Chéridanh TSIELA

Windows Server

VPN L2TP avec clé pré-partagée

I – Introduction

En entreprise, il arrive que des employés ou le patron doivent partir en mission à l'extérieur. Lorsque ceux-ci sortent de la société, ils n'ont plus accès aux services hébergés dans leurs locaux. Pour remédier à ça, il existe ce que l'on appelle les tunnels VPN. Cette technologie vous permet d'accéder à l'intégralité de votre réseau local depuis l'extérieur, et ce de façon entièrement sécurisée. Une fois connecté au serveur VPN de votre société, votre ordinateur se retrouvera virtuellement dans le réseau local de votre société comme si vous y étiez physiquement.

Cette technologie est donc très pratique, mais attention aux tentatives de piratage, car si votre serveur VPN n'est pas sécurisé correctement, un pirate pourrait s'en servir pour avoir accès à l'intégralité de votre réseau. Jusqu'à ce que vous lui bloquiez l'accès (mais il sera surement trop tard).

II – Prérequis

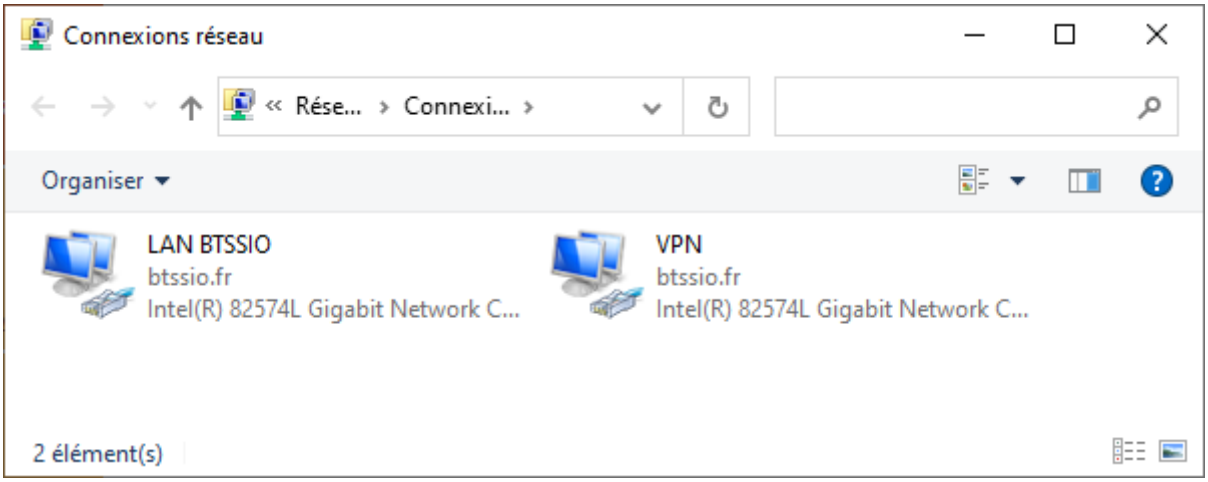
- 1 Active Directory
- 1 Serveur VPN
- Mot de passe Administrateur du domaine

Dans ce TP, notre serveur VPN sera installé sur notre contrôleur de domaine. Avec de bonne connaissance en réseau, vous pouviez séparer les deux services sur deux serveurs différents et adapter l'adressage réseau en fonction de votre topologie.

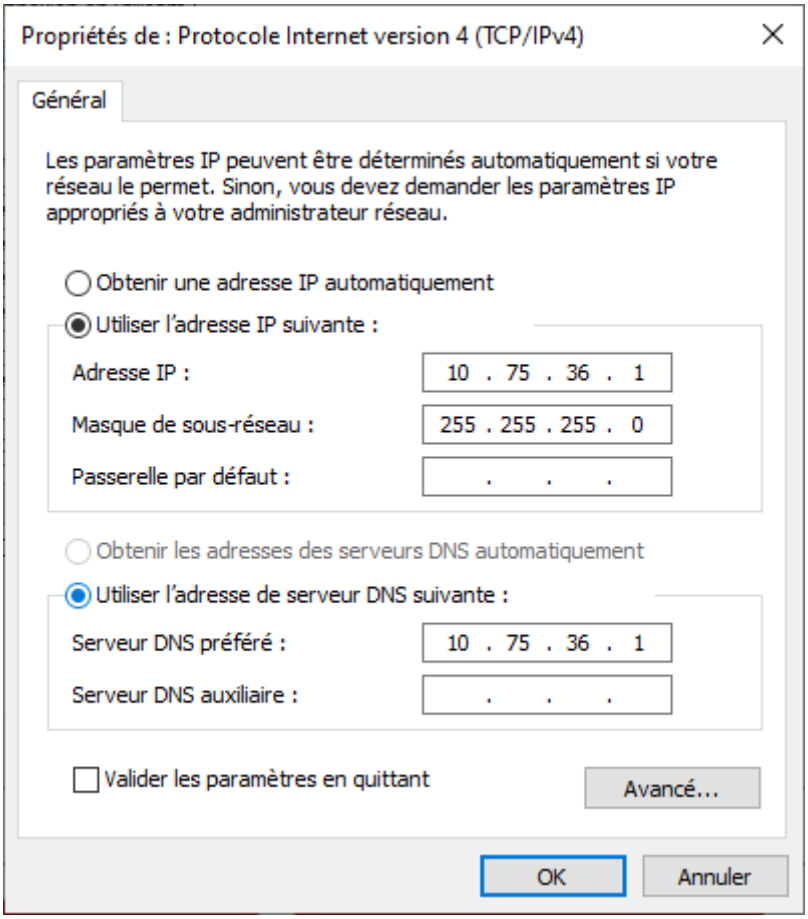
III – Préparation du serveur

Pour que les utilisateurs distants puissent avoir accès au service interne de l'entreprise, il est nécessaire que notre serveur soit aussi connecté à l'extérieur. Raison pour laquelle notre

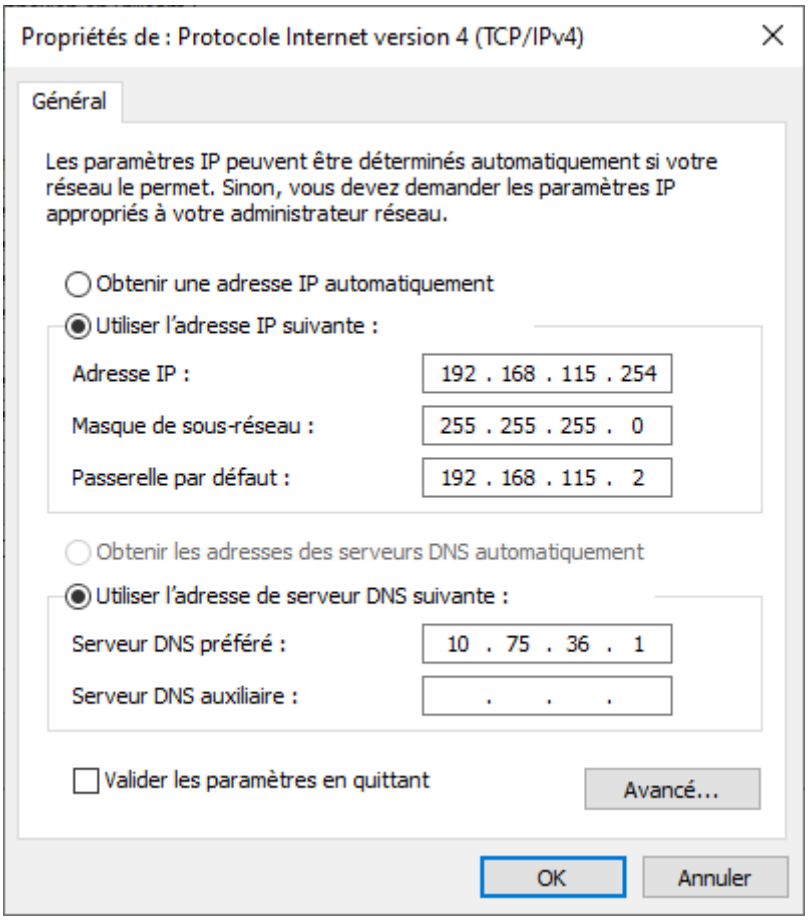
serveur possède deux cartes réseaux que j'ai renommé LAN pour le réseau locale et VPN qui l'interface connectée à l'extérieur à laquelle nos utilisateurs accèderont pour se connecter au réseau local.



Configuration réseau carte LAN

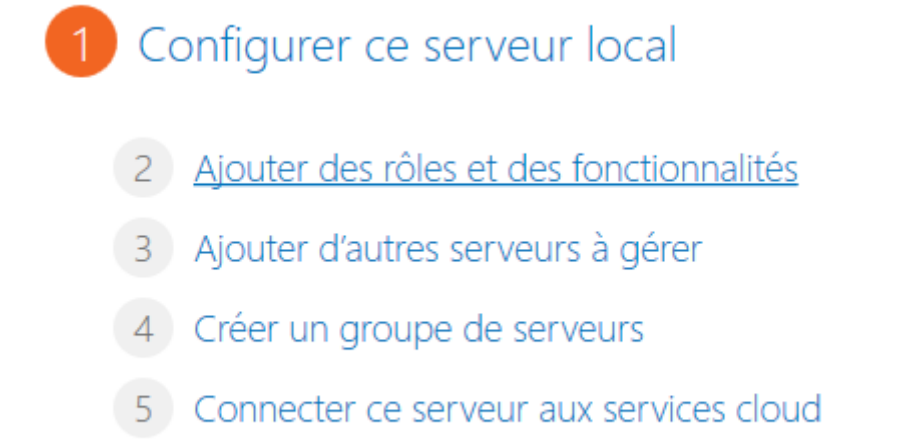


Configuration réseau carte VPN

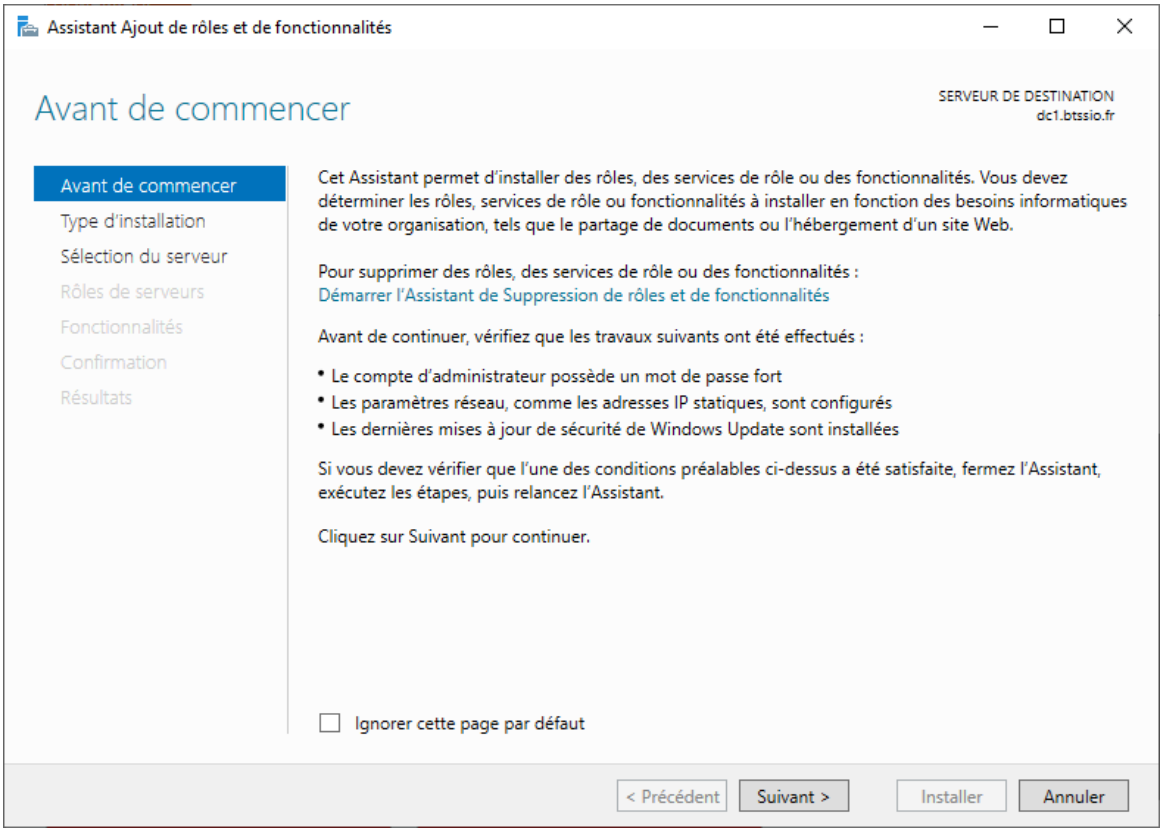


III – Installation du servie VPN

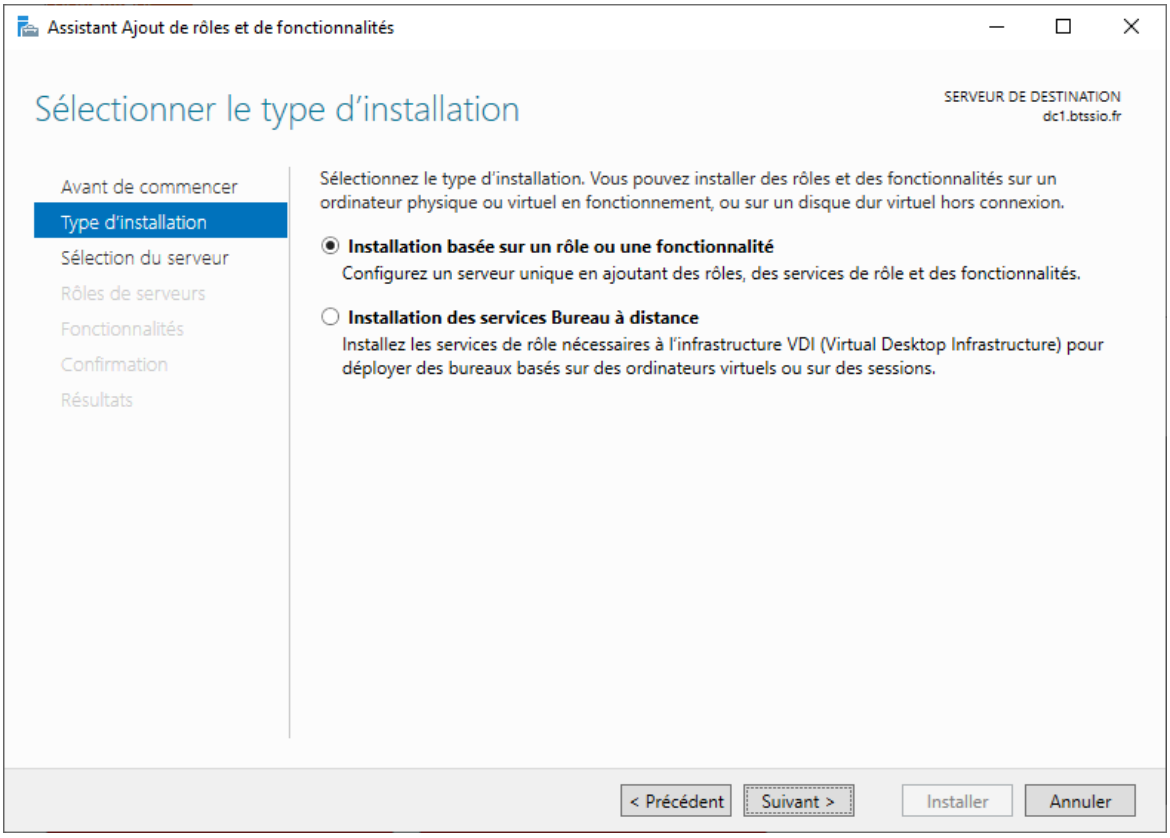
Pour installer notre service VPN, rendez-vous sur le tableau de bord du Gestionnaire de serveur et cliquez sur **« Ajouter des rôles et des fonctionnalités »**



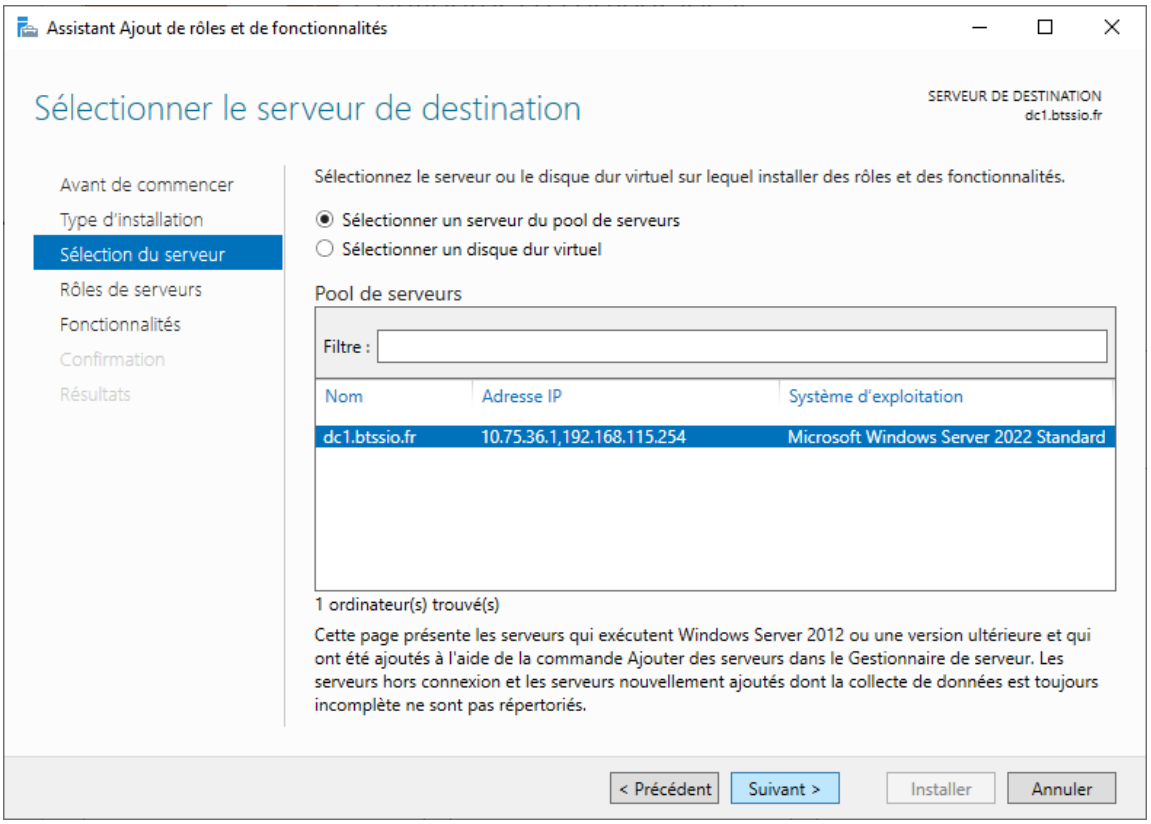
L'assistant se lance, cliquez sur **« Suivant »**



