

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 sûrement trop tard).

II – Prérequis

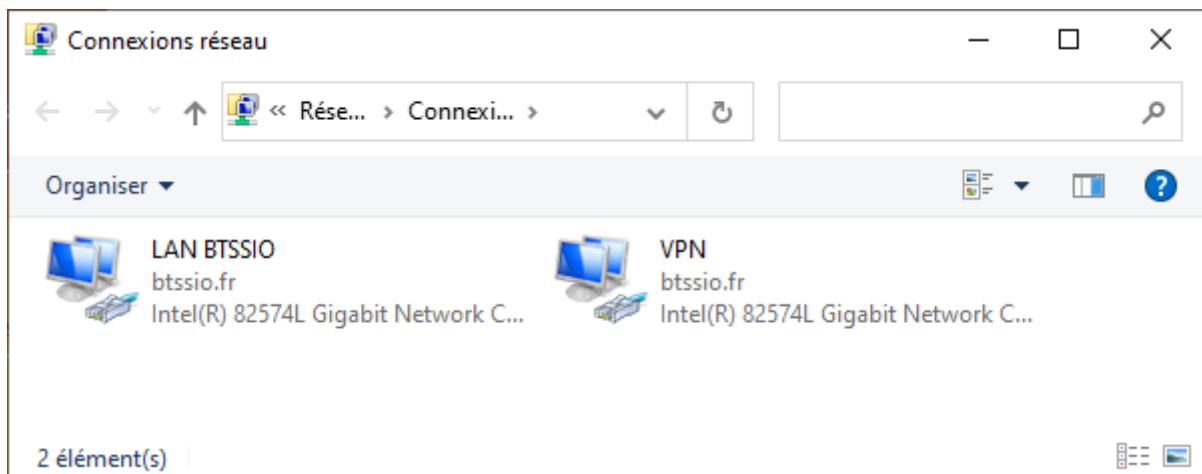
- 1 Active Directory
- 1 Serveur VPN
- Mot de passe Administrateur du domaine

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

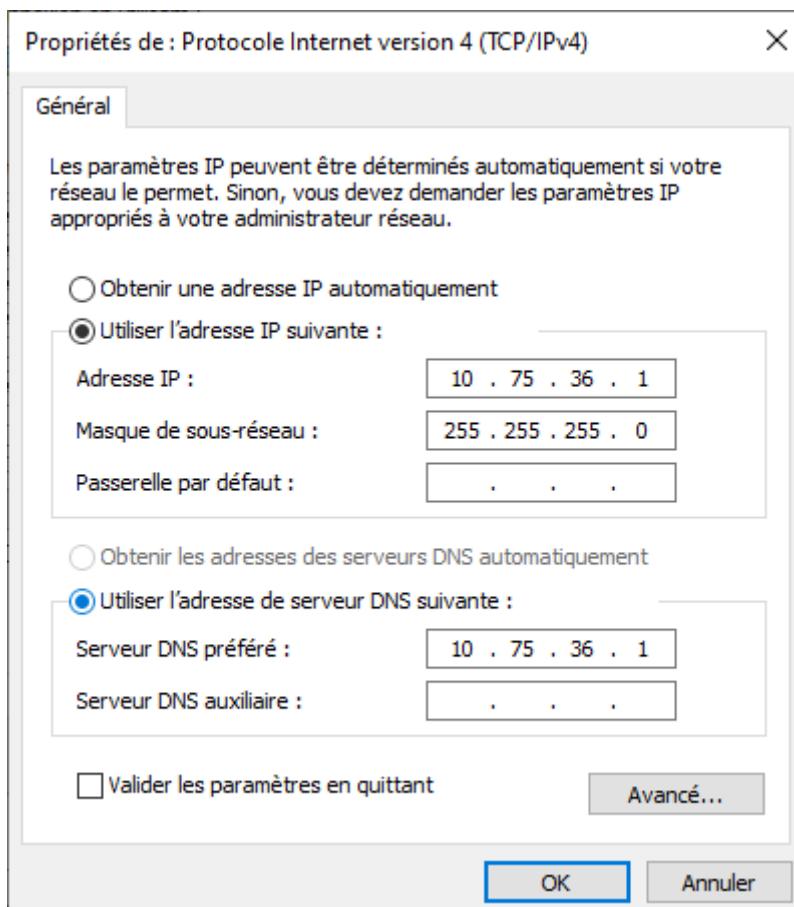
III – Préparation du serveur

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

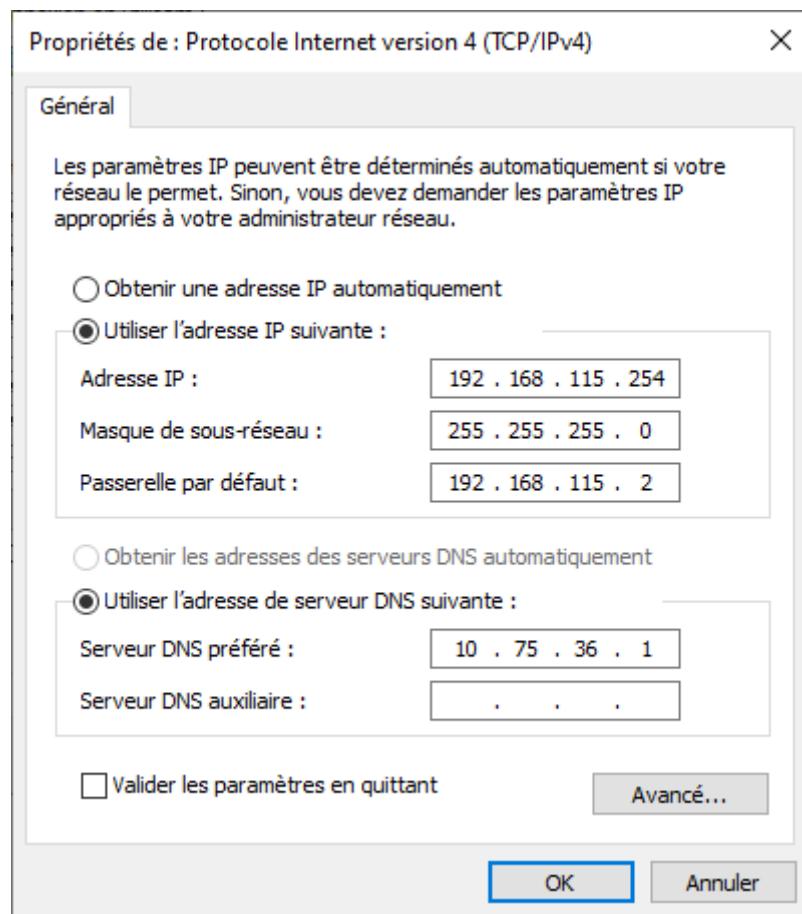
serveur possède deux cartes réseaux que j'ai renommé LAN pour le réseau locale et VPN qui l'interface connectée à l'extérieur à laquelle nos utilisateurs accèderont pour se connecter au réseau local.



Configuration réseau carte LAN



Configuration réseau carte VPN



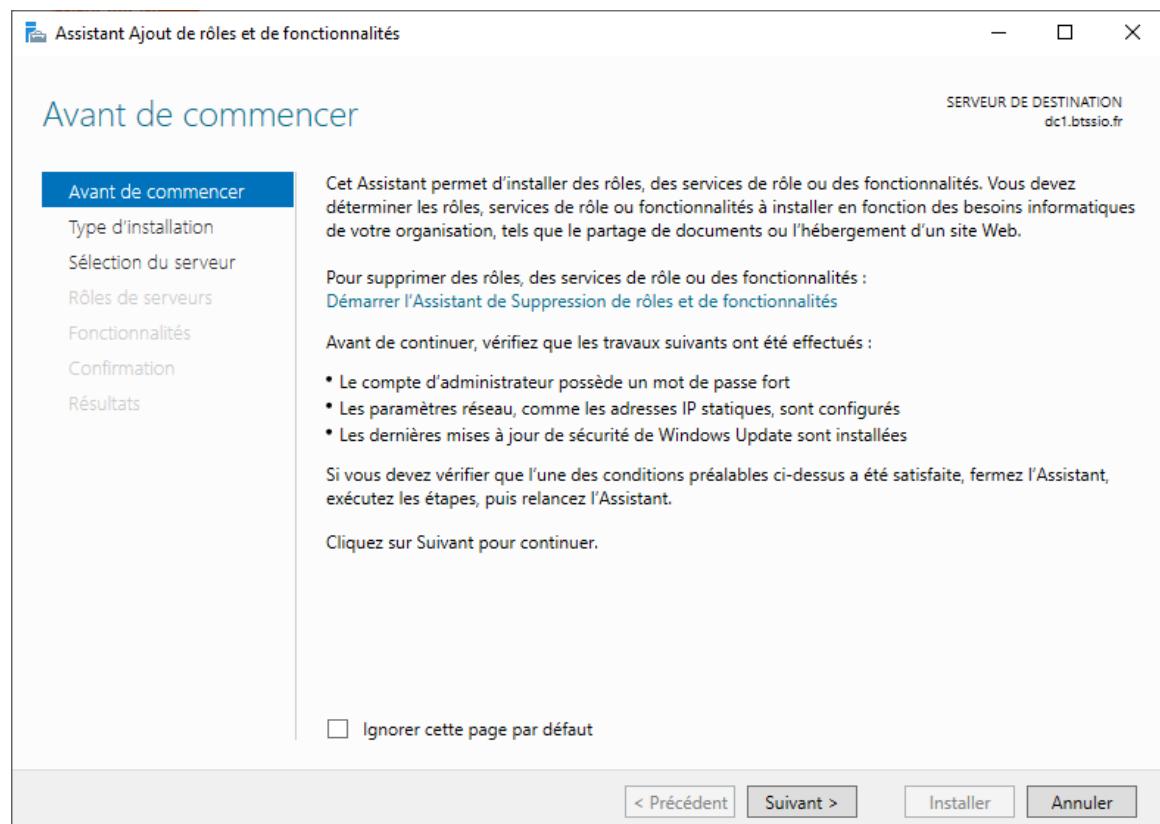
III – Installation du service VPN

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** »

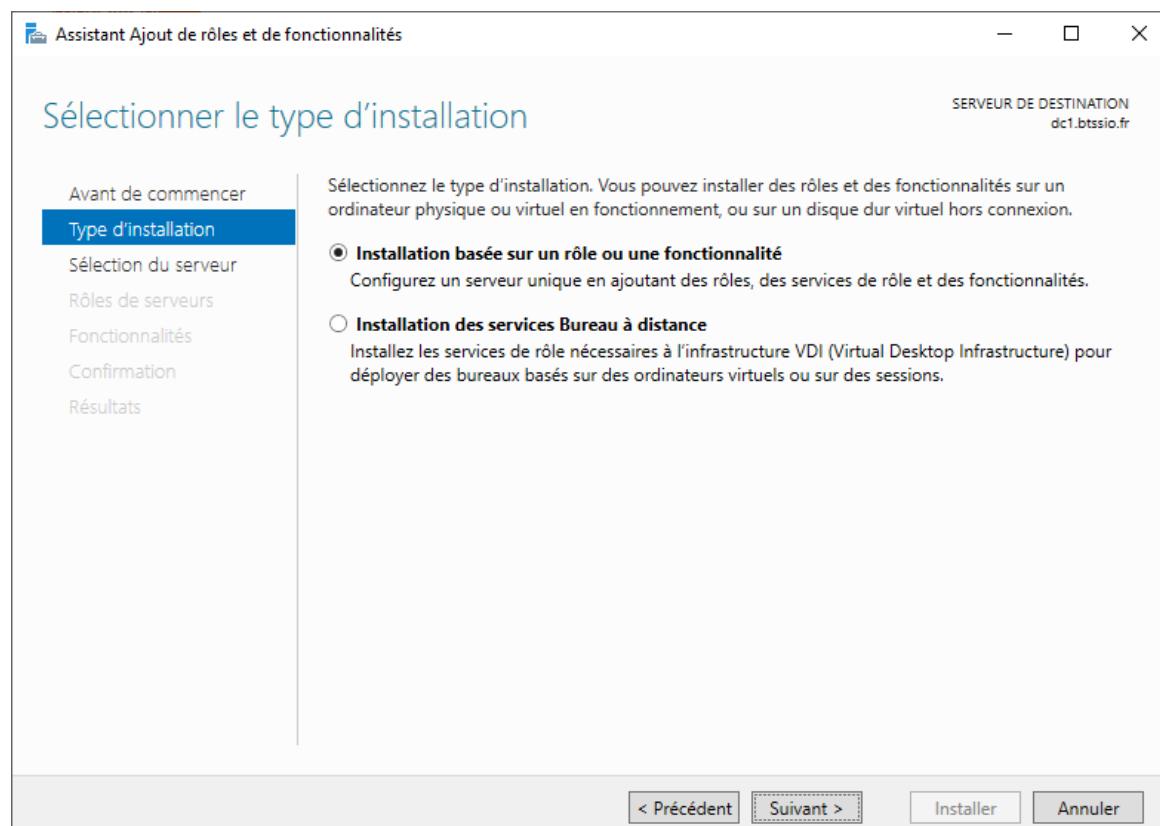
1 Configurer ce serveur local

- 2 [Ajouter des rôles et des fonctionnalités](#)
- 3 Ajouter d'autres serveurs à gérer
- 4 Créer un groupe de serveurs
- 5 Connecter ce serveur aux services cloud

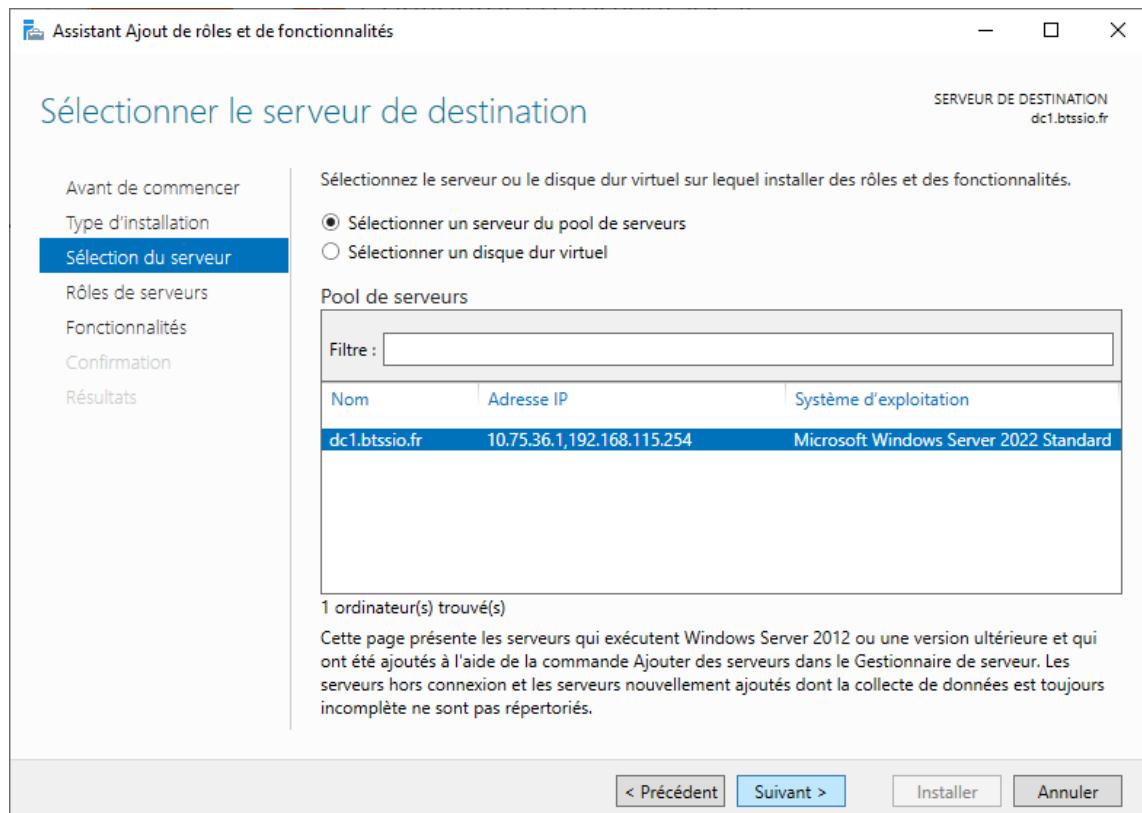
L'assistant se lance, cliquez sur « **Suivant** »



