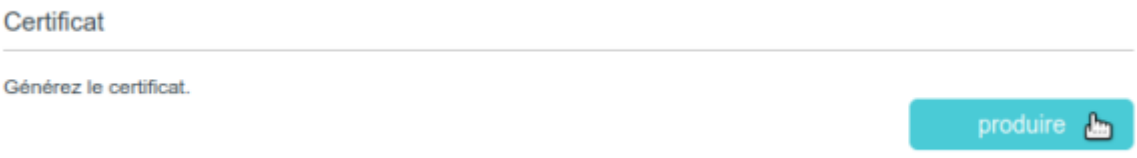
**Port de service** : port auquel un périphérique VPN se connecte (numéro de port compris entre 1024 et 65535).

**VPN Subnet / Netmask** : plage d'adresses IP qui peuvent être allouées à l'appareil par le serveur OpenVPN.

**Accès client** : ne sélectionnez **Réseau domestique** que si vous souhaitez que l'appareil distant n'accède qu'à votre réseau domestique ; sélectionnez Internet et réseau domestique si vous souhaitez que l'appareil distant accède aussi à Internet via le serveur VPN.

Cliquez sur Sauvegarder.

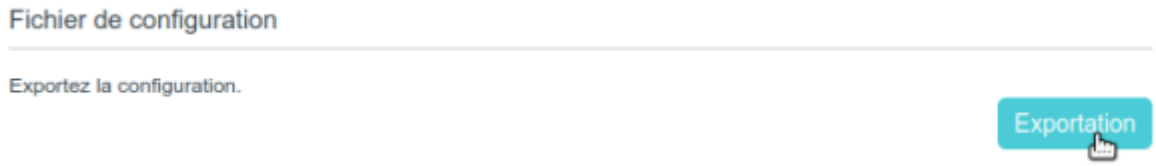
3. Cliquez sur Produire pour obtenir un nouveau certificat.




Si vous en avez déjà généré un, ignorez cette étape ou cliquez sur Produire pour mettre à jour le

certificat.

4. Cliquez sur Exportation pour enregistrer le fichier de configuration OpenVPN qui sera utilisé par l'appareil distant pour accéder à votre routeur.




### Étape 2. Configurez la connexion OpenVPN sur votre appareil distant

Visitez http://openvpn.net/index.php/download/community-downloads.html pour télécharger le logiciel OpenVPN et installez-le sur votre appareil sur lequel vous souhaitez exécuter l'utilitaire client OpenVPN.
**Remarque** : Vous devez installer l'utilitaire client OpenVPN sur chaque appareil sur lequel vous prévoyez d'appliquer la fonction VPN pour accéder à votre routeur. Les appareils mobiles doivent télécharger une application tierce depuis Google Play ou Apple App Store.

Après l'installation, copiez le fichier exporté depuis votre routeur dans le dossier « config » de l'utilitaire client OpenVPN (par exemple, C:\Program Files\OpenVPN\config sous Windows).Le chemin dépend de l'endroit où l'utilitaire client OpenVPN est installé.

Exécutez l'utilitaire client OpenVPN et connectez-le au serveur OpenVPN.

## Utilisation du VPN PPTP pour accéder à votre réseau domestique

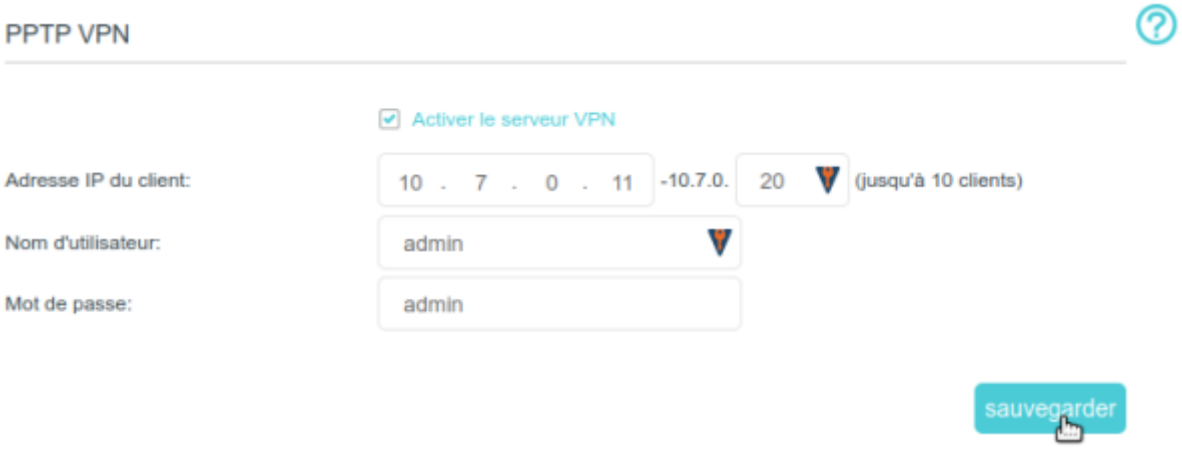
Le serveur VPN PPTP est utilisé pour créer une connexion VPN pour un périphérique distant.