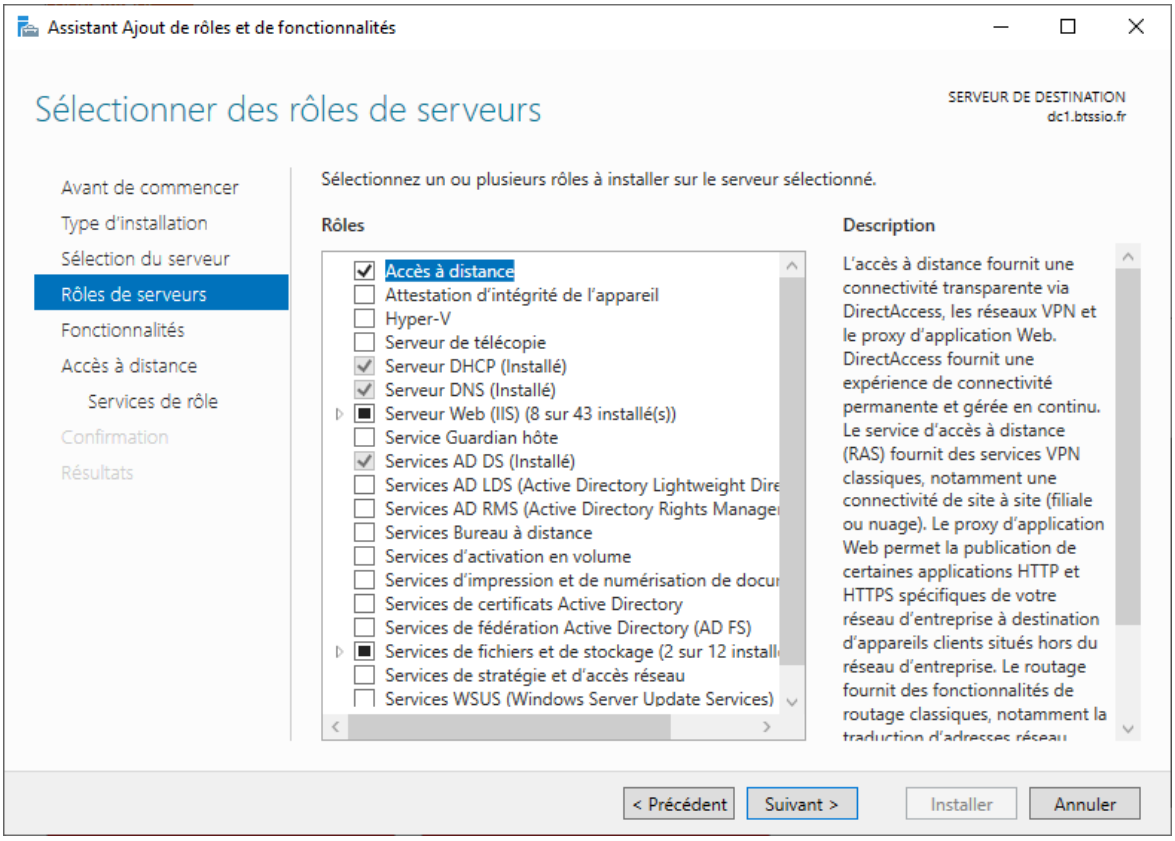
Le choix par défaut nous convient cliquez sur **« Suivant »**



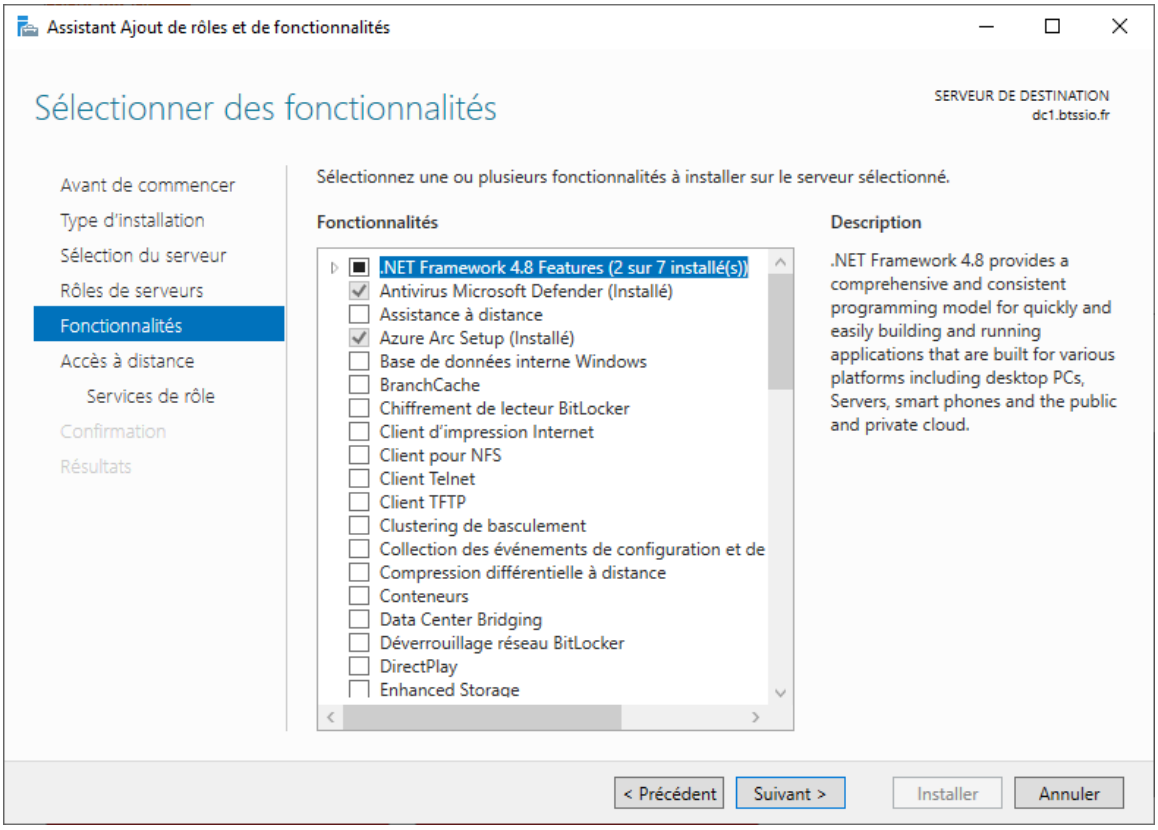
Notre serveur est choisi par défaut, cliquez sur **« Suivant »**



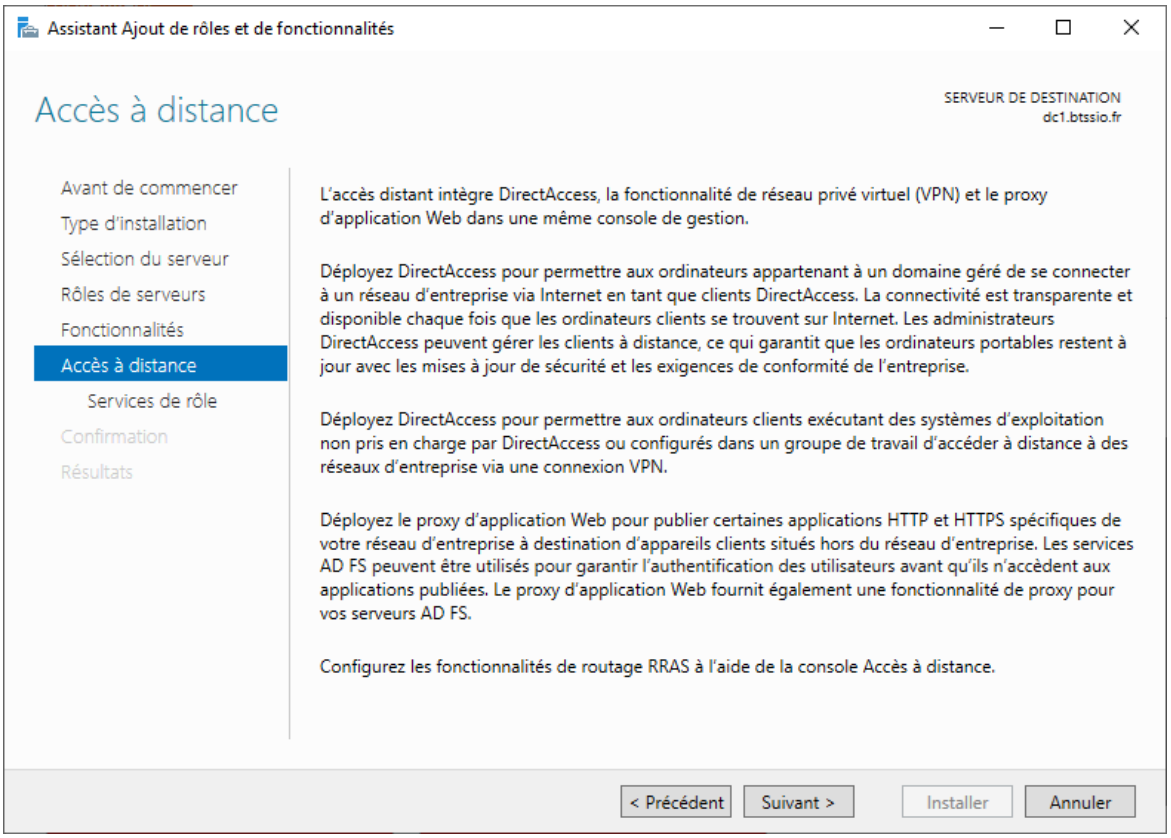
Cochez **« Accès à distance »** et cliquez sur **« Suivant »**



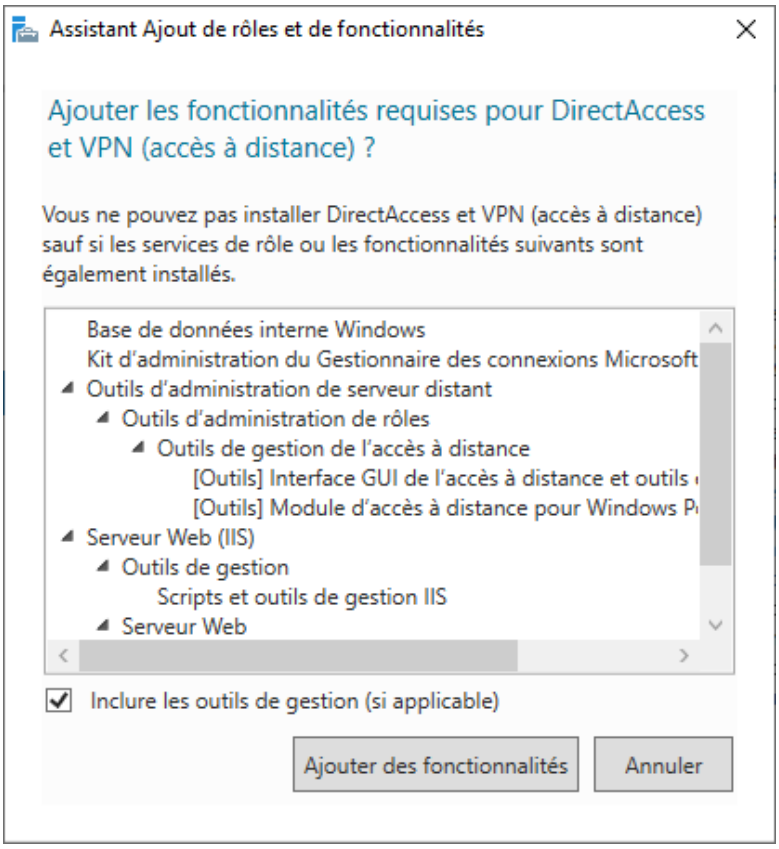
Laissez les fonctionnalités choisies par défaut et cliquez sur **« Suivant »**



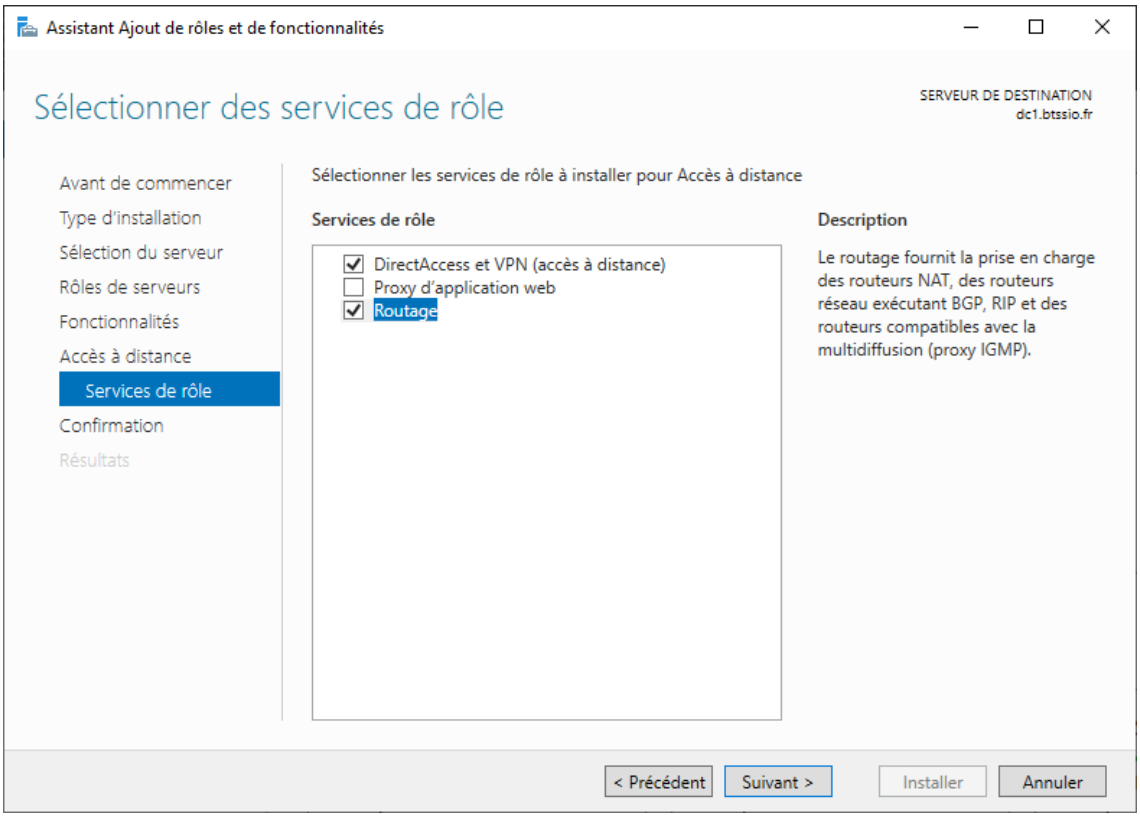
Cliquez sur **« Suivant »**



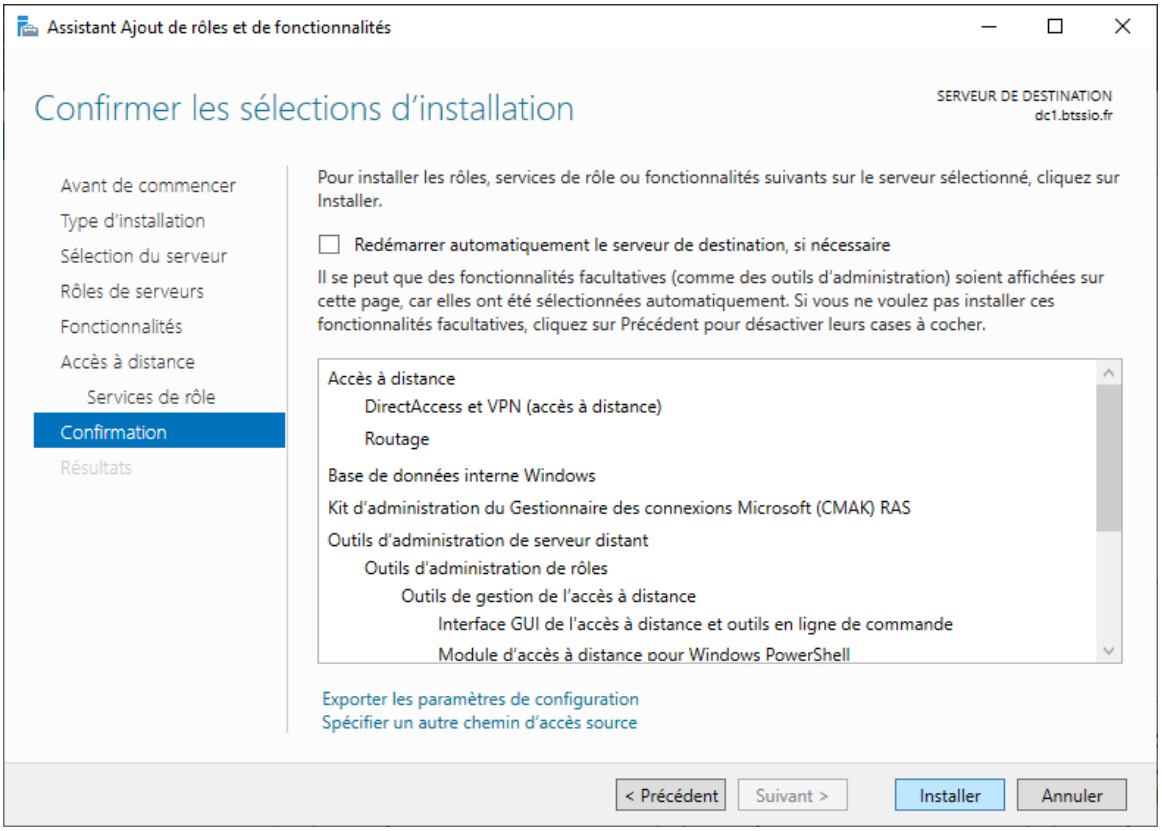
Cliquez sur **« Ajouter les fonctionnalités »**