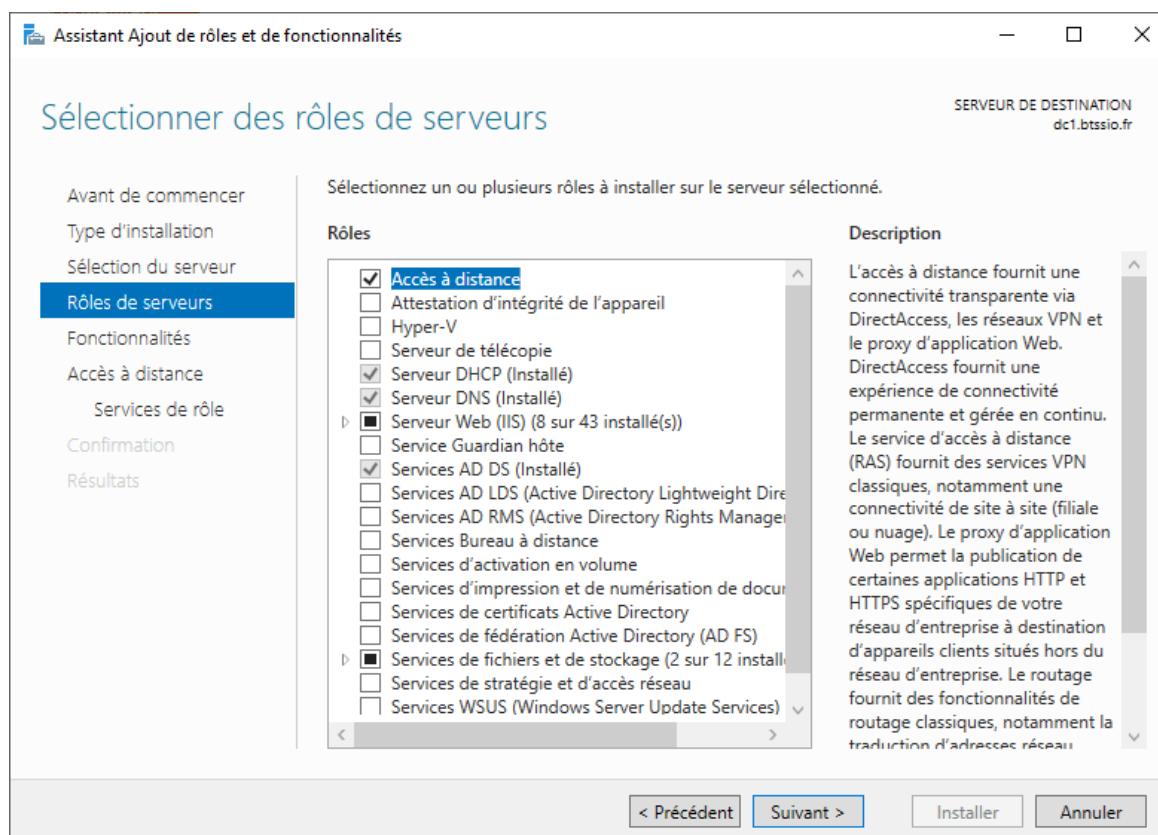
Le choix par défaut nous convient cliquez sur « **Suivant** »



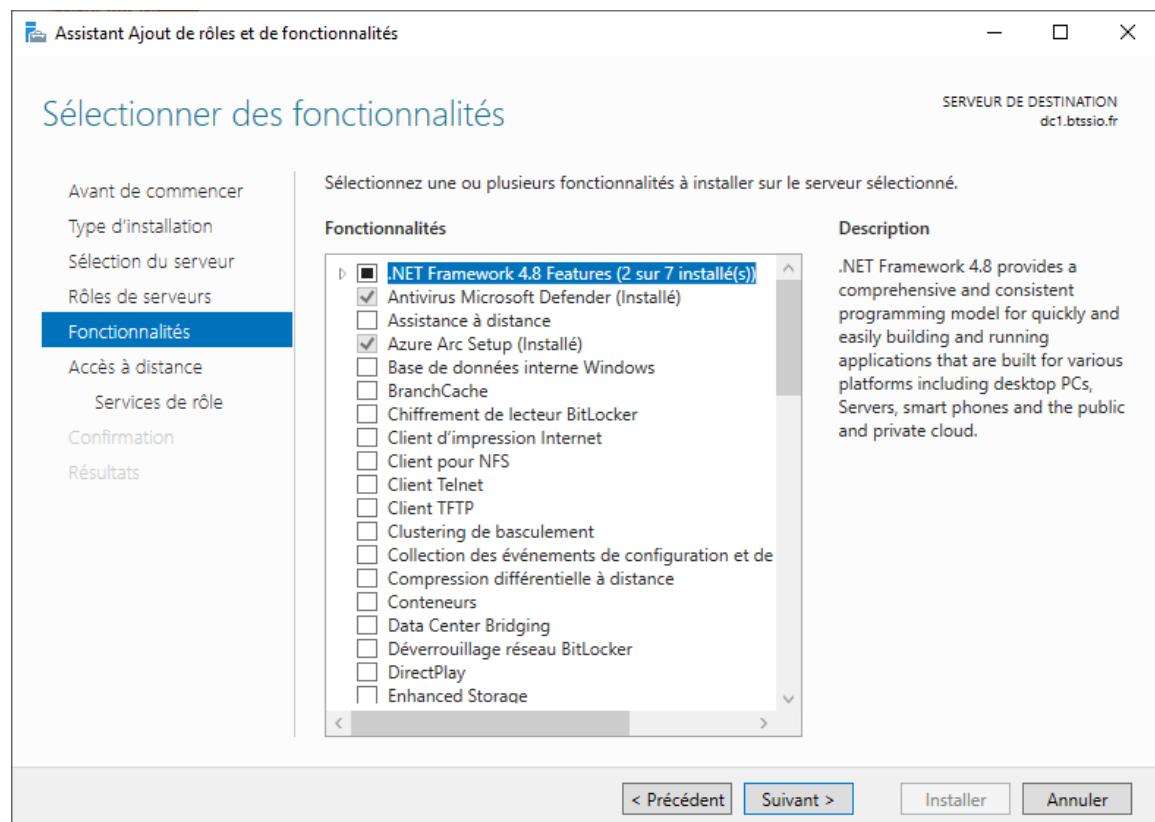
Notre serveur est choisi par défaut, cliquez sur « Suivant »



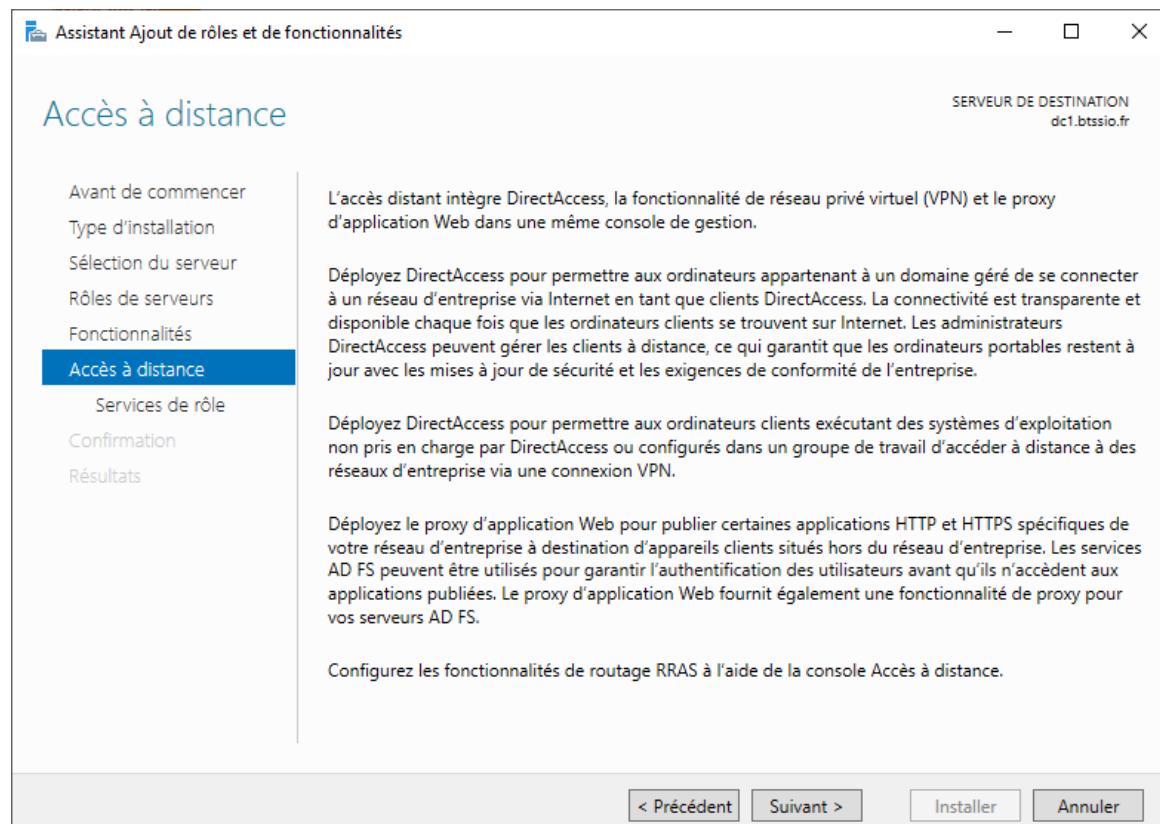
Cochez « Accès à distance » et cliquez sur « Suivant »



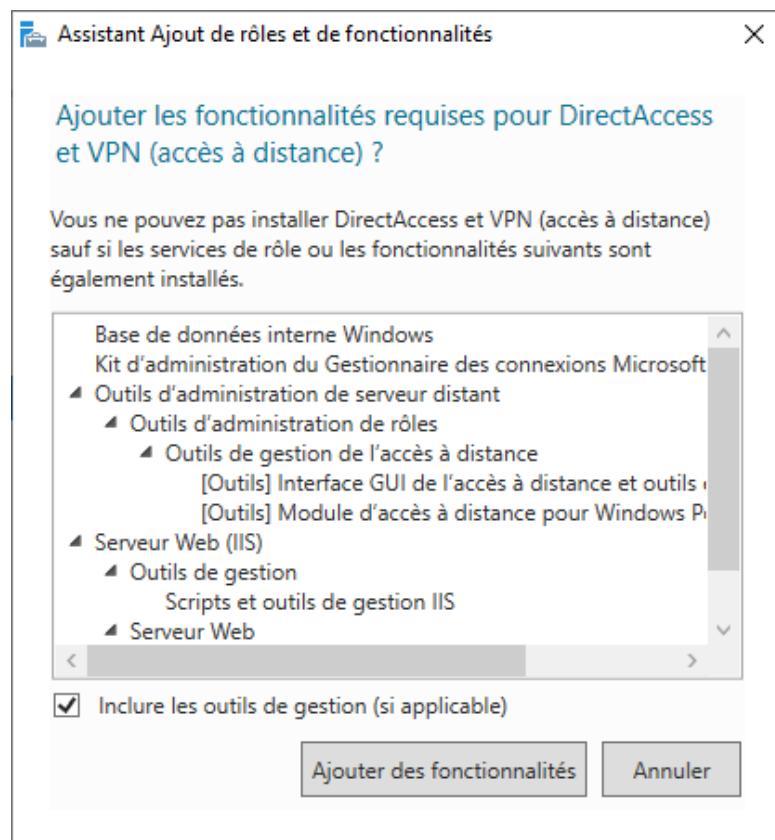
Laissez les fonctionnalités choisies par défaut et cliquez sur « **Suivant** »



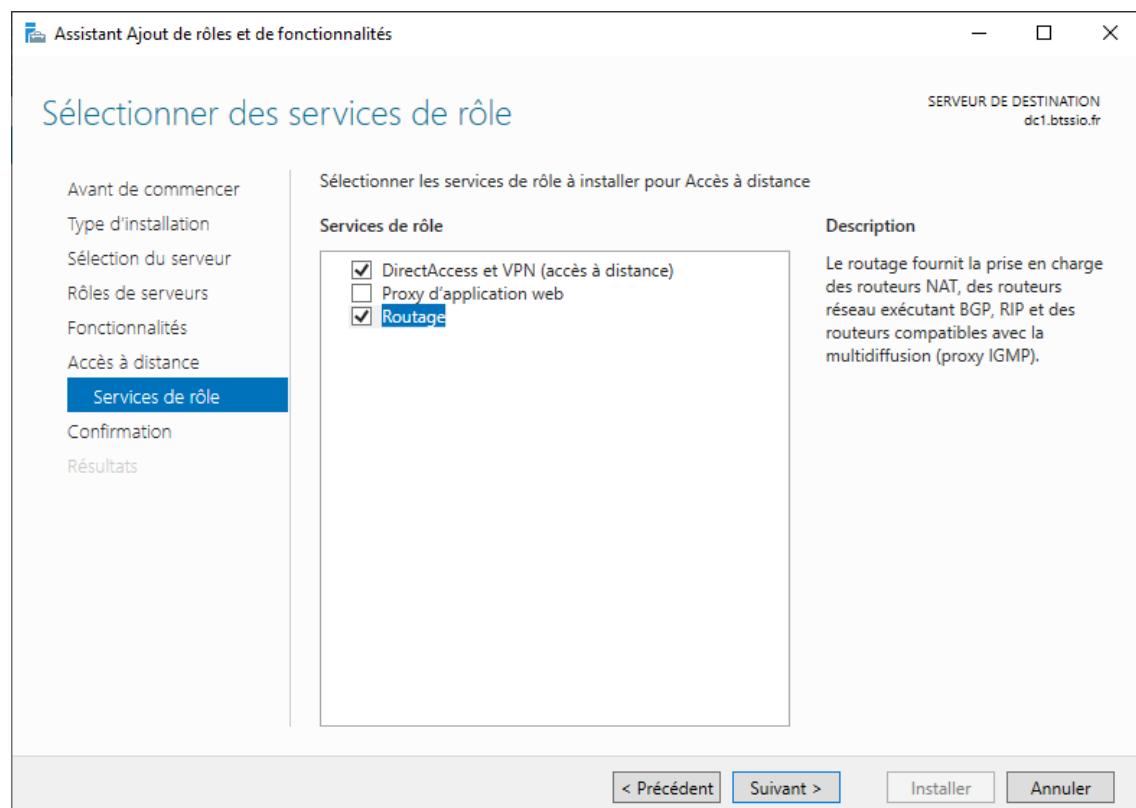
Cliquez sur « **Suivant** »



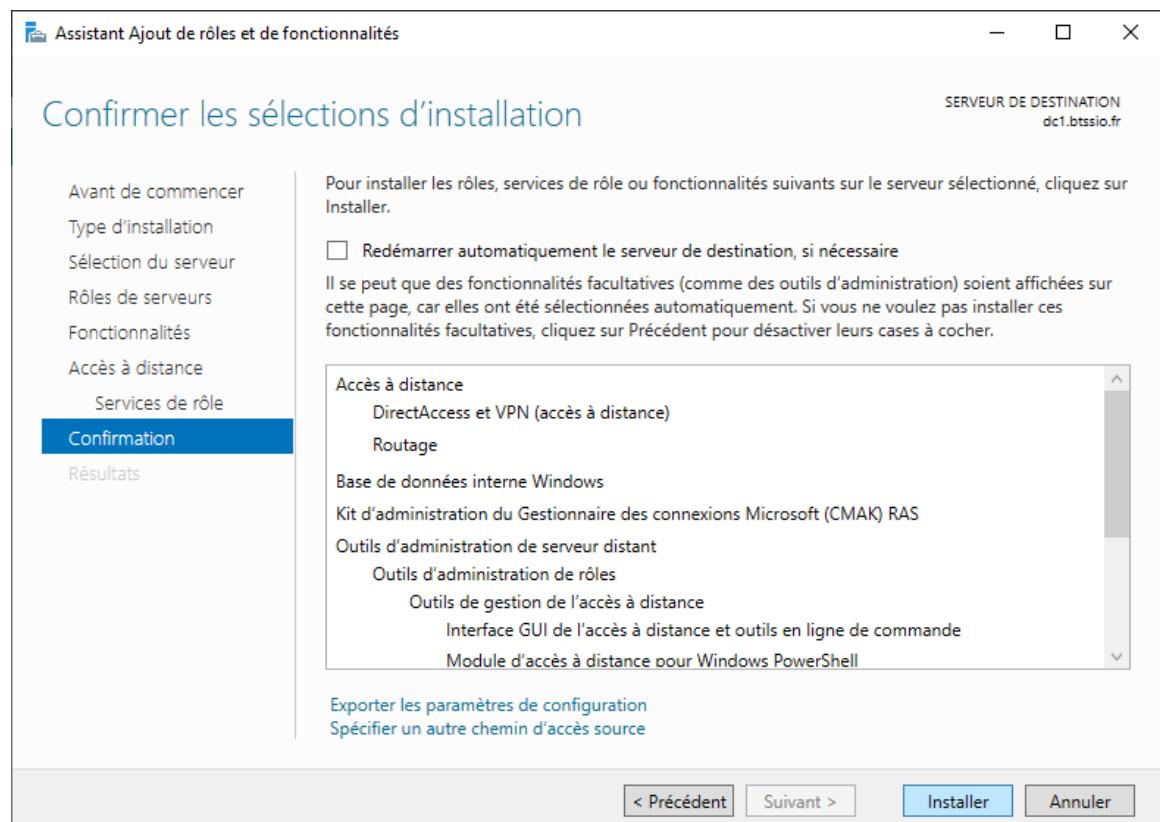
Cliquez sur « Ajouter les fonctionnalités »



