



OFPPT

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de
l'Offshoring et de l'Electronique -Oujda

Module : Administration d'un Réseau

Installation et configuration du serveur VPN sous Windows Server 2012R2

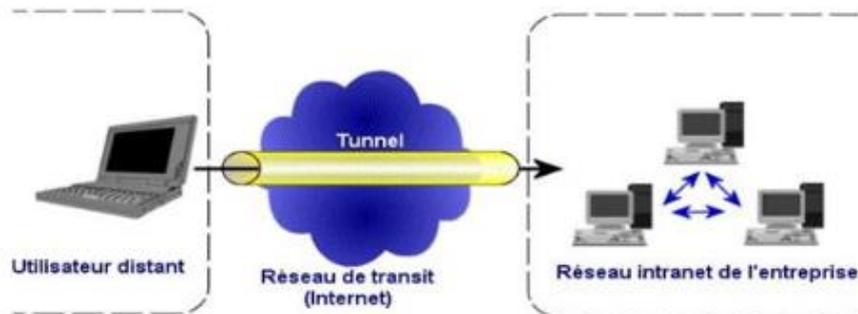
Formatrice : ZIT I ILHAM

Sommaire

| | |
|-----------------------------------|----|
| 1. Présentation | 3 |
| 2. Mise en place du VPN..... | 3 |
| 3. Configuration VPN..... | 10 |
| 4. Accès utilisateurs..... | 16 |
| 5. Autorisation du Pare-Feu | 18 |
| 6. Connexion au tunnel | 20 |
| 7. Référence | 23 |

1. Présentation

Un VPN (Virtual Private Network), réseau privé virtuel en français, permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local. On peut ainsi avoir un accès au réseau interne (réseau d'entreprise, par exemple).



2. Protocoles du serveur VPN

2.1 PPTP

Le PPTP (point to point tunneling protocol) crée un tunnel privé pour envoyer des données depuis un périphérique distant, authentifié uniquement par un mot de passe. Il n'implique donc aucune installation de matériel supplémentaire. L'un des avantages de ce protocole est sa facilité d'installation et de configuration sur toutes plateformes que ce soit (Windows, Mac Os, Linux, Os mobiles...), ainsi que sa rapidité. Mais le PPTP ne fournit aucun cryptage de données ce qui lui donne un niveau de sécurité assez faible par rapport aux autres protocoles. Il fonctionne sur la couche 2 du modèle OSI et utilise le port TCP 1723.

2.2 L2TP sur IPSec

Le L2TP (layer 2 tunneling protocol) sur IPSec (internet protocol security) est un protocole qui utilise le même fonctionnement que PPTP à la différence près qu'il offre l'intégrité et la confidentialité des données grâce à un protocole de cryptage (IPSec). L2TP est donc également un protocole qui s'appuie sur la couche 2 du modèle OSI et utilise le port UDP 500 pour l'échange des clés et le port 50 pour le cryptage via l'IPSec. L'IPSec est une suite de protocoles utilisant la couche 3 du modèle OSI et qui crypte chaque paquet IP afin d'assurer le chiffrement des données.

2.3 OpenVPN

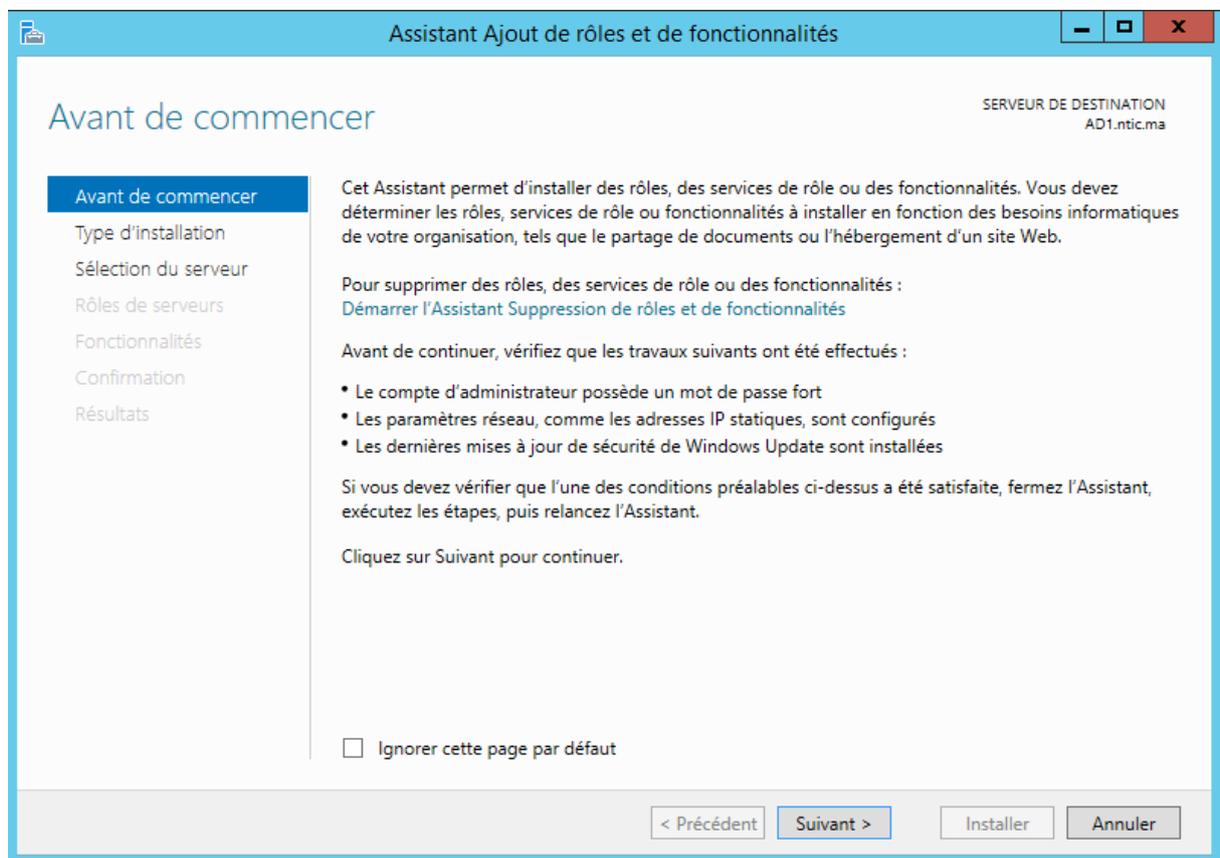
OpenVPN est un logiciel open source qui est utilisé pour les VPN basés sur le SSL (secure sockets layer). Il permet aux réseaux distants de se connecter de manière sécurisée par l'utilisation de clés partagées, de certificats, de noms d'utilisateurs ou des mots de passe. Il fait preuve d'une grande stabilité et d'une vitesse optimale, même avec des connexions lentes. De plus, OpenVPN est aussi sécurisé que L2TP/IPSec.

2.4 SSTP

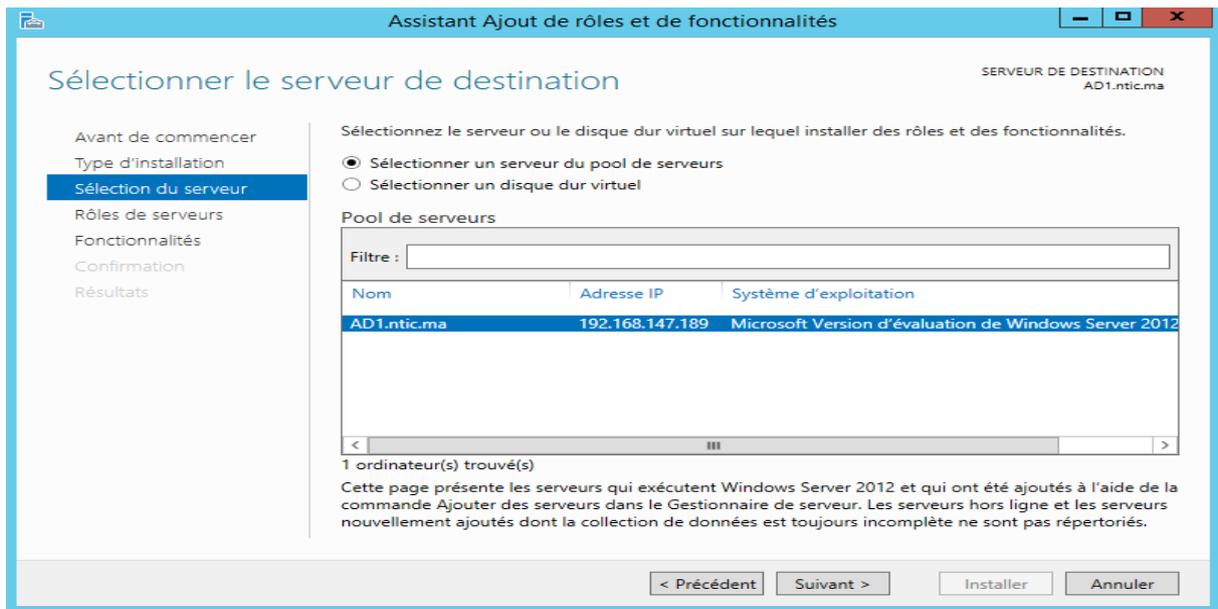
Le SSTP (secure socket tunneling protocol) utilise le SSL pour le transfert et le cryptage des données. Il utilise le plus souvent le port TCP 443. C'est l'un des protocoles VPN les plus stables et sa vitesse est similaire au PPTP, même s'il faut plus de temps pour obtenir la connexion initiale. En ce qui concerne la sécurité, ce protocole SSTP s'avère être bien supérieur à L2TP ou PPTP. Il est cependant plutôt compliqué à installer pour un novice et ne peut être utilisé uniquement que sur Linux, BSD, et les versions Windows postérieures à Vista.

3. Mise en place du VPN

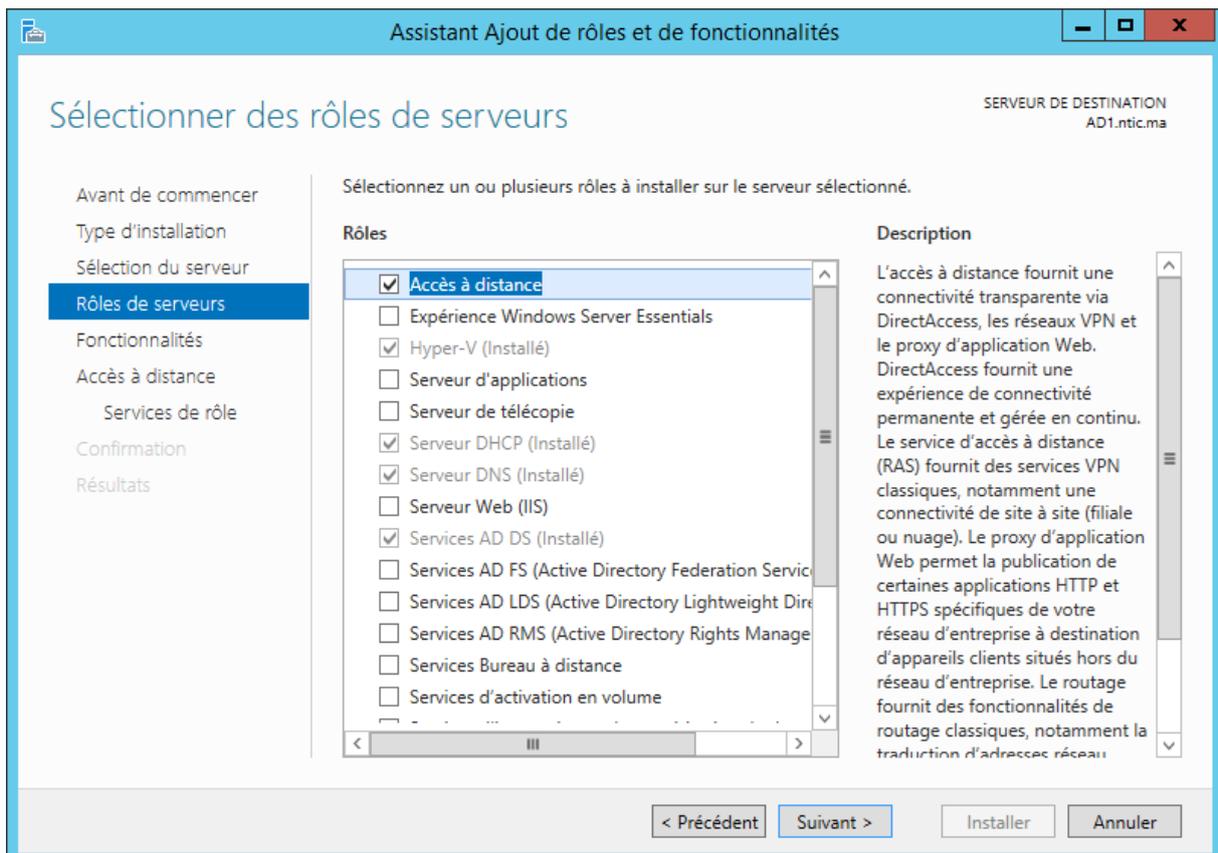
Après avoir cliqué sur « Ajouter des rôles et des fonctionnalités », une fenêtre d'assistance s'affiche. Cliquons sur « Suivant ».