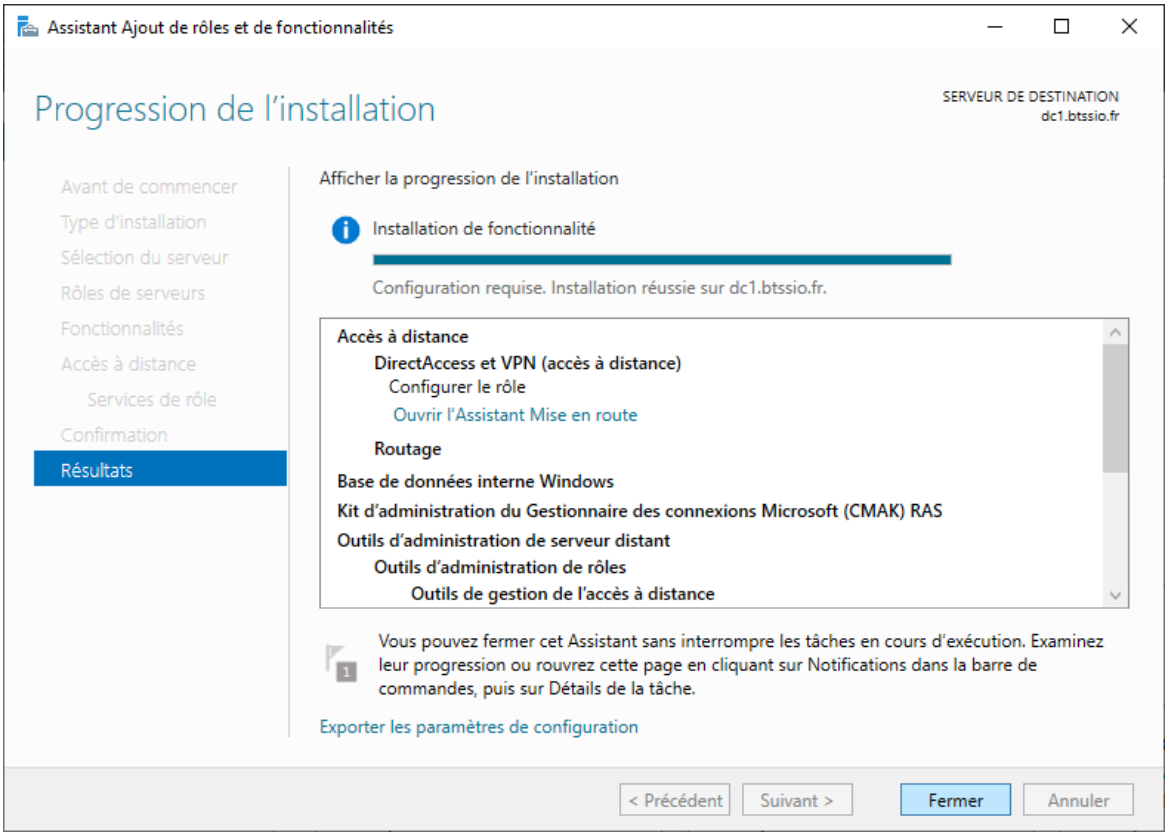
Cochez **« DirectAccess et VPN »** et **« Routage »** puis cliquez sur **« Suivant »**



Cliquez sur **« Installer »**



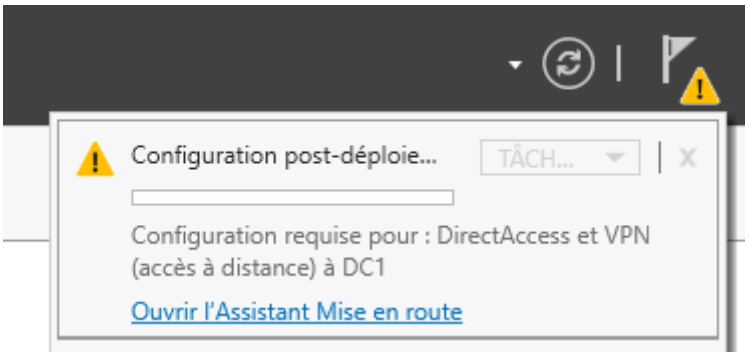
Une fois l'installation terminée, cliquez sur **« Fermer »**



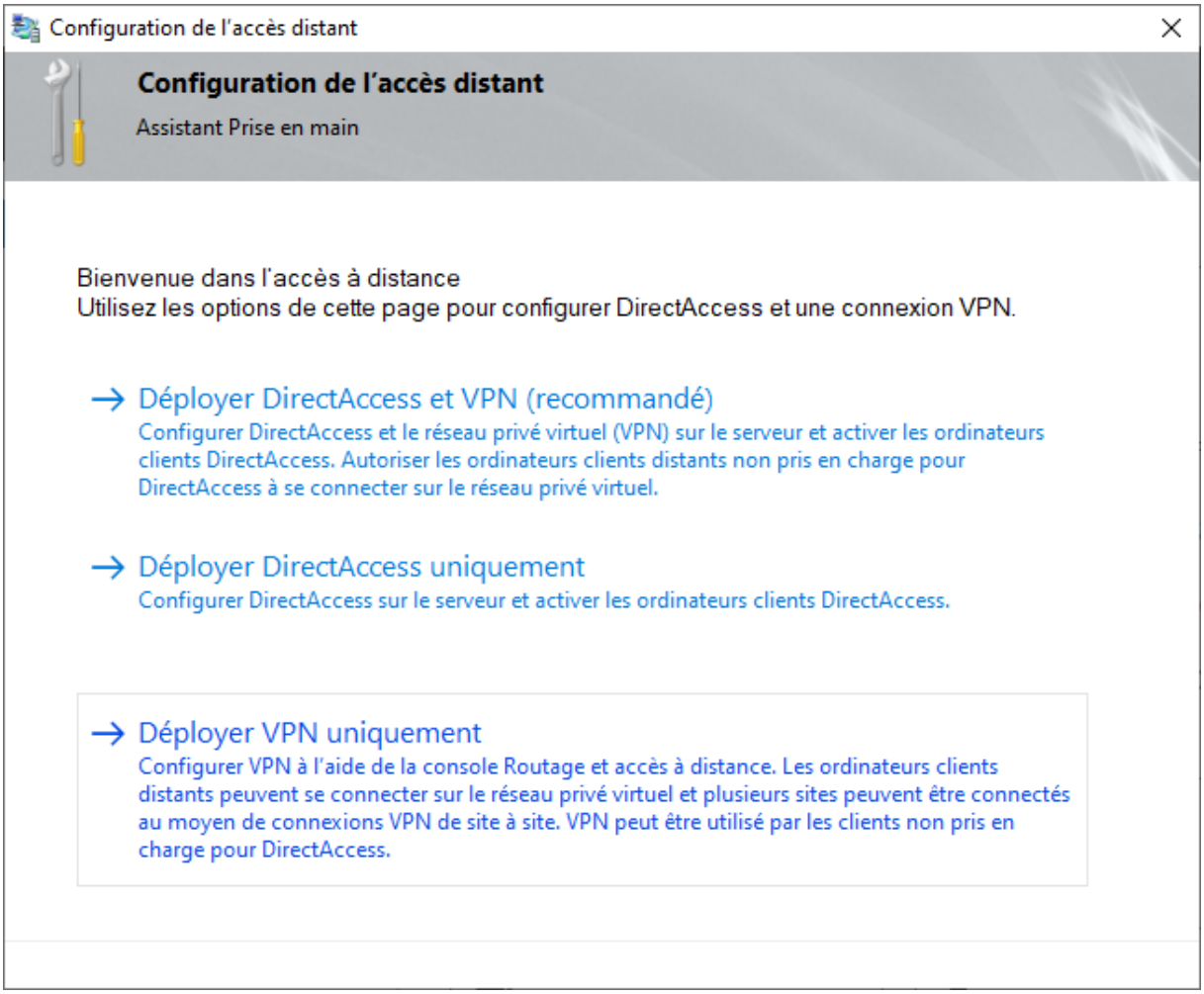
III – Configuration du servie VPN

Notre service étant installé, il faut le configurer en fonction des besoins de l'entreprise.

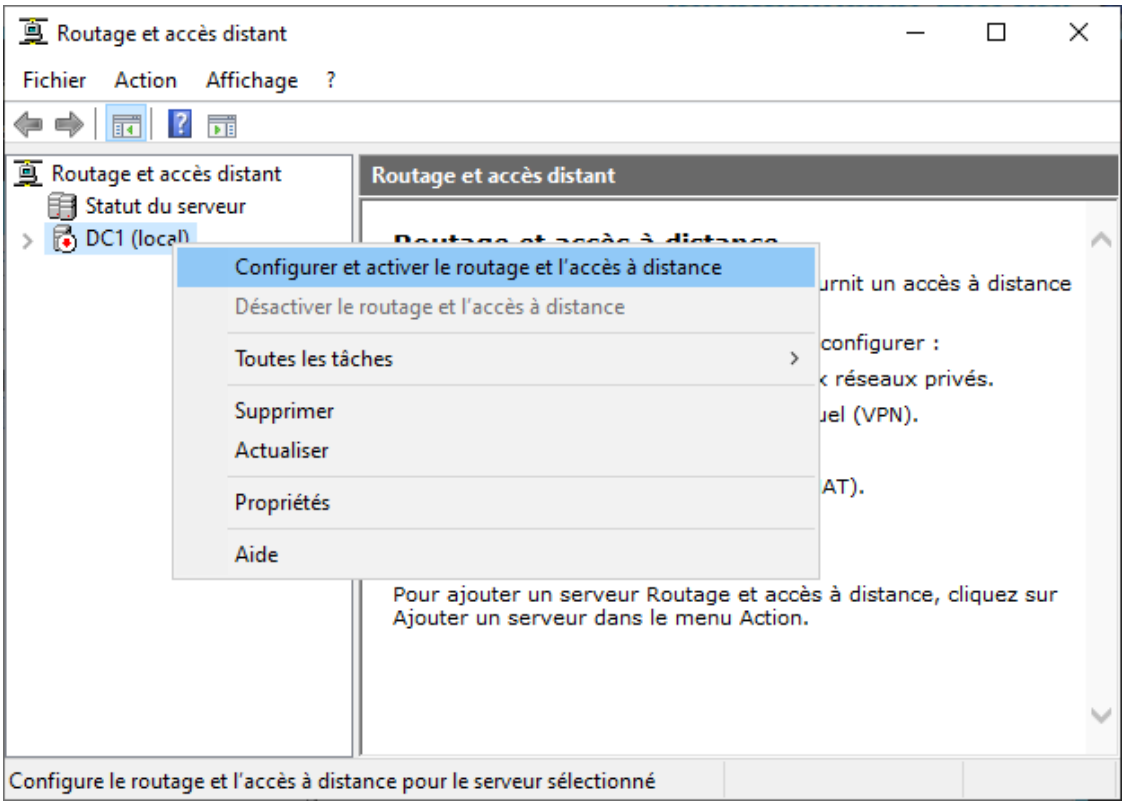
Rendez-vous dans le centre de notification du Gestionnaire de serveur et cliquez sur **« Ouvrir l'Assistant Mise en route »**



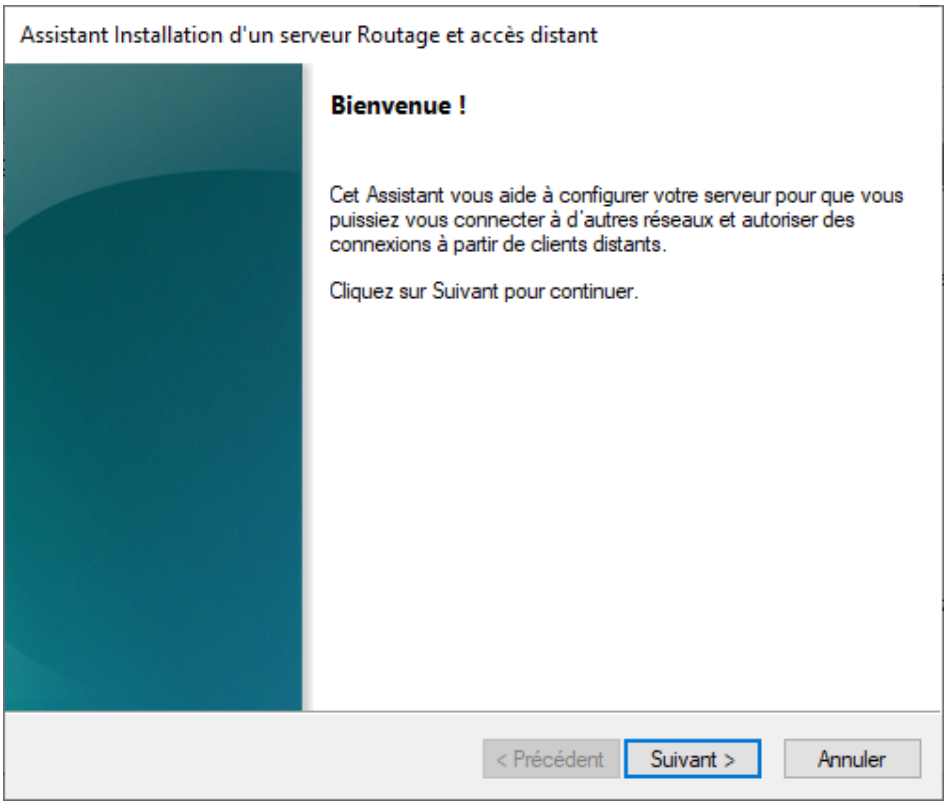
Une foi l'assistant lancé, cliquez sur **« Déployer VPN uniquement »**



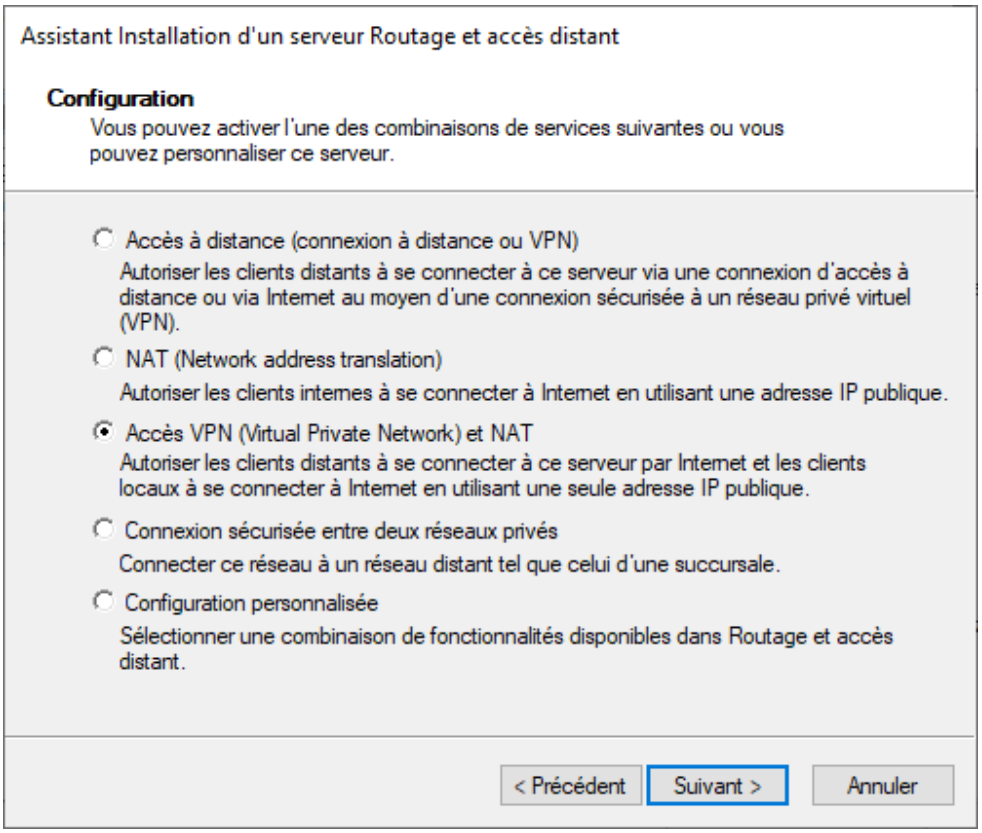
La console **« Routage et accès distant »** se lance et faites un clic droit sur le nom du serveur local et cliquez sur **« Configurer et activer le routage et l'accès à distance »**



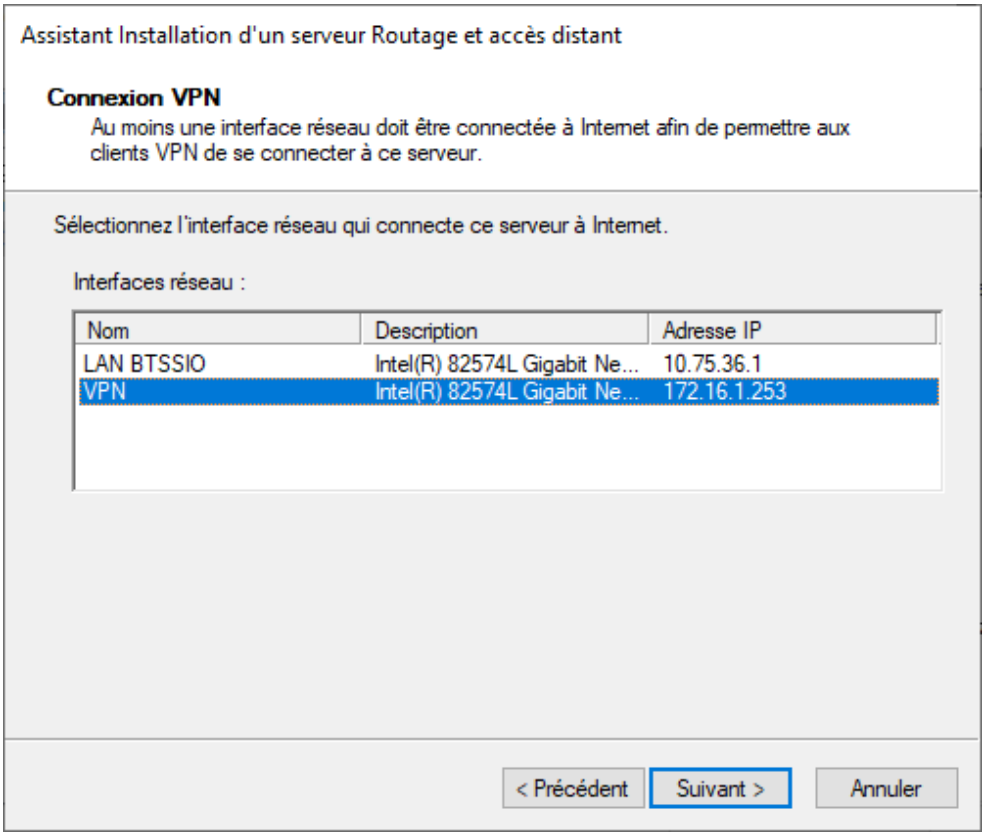
L'assistant Windows se lance, cliquez sur **« Suivant »**