Pour utiliser la fonction VPN, vous devez activer le serveur VPN PPTP sur votre routeur et configurer la connexion PPTP sur l'appareil distant.

Veuillez suivre les étapes ci-dessous pour configurer une connexion VPN PPTP.

### Étape 1. Configuration du serveur VPN PPTP sur votre routeur

**Connectez-vous sur la page http://tplinkmodem.net** avec le mot de passe du routeur.
Onglet **Avancée**, **VPN > PPTP VPN** : cochez **Activer le serveur VPN** :



**Remarque** : avant d'activer le serveur VPN, nous vous recommandons de **configurer le service DNS dynamique** ou d'attribuer une adresse **IP statique** au port WAN du routeur et de **synchroniser votre heure système avec Internet**.
**Adresse IP du client** : saisissez la plage d'adresses IP (jusqu'à 10) pouvant être allouées aux appareils par le serveur VPN PPTP.

**Nom d'utilisateur**, **Mot de passe** : saisissez le nom d'utilisateur et le mot de passe pour authentifier les clients auprès du serveur VPN PPTP.

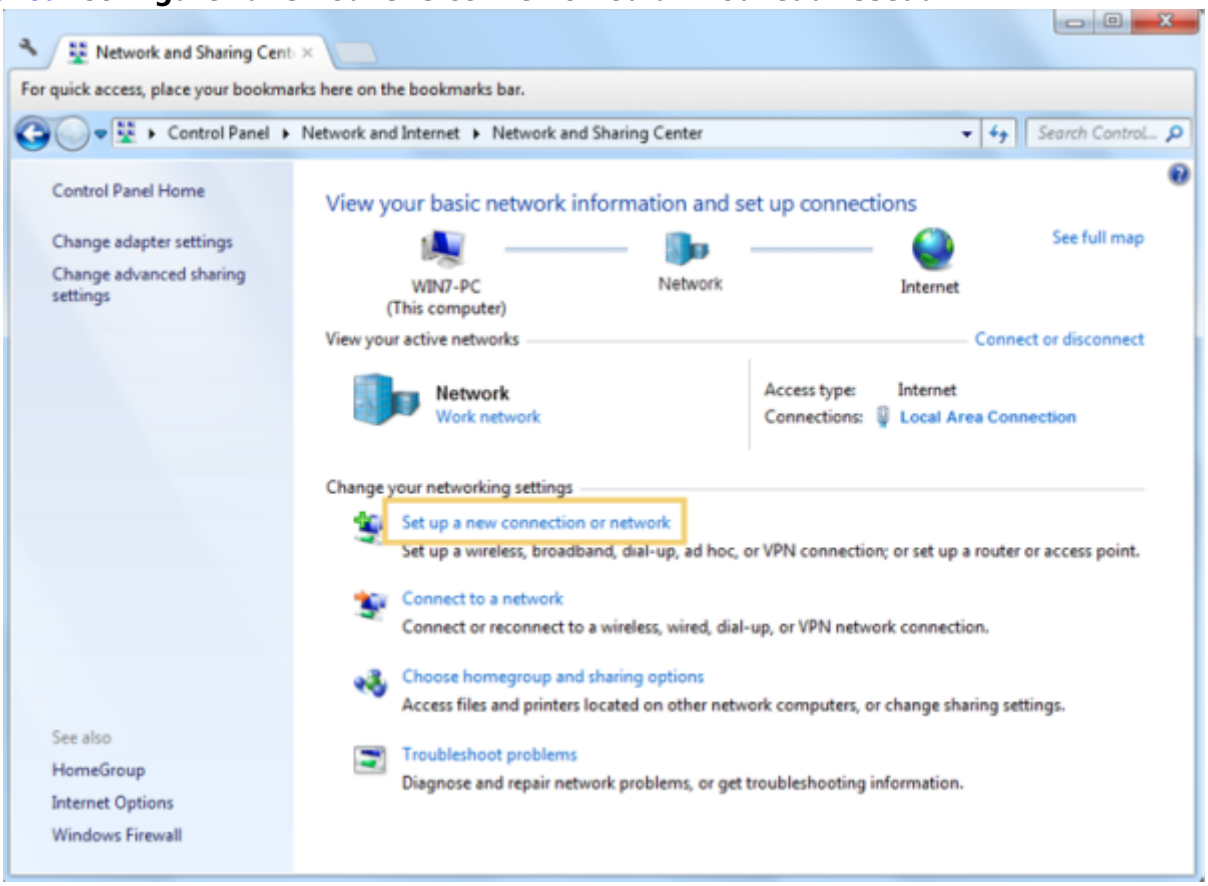
3. Cliquez sur Sauvegarder

## Étape 2. Configurez la connexion VPN PPTP sur l'appareil distant

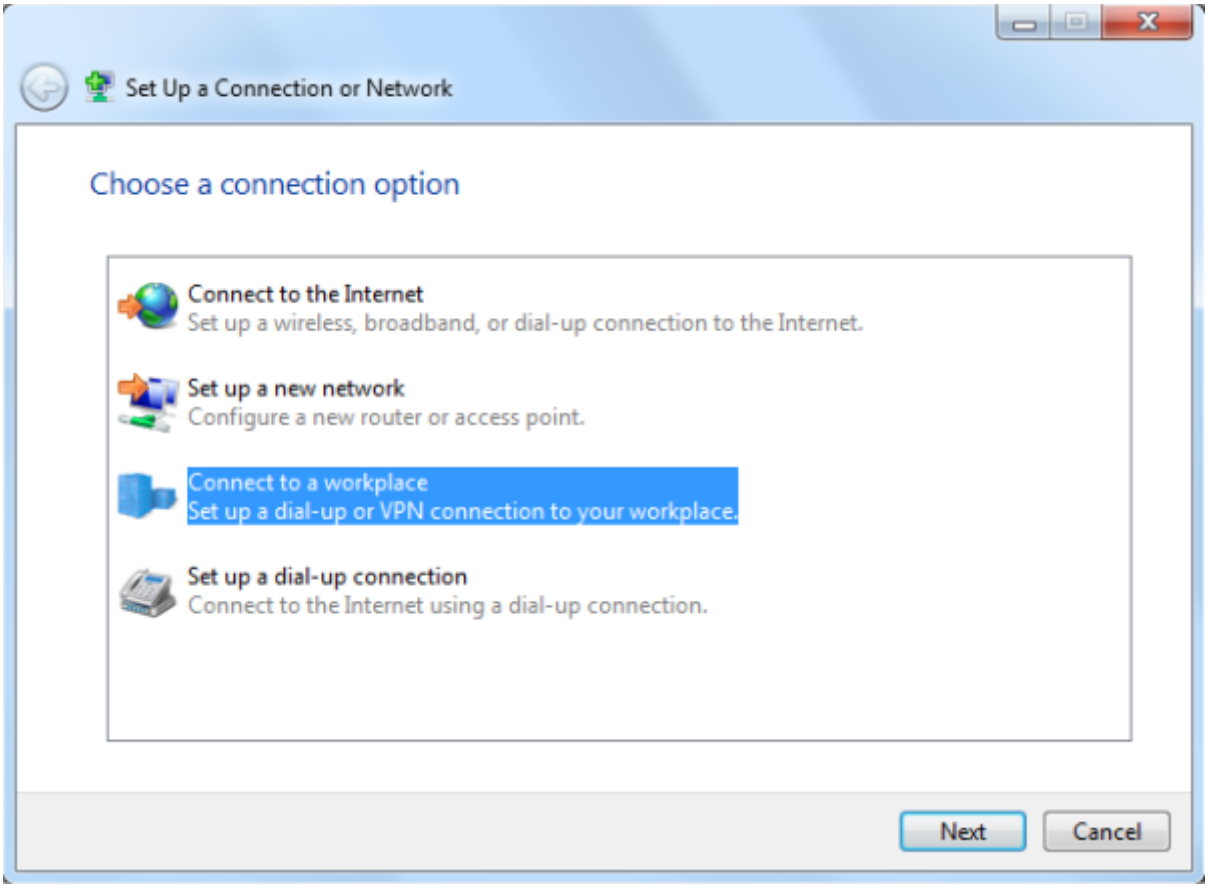
L'appareil distant peut utiliser le logiciel PPTP intégré de Windows ou un logiciel tiers PPTP pour se connecter au serveur PPTP.