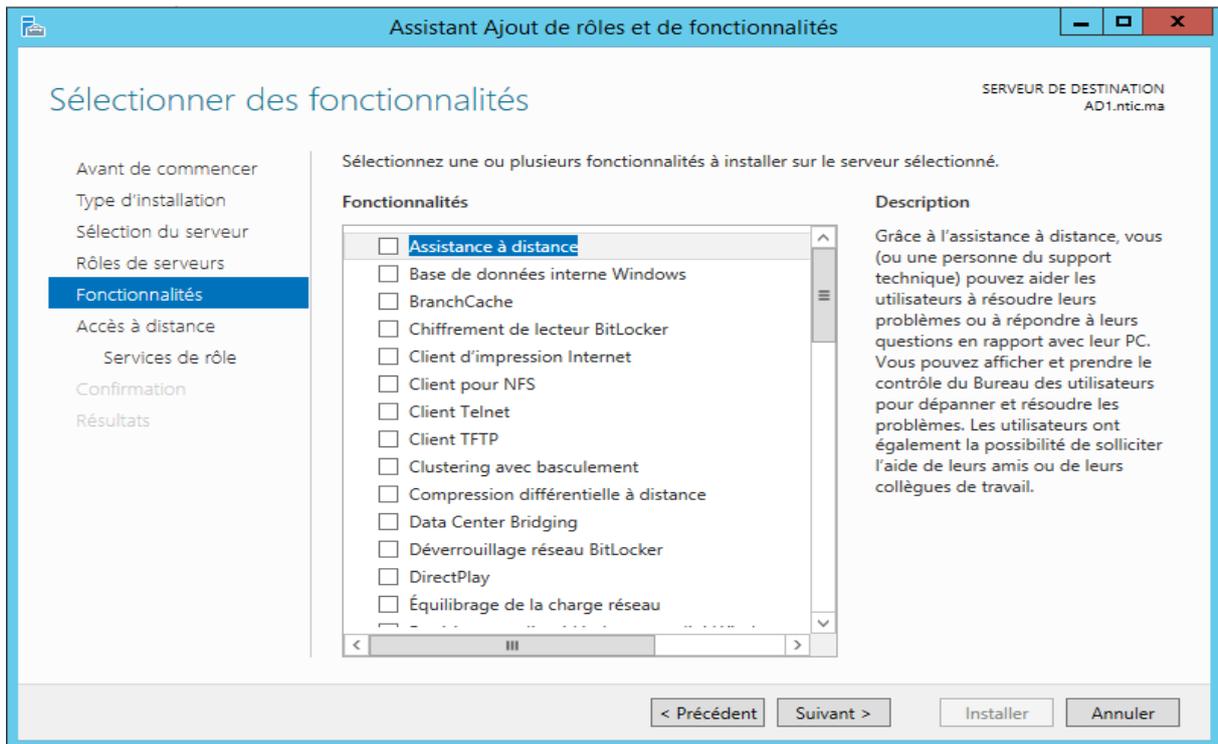


La page demande quel type de service nous voulons installer. Pour créer un VPN, il faut sélectionner « Installation basée sur un rôle ou une fonctionnalité ». Cliquons ensuite sur « Suivant ». Nous devons maintenant sélectionner le serveur sur lequel nous allons mettre en place le VPN. Ici un seul choix s'offre à nous. Nous pouvons cliquer sur « Suivant ».

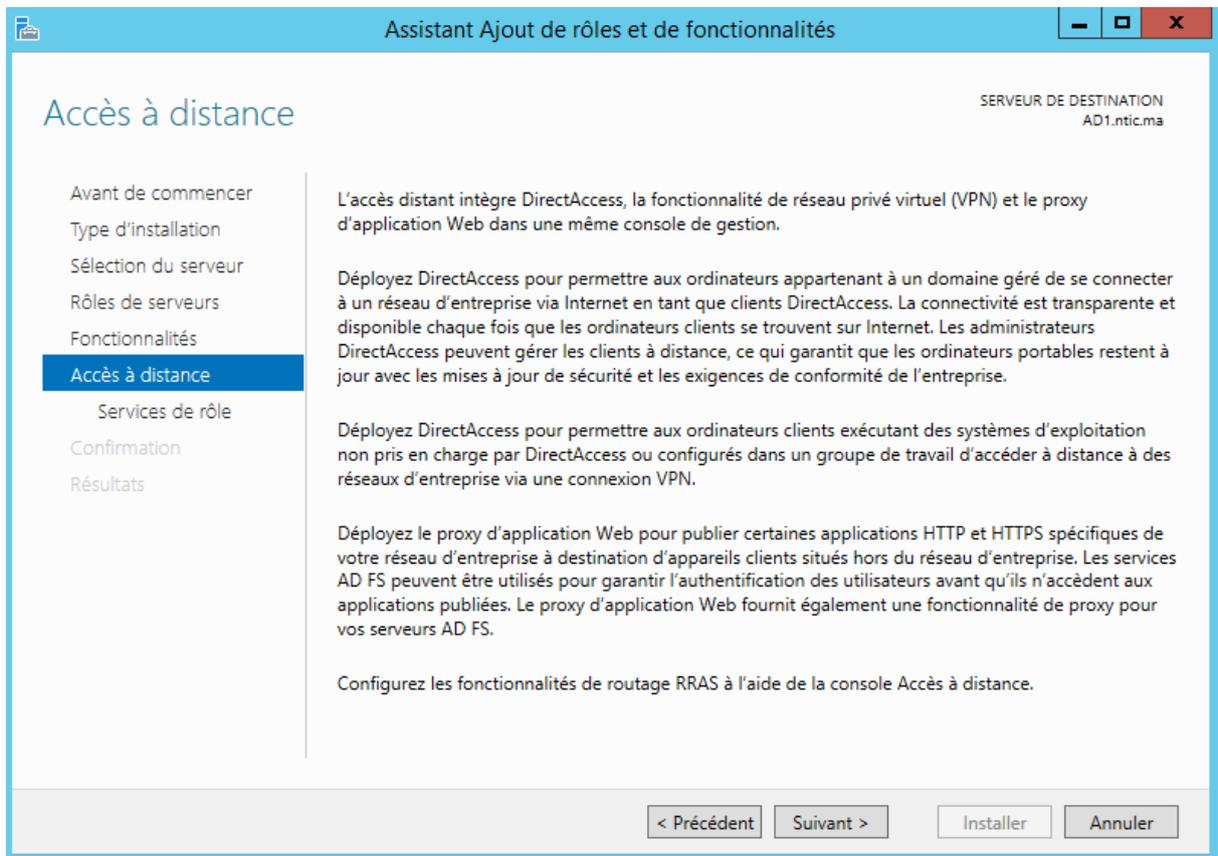


Il faut à présent déterminer le rôle de l'outil que nous voulons créer. Dans le cas d'un VPN, nous devons sélectionner **l'accès à distance**. Une fois coché, cliquons sur « Suivant ».



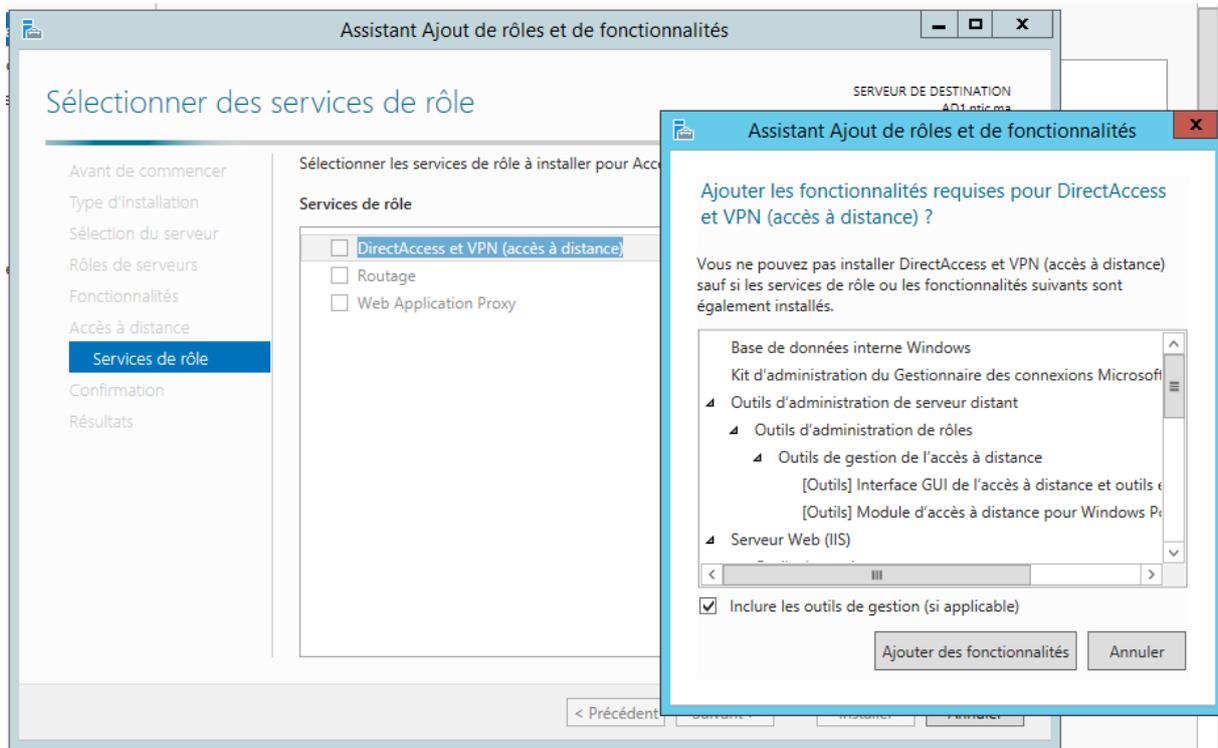


L'assistant décrit à quoi sert un VPN et que faire pour le configurer. Cliquons sur « Suivant »