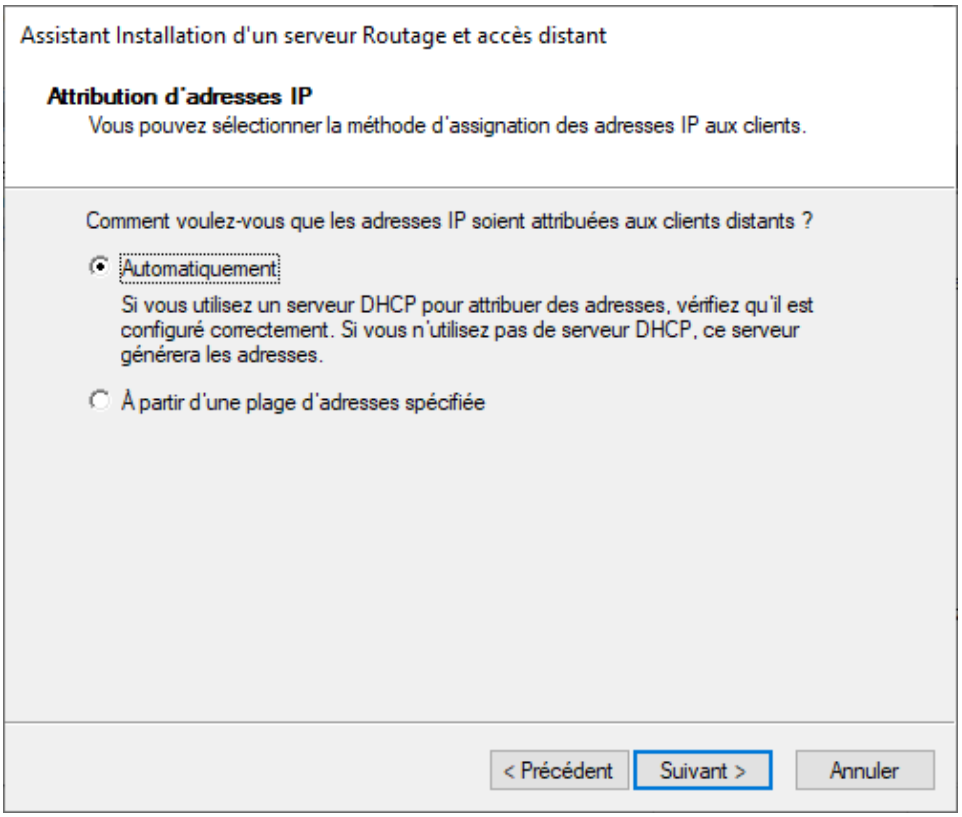
Choisissez **« Accès VPN »** et cliquez sur **« Suivant »**



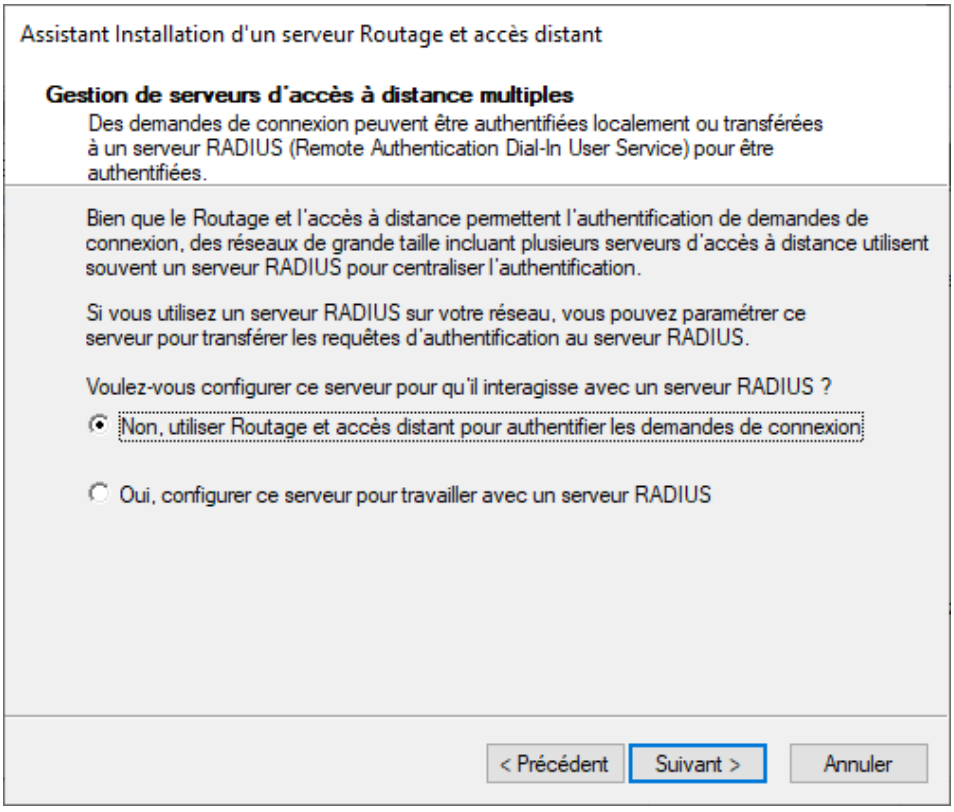
Choisissez l'interface **« VPN »** puis cliquez sur **« Suivant »**



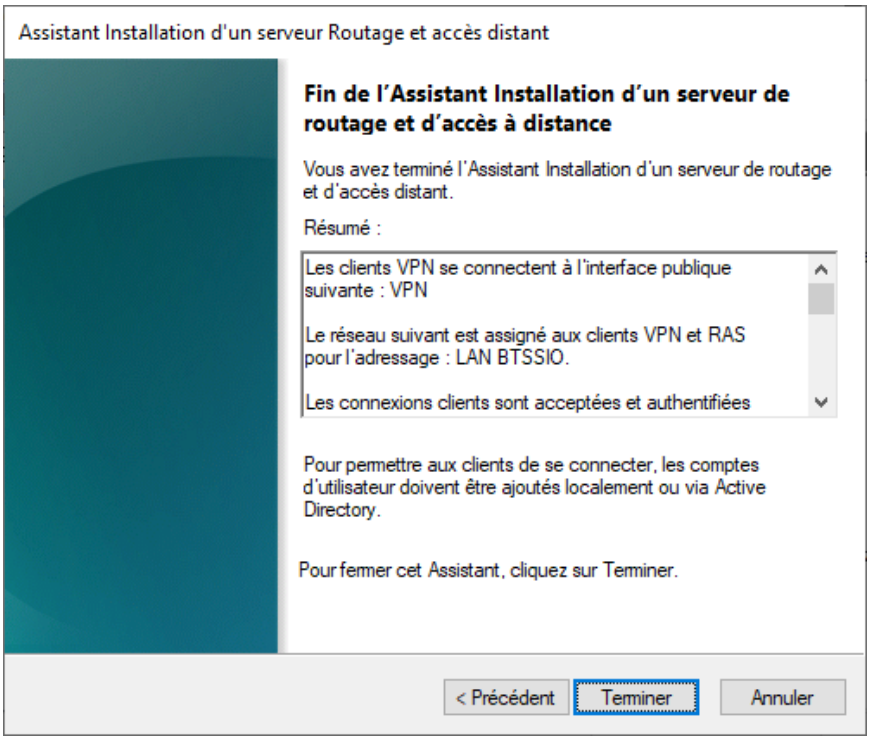
Pour le mode d'attribution des adresses IP de nos utilisateurs qui se connecteront au VPN choisissez **« Automatiquement »**



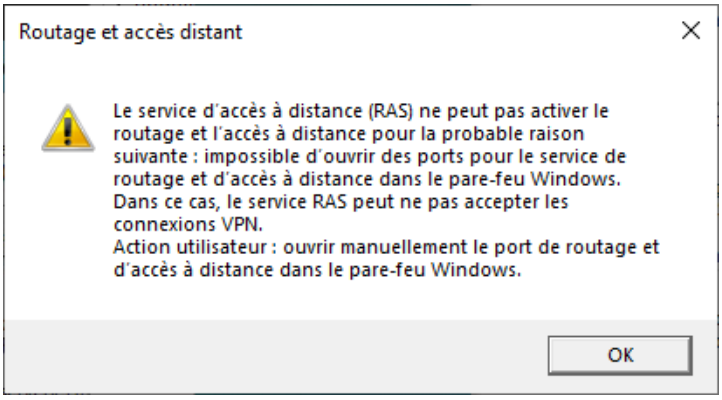
Laissez le choix par défaut car nous n'utiliserons pas de serveur RADIUS



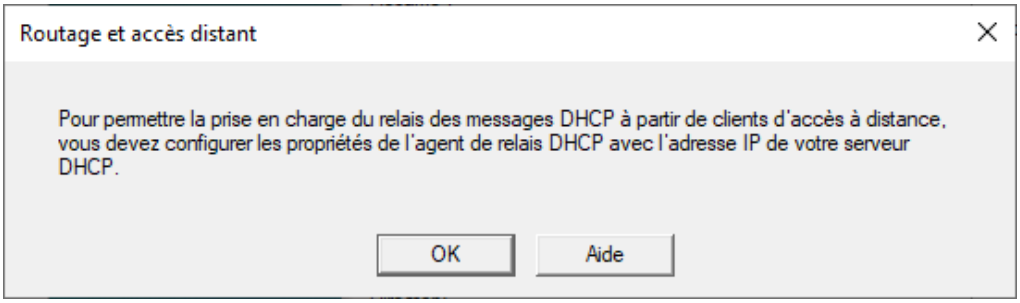
L'assistant affiche un résumé des configurations, cliquez sur **« Terminer »**



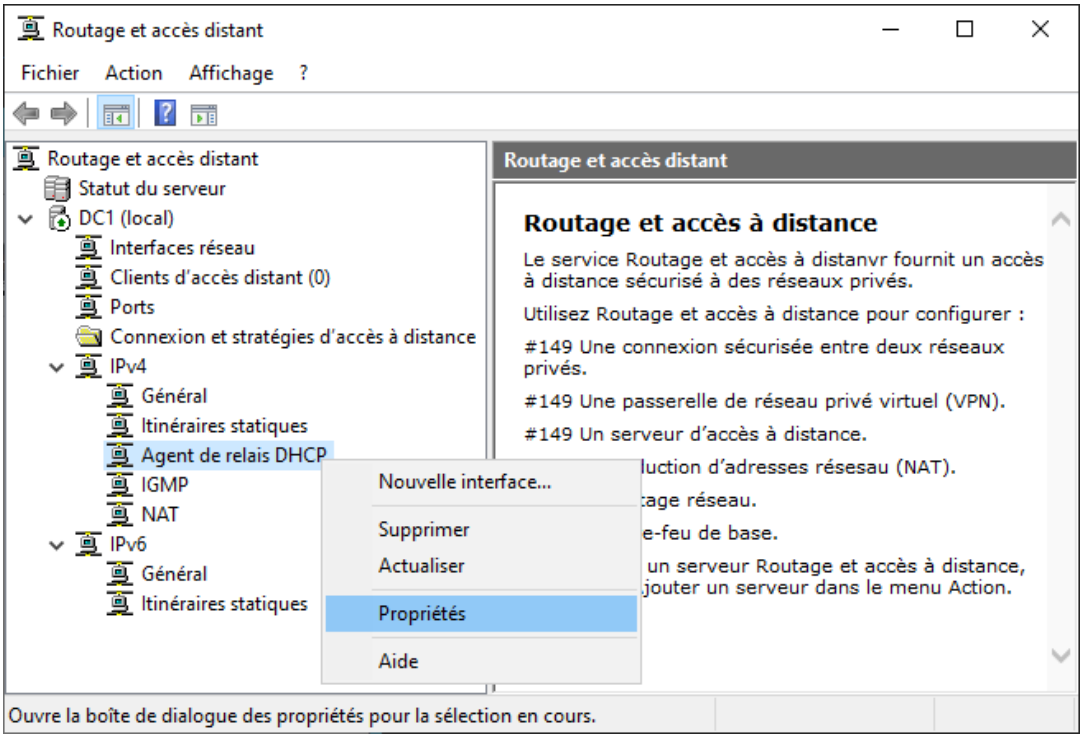
Pour l'avertissement concernant l'ouverture des ports, nous ouvriront ces ports manuellement. Cliquez sur **« OK »**



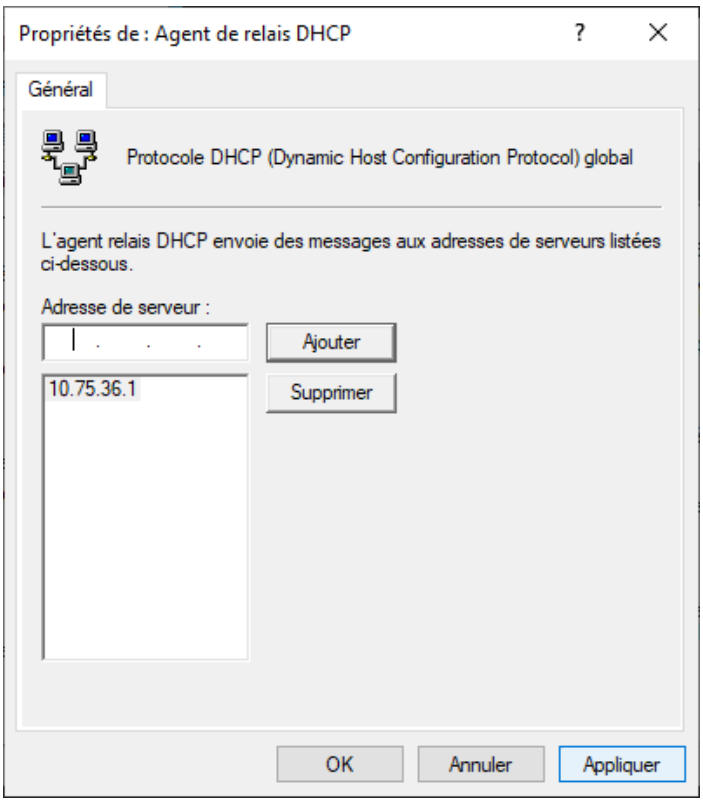
En ce qui concerne l'agent relais DHCP cliquez sur **« OK »** et nous allons configurer dans la partie tout juste après.



Comme affiché précédemment, nous allons mettre en place un relais DHCP pour nos utilisateurs VPN. Pour ce faire Déplier la section **« IPv4 »** clic droit puis afficher les **« Propriétés »** de la partie **« Agent de relais DHCP »**

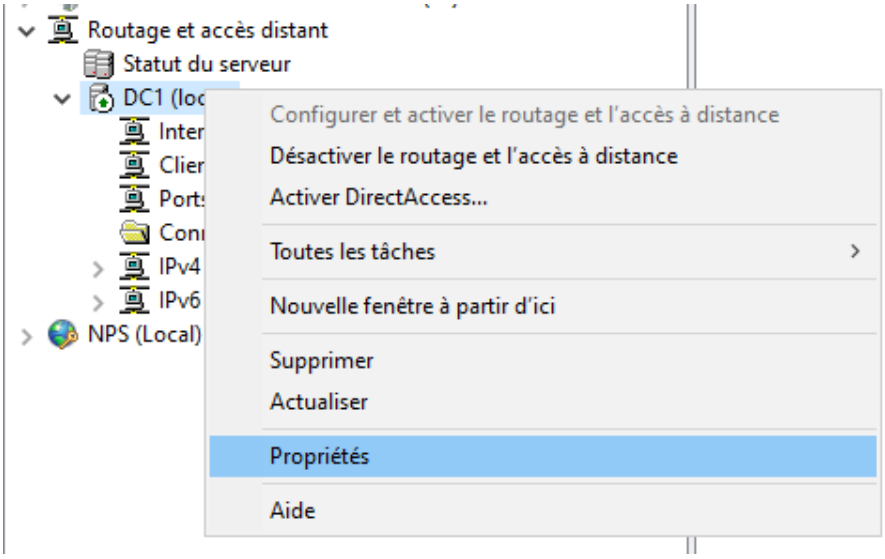


Préciser ici l'adresse IP du serveur DHCP (dans mon cas ici c'est l'adresse de mon contrôleur de domaine) puis cliquez sur **« Appliquer »**

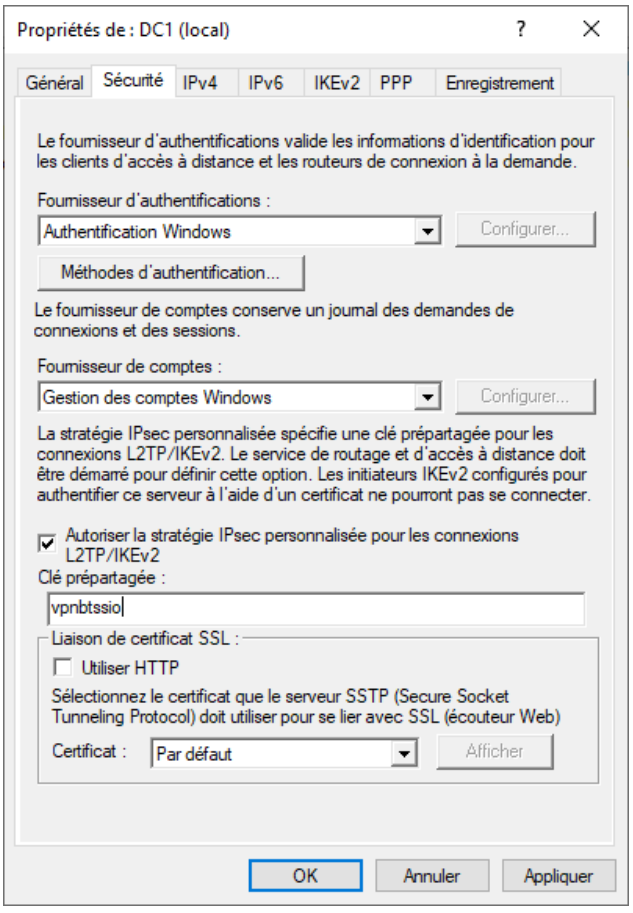


Actuellement avec le service VPN installé, il est par défaut en **PPTP (Point-to-Point Tunneling Protocol)**, nous allons activer le protocole **L2TP (Layer 2 Tunneling Protocol)** avec une clé prépartagée.