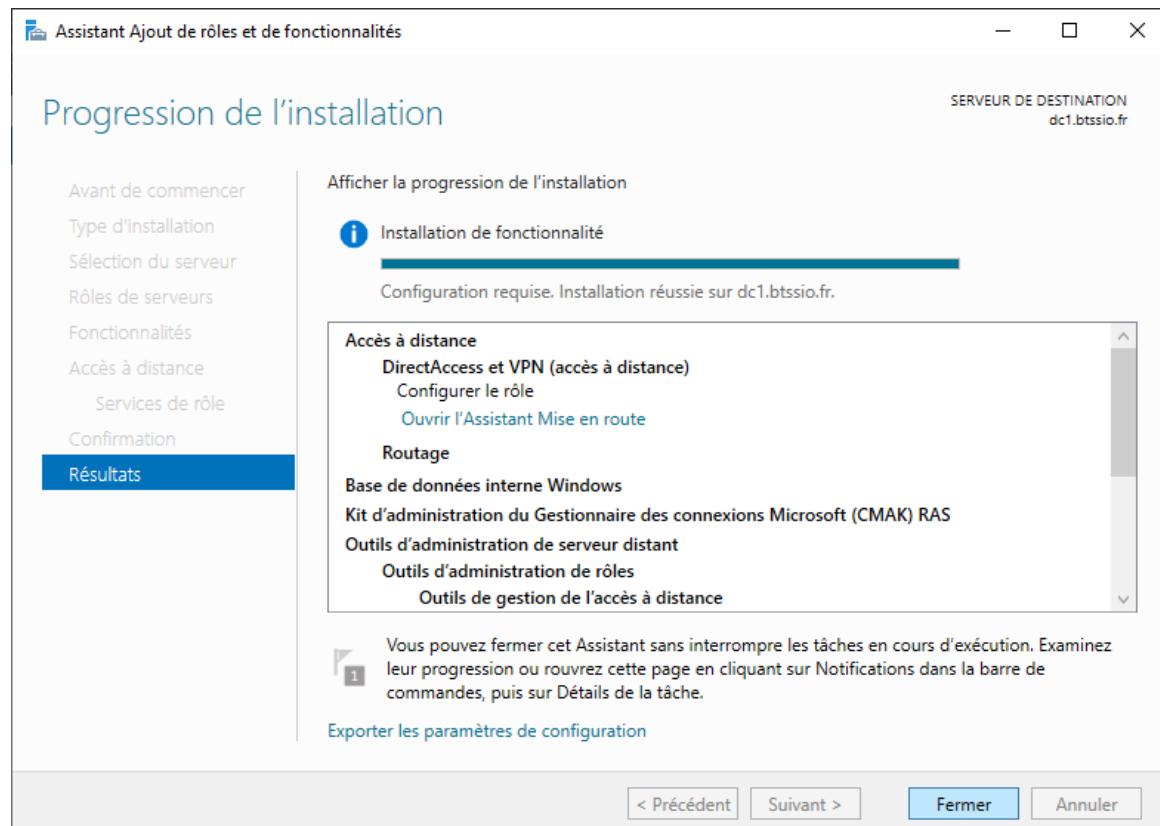
Cochez « DirectAccess et VPN » et « Routage » puis cliquez sur « Suivant »



Cliquez sur « Installer »



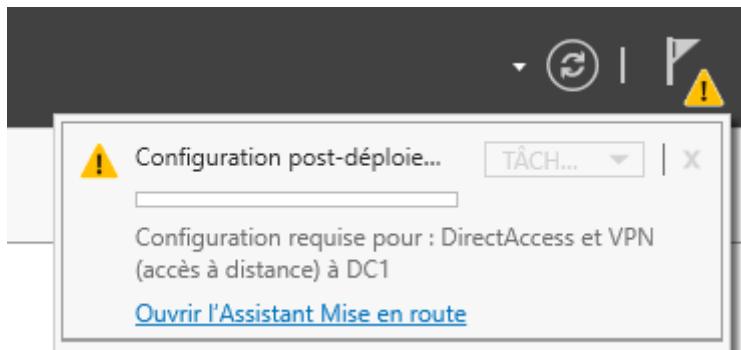
Une fois l'installation terminée, cliquez sur « Fermer »



III – Configuration du service VPN

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

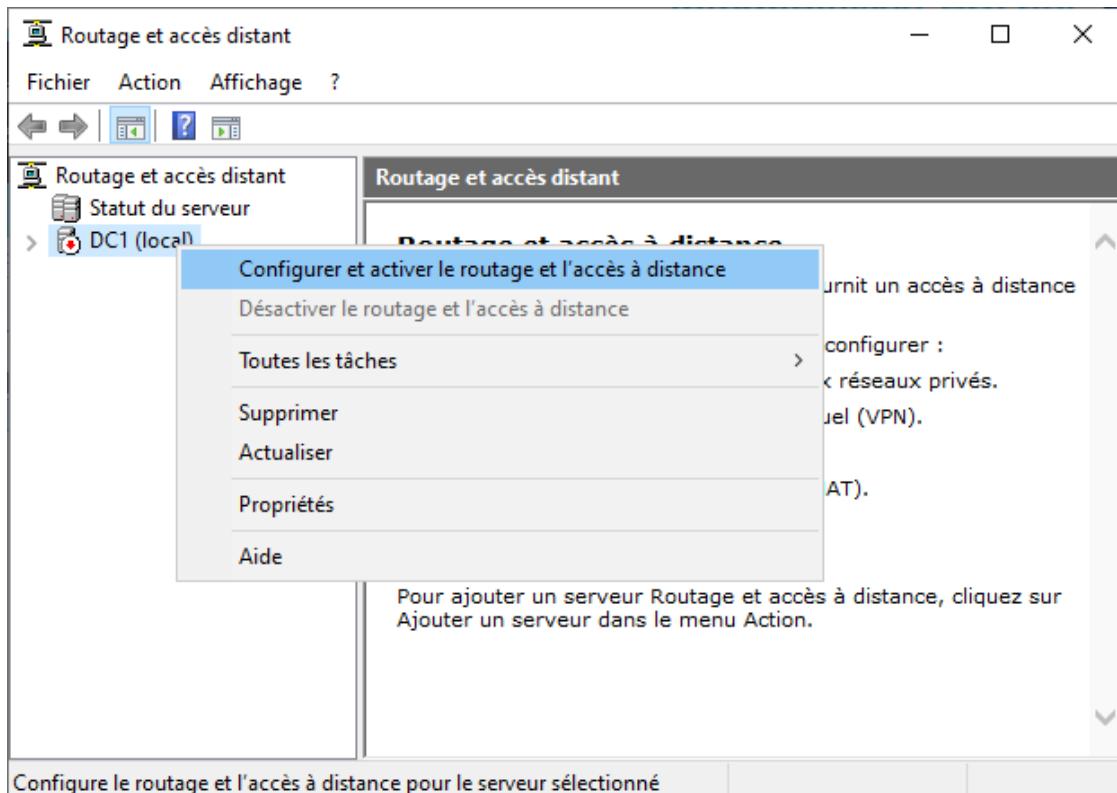
Rendez-vous dans le centre de notification du Gestionnaire de serveur et cliquez sur « **Ouvrir l'Assistant Mise en route** »



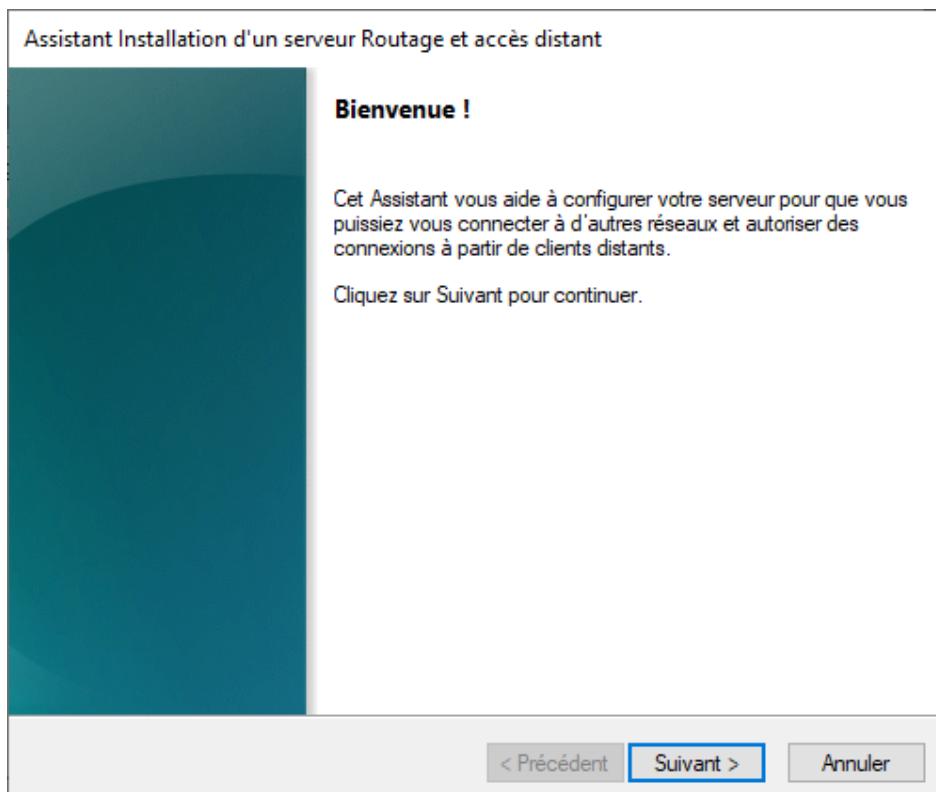
Une fois l'assistant lancé, cliquez sur « **Déployer VPN uniquement** »



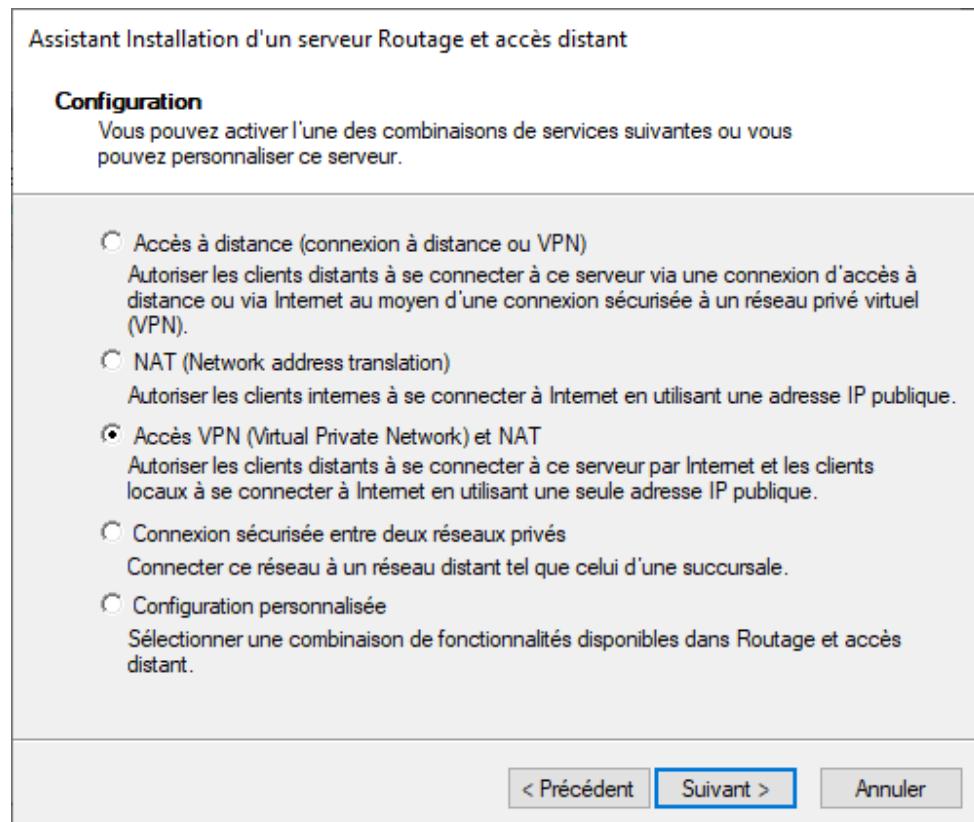
La console « Routage et accès distant » se lance et faites un clic droit sur le nom du serveur local et cliquez sur « Configurer et activer le routage et l'accès à distance »



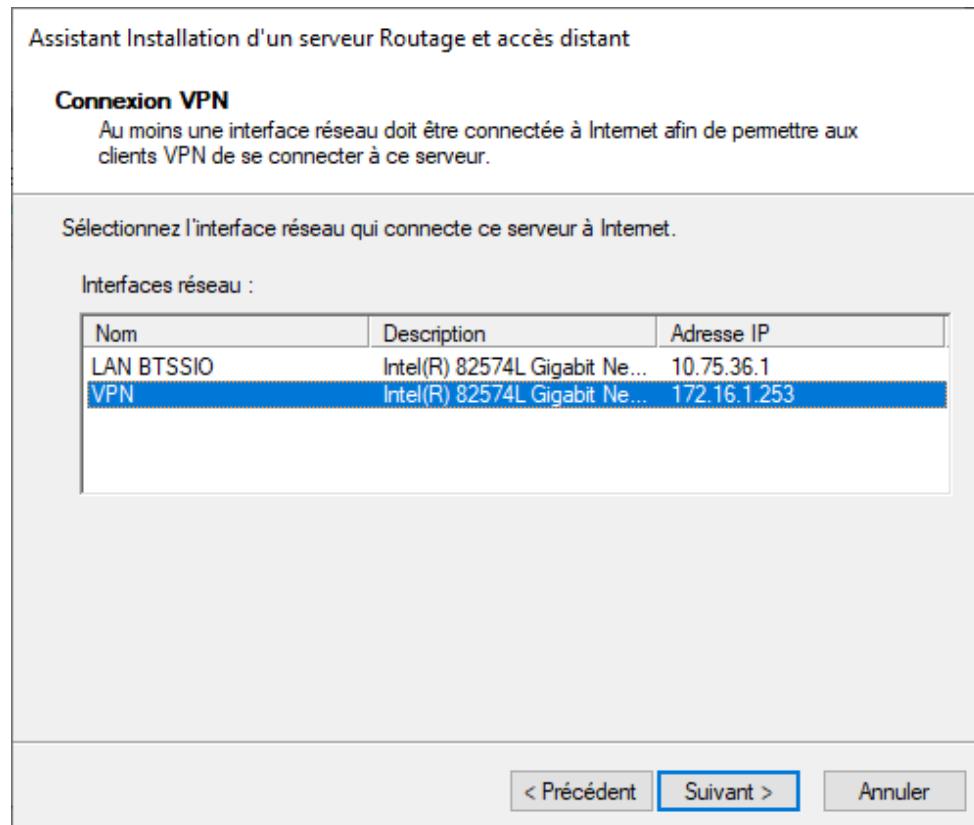
L'assistant Windows se lance, cliquez sur « **Suivant** »