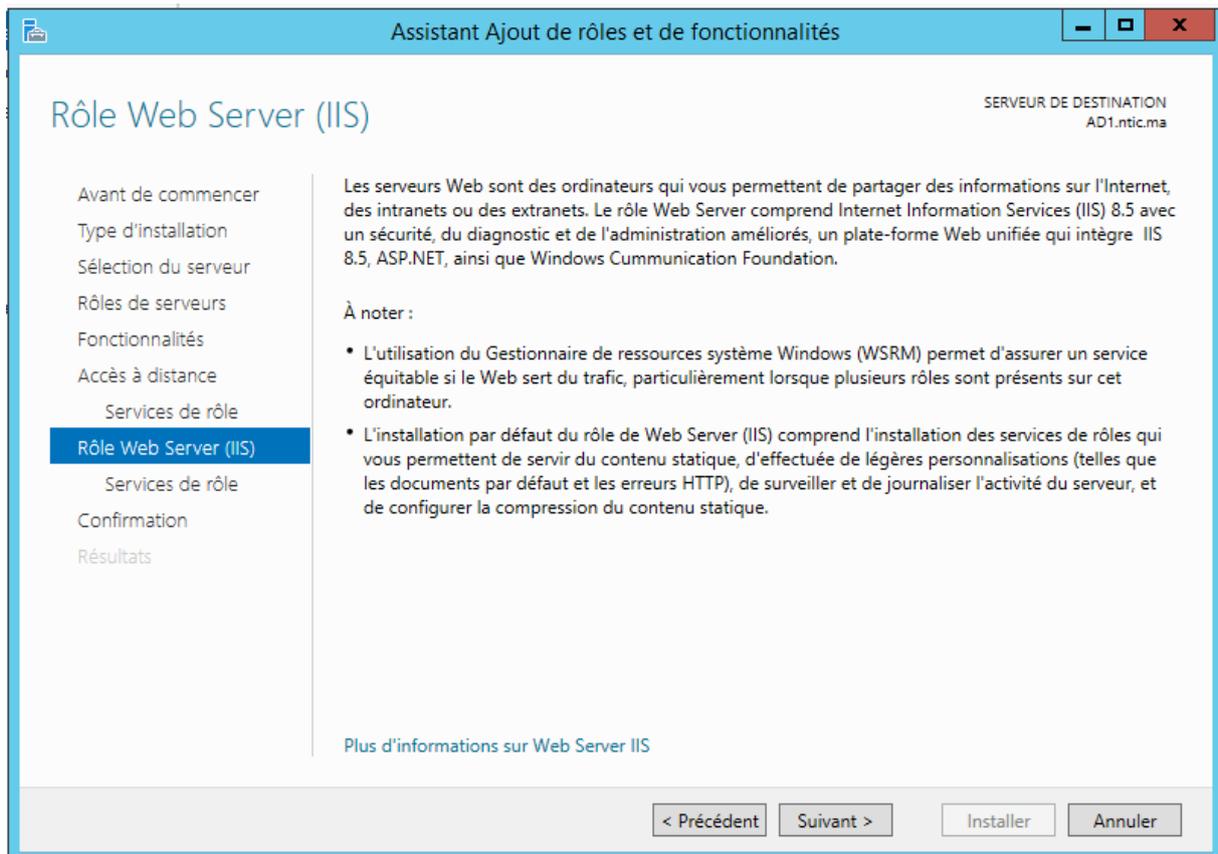


Sélectionner les services du VPN. Il faut donc cocher « DirectAccess et VPN ».

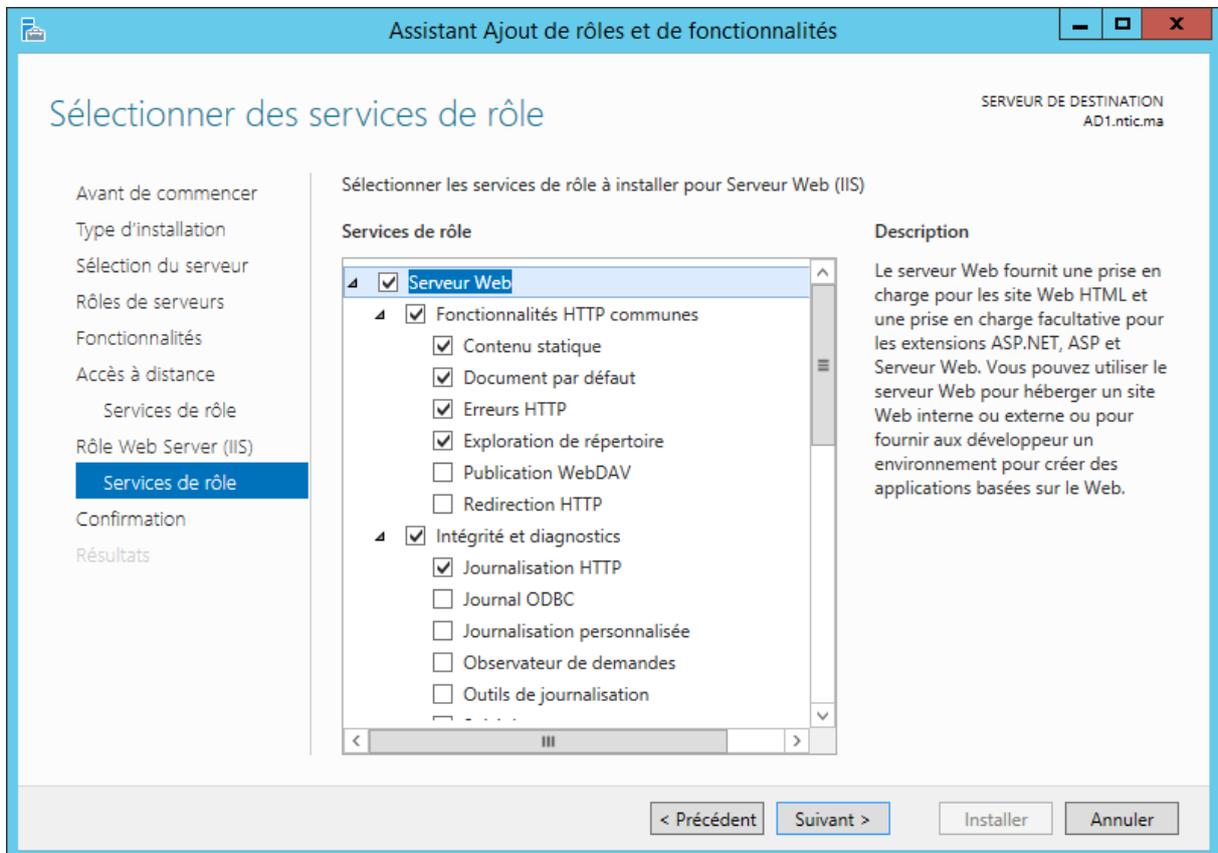
L'assistant nous demande de valider notre choix. Cliquons simplement sur « Ajouter des fonctionnalités » puis sur « Suivant » pour continuer l'installation



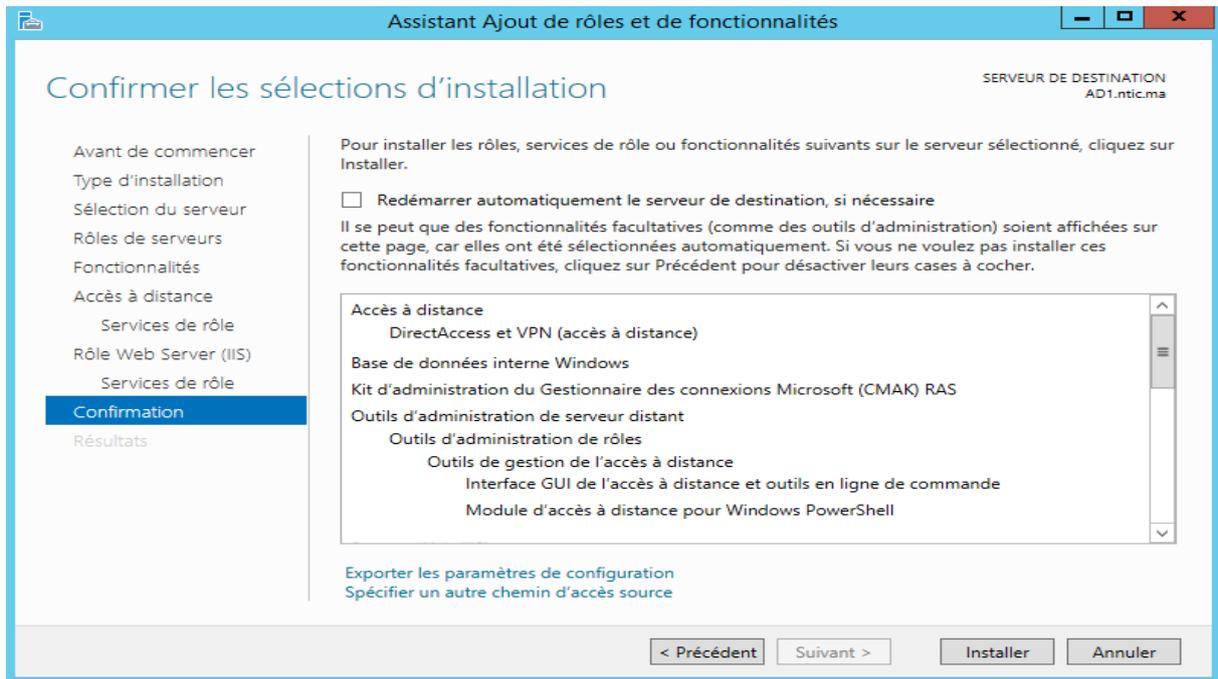
Cette page décrit le rôle du serveur Web. Cliquons sur « Suivant »..



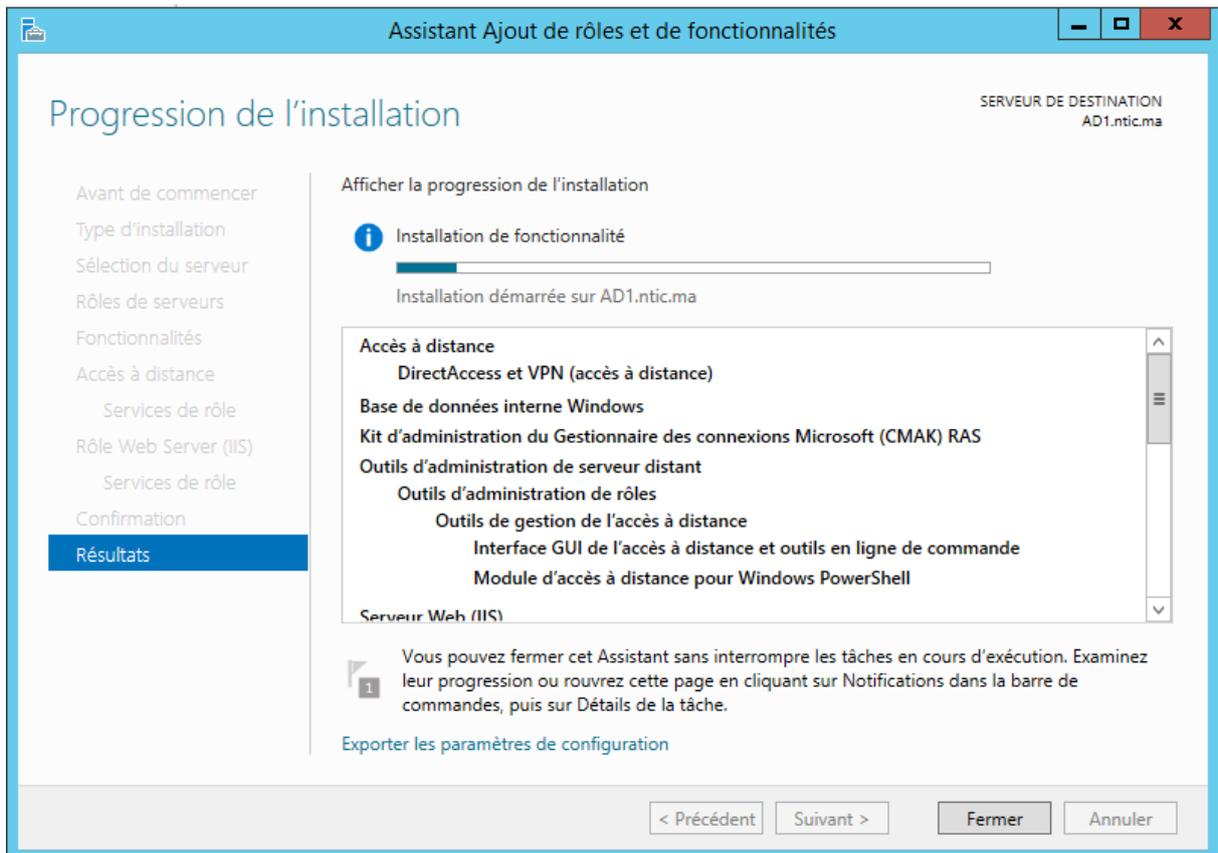
Ici, rien à cocher. Cliquons sur « Suivant ».