Pour se faire, clic droit sur le nom du serveur VPN puis cliquez sur **« Propriétés »**

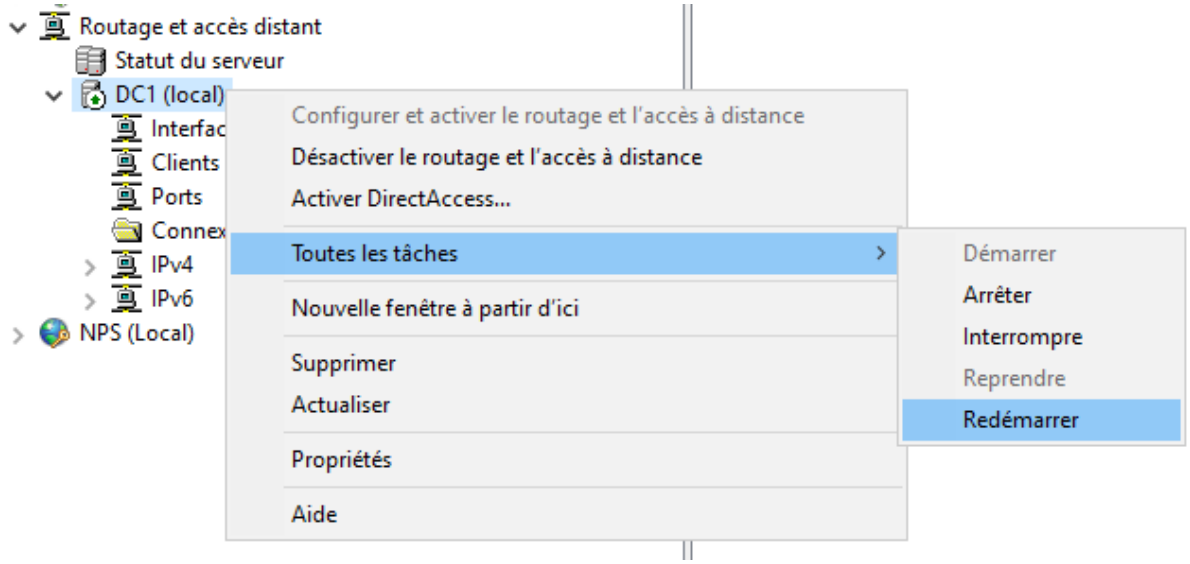


Allez dans l'onglet **« Sécurité »** et cochez la case pour autoriser le protocole L2TP et saisissez votre clé pré-partagée.



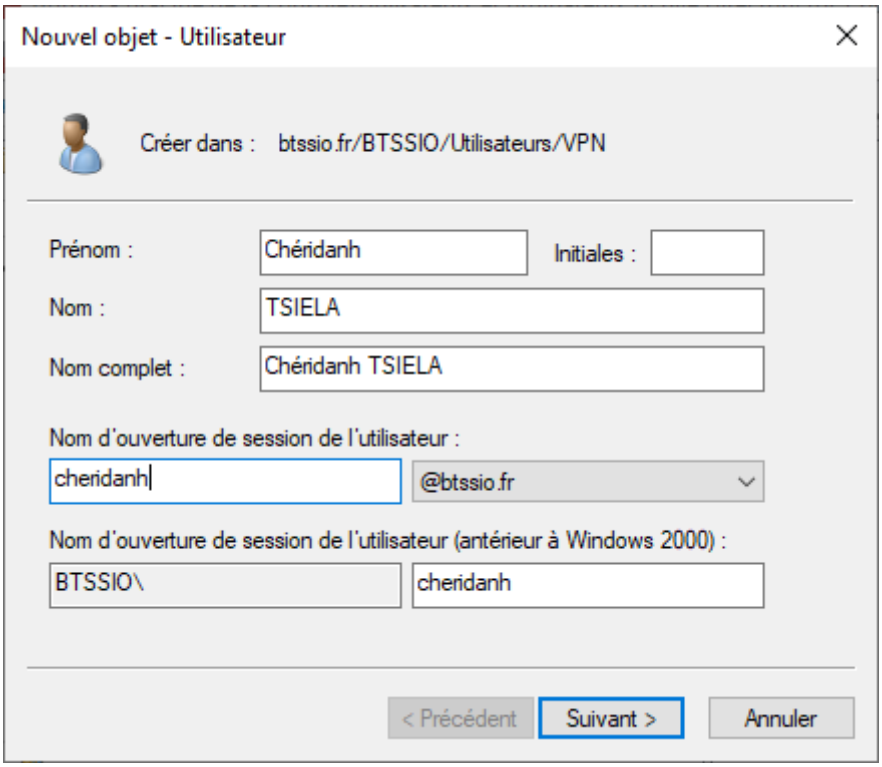
Pour que les modifications soient prises en compte, il faudra redémarrer le service VPN.

Clic droit sur le nom du serveur VPN => **Toutes les tâches => Redémarrer**



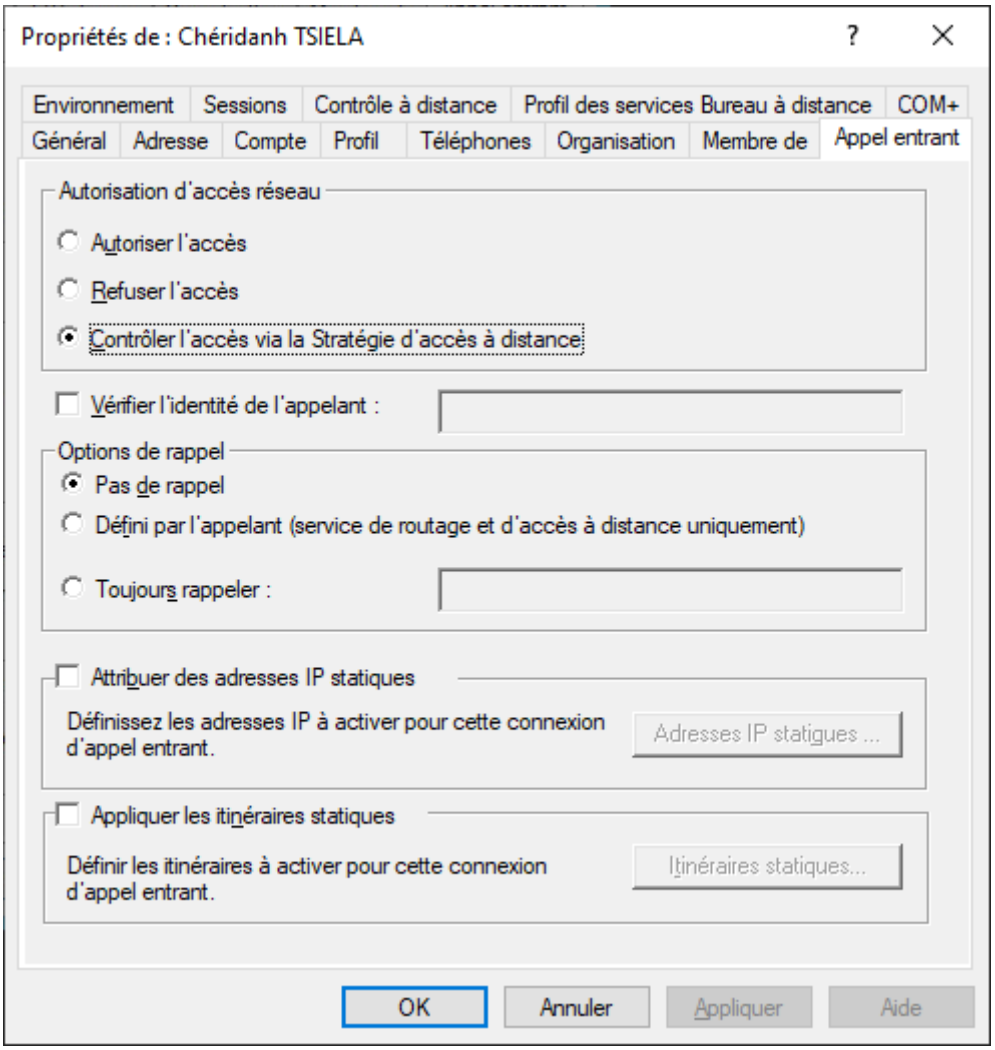
III – Utilisateur VPN

Dans Active Directory, si ce n'est pas déjà fait créer un utilisateur pour tester notre connexion VPN



Mon utilisateur appartient à un groupe de sécurité qui s'appelle **« VPN »**

Par défaut, l'accès des utilisateurs au service VPN est gérer par une stratégie d'accès à distance

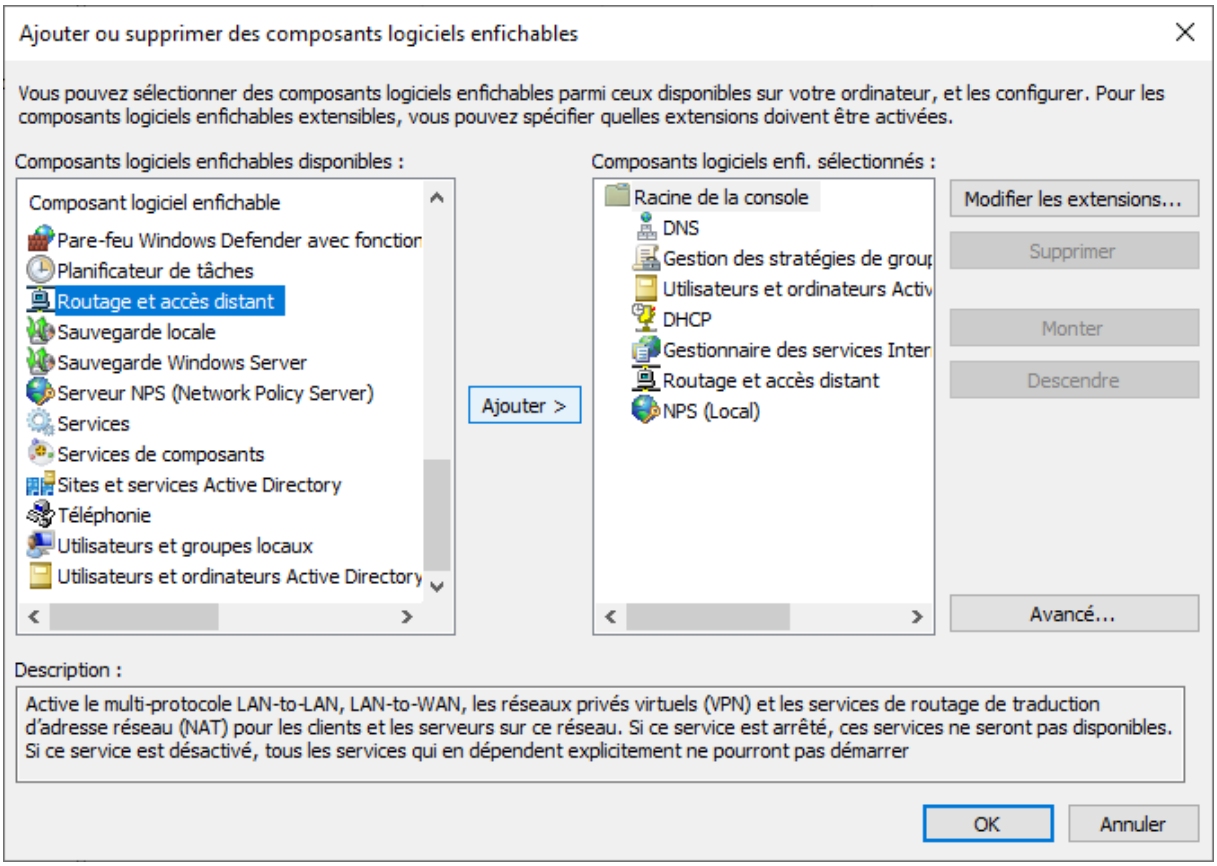


III – Stratégie d'accès réseau

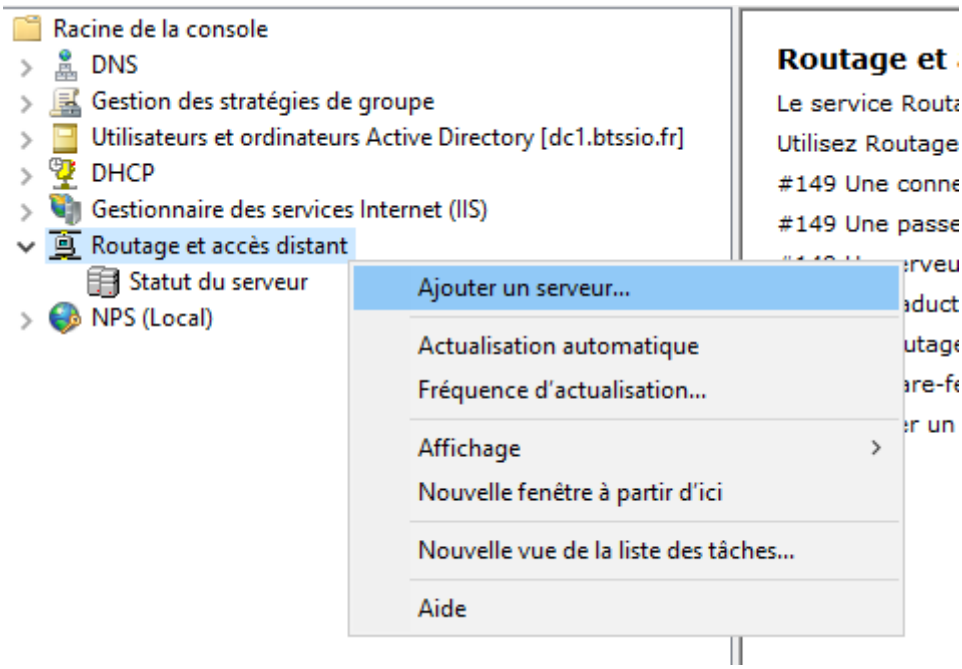
Commencez par ajouter les consoles d''administration créer lors de notre installation du service VPN.

Dans notre console MMC ajoutez les composants suivants :

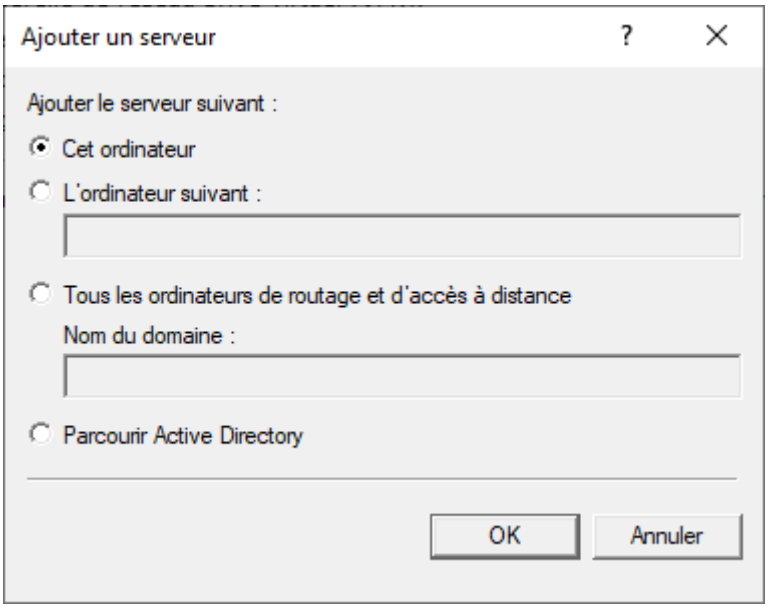
Routage et accès distant et **NPS**



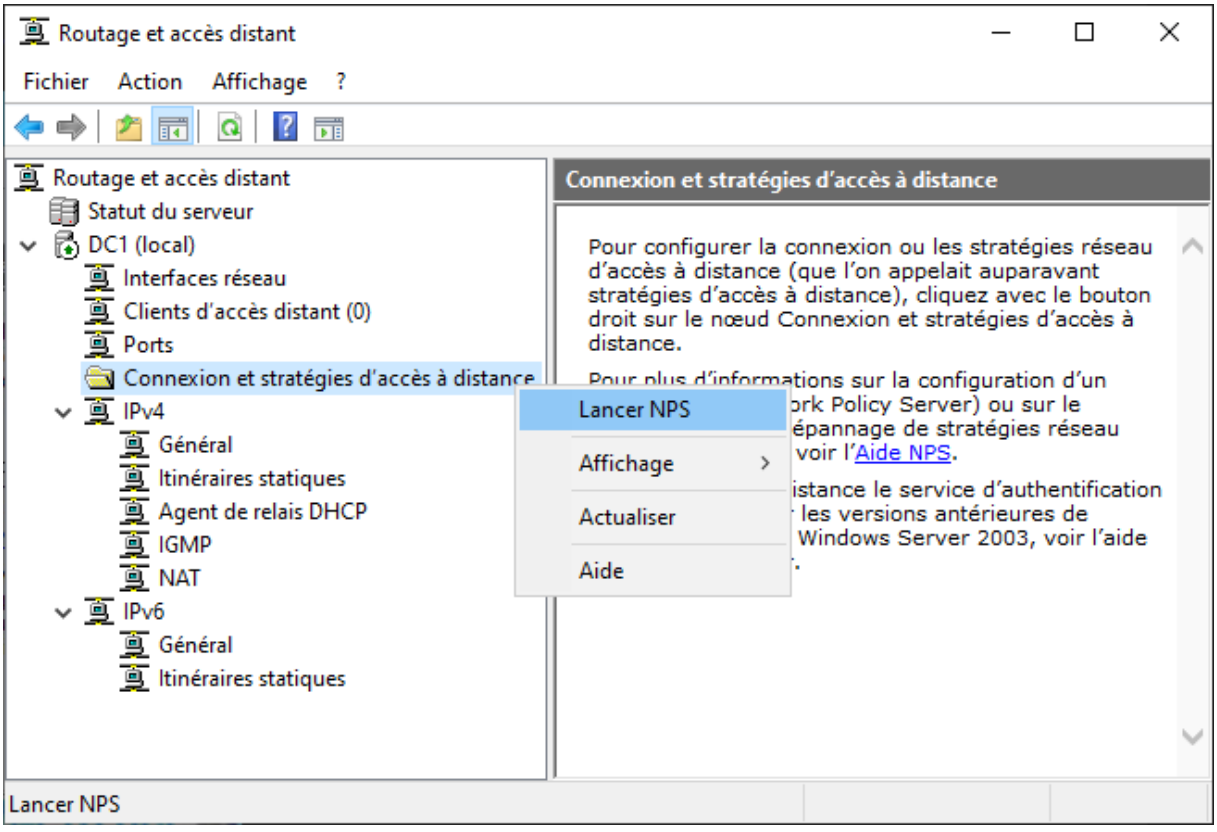
Une fois les composants ajoutés, clic droit sur routage et accès distant et cliquez sur **« Ajouter un serveur »**