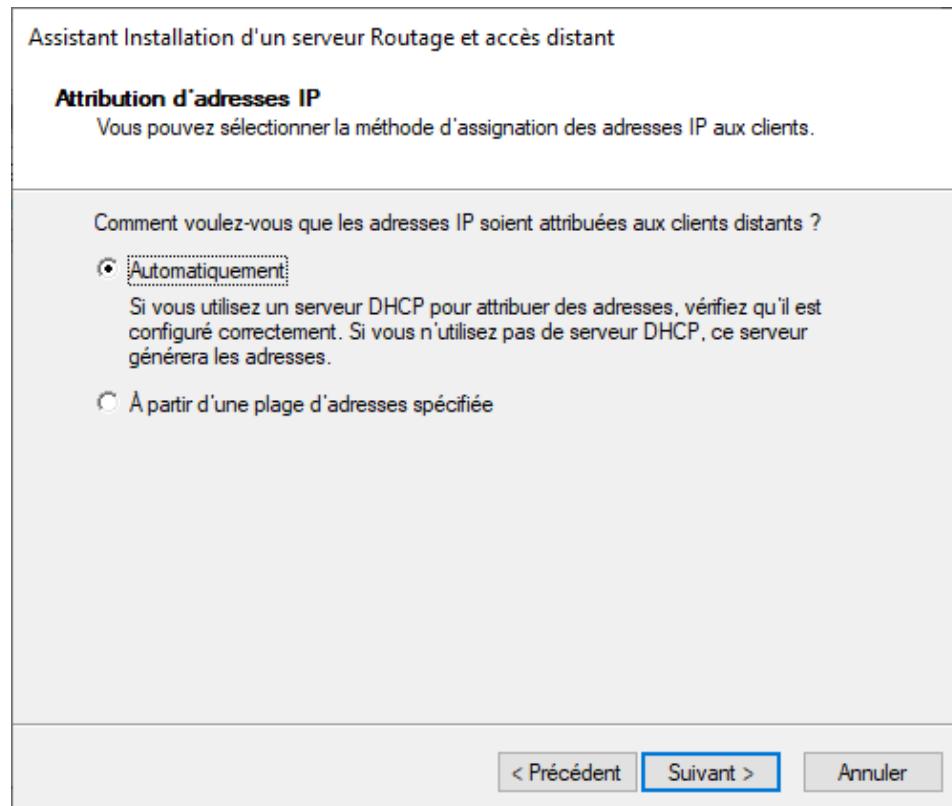
Choisissez « Accès VPN » et cliquez sur « Suivant »



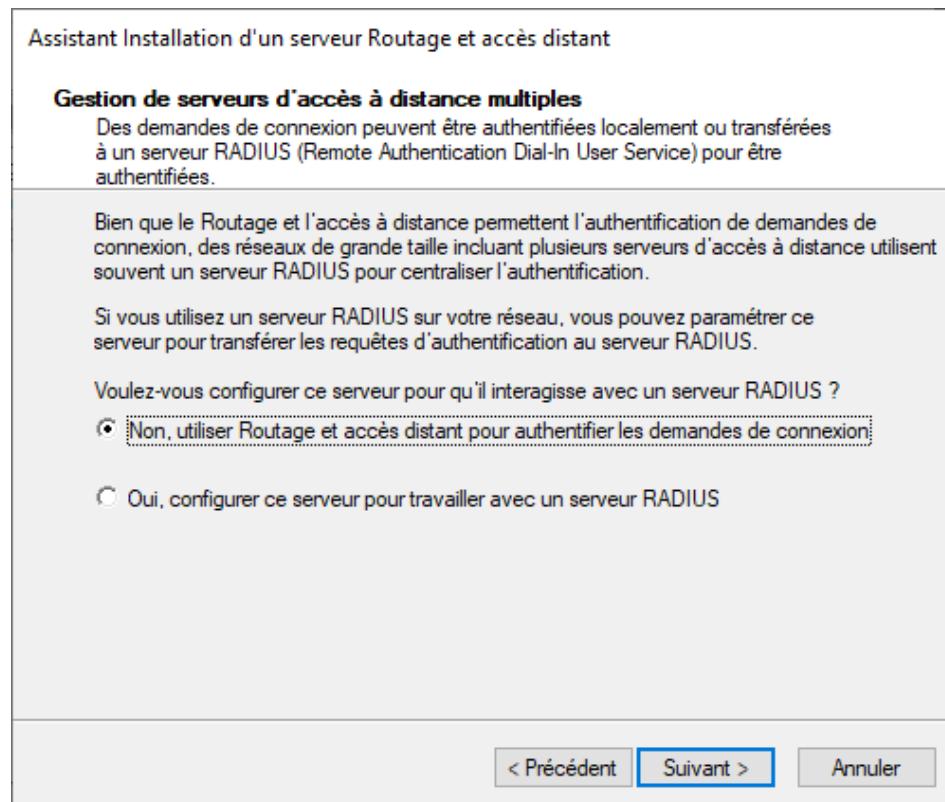
Choisissez l'interface « VPN » puis cliquez sur « Suivant »



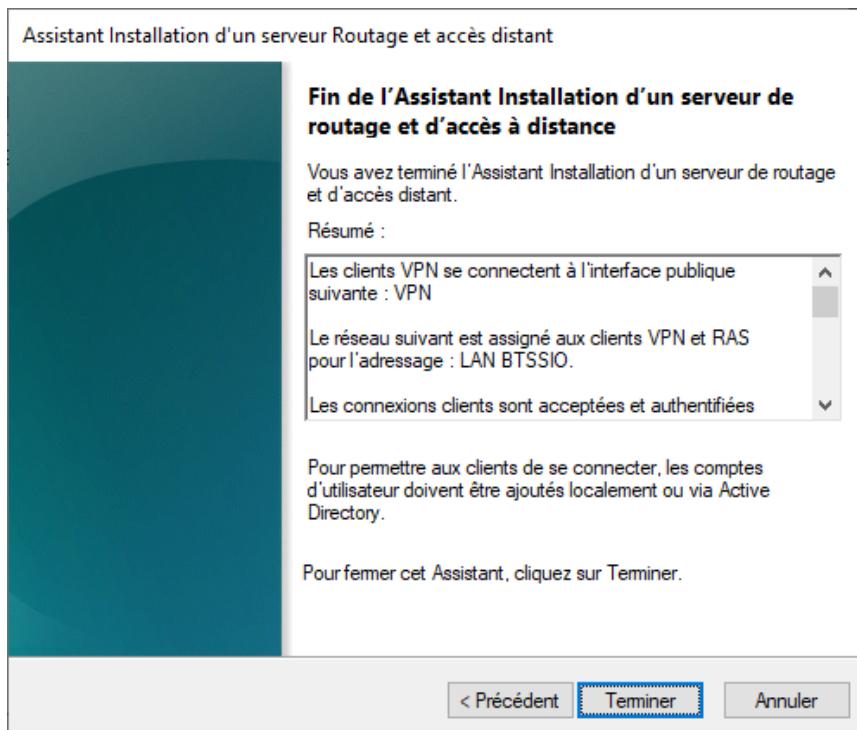
Pour le mode d'attribution des adresses IP de nos utilisateurs qui se connecteront au VPN choisissez « **Automatiquement** »



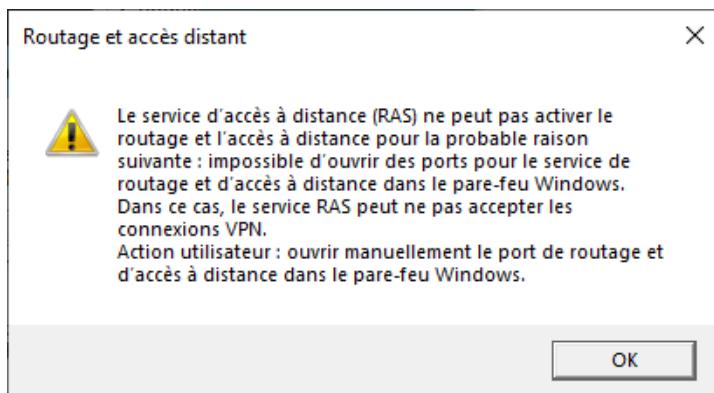
Laissez le choix par défaut car nous n'utiliserons pas de serveur RADIUS



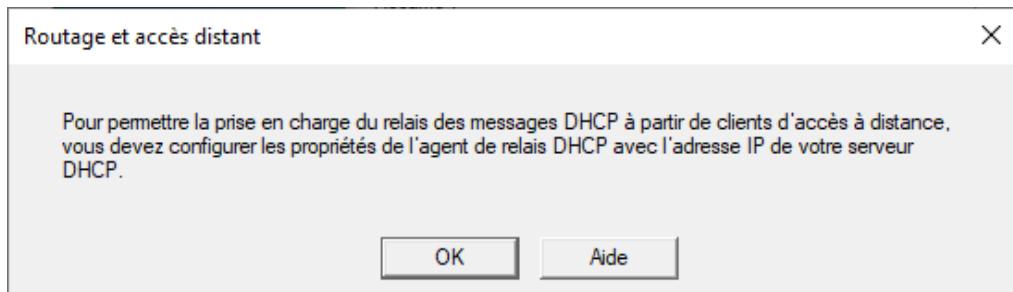
L'assistant affiche un résumé des configurations, cliquez sur « **Terminer** »



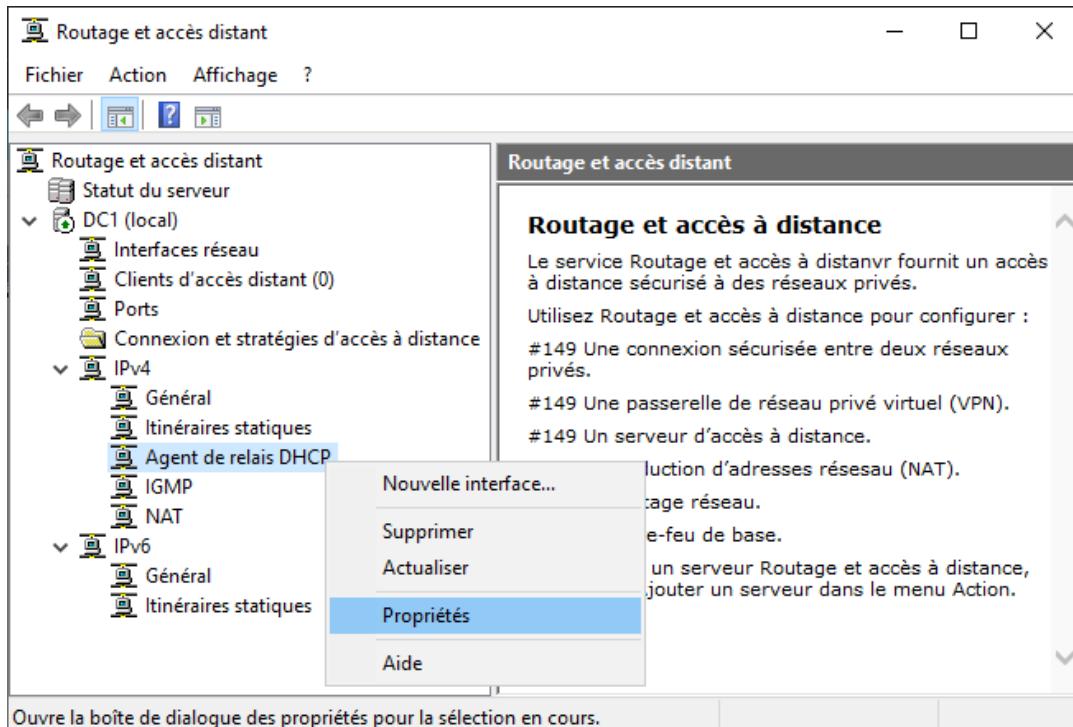
Pour l'avertissement concernant l'ouverture des ports, nous ouvriront ces ports manuellement. Cliquez sur « **OK** »



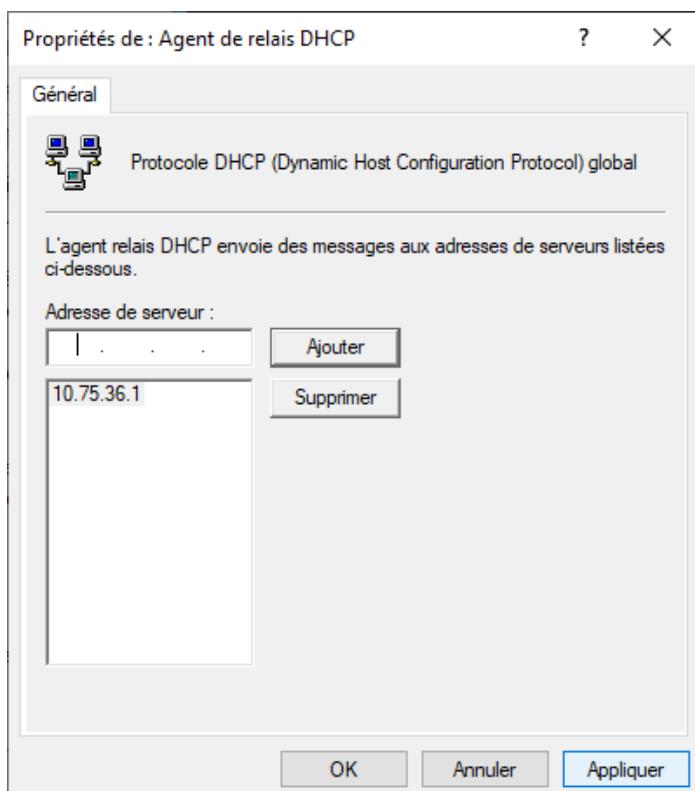
En ce qui concerne l'agent relais DHCP cliquez sur « **OK** » et nous allons configurer dans la partie tout juste après.



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 »

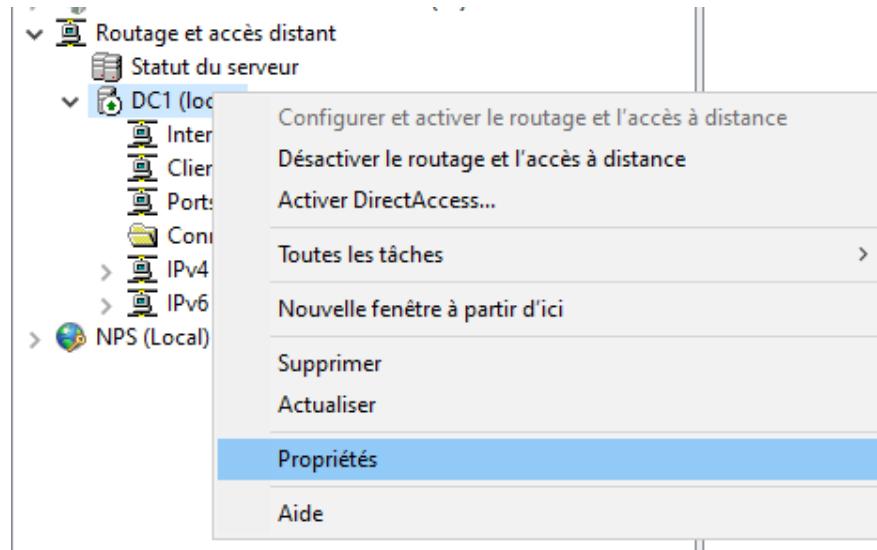


Préciser ici l'adresse IP du serveur DHCP (dans mon cas ici c'est l'adresse de mon contrôleur de domaine) puis cliquez sur « **Appliquer** »

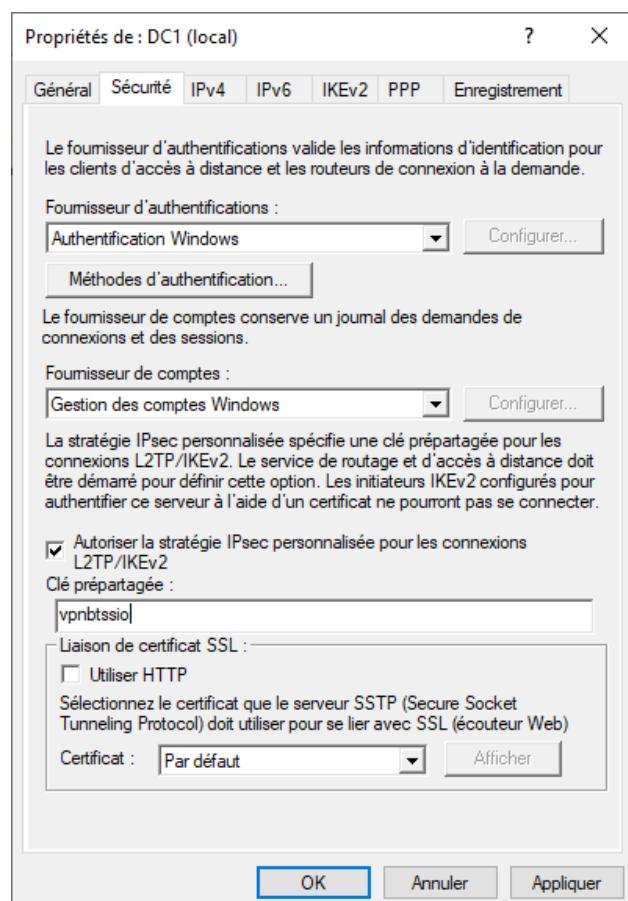


Actuellement avec le service VPN installé, il est par défaut en **PPTP (Point-to-Point Tunneling Protocol)**, nous allons activer le protocole **L2TP (Layer 2 Tunneling Protocol)** avec une clé prépartagée.