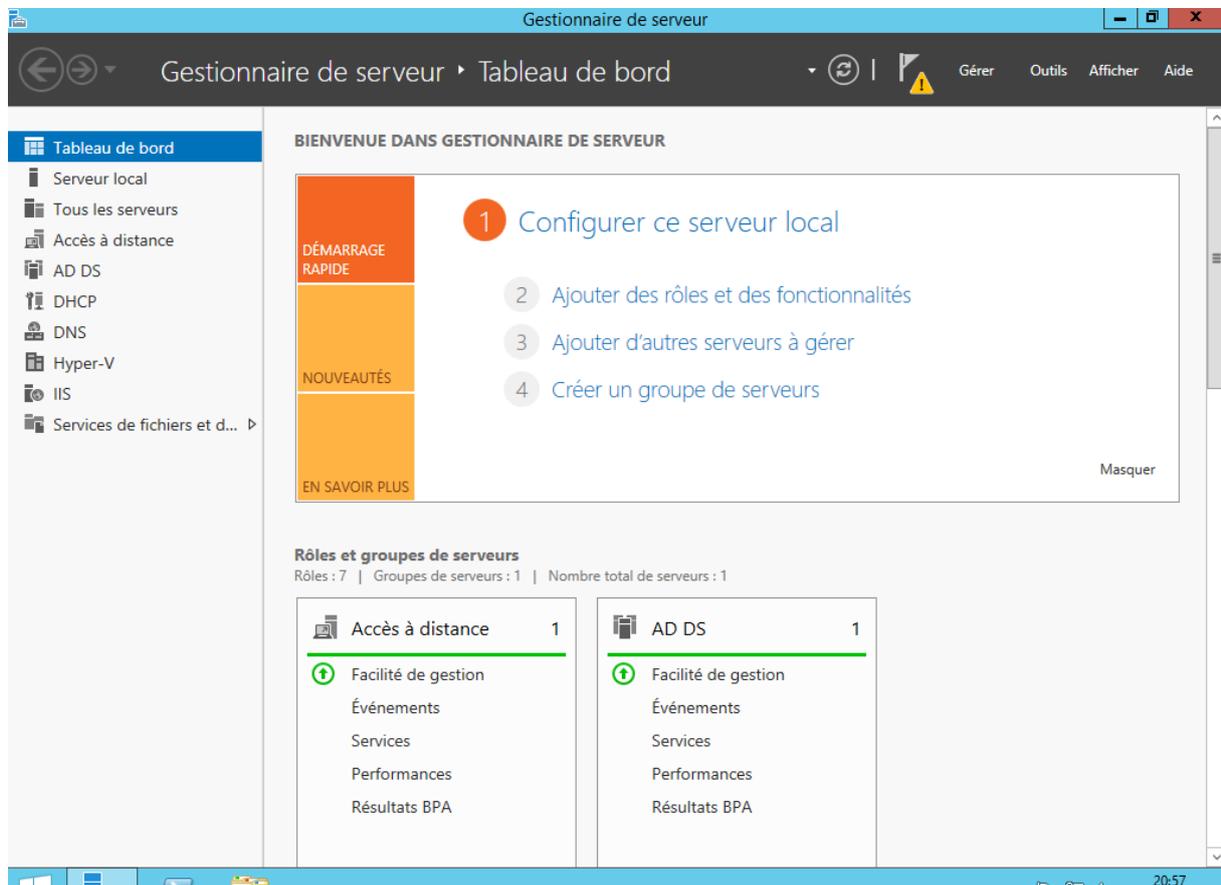
Nous avons désormais inclus tous les services et toutes les options nécessaires à la création du VPN. Cliquer à présent sur « Installer » pour créer le VPN dans le serveur.



Une fois l'installation terminée, cliquons sur « Fermer ».



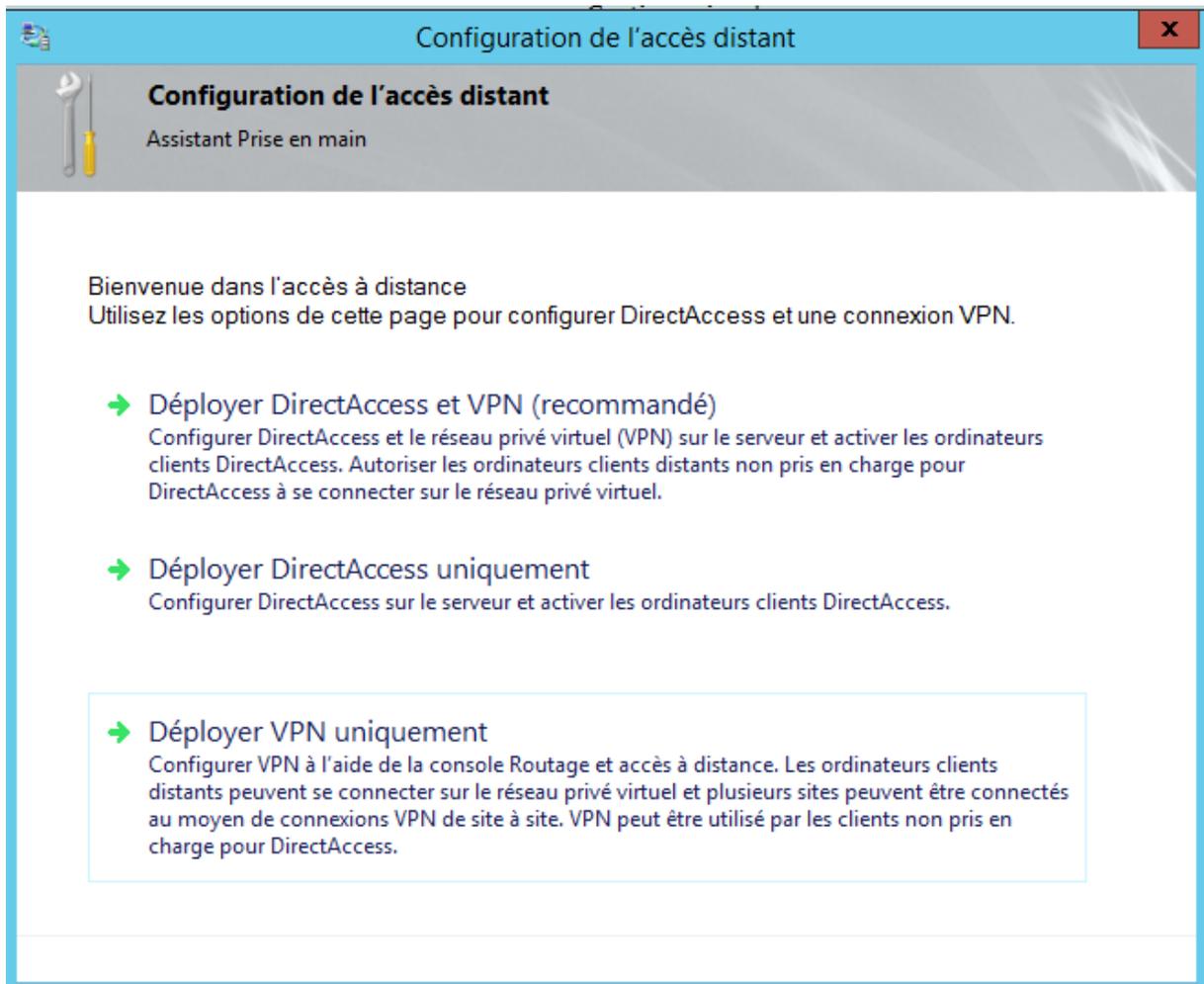
Nous pouvons donc remarquer que l'accès à distance a bien été créé dans le serveur. Il faut désormais le configurer



4. Configuration VPN

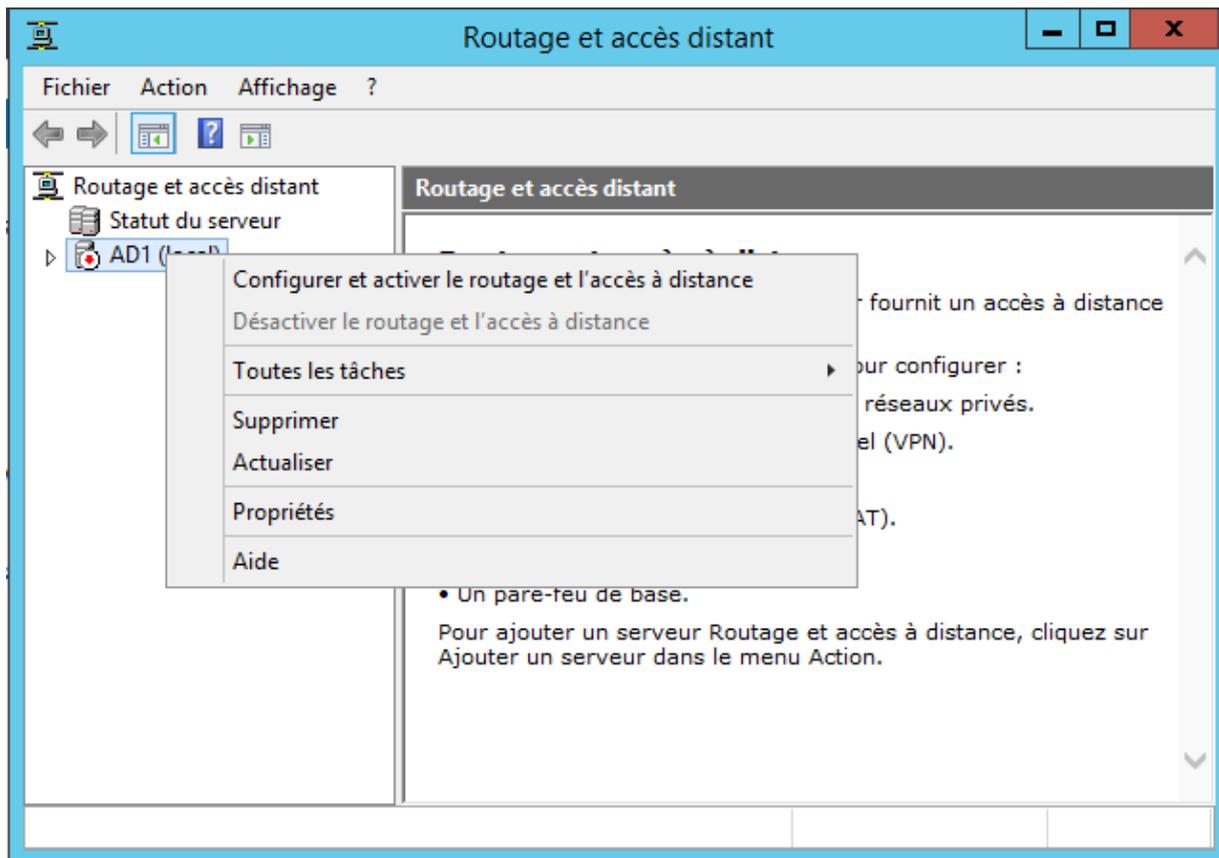
Après avoir cliqué sur « Accès à distance », nous pouvons remarquer un message d'alerte nous disant qu'une configuration est requise afin que le VPN soit opérationnel. Cliquons donc sur « Autres... » afin de le configurer.