Dans notre cas, le service VPN se trouve sur ce serveur, donc on laisse le choix par défaut et cliquez sur **« OK »**



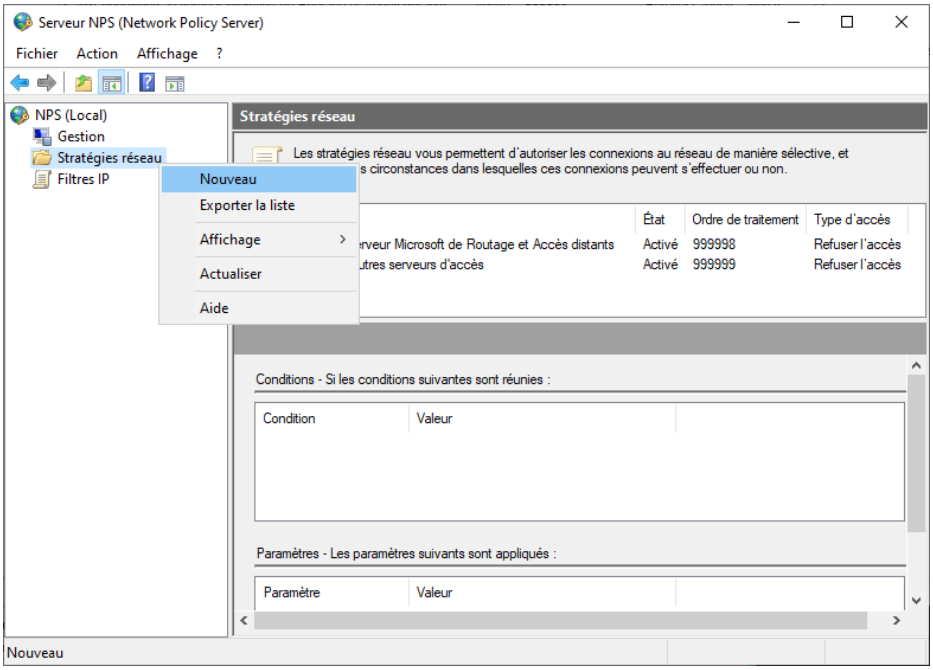
Faites un clic droit sur **« Connexion et stratégies d'accès à distance »** puis cliquez sur **« Lancer NPS »**



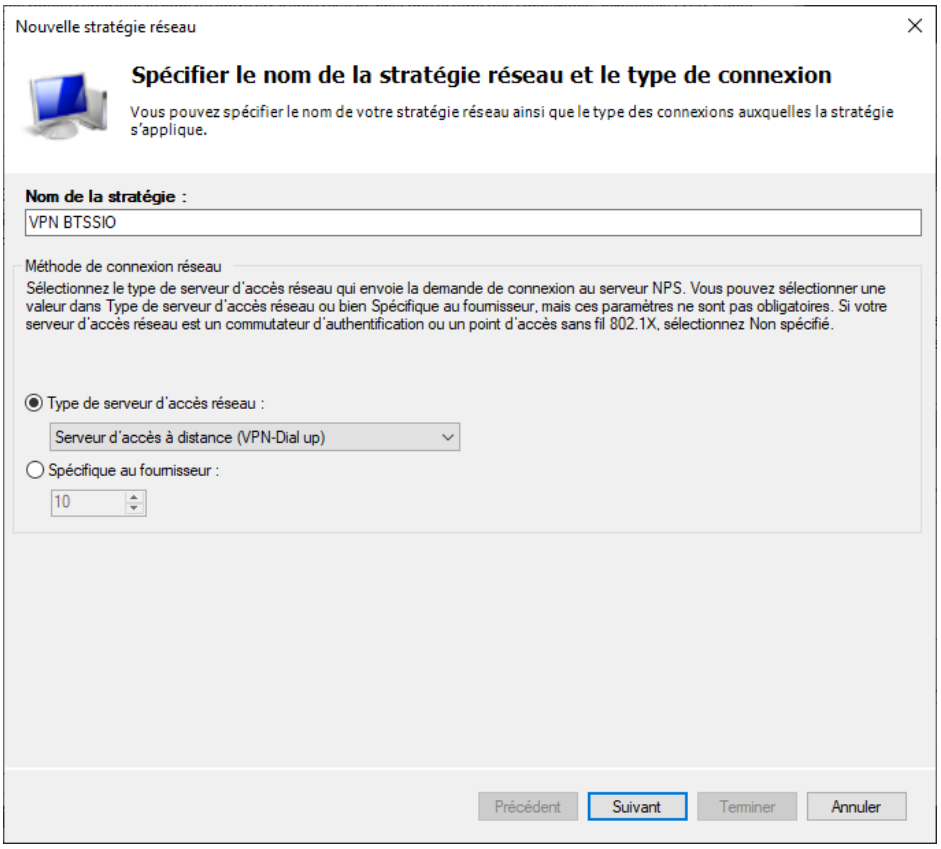
Vous serez redirigé dans une nouvelle interface de NPS.

Dans cette console, par défaut il y a deux stratégies d'accès réseau qui refuse l'accès au service VPN. Nous allons créer une règle qui en autorise.

Clic droit sur **« Stratégie réseau »** puis cliquez sur **« Nouveau »**

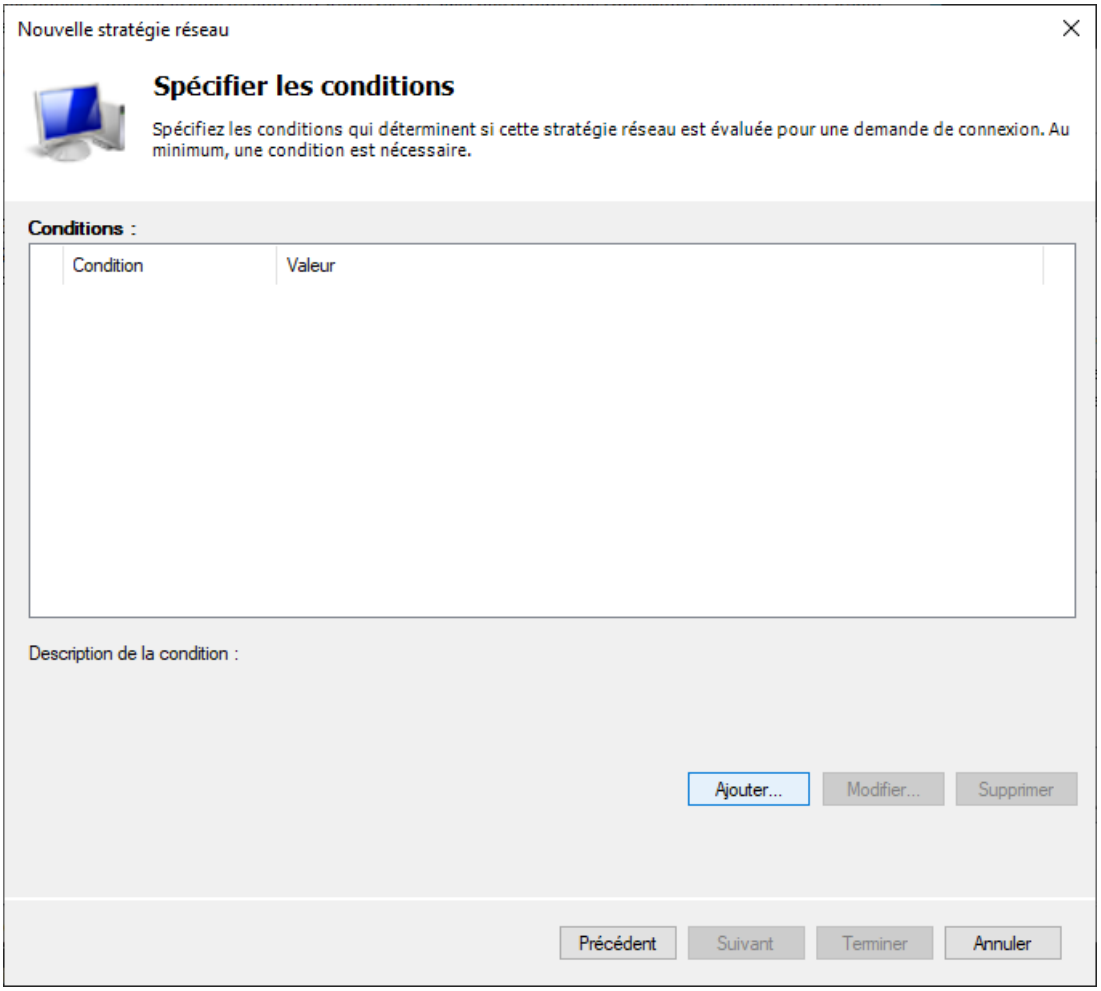


Saisissez un nom de la stratégie et dans de serveur d'accès réseau prenez **« Serveur d'accès à distance (VPN-Dial UP) »**

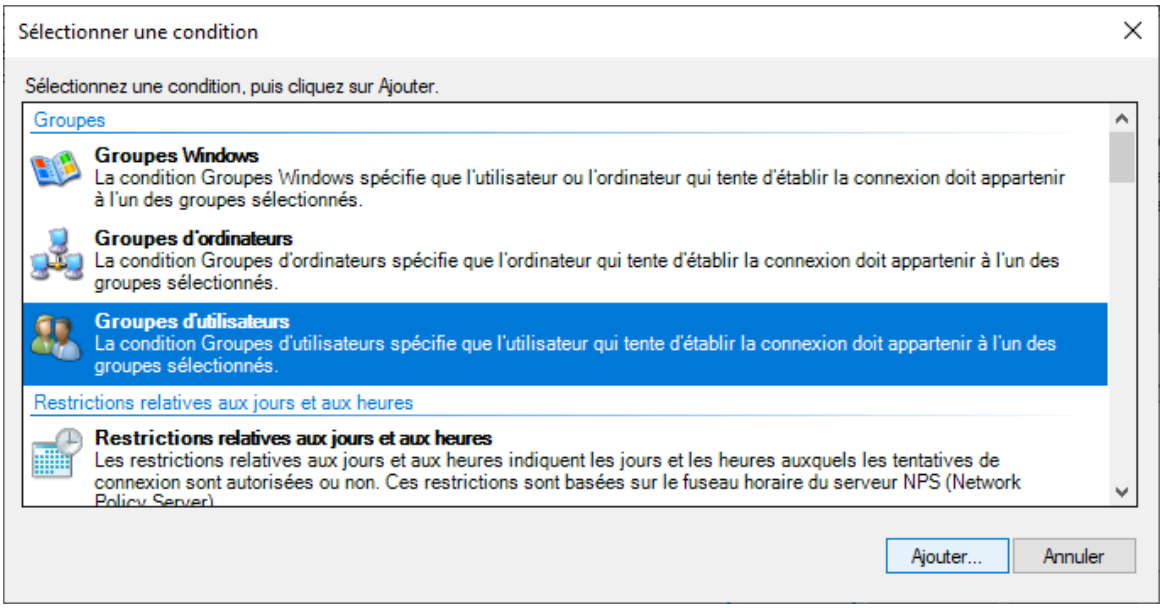


Dans les conditions, nous allons ajouter le groupe d'utilisateurs qui aura accès au service VPN.

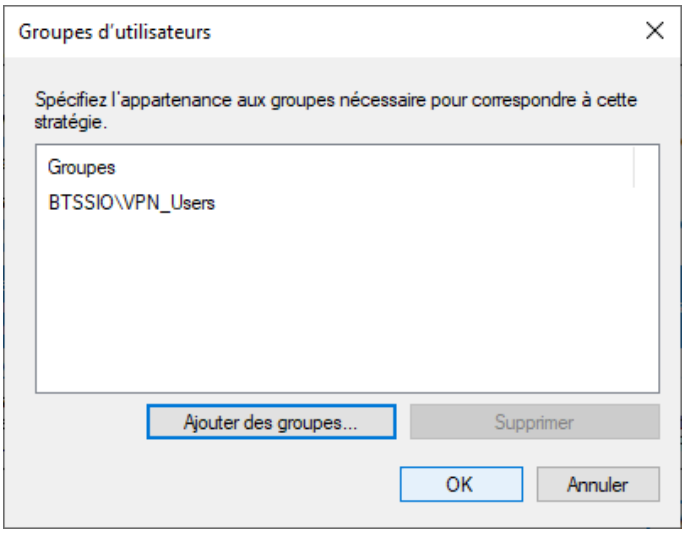
Cliquez sur **« Ajouter »**



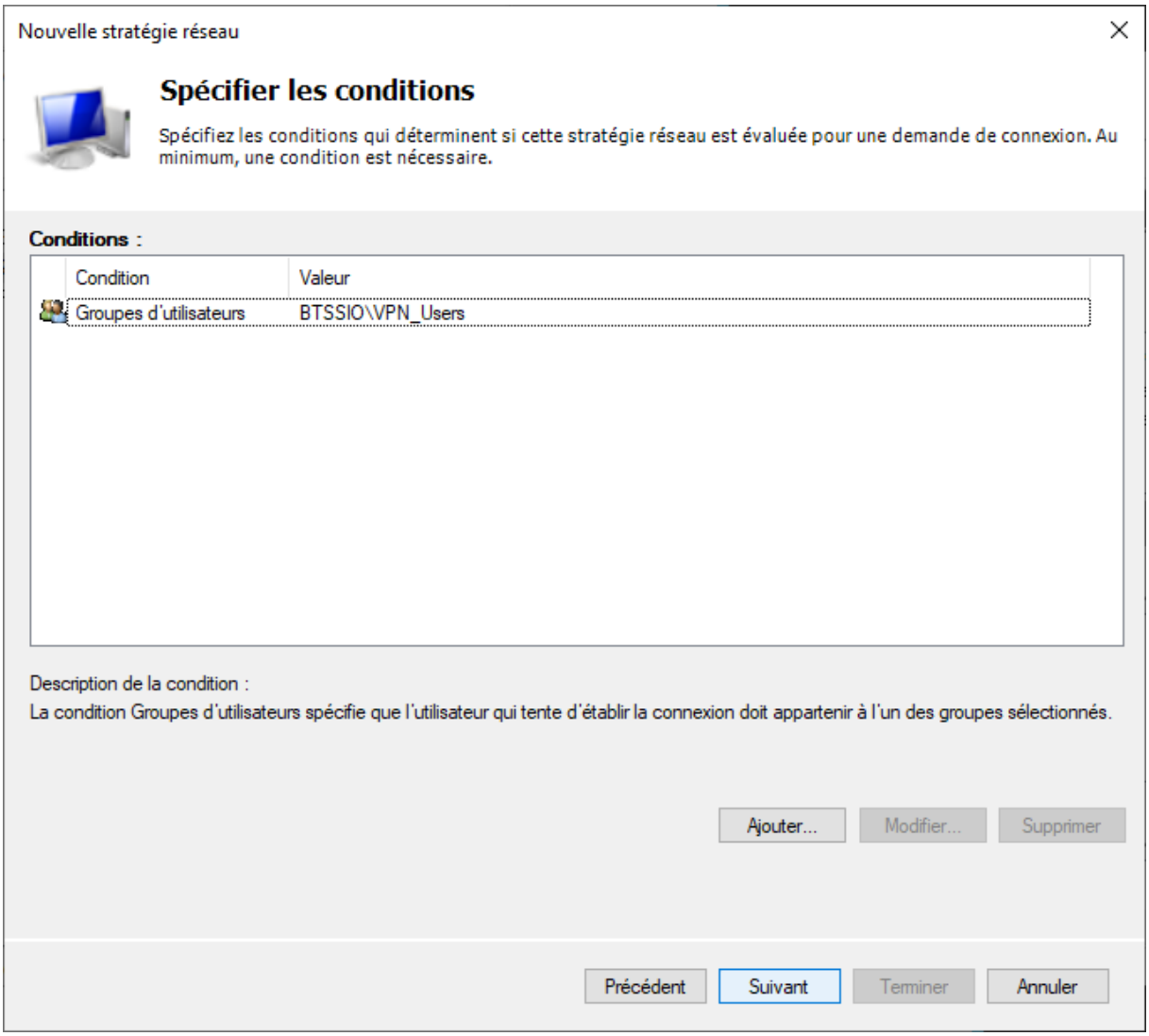
Sélectionner **« Groupe d'utilisateurs »**