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

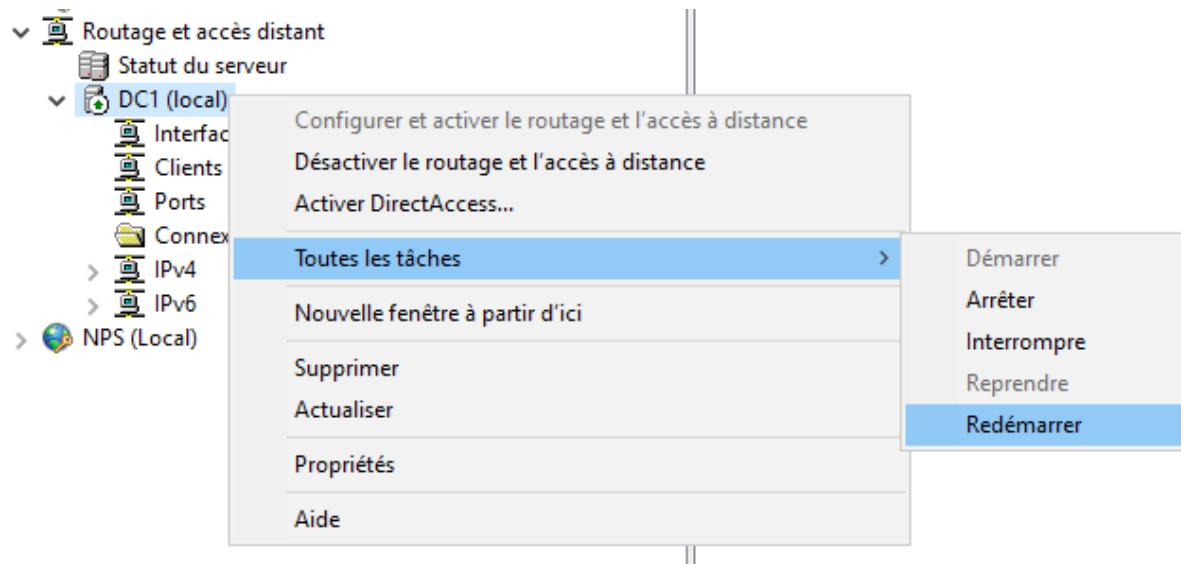


Allez dans l'onglet « **Sécurité** » et cochez la case pour autoriser le protocole L2TP et saisissez votre clé pré-partagée.



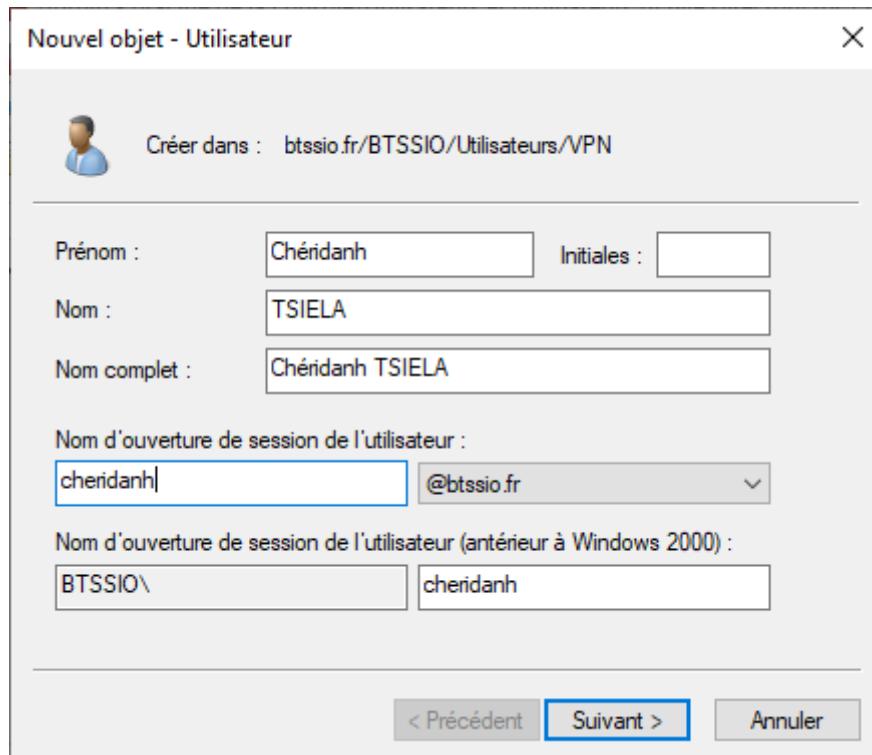
Pour que les modifications soient prises en compte, il faudra redémarrer le service VPN.

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



Nouvel objet - Utilisateur

Créer dans : btssio.fr/BTSSIO/Utilisateurs/VPN

Prénom : Chéridanh Initials :

Nom : TSIELA

Nom complet : Chéridanh TSIELA

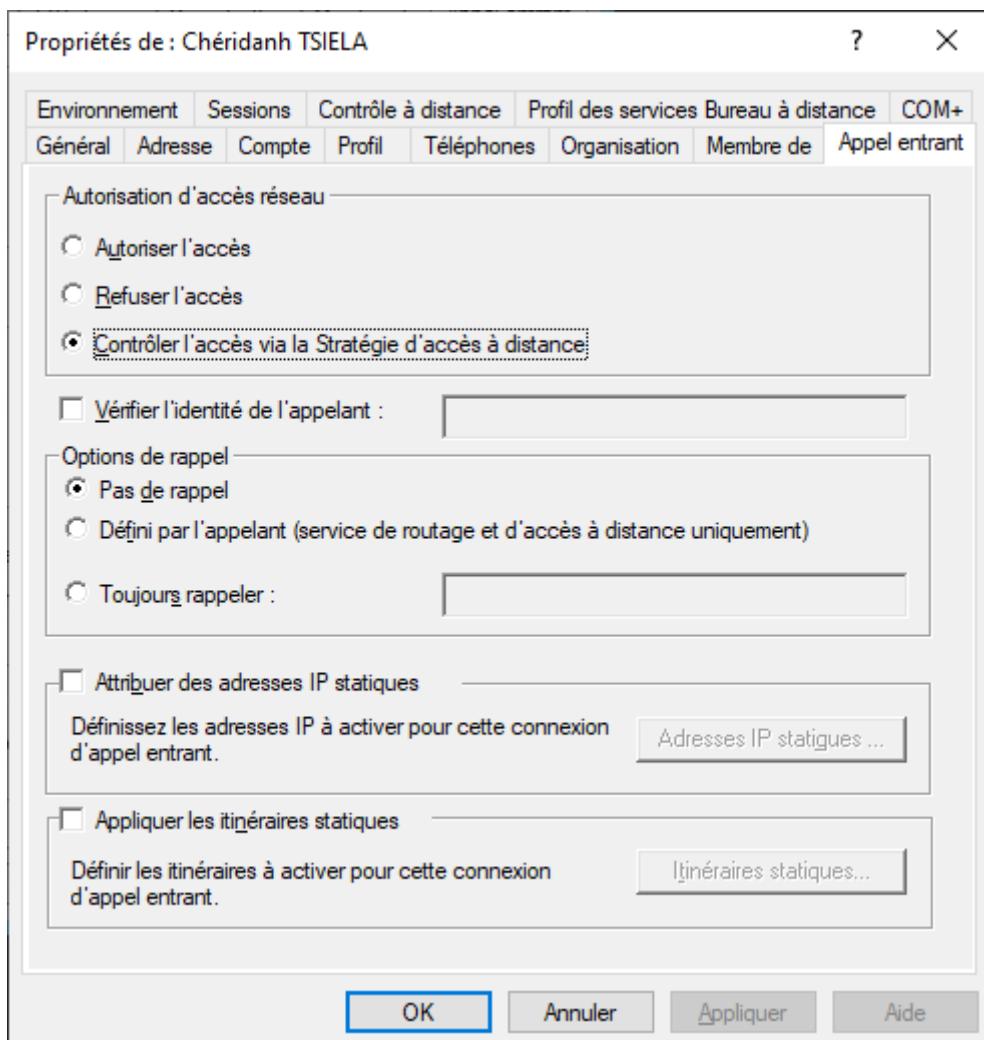
Nom d'ouverture de session de l'utilisateur :
cheridanhl @btssio.fr

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
BTSSIO\cheridanhl

< Précédent Suivant > Annuler

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

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

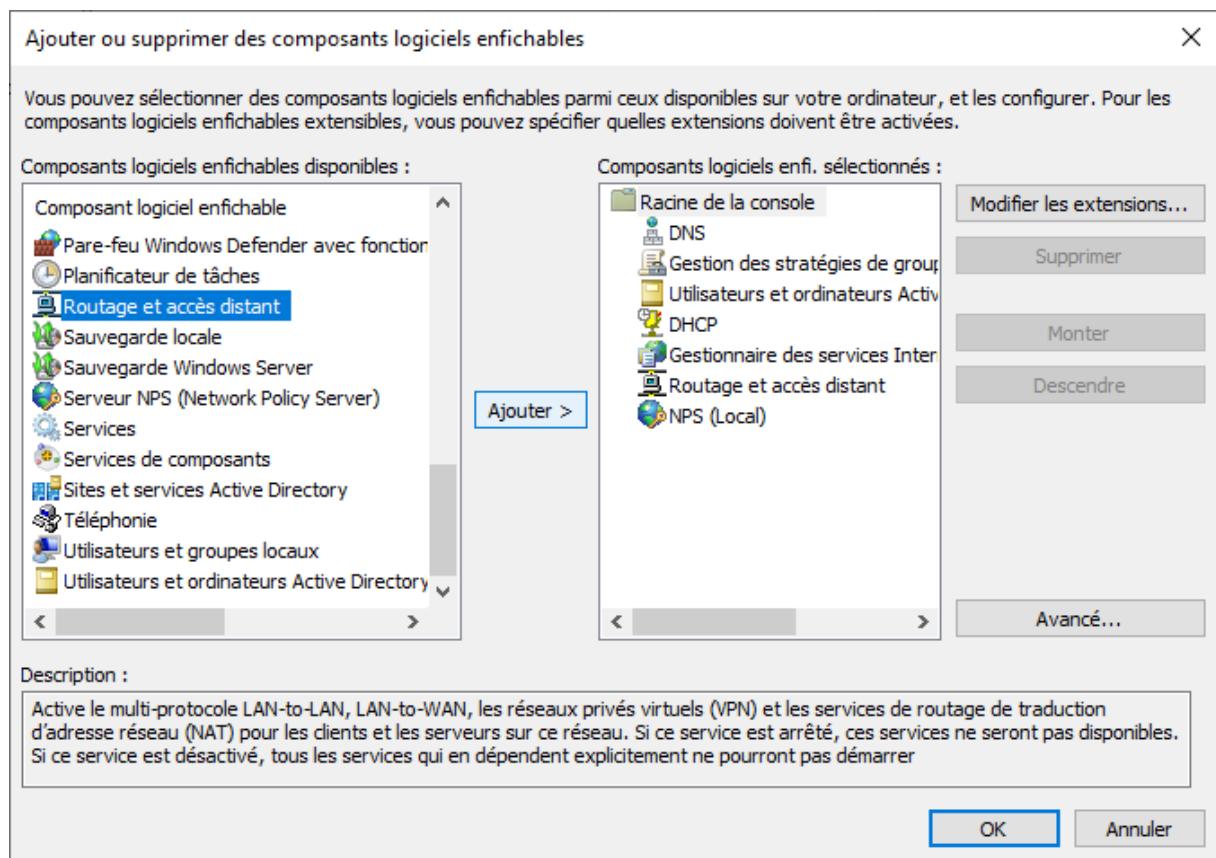


III – Stratégie d'accès réseau

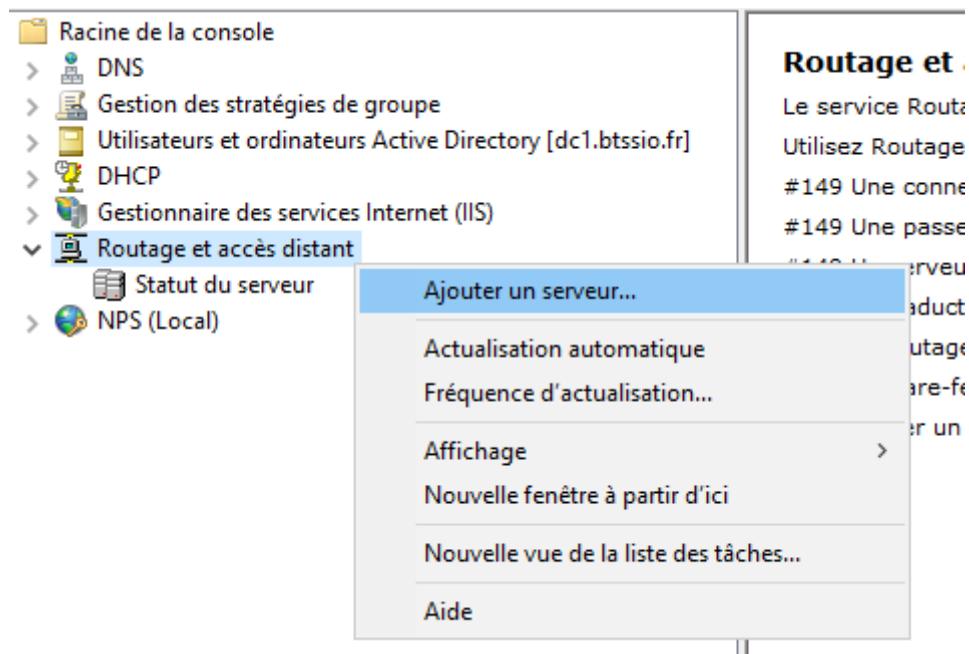
Commencez par ajouter les consoles d'administration créées lors de notre installation du service VPN.