Une nouvelle fenêtre s'ouvre. Nous allons déployer le VPN uniquement.

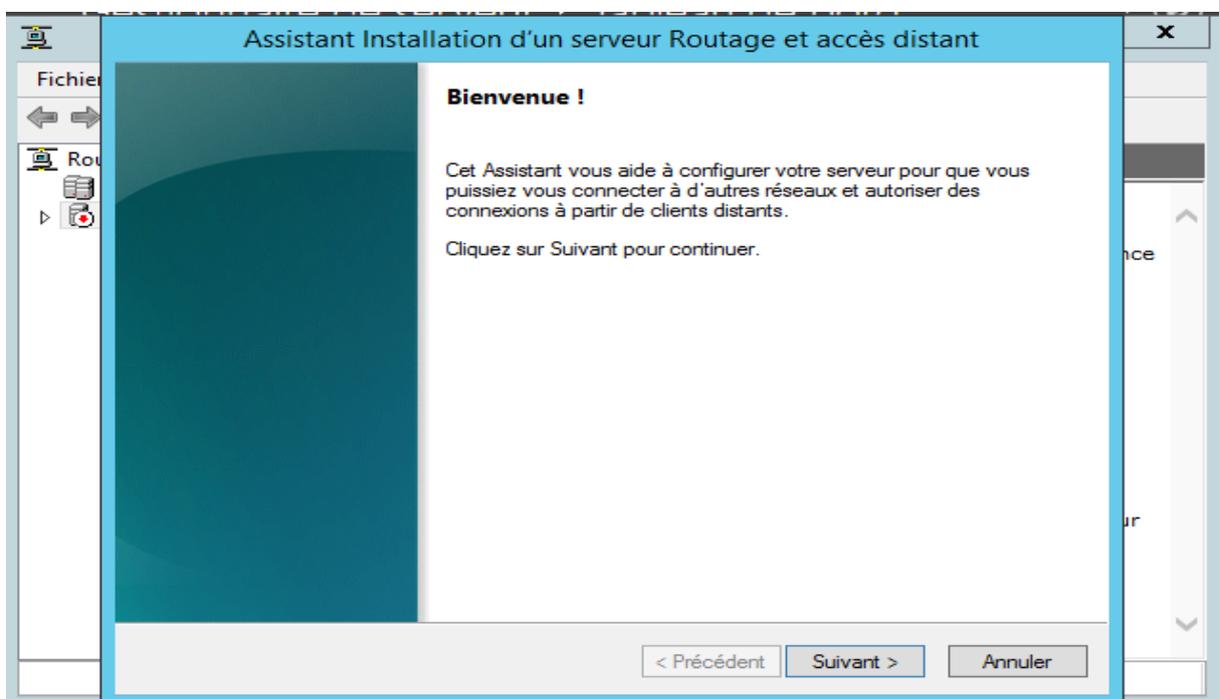


Ensuite, une nouvelle fenêtre s'ouvre. Nous allons faire un clique-droit sur le serveur local puis sélectionné « Configurer et activer le routage et l'accès à distance ».

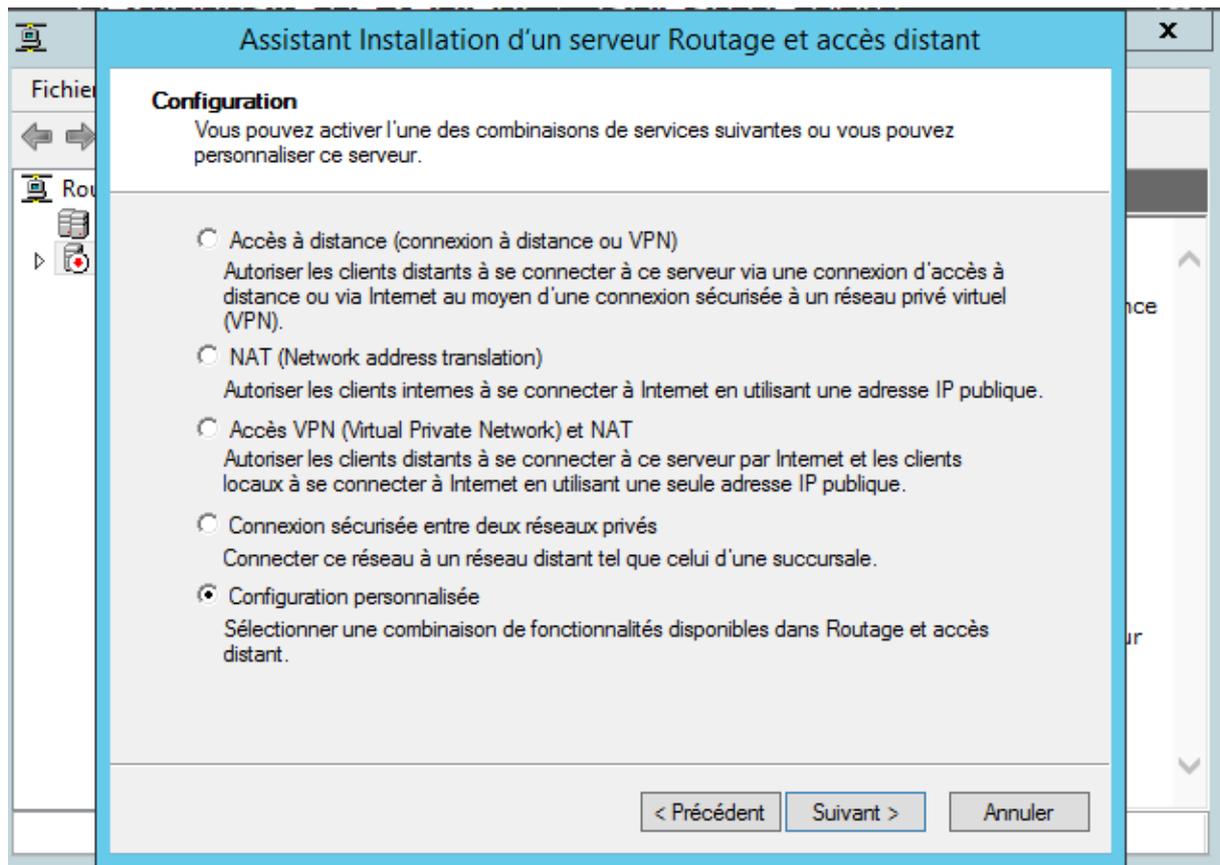




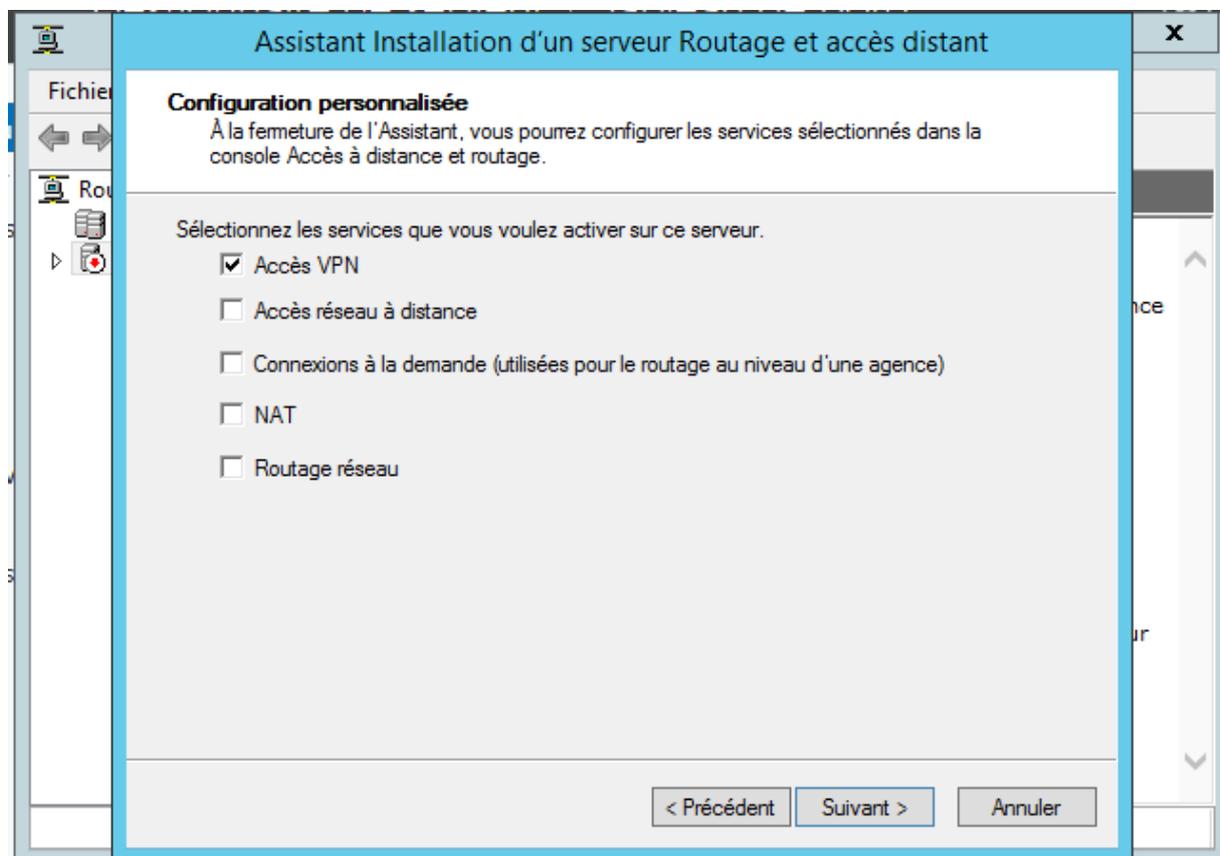
Un assistant d'installation se met en marche. Nous allons donc suivre ses instructions et cliquer sur « Suivant ».



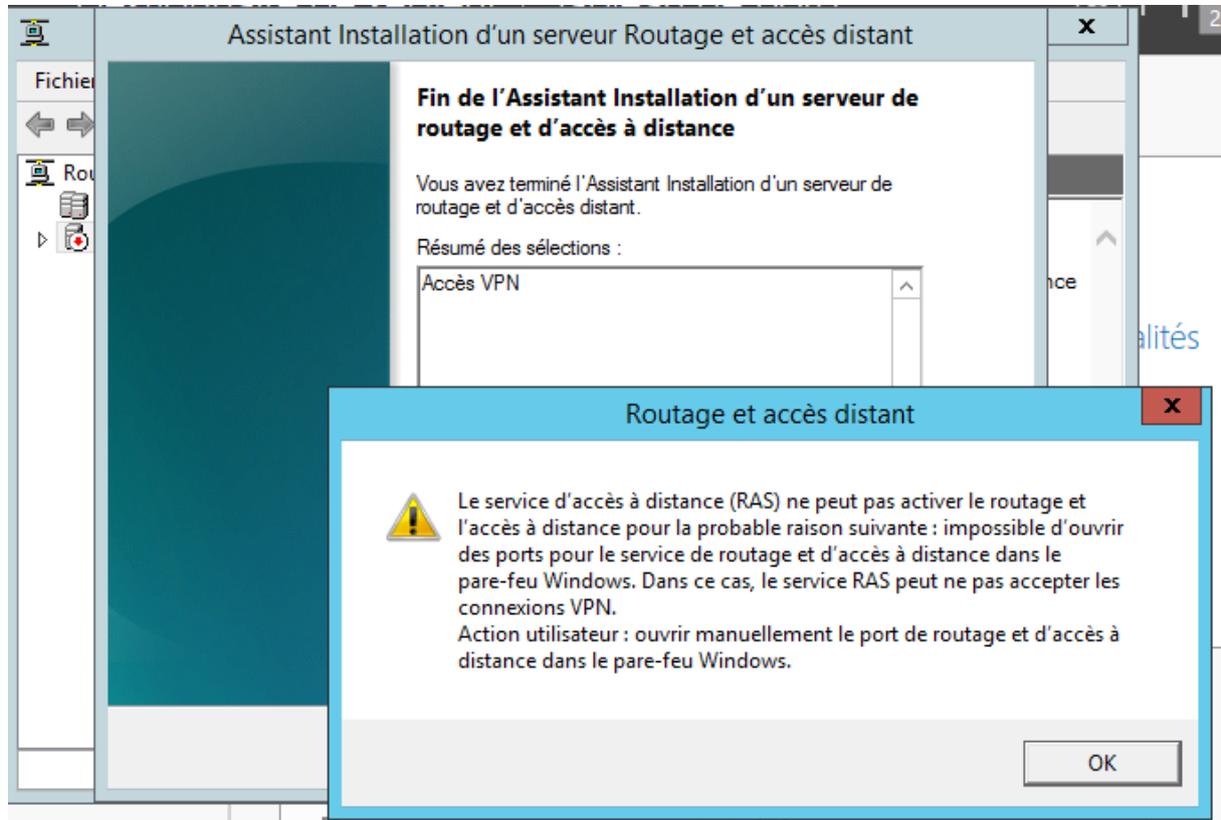
Sélectionnons une « Configuration personnalisée » et cliquons sur « Suivant ».