Ici, nous utilisons le logiciel PPTP intégré à Windows comme exemple.

Ouvrez **Démarrer > Panneau de configuration > Réseau et Internet > Centre Réseau et partage**.
Cliquez sur **Configurer une nouvelle connexion ou un nouveau réseau** :

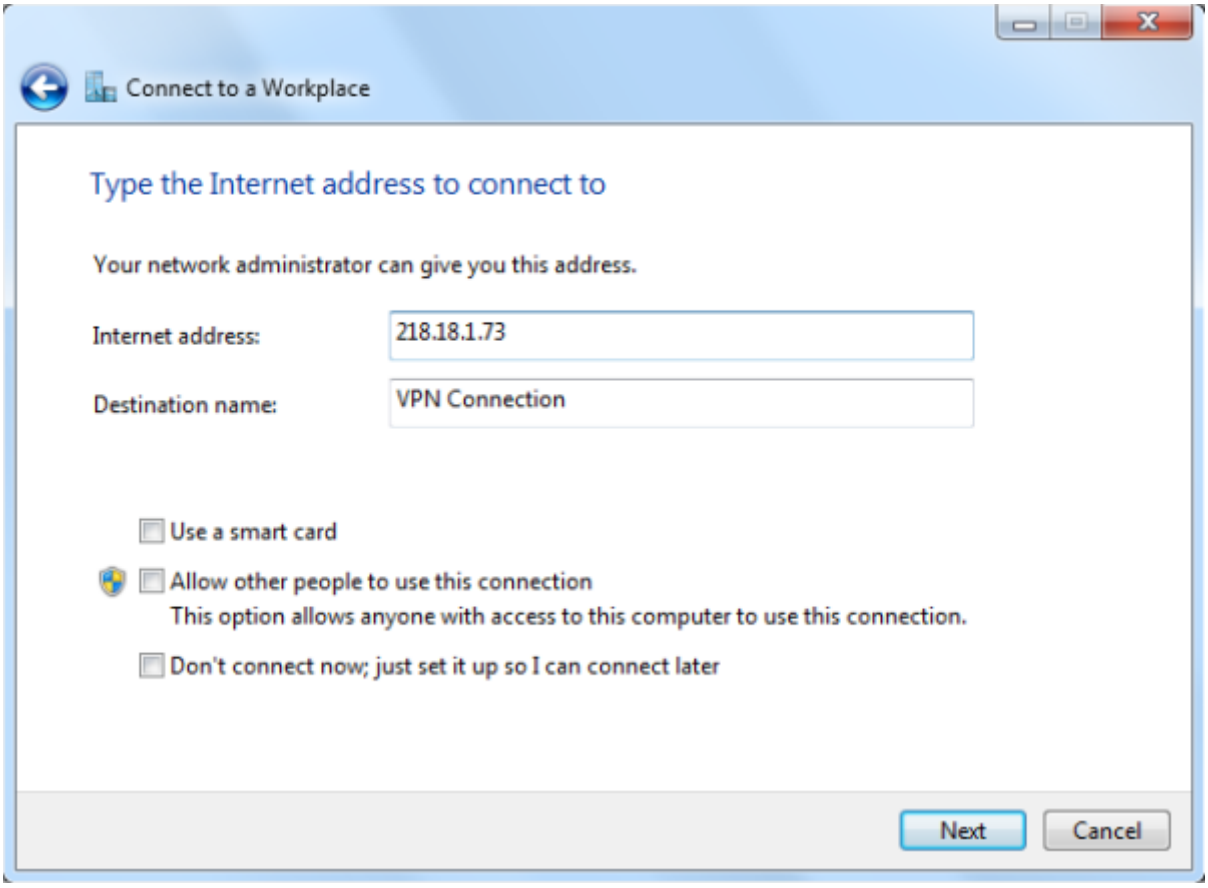



Cliquez sur **Se connecter à un espace de travail** et cliquez sur Suivant :

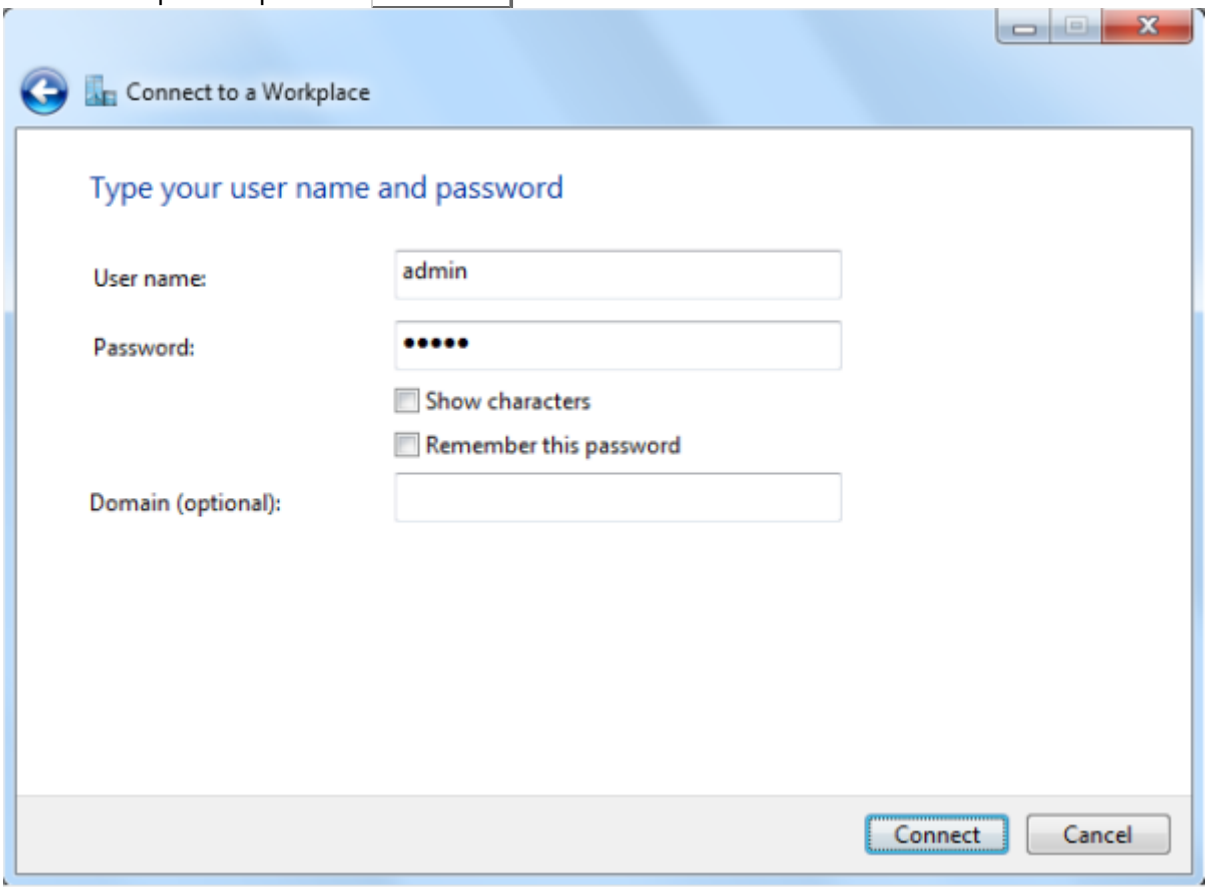



Cliquez sur **Utiliser ma connexion Internet (VPN)** :