Dans notre console MMC ajoutez les composants suivants :

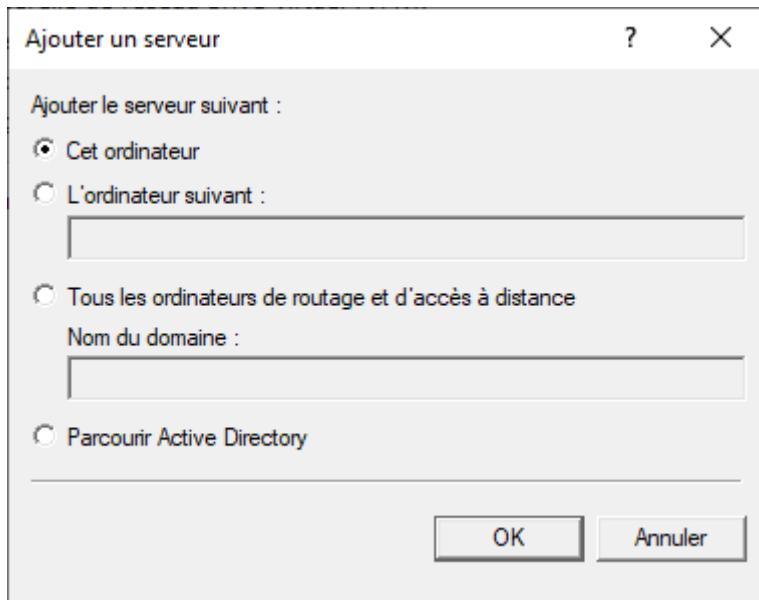
Routage et accès distant et NPS



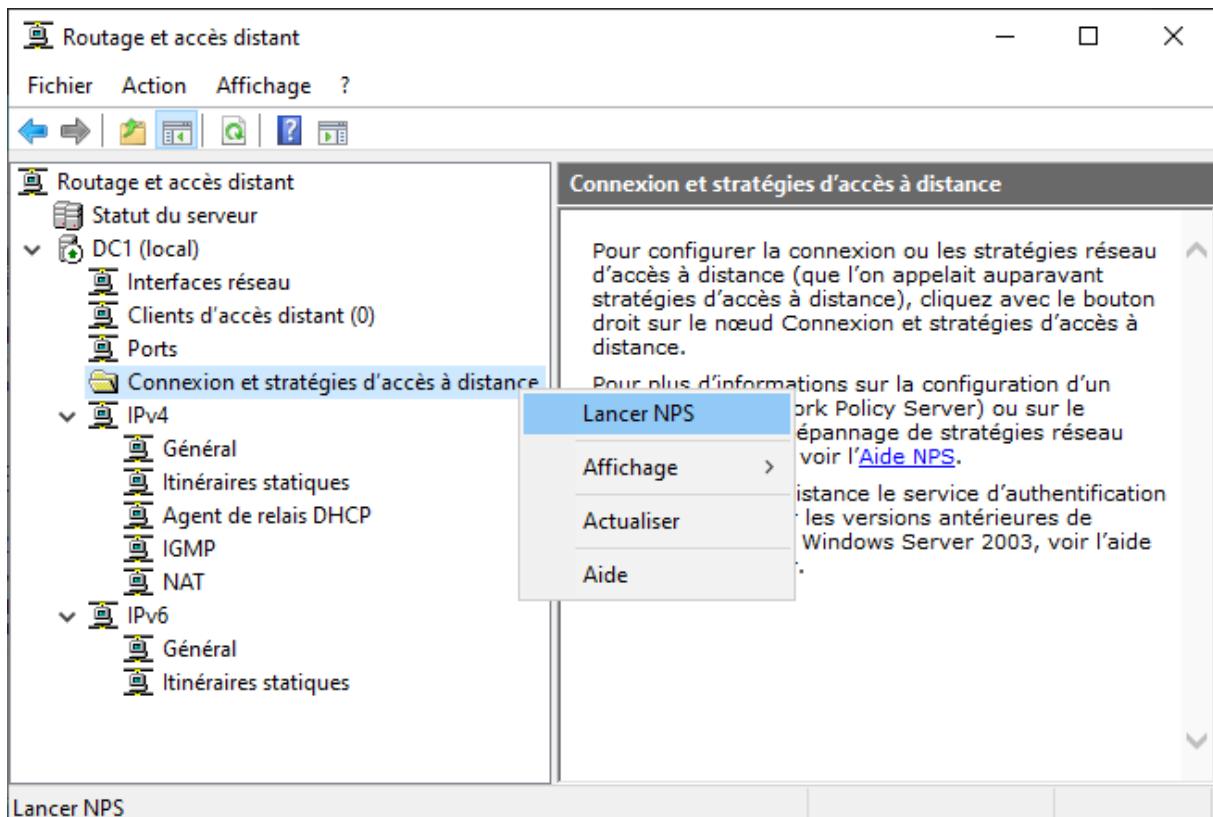
Une fois les composants ajoutés, clic droit sur routage et accès distant et cliquez sur « Ajouter un serveur »



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



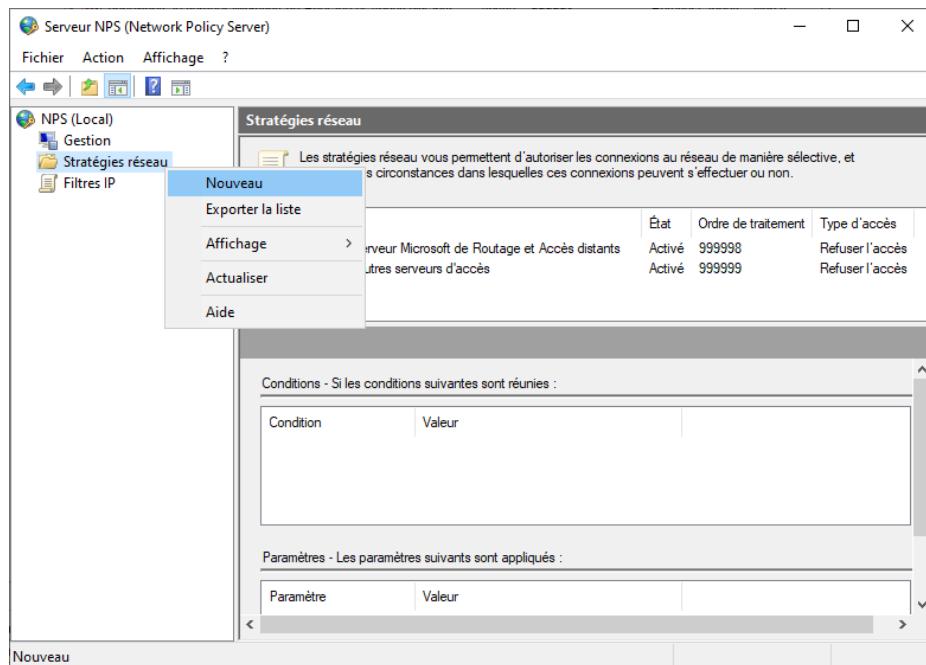
Faites un clic droit sur « Connexion et stratégies d'accès à distance » puis cliquez sur « Lancer NPS »



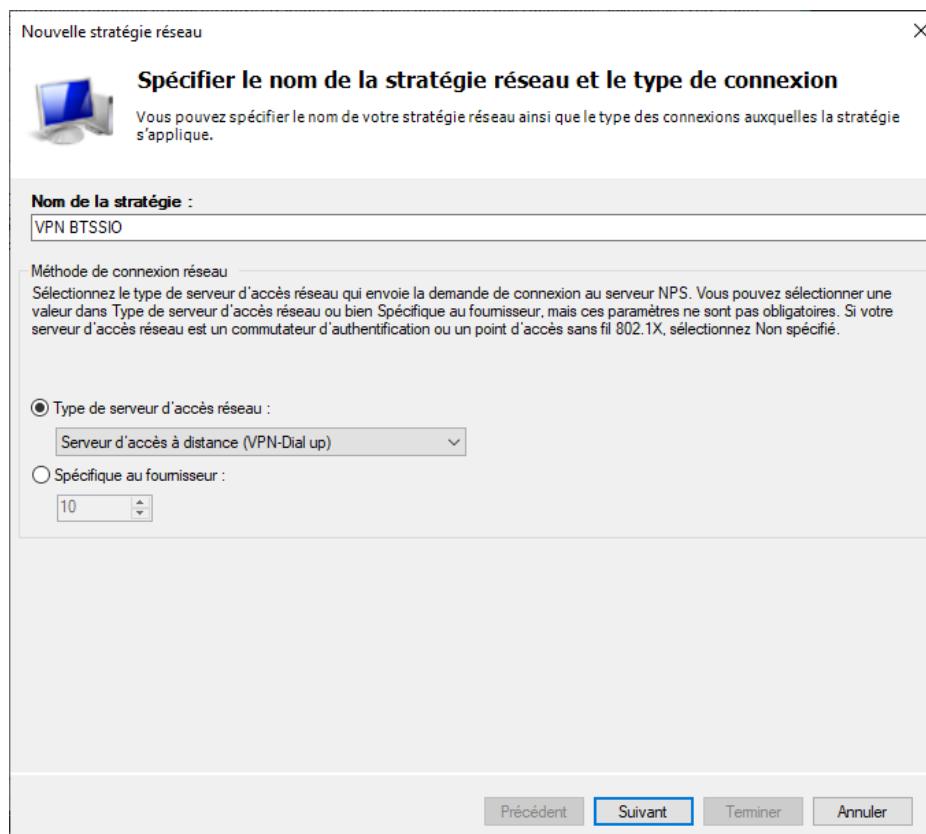
Vous serez redirigé dans une nouvelle interface de NPS.

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 »

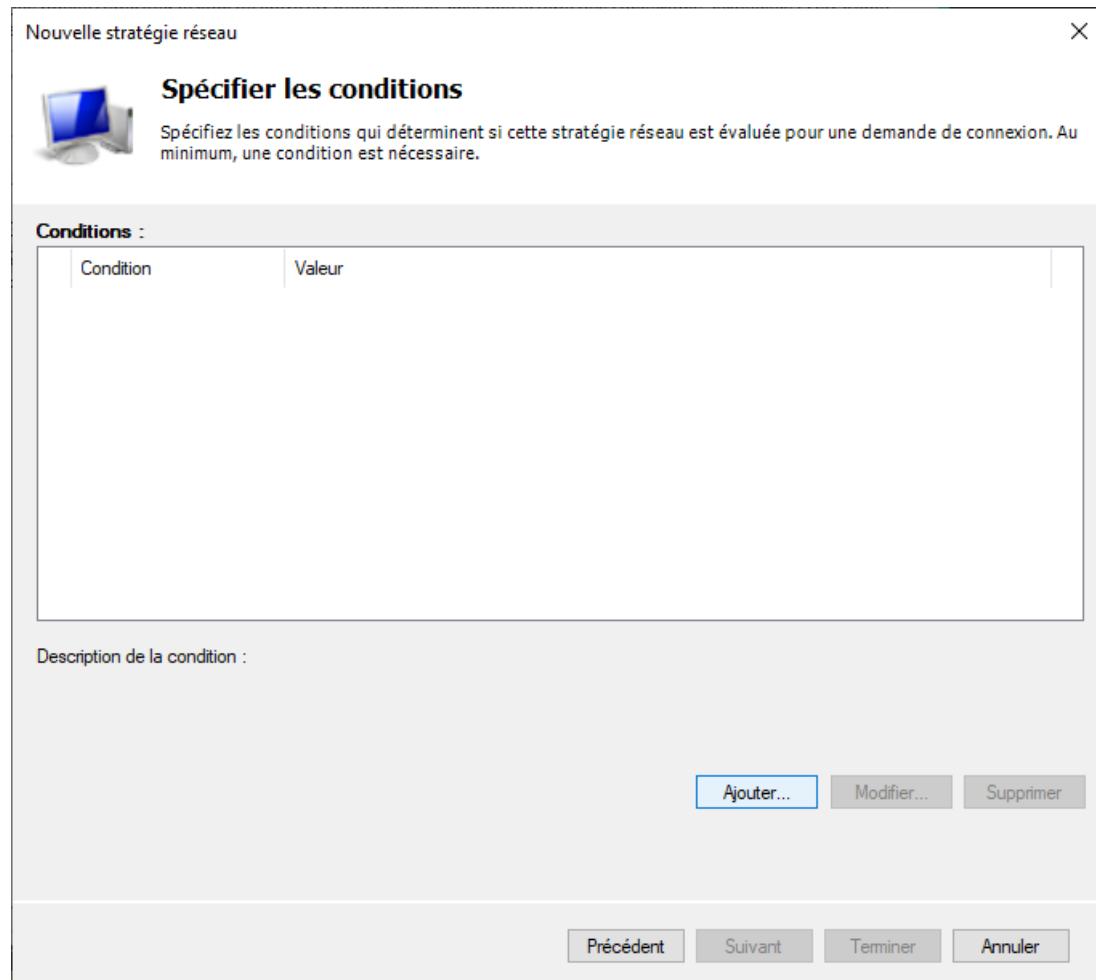


Saisissez un nom de la stratégie et dans de serveur d'accès réseau prenez « Serveur d'accès à distance (VPN-Dial UP) »

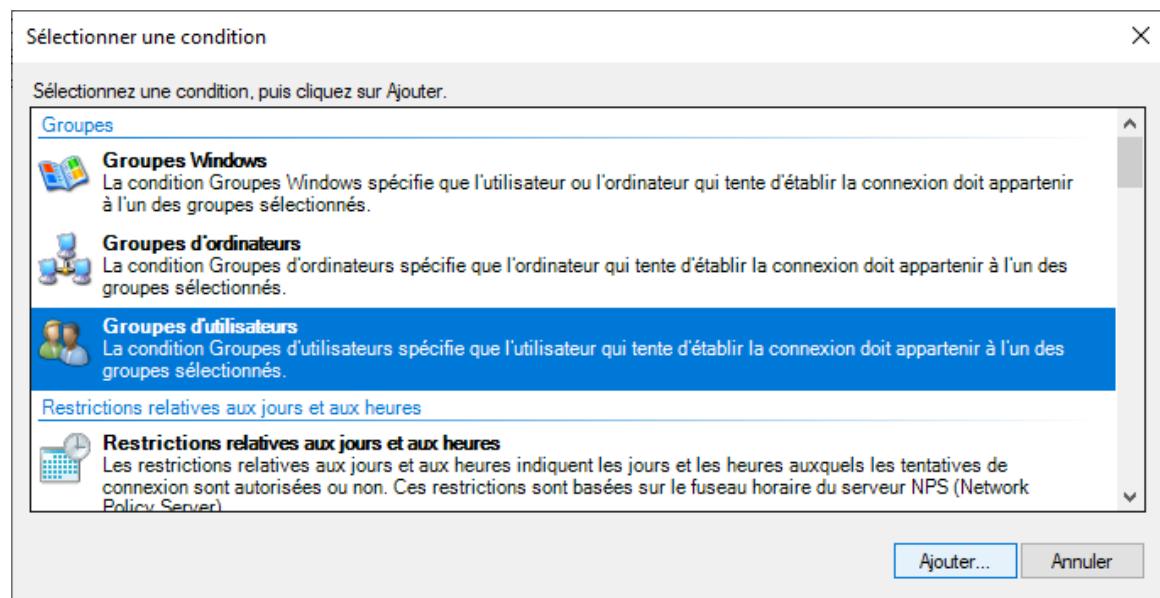


Dans les conditions, nous allons ajouter le groupe d'utilisateurs qui aura accès au service VPN.