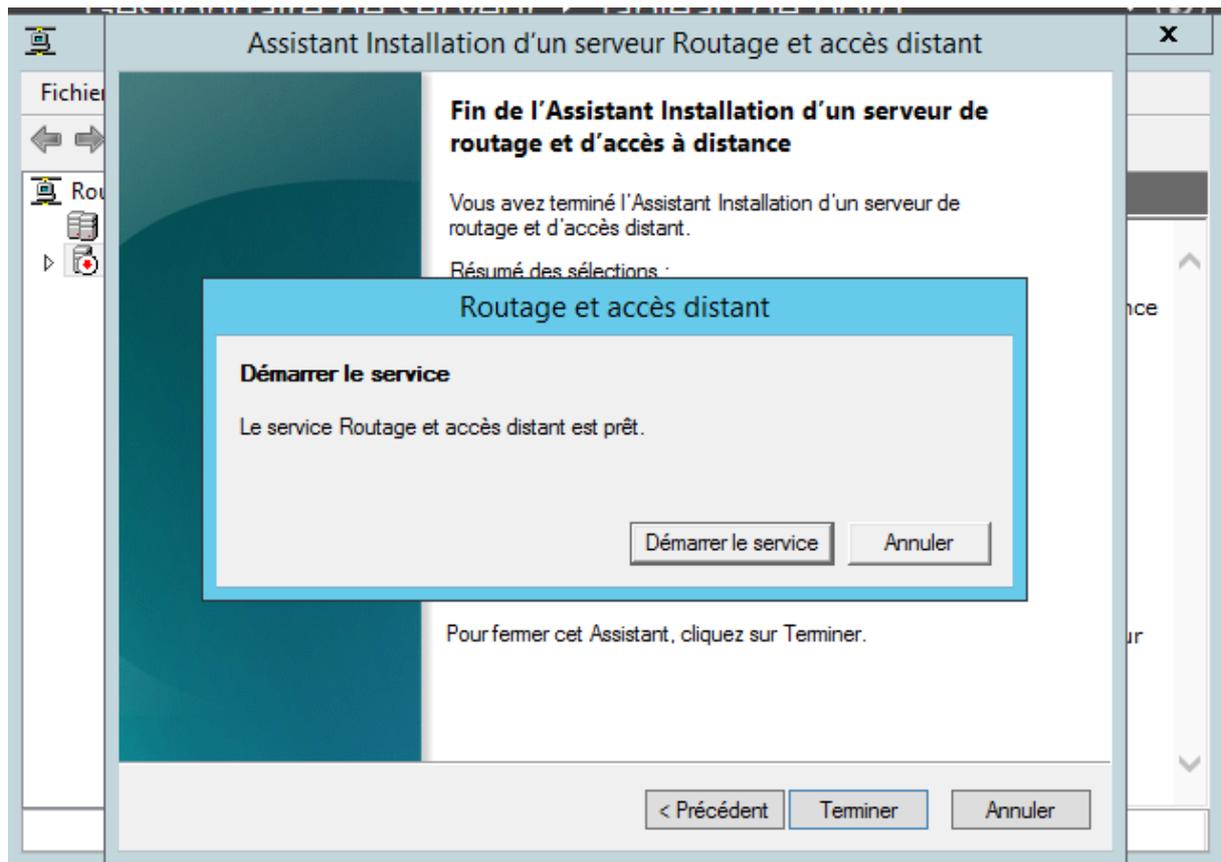
Cochons uniquement « Accès VPN » et cliquons sur « Suivant ».



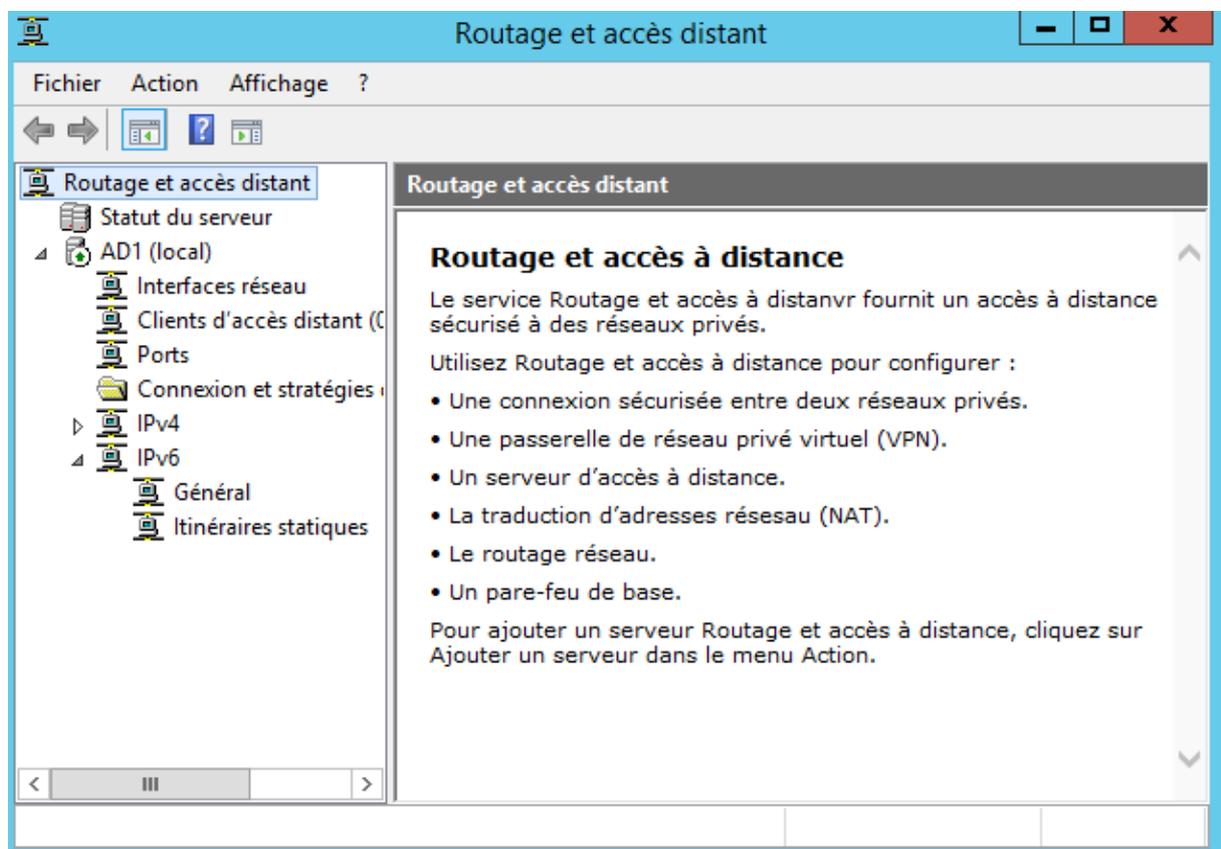
Après avoir cliqué sur « Terminer », une fenêtre d'avertissement apparaît nous informant que le Pare-feu bloque le port 1723, celui du VPN, et qu'il faudra donc l'autoriser à s'ouvrir. Nous nous en occuperons plus tard. Cliquons sur « OK ».



Nous pouvons maintenant cliquer sur « Démarrer le service ».



Le VPN est désormais opérationnel. Nous pouvons fermer cette fenêtre.