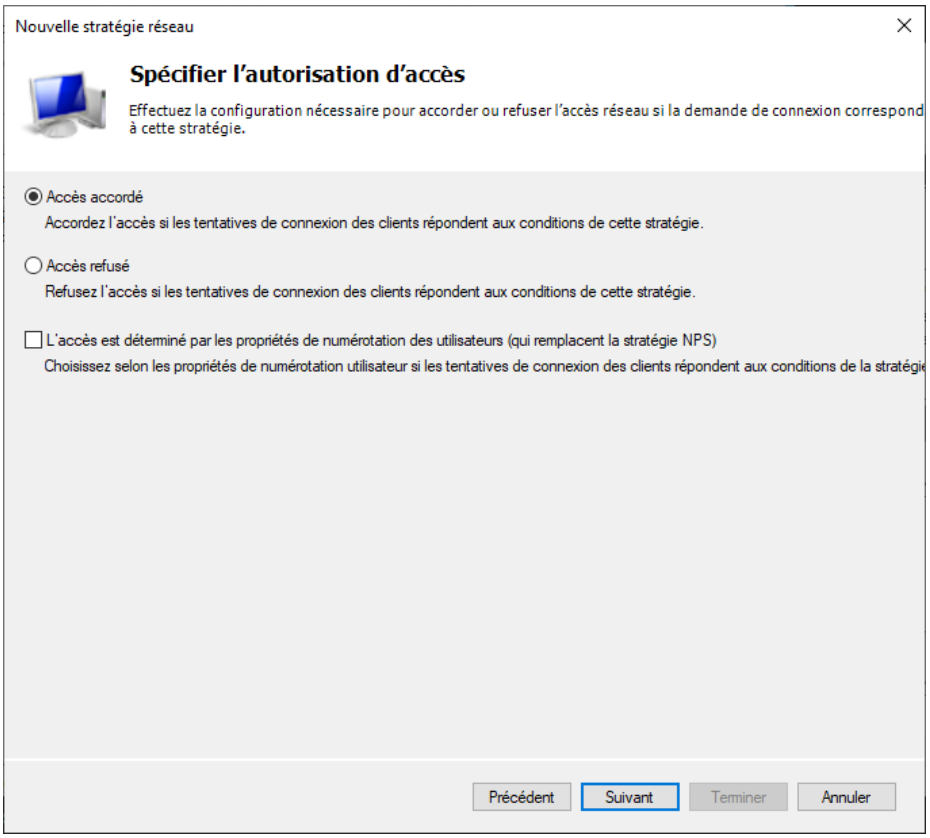
Sélectionner le groupe d'utilisateurs concerné puis cliquez sur **« OK »**



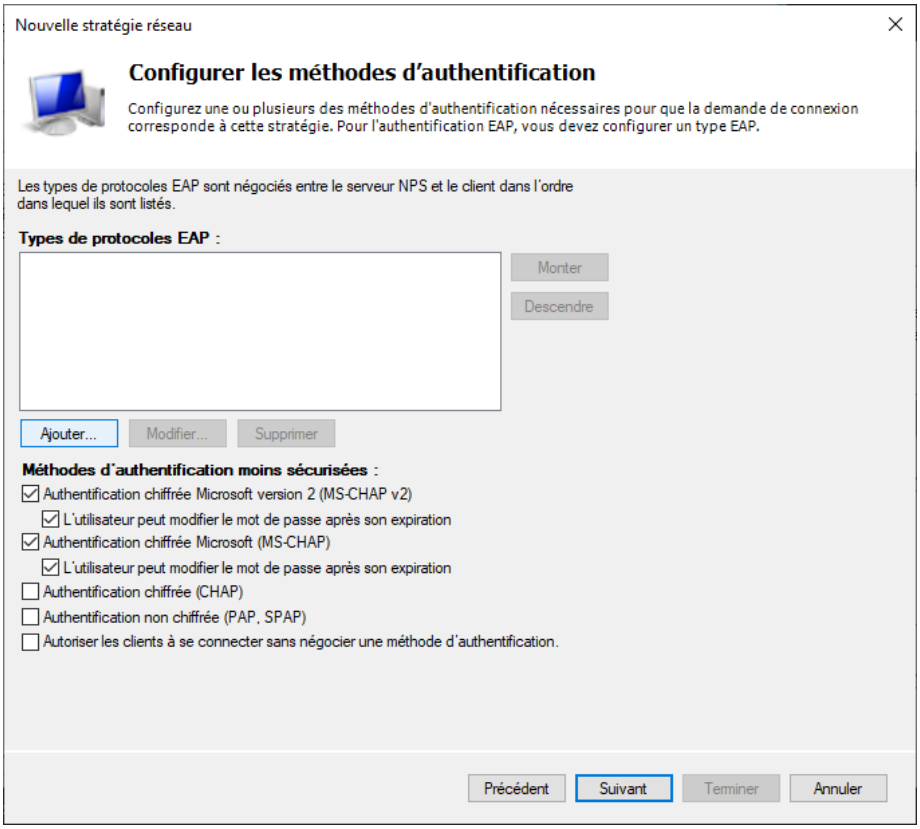
Une fois le groupe ajouter, cliquez sur **« Suivant »**



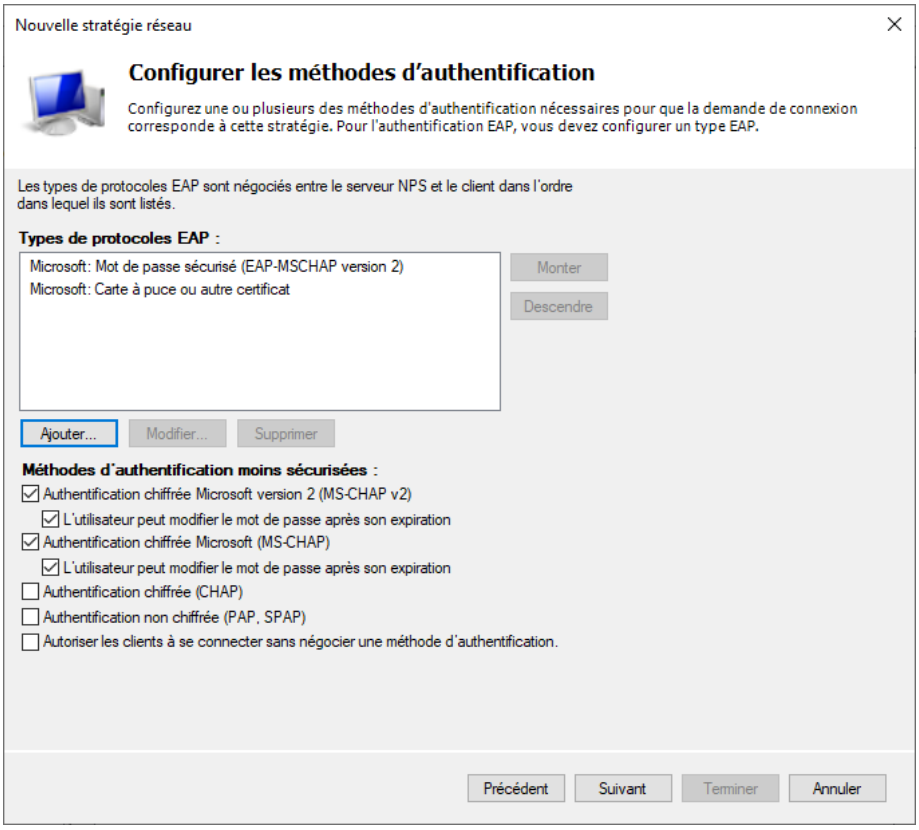
Bien entendu, il faut prendre **« Accès accordé »**



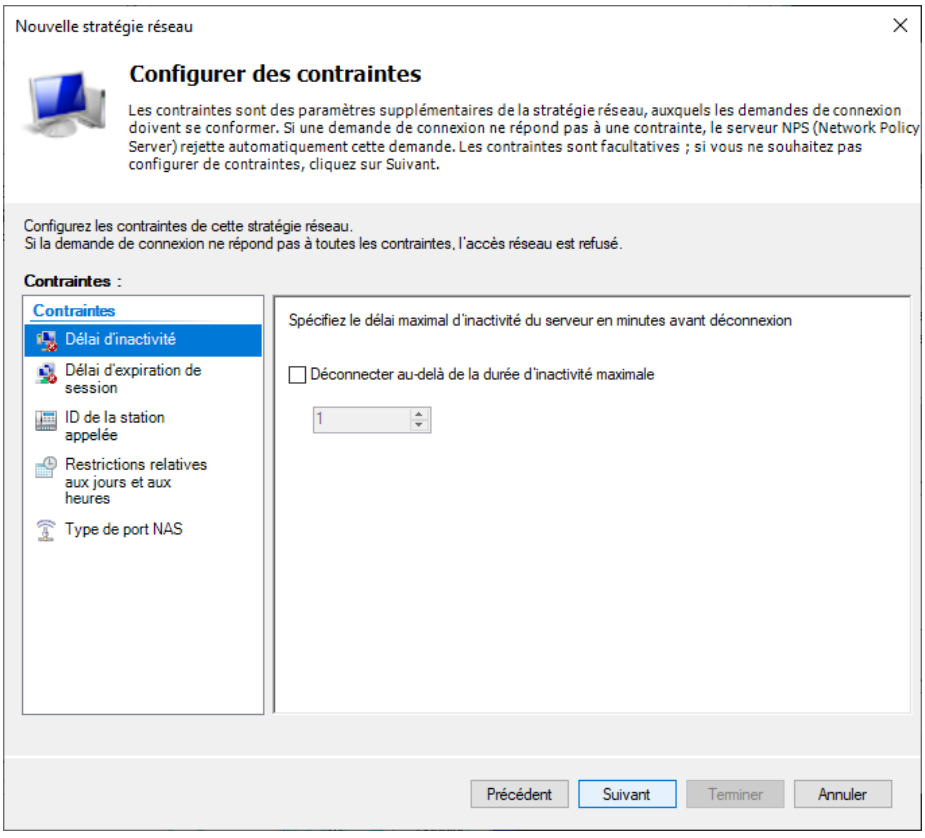
Cliquez sur **« Ajouter »** pour ajouter les méthodes d'authentification



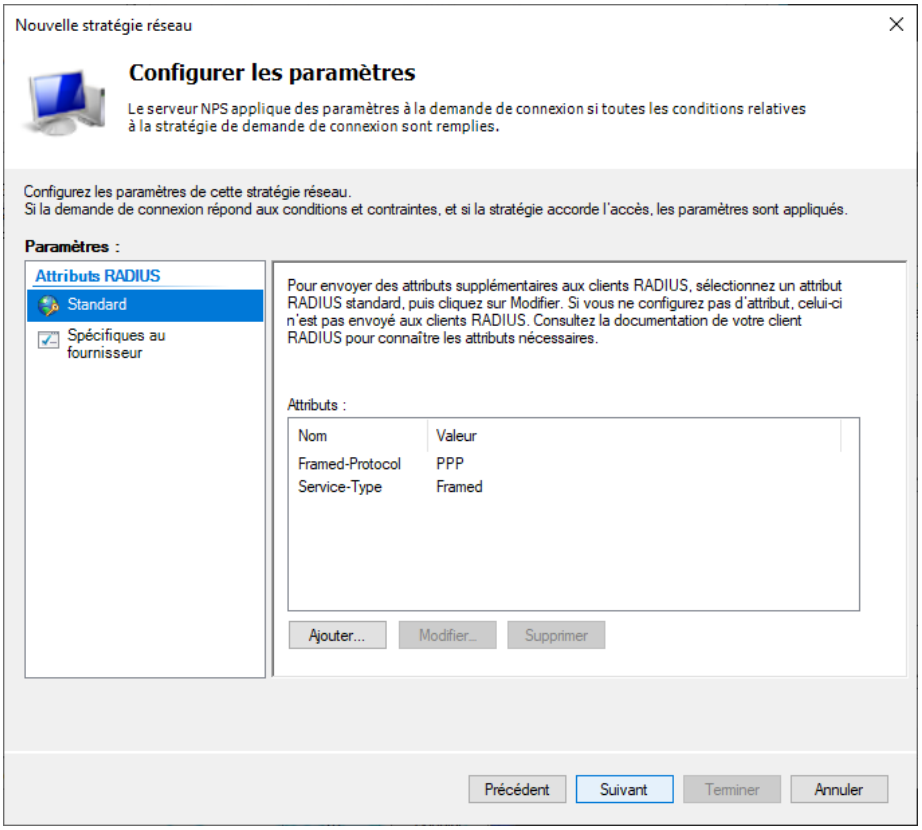
Ajouter les méthodes d'authentification comme ci-dessous :



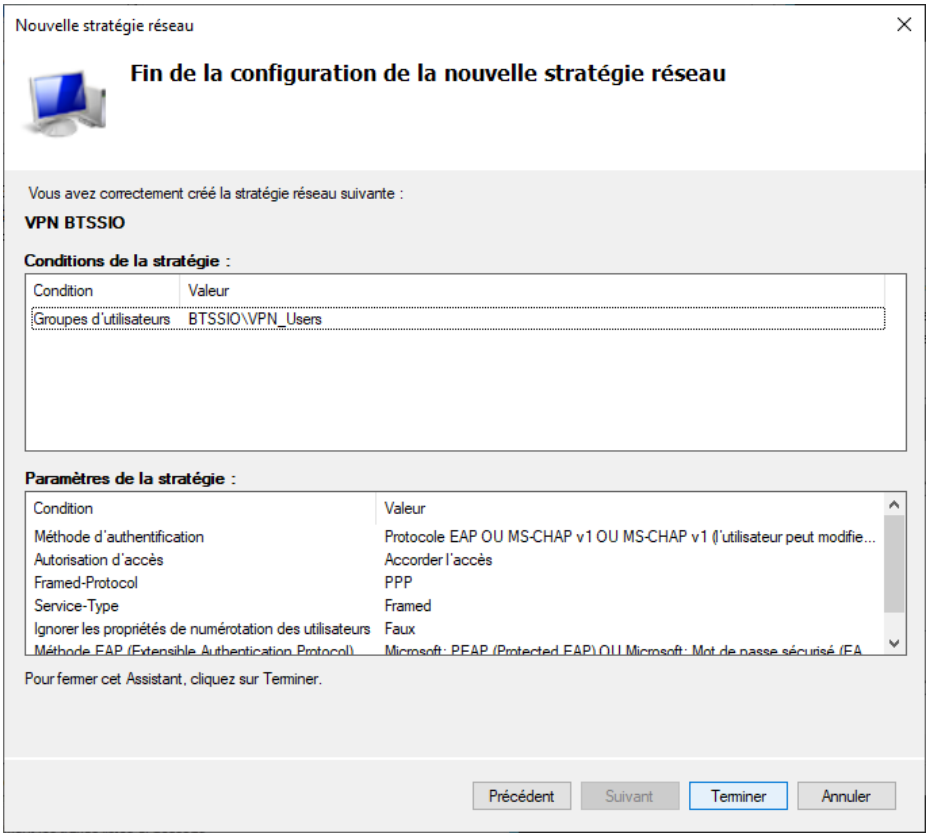
Dans notre cas, pas besoin des contraintes, cliquez sur **« Suivant »**



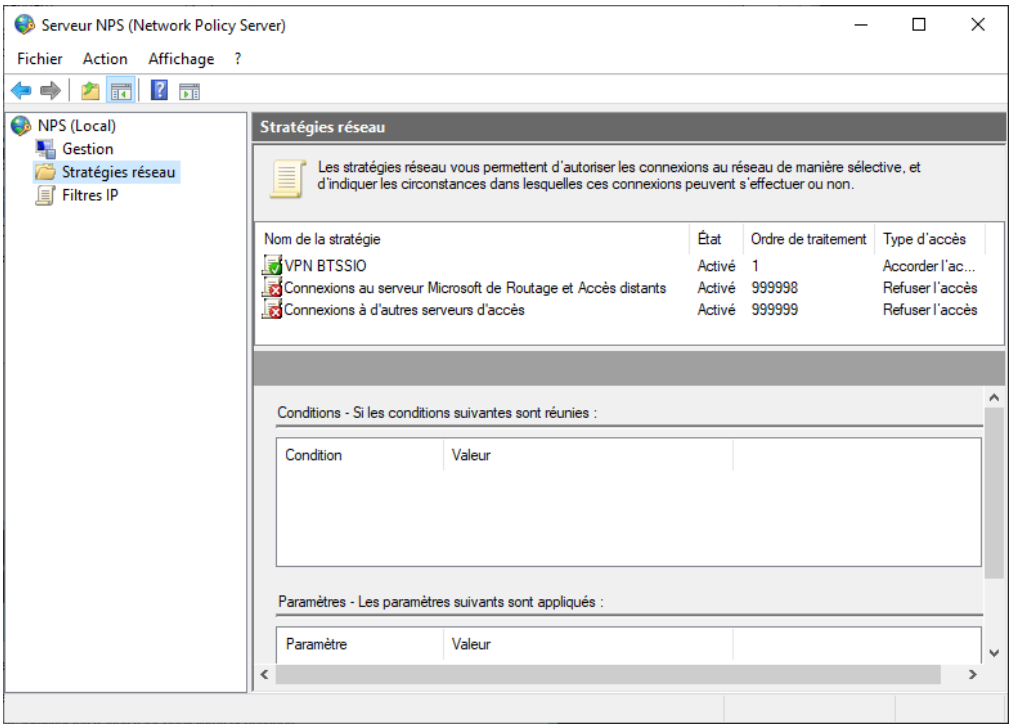
Cliquez sur **« Suivant »**



Cliquez sur **« Terminer »**

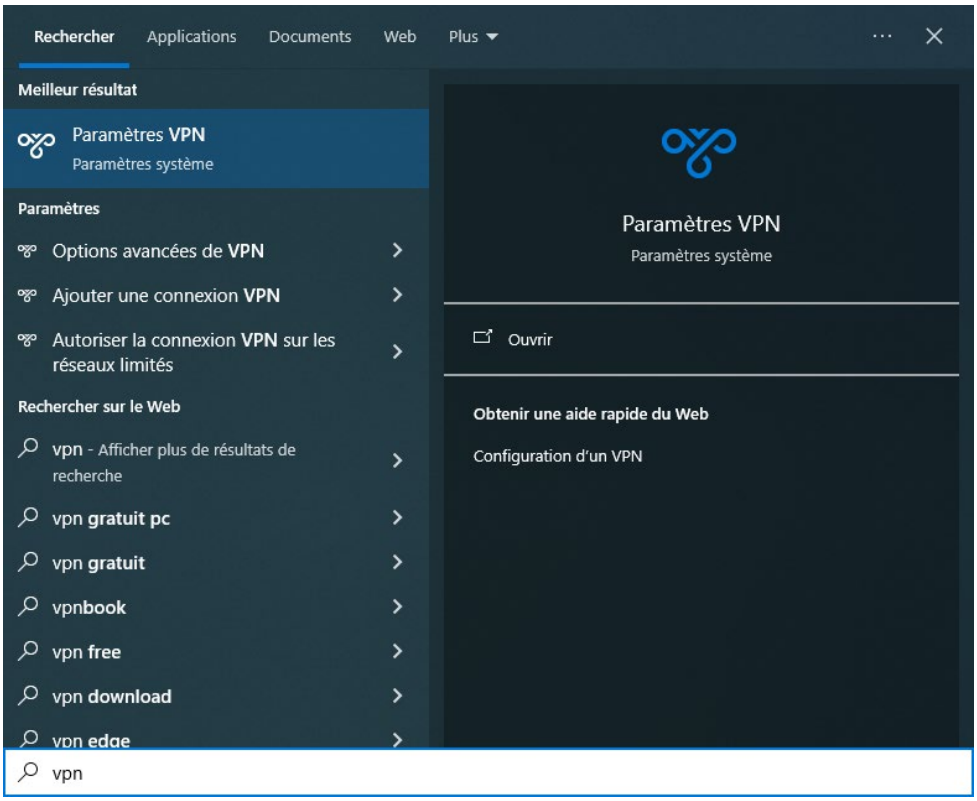


Notre stratégie réseau a bien été créé avec succès !