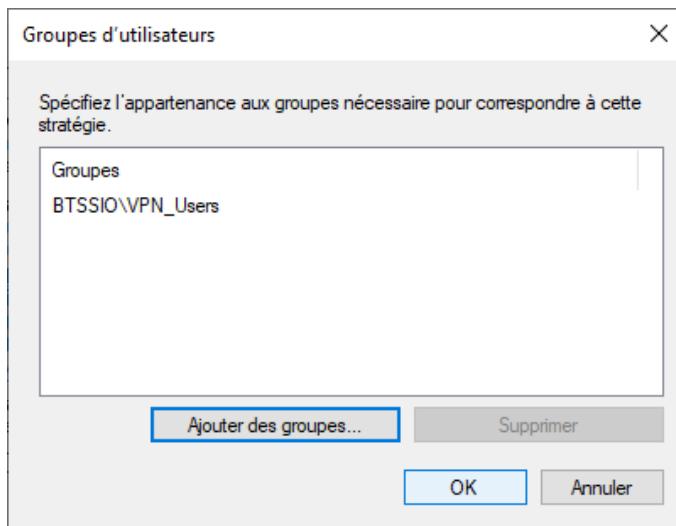
Cliquez sur « Ajouter »



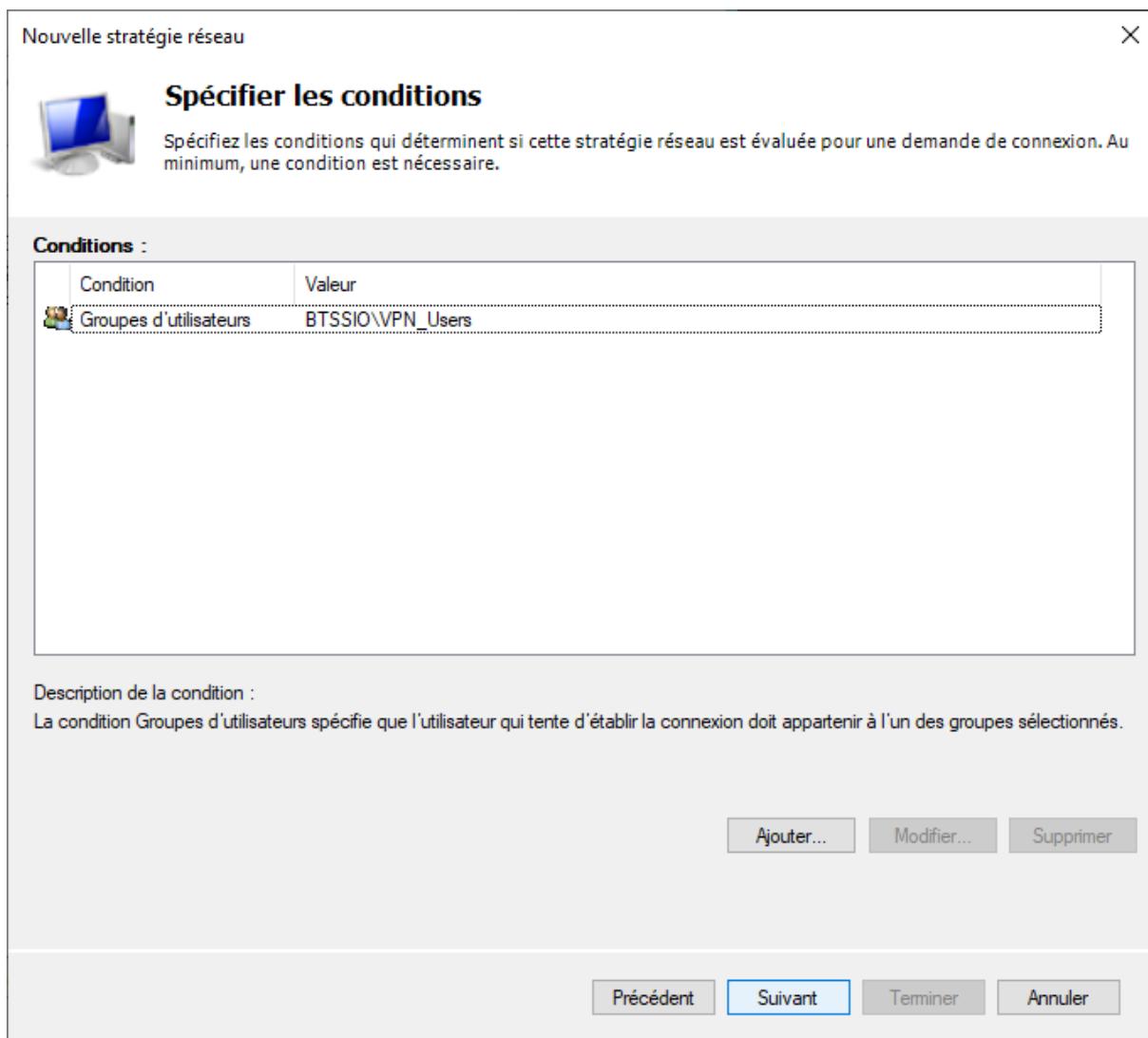
Selectionner « Groupe d'utilisateurs »



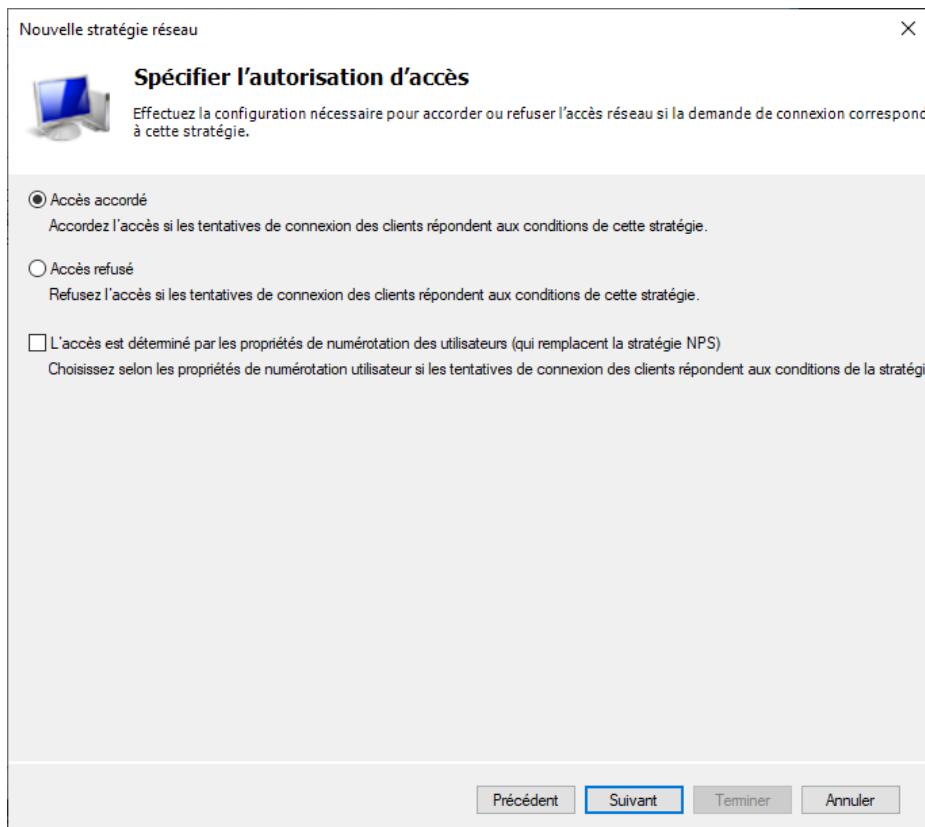
Sélectionner le groupe d'utilisateurs concerné puis cliquez sur « **OK** »



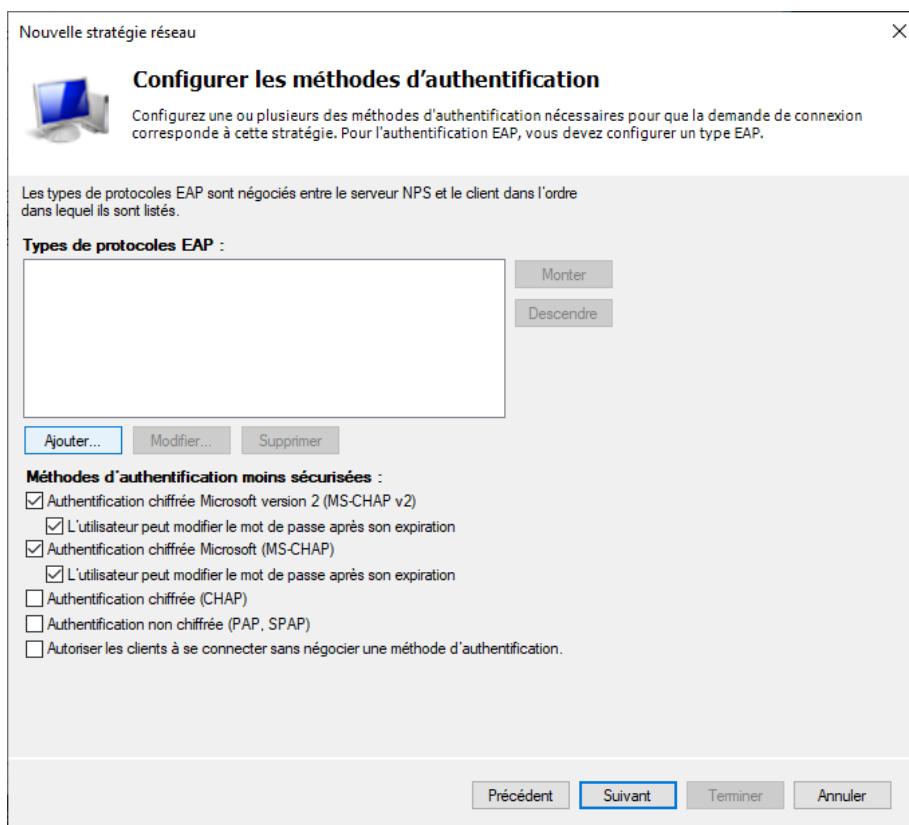
Une fois le groupe ajouter, cliquez sur « **Suivant** »



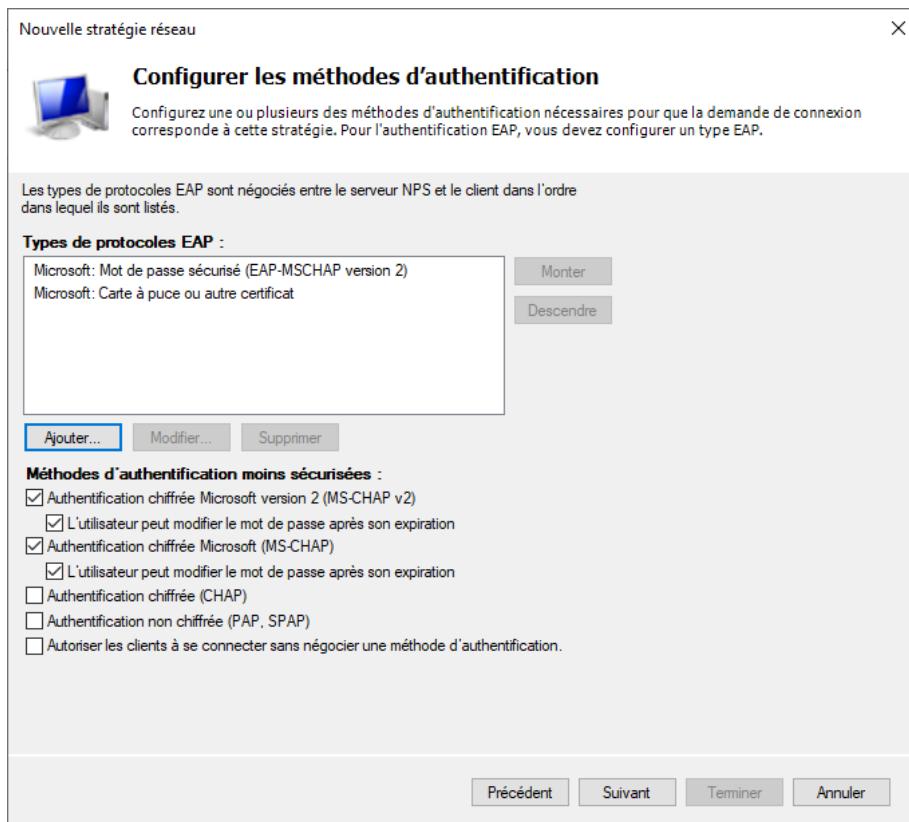
Bien entendu, il faut prendre « **Accès accordé** »



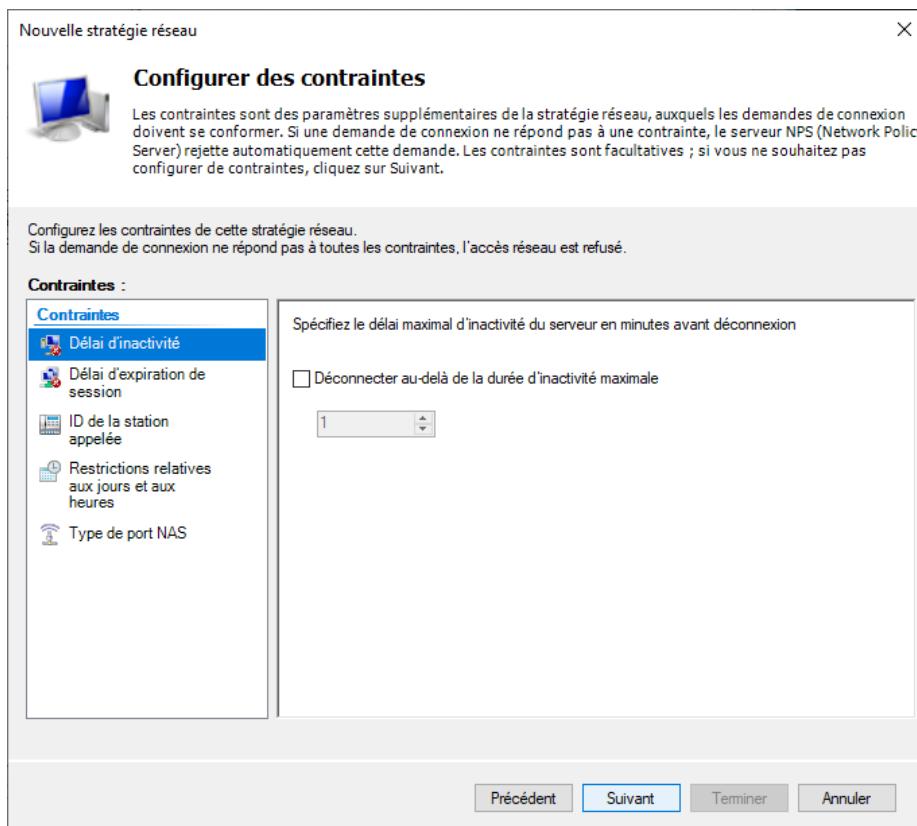
Cliquez sur « **Ajouter** » pour ajouter les méthodes d'authentification



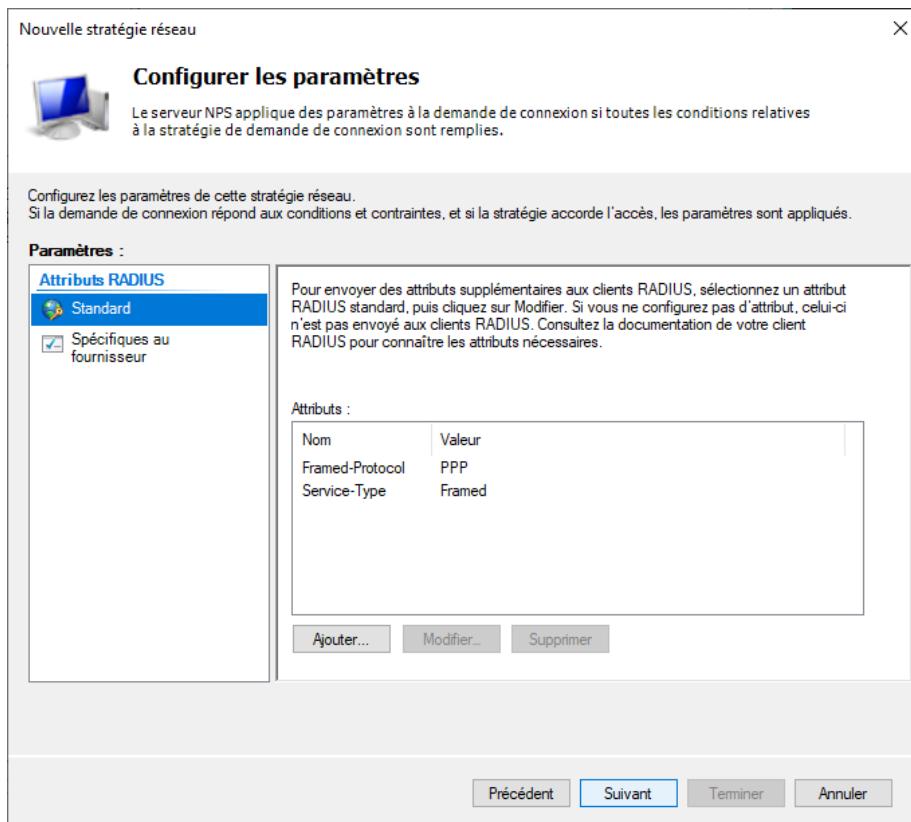
Ajouter les méthodes d'authentification comme ci-dessous :



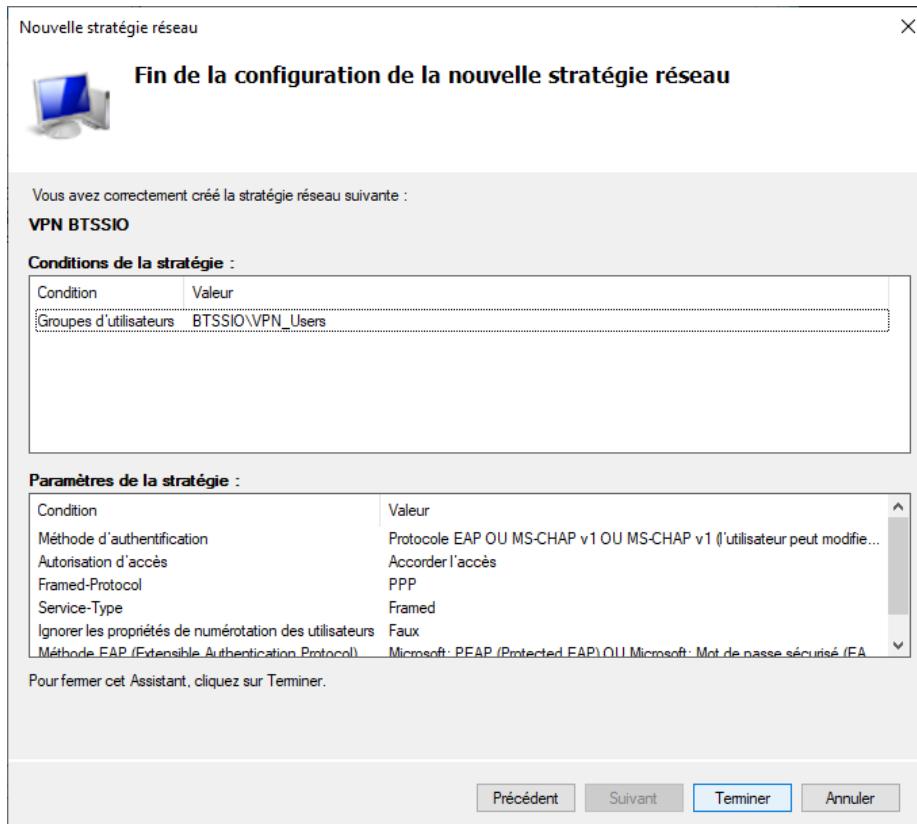
Dans notre cas, pas besoin des contraintes, cliquez sur « Suivant »



Cliquez sur « Suivant »



Cliquez sur « Terminer »



Notre stratégie réseau a bien été créé avec succès !