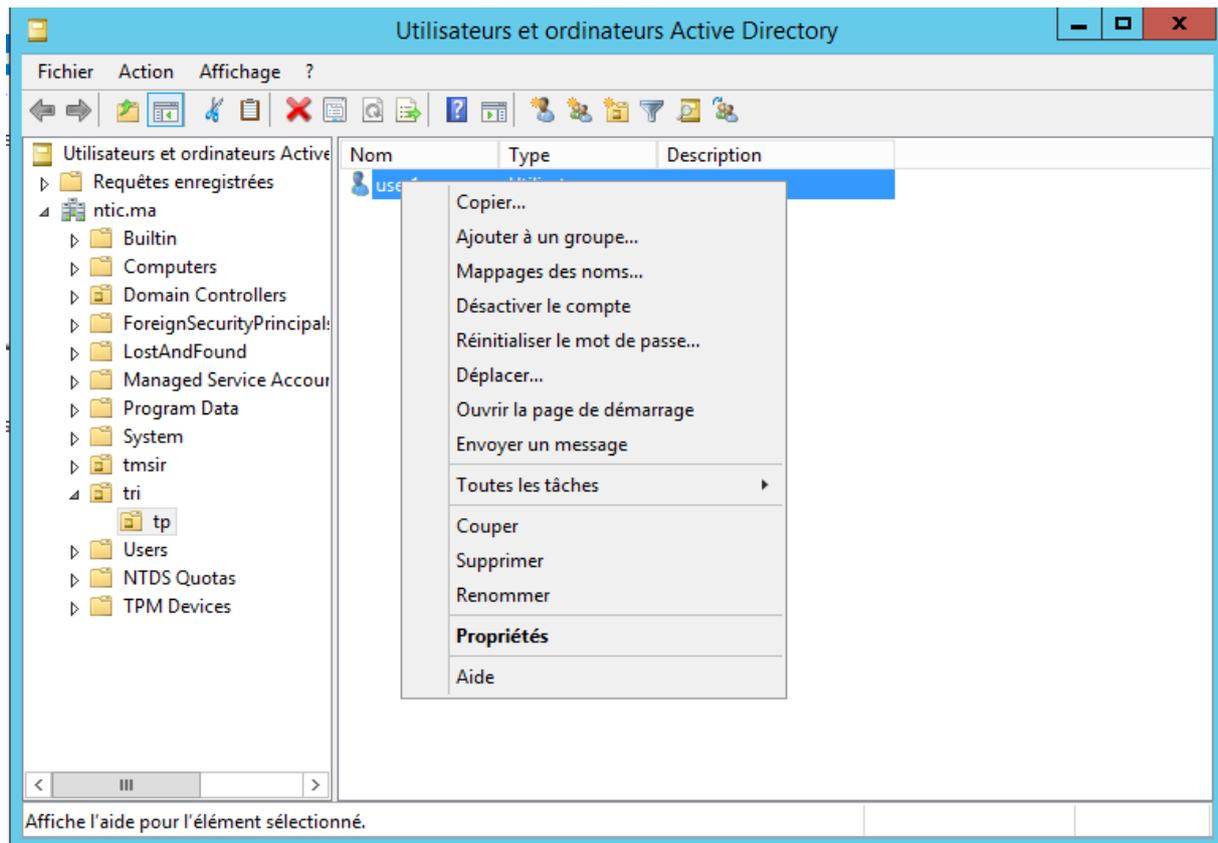


5. Accès utilisateurs

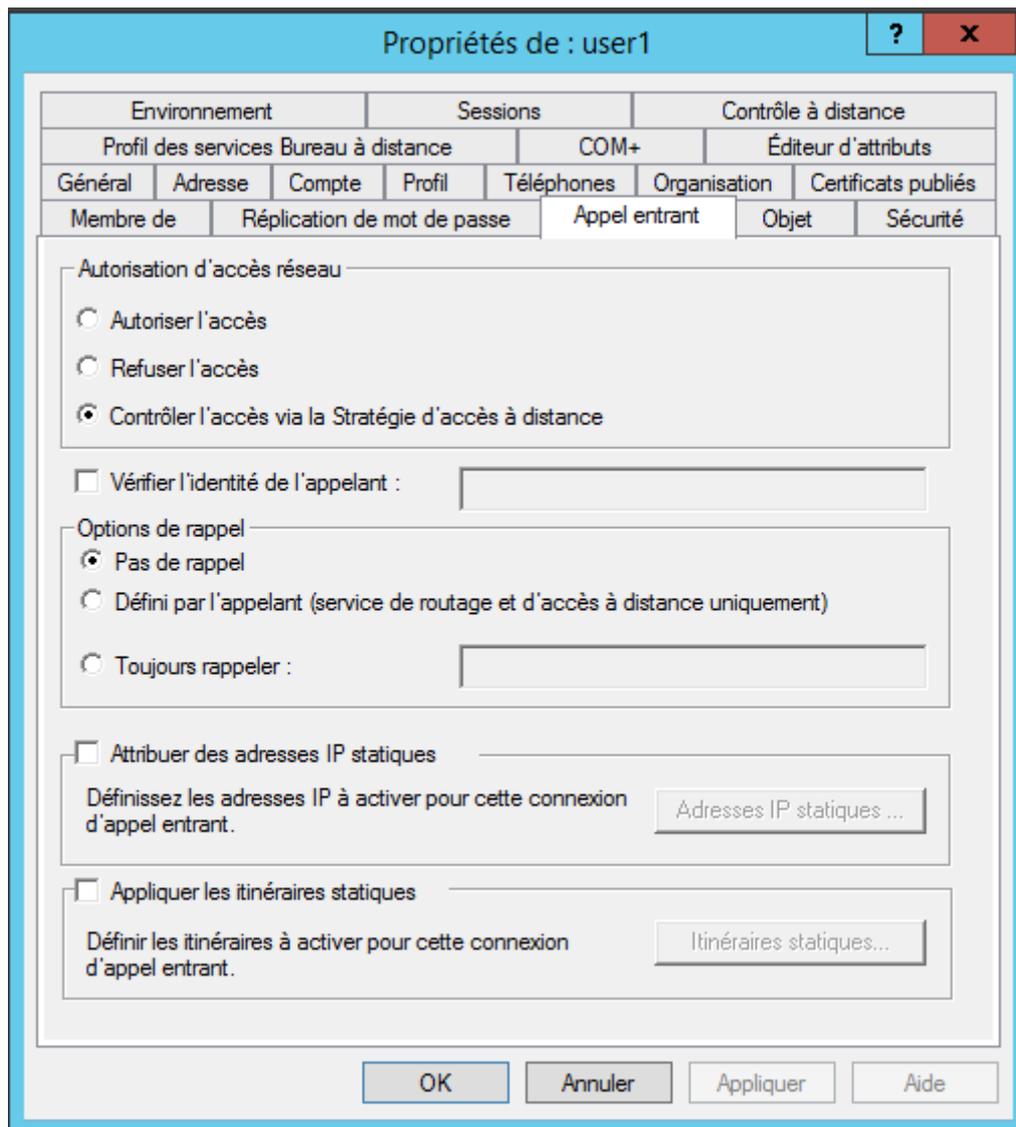
Dans les outils du serveur, cliquer sur « Utilisateurs et ordinateurs Active Directory ».

Prenons comme exemple l'utilisateur « user1 »

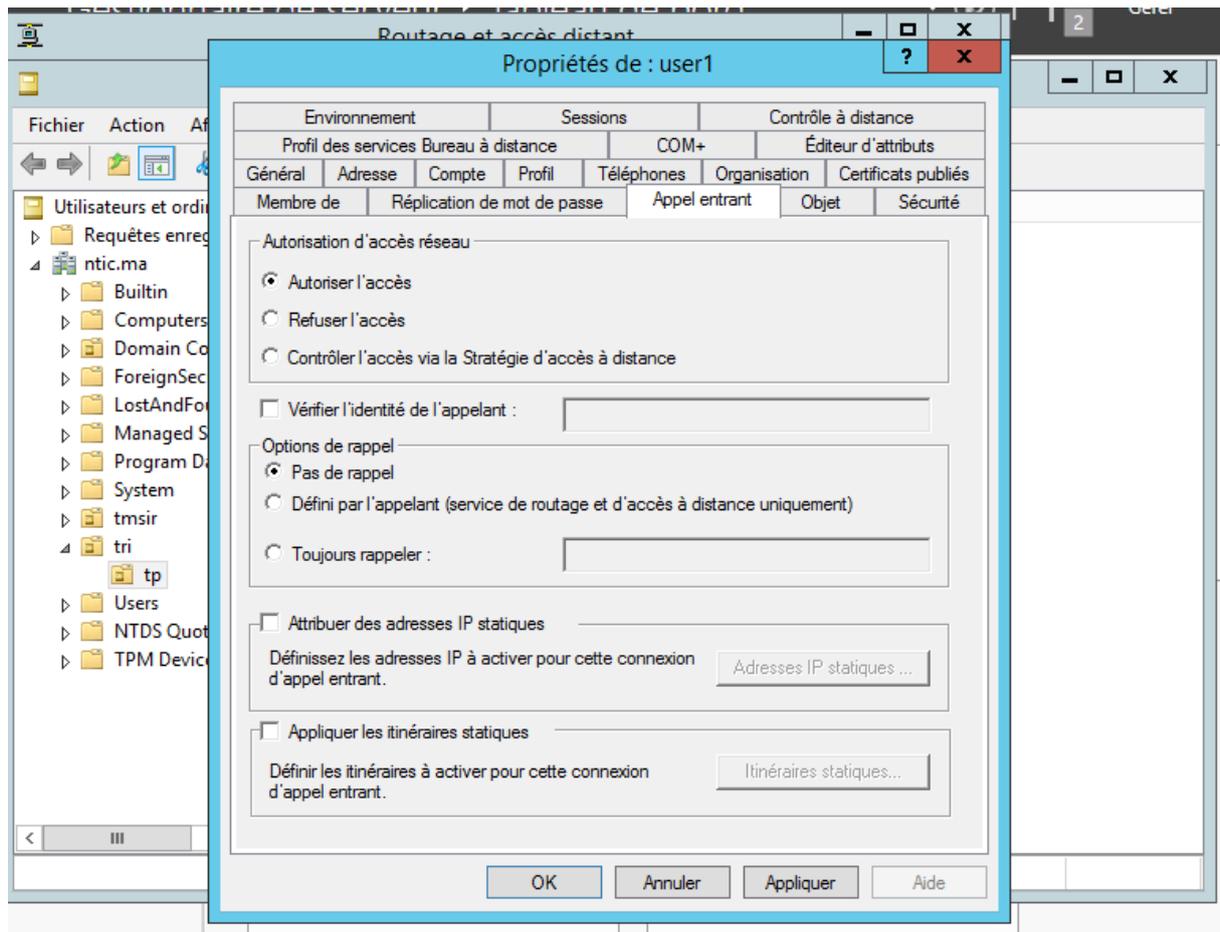
Faisons un clique-droit sur l'utilisateur et cliquons sur « Propriétés ».



Une nouvelle fenêtre s'ouvre, allons dans l'onglet « Appel entrant ».

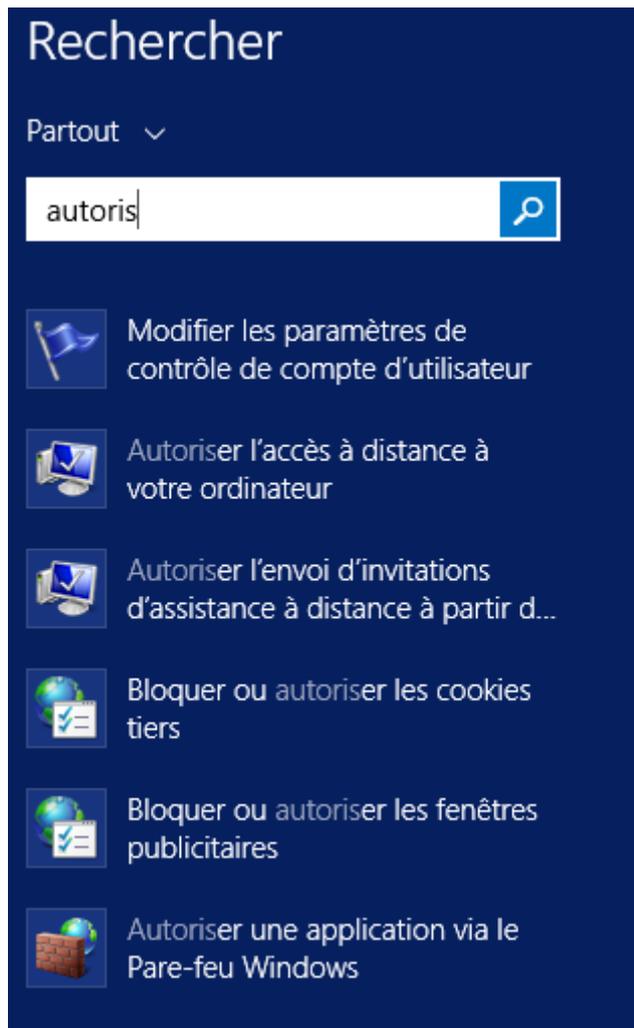


Une fois dans cet onglet, sélectionnons « Autoriser l'accès » dans l'autorisation d'accès réseau. Appliquons les modifications et cliquons sur « OK ». L'utilisateur est maintenant autorisé à se connecter au VPN.