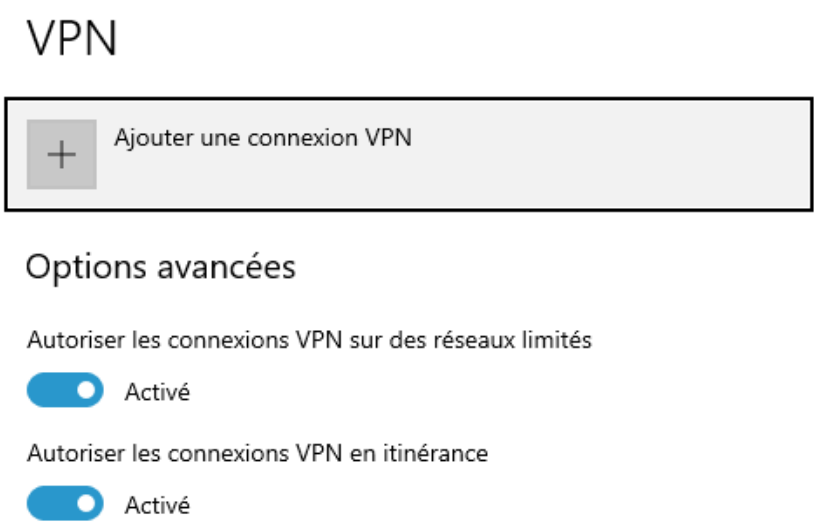


III – Test de connexion

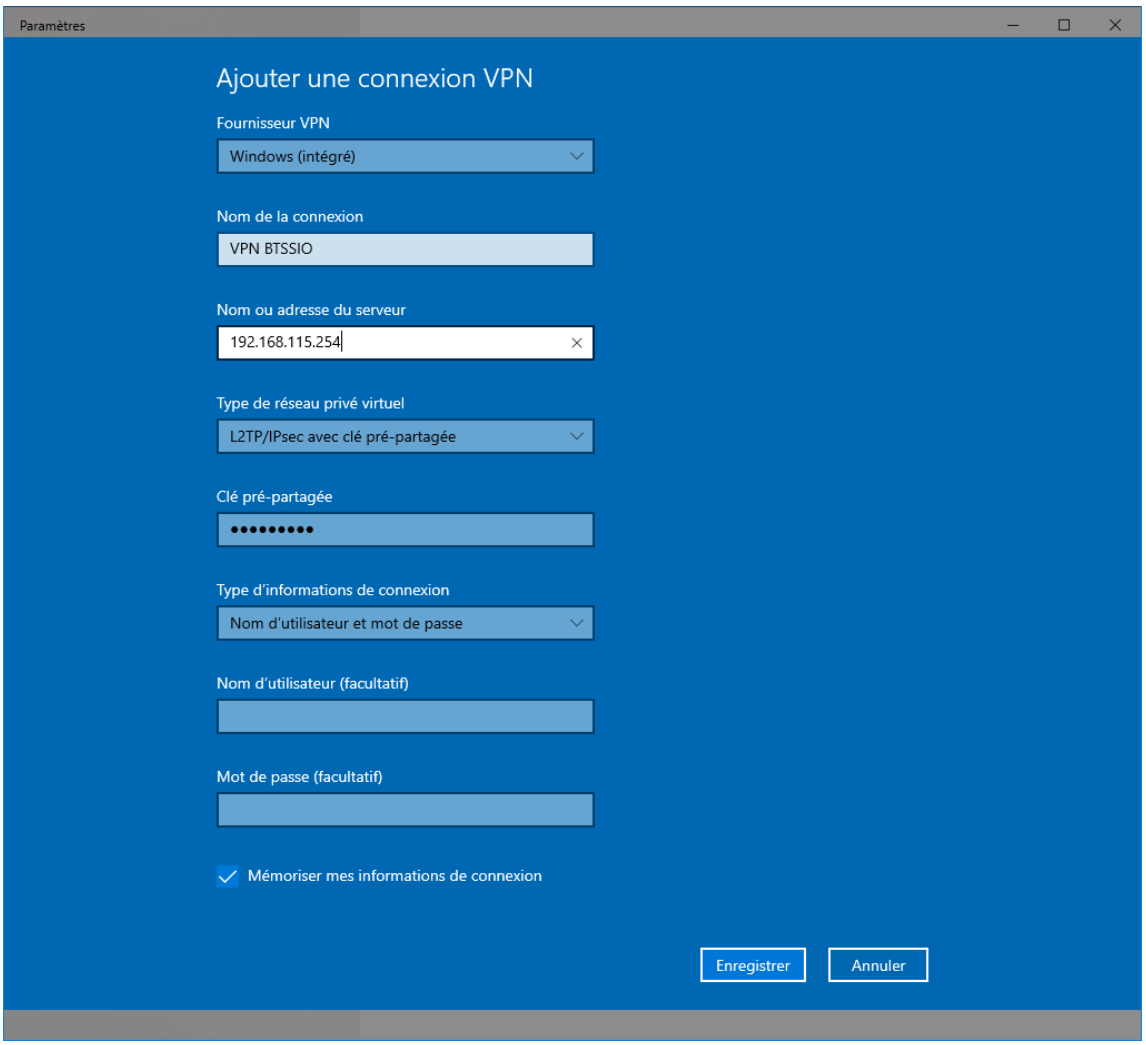
Dans la machine connectée hors du réseau locale, accédez au paramètres VPN



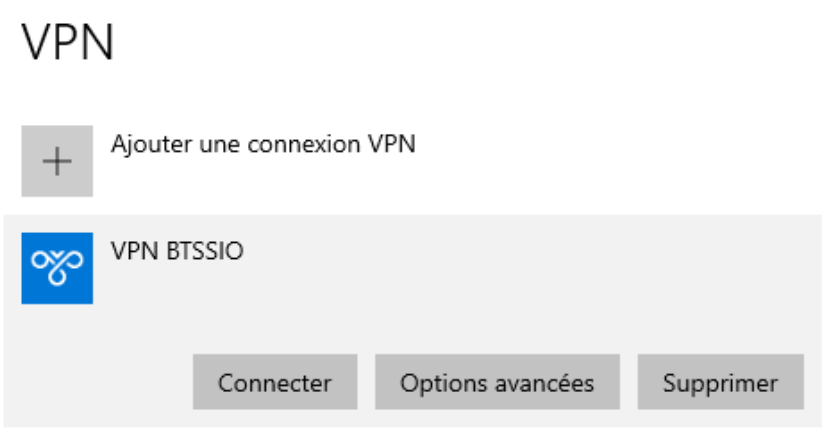
Cliquez sur **« Ajouter une connexion VPN »**



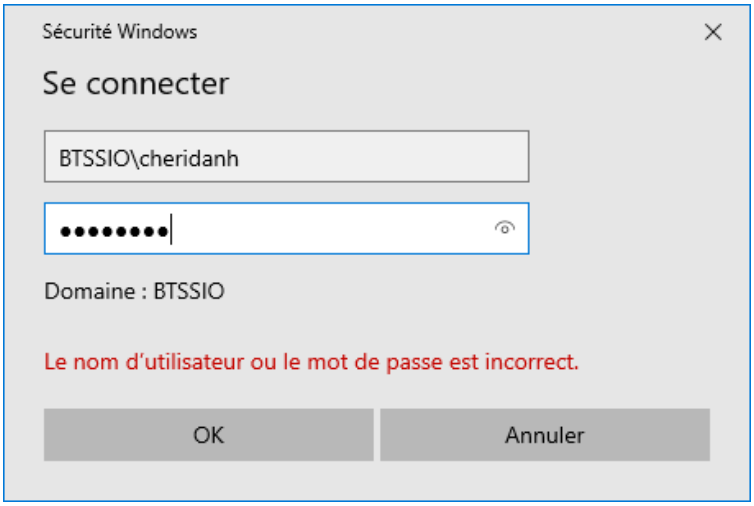
Saisissez un nom pour la connexion VPN, mettez l'adresse IP de la carte réseau connecté à l'extérieur et saisissez la clé pré-partagée puis cliquez sur **« Enregistrer »**



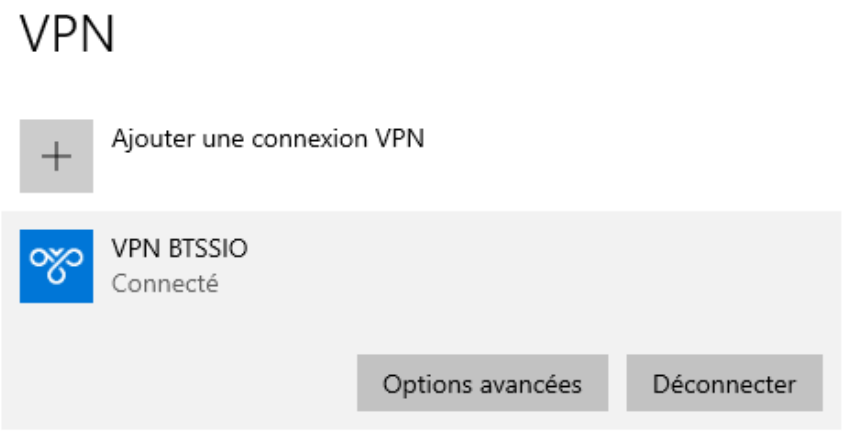
Une fois les informations enregistrées, cliquez sur **« Connecter »**



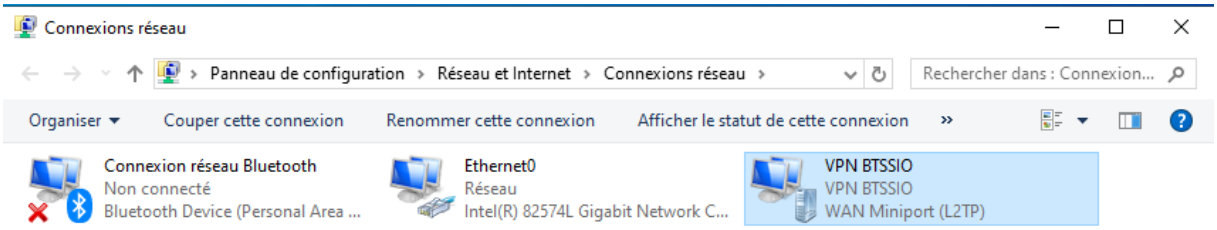
Une fois la connexion établie, les informations de connexion vous seront demandées. Saisissez le nom d'utilisateur appartenant au groupe de sécurité ajouté dans la stratégie de réseau NPS.



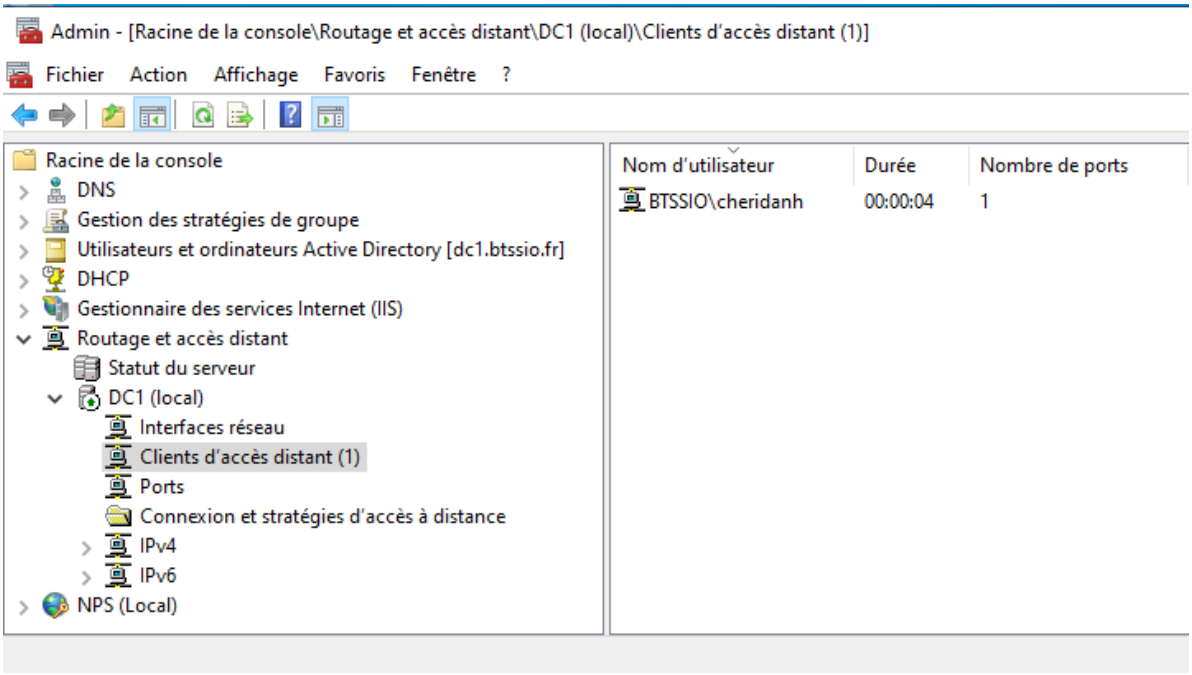
La connexion s'est effectuée avec succès !



Dans le PC client, on peut voir une nouvelle carte de connexion qui s'est ajoutée.

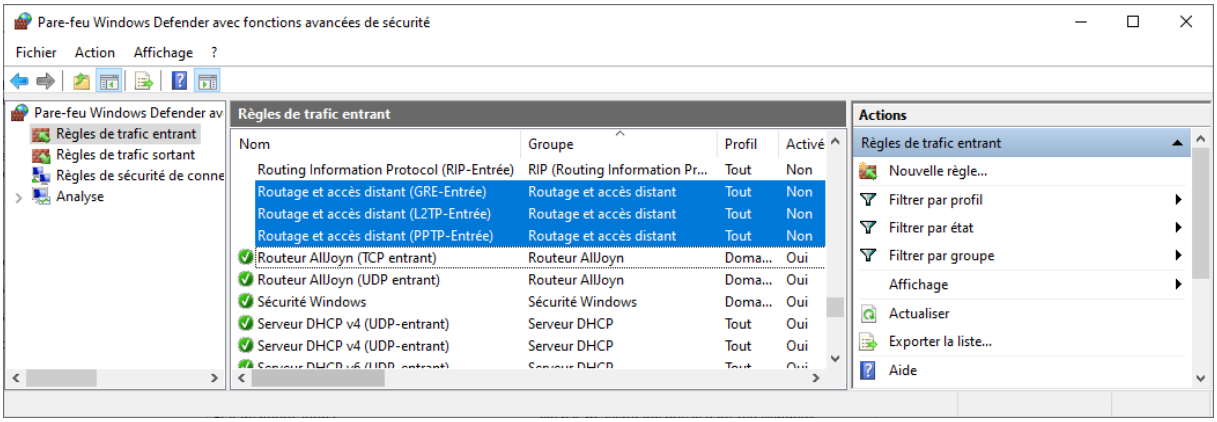


Au niveau de notre serveur VPN, on peut voir les utilisateurs connectés dans **« Clients d'accès distant »**

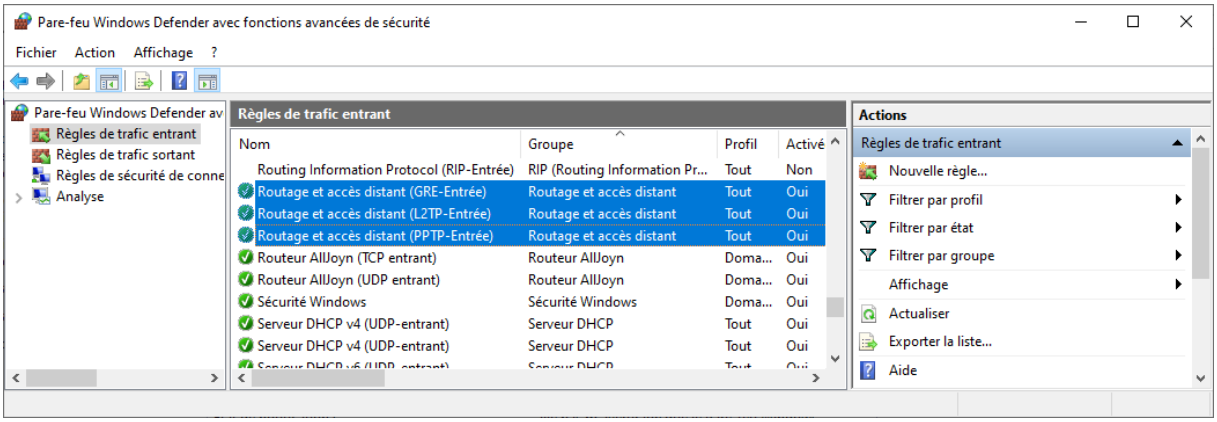


Rappelez-vous pendant la configuration de notre serveur, nous avions un avertissement concernant l'ouverture des ports.

Rendez-vous dans les paramètres avancés du pare-feu de Windows au niveau des règles entrants : **Panneau de configuration => Pare-feu Windows => Paramètres avancés**



Activez les règles concernant les communications VPN.



C’est la fin de ce TP sur la mise en place d’un service VPN en L2TP avec clé pré-partagée sur Windows Server. J’espère que cette procédure vous a aidé.

Merci ! A bientôt !

Chéridanh TSIELA

N’hésitez pas à me laisser un message sur mon site :

https://cheridanh.cg/about