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Gestion
- Stratégies réseau
- Filtres IP

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès
VPN BTSSIO	Activé	1	Accorder l'accès
Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès
Connexions à d'autres serveurs d'accès	Activé	99999	Refuser l'accès

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur

III – Test de connexion

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

Rechercher Applications Documents Web Plus ▾

Meilleur résultat

Paramètres VPN

Paramètres système

Paramètres

- Options avancées de VPN
- Ajouter une connexion VPN
- Autoriser la connexion VPN sur les réseaux limités

Rechercher sur le Web

- vpn - Afficher plus de résultats de recherche
- vpn gratuit pc
- vpn gratuit
- vpnbook
- vpn free
- vpn download
- von edae
- vpn

Cliquez sur « Ajouter une connexion VPN »

VPN



Options avancées

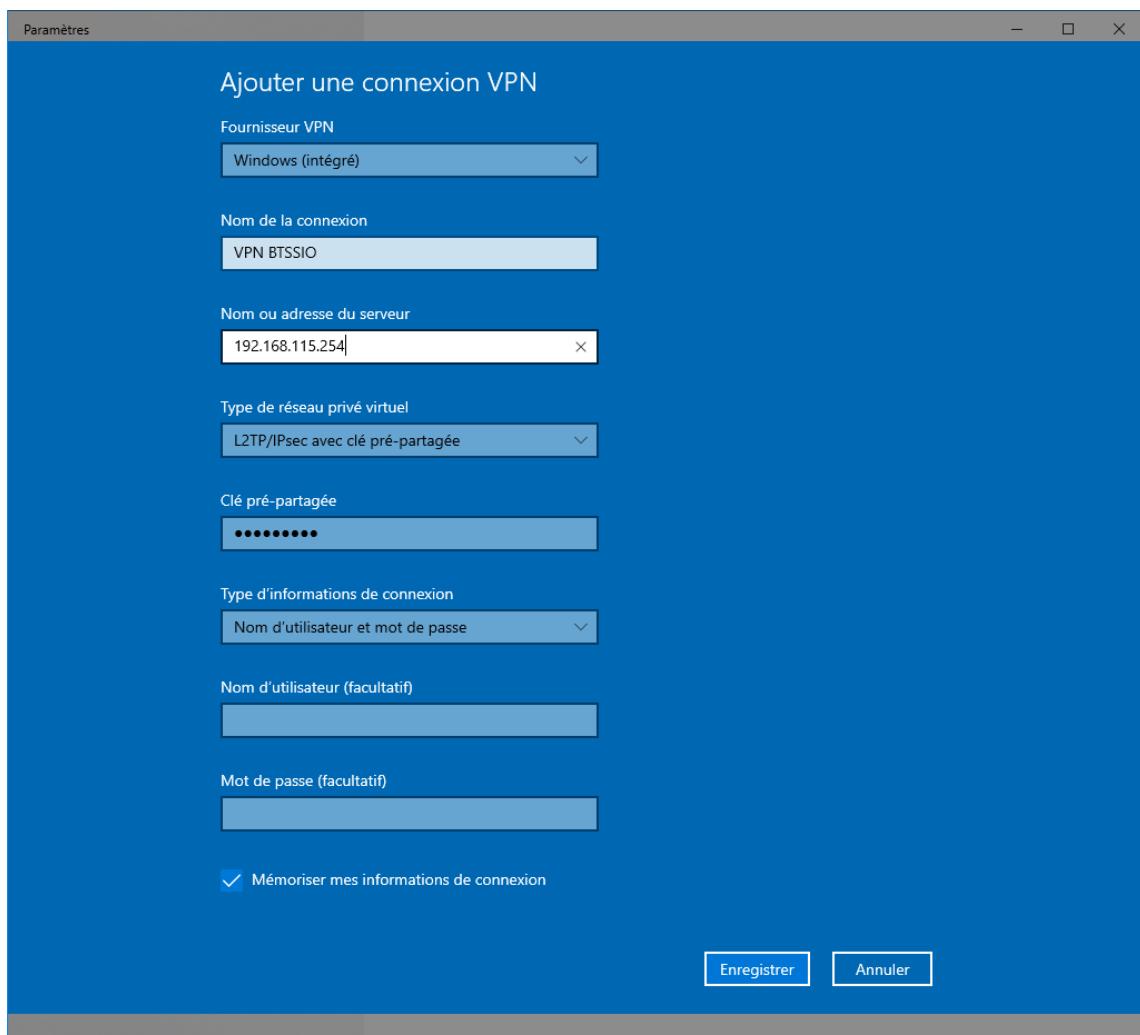
Autoriser les connexions VPN sur des réseaux limités



Autoriser les connexions VPN en itinérance



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 »

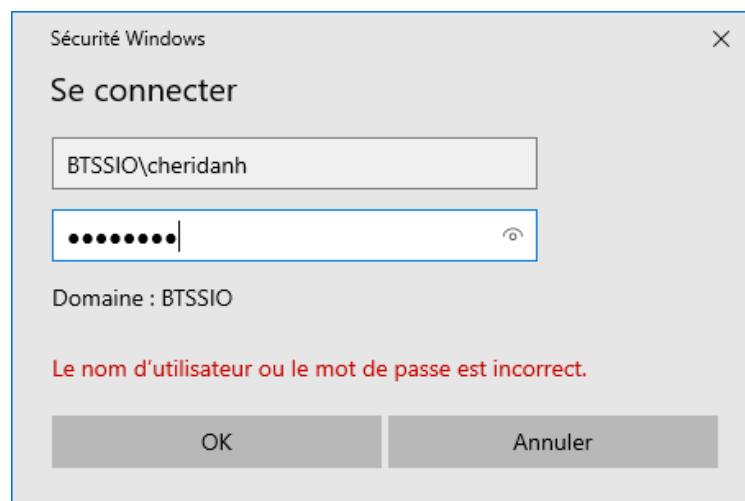


Une fois les informations enregistrées, cliquez sur « **Connecter** »

VPN

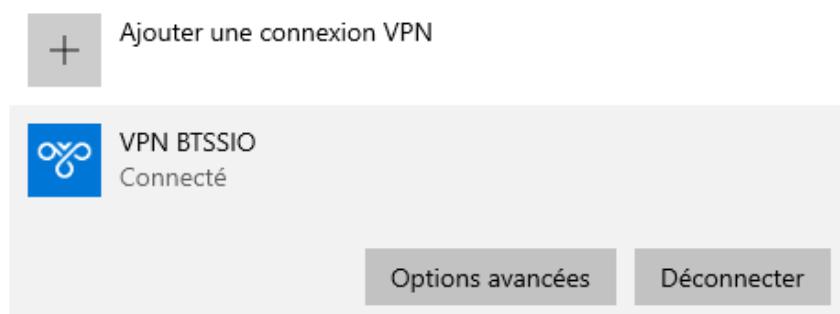


Une fois la connexion établie, les informations de connexion vous seront demandées. Saisissez le nom d'utilisateur appartenant au groupe de sécurité ajouté dans la stratégie de réseau NPS.

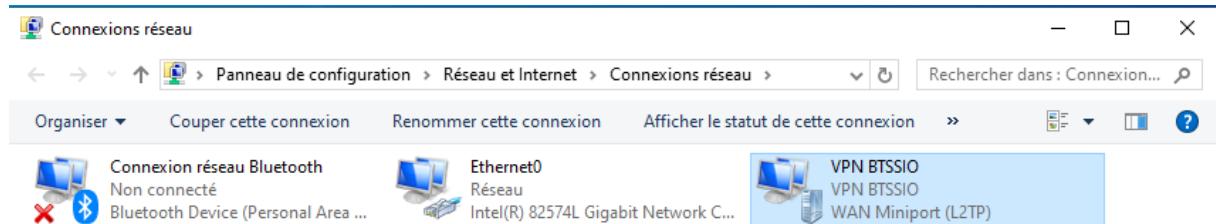


La connexion s'est effectuée avec succès !

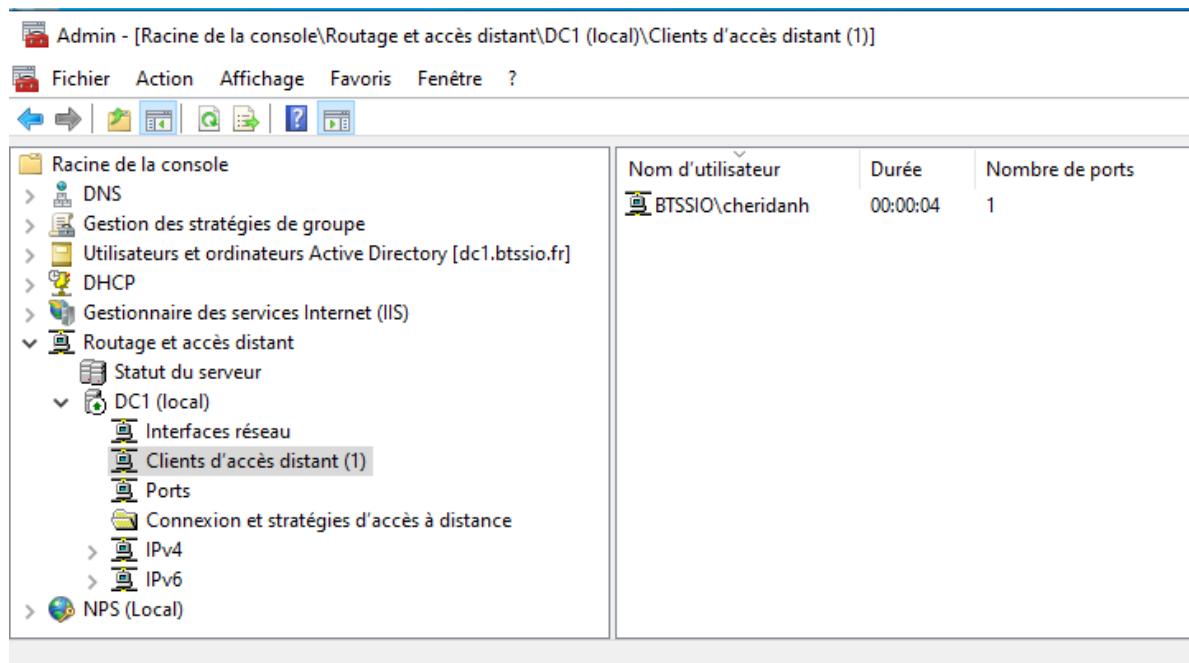
VPN



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

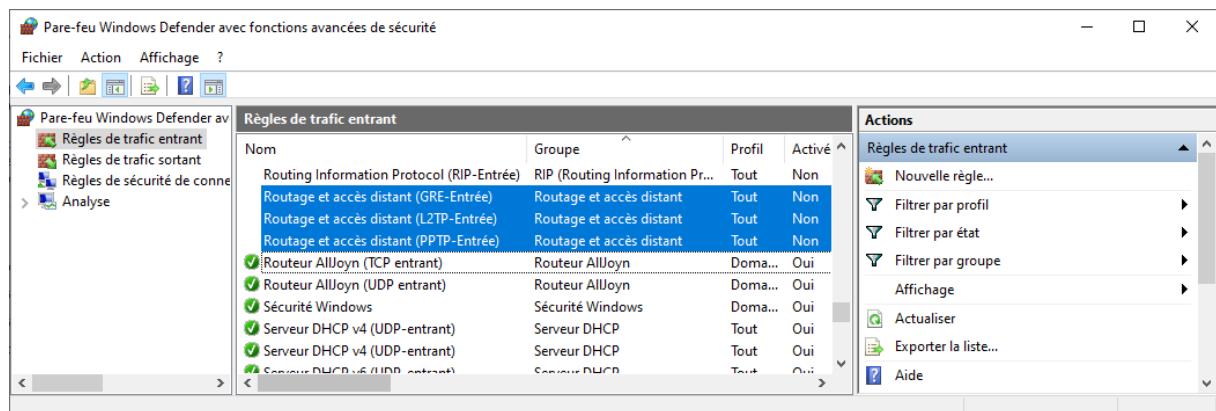


Au niveau de notre serveur VPN, on peut voir les utilisateurs connectés dans « **Clients d'accès distant** »

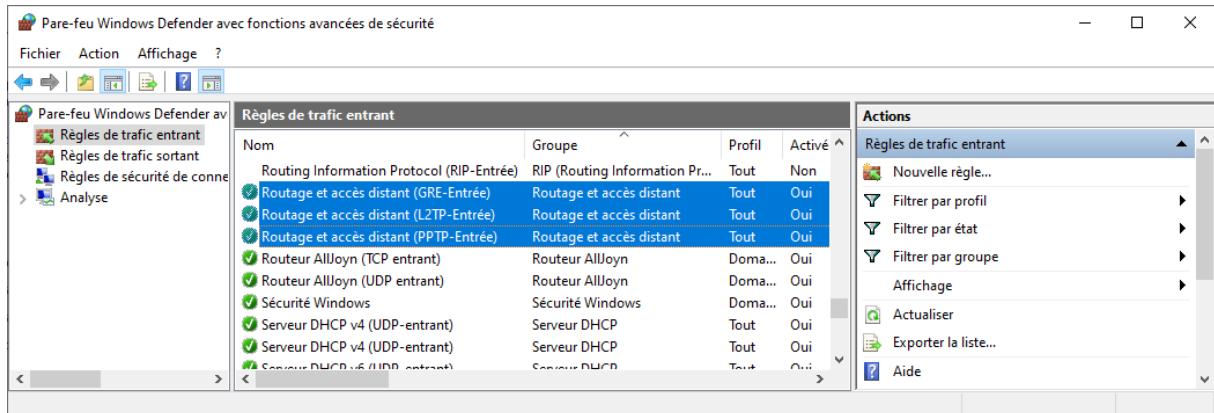


Rappelez-vous pendant la configuration de notre serveur, nous avions un avertissement concernant l'ouverture des ports.

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.



The screenshot shows the Windows Firewall with Advanced Security interface. The main window displays the 'Inbound Rules' list. The 'Actions' pane on the right lists various management options. The 'Inbound Rules' table includes the following entries:

Nom	Groupe	Profil	Activé
Routing Information Protocol (RIP-Entrée)	Routing et accès distant	Tout	Non
Routage et accès distant (GRE-Entrée)	Routage et accès distant	Tout	Oui
Routage et accès distant (L2TP-Entrée)	Routage et accès distant	Tout	Oui
Routage et accès distant (PPTP-Entrée)	Routage et accès distant	Tout	Oui
Routeur AllJoyn (TCP entrant)	Routeur AllJoyn	Dom... Oui	
Routeur AllJoyn (UDP entrant)	Routeur AllJoyn	Dom... Oui	
Sécurité Windows	Sécurité Windows	Dom... Oui	
Serveur DHCP v4 (UDP-entrant)	Serveur DHCP	Tout Oui	
Serveur DHCP v4 (UDP-entrant)	Serveur DHCP	Tout Oui	
Serveur DHCP v6 (UDP-entrant)	Serveur DHCP	Tout Oui	

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>