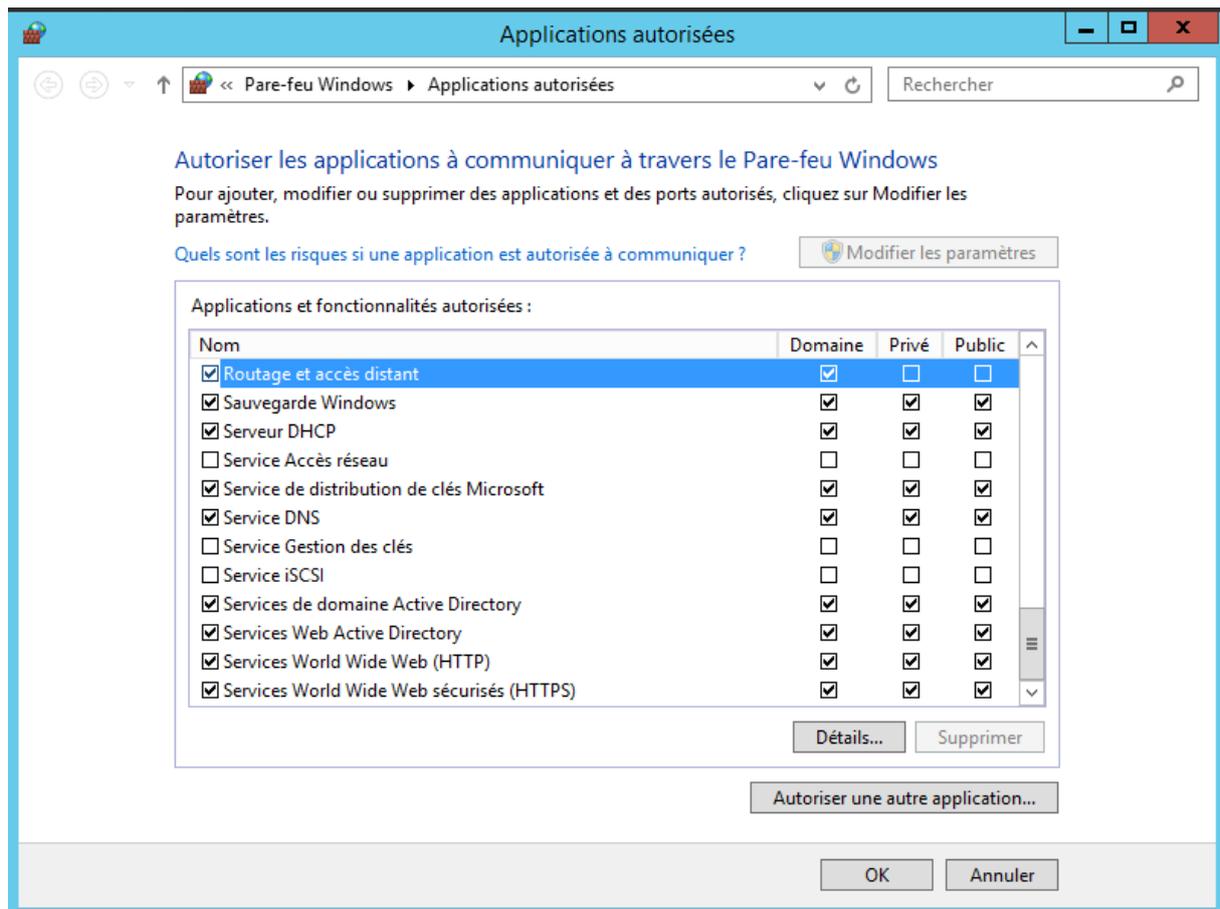


6. Autorisation du Pare-Feu

Nous allons maintenant autoriser l'accès au VPN dans le pare-feu de Windows Server. Cherchons donc « Autoriser une application via le Pare-feu Windows ».



Une fenêtre apparaît. Cherchons « Routage et accès distant » et cochons toutes les cases afin d'autoriser tout utilisateur du serveur à se connecter au VPN. Cliquons sur « OK » puis fermons la fenêtre.



Nous allons maintenant autoriser le port 1723 à s'ouvrir. Tout d'abord faisons un clique-droit sur l'icône du réseau et ouvrons le « Centre Réseau et partage ».

7. Connexion au tunnel

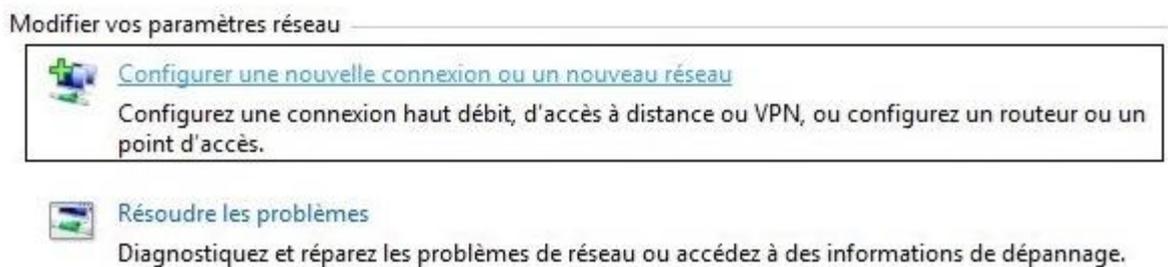
Nous nous trouvons maintenant sur l'ordinateur de l'utilisateur que nous avons pris comme exemple tout à l'heure.

User1 souhaite se connecter au serveur de son entreprise depuis chez lui. Il possède une connexion à Internet, il va donc pouvoir passer par le VPN.

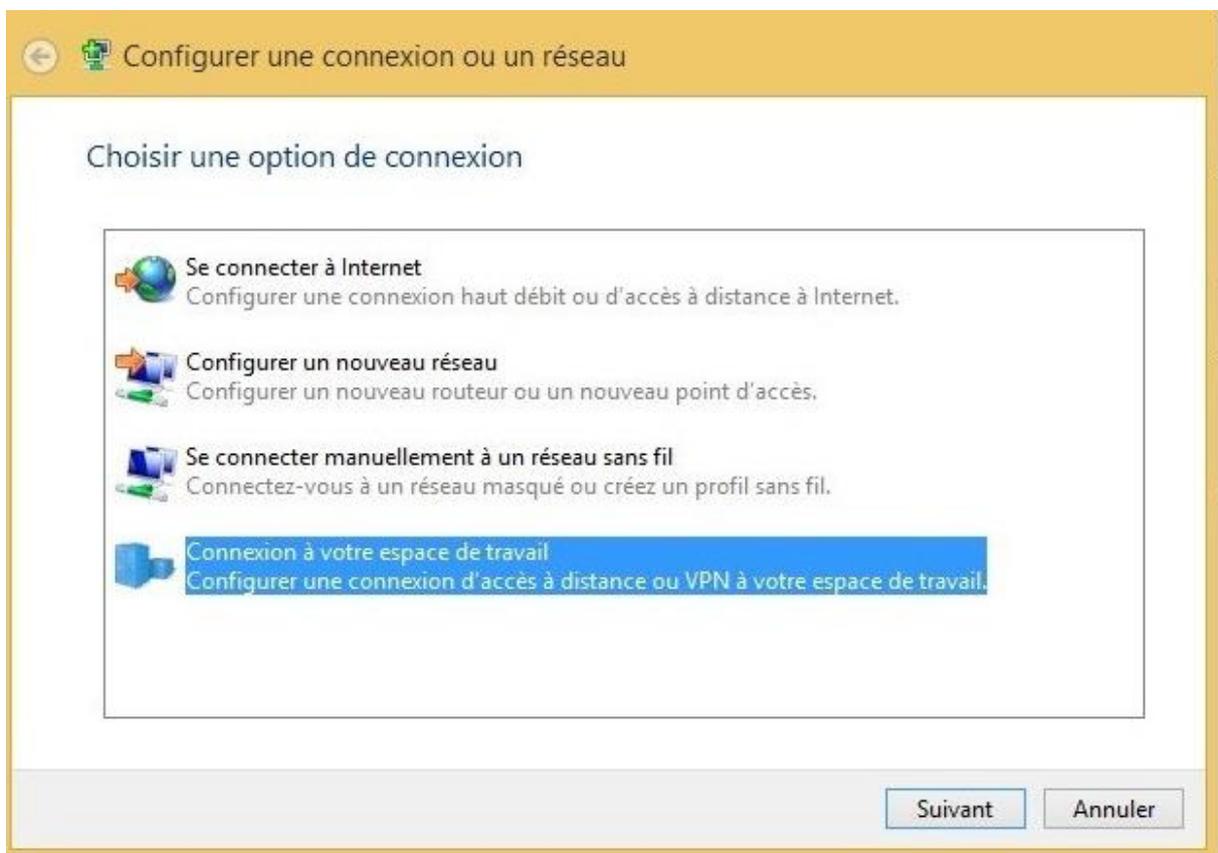
Tout d'abord faisons un clique-droit sur l'icône du réseau et ouvrons le « Centre Réseau et partage ».



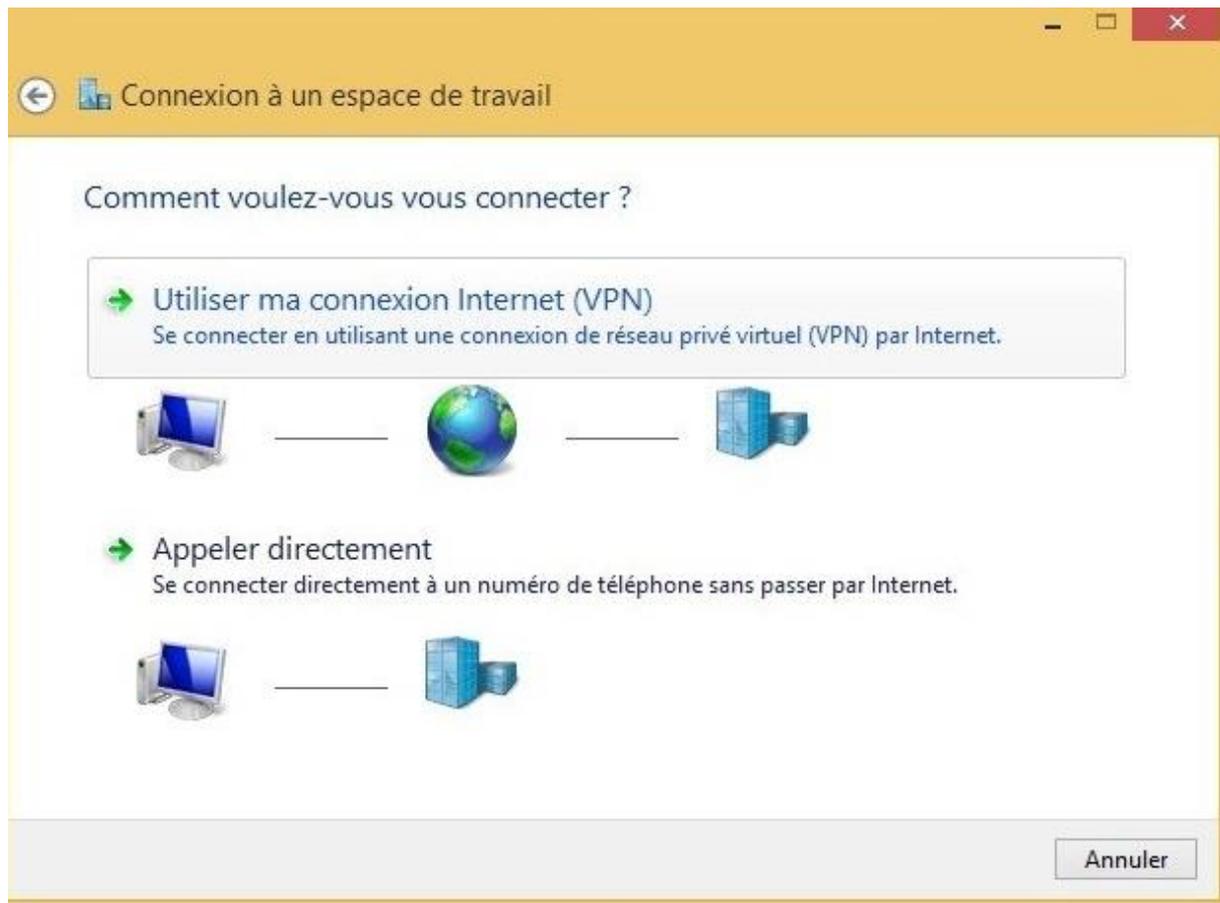
Cliquer ensuite sur « Configurer une nouvelle connexion ou un nouveau réseau » afin de créer le tunnel entre le serveur et l'ordinateur.



Choisir « Connexion à votre espace de travail » puis cliquer sur « Suivant ».



Cliquer sur « Utiliser ma connexion Internet (VPN) ».



Une nouvelle fenêtre s'ouvre et vous demande l'adresse Internet ou l'IP du serveur auquel nous voulons nous connecter. Nous pouvons également renommer le nom de la connexion.

Connexion à un espace de travail

Entrez l'adresse Internet à laquelle vous souhaitez vous connecter

Votre administrateur réseau peut vous fournir cette adresse.

Adresse Internet :

Nom de la destination :

Utiliser une carte à puce

Mémoriser mes informations d'identification

Autoriser d'autres personnes à utiliser cette connexion
Cette option permet à toute personne disposant d'un accès à cet ordinateur d'utiliser cette connexion.

8. Référence

<https://www.supinfo.com/articles/single/1165-creation-vpn-windows-server-2012-r2>

<https://www.supinfo.com/articles/single/557>