Windows Server

Service VPN

Morgan bissey

Date de dernière modification : 06/05/24 Version : 1.2

Sommaire

page

2 Introduction

2.1 Présentation de Windows Server

Windows Server est un système d'exploitation développé par Microsoft pour prendre en charge la gestion au niveau de l'entreprise, le stockage des données, les applications et les communications. Malgré le fait qu'il partage une partie de son code avec les systèmes d'exploitation Windows standards, Windows Server a pour but de gérer une multitude d'appareils, de réseaux et de service via un seul serveur. En effet, si l'on compare Windows 10 à son équivalent Windows Server (WS2019), ce dernier supporte des configurations plus puissantes (allant jusqu'à 24To de RAM), peut être configuré sans interface graphique, et offre de nombreux outils et services de gestion qui ne sont pas disponibles dans les autres systèmes d'exploitation Microsoft. Enfin, la position dominante de Microsoft dans le marché des OS fait que Windows Server propose généralement une excellente compatibilité avec les différents softwares et hardwares utilisés par les entreprises.

2.2 Services Essentiels

2.2.1 Gestionnaire de Serveur

Le gestionnaire de serveur est l'interface principale de Windows Server. Ce programme