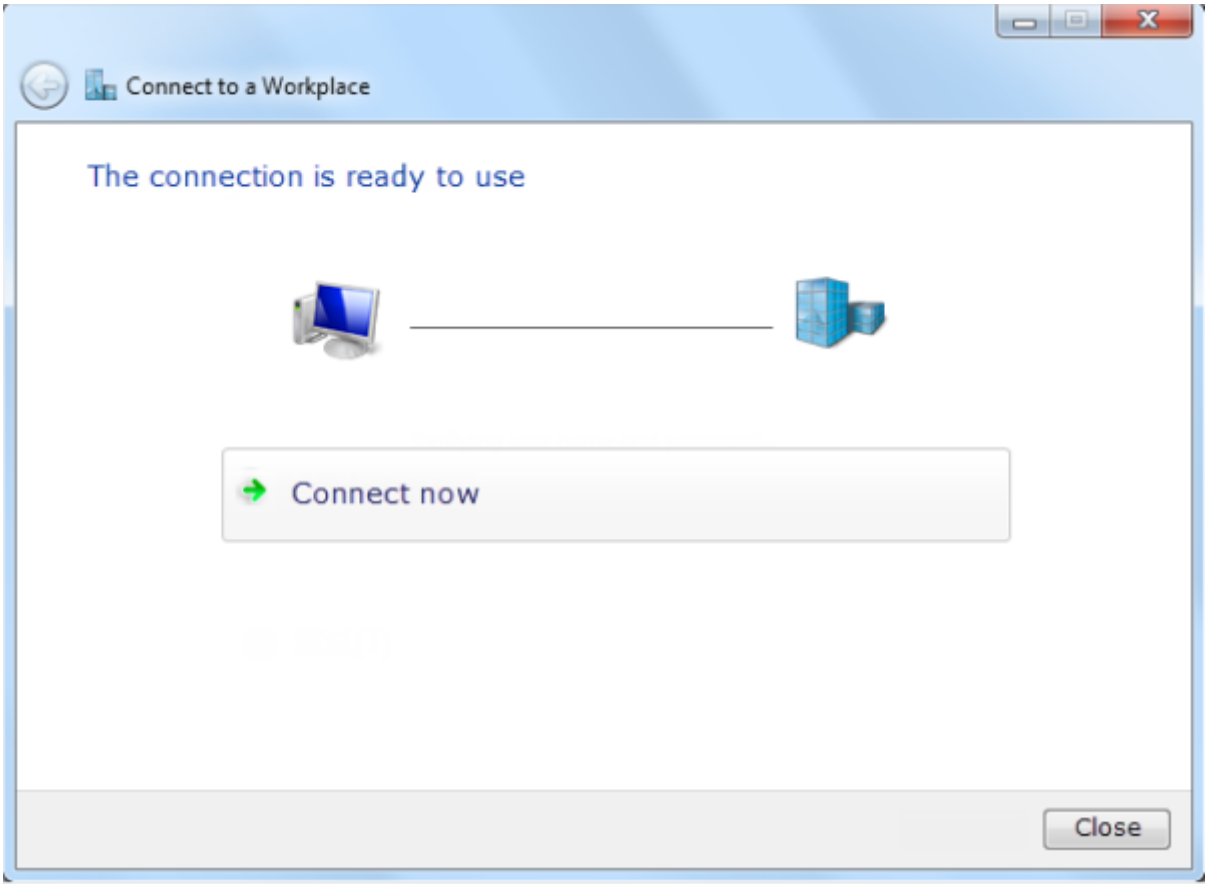

Saisissez l'adresse IP Internet du routeur (par exemple : 218.18.1.73) dans le champ **Adresse Internet**. Cliquez sur Suivant :




Saisissez le **nom d'utilisateur** et le **mot de passe** que vous avez définis pour le serveur VPN PPTP sur votre routeur puis cliquez sur Connecter :




La connexion VPN PPTP est créée et prête à être utilisée :




# Voir aussi

- **(en)** //www.tp-link.com/us/user-guides/Archer-MR400_V3/

---

*Basé sur « Archer MR400 V3 User Guide » par tp-link.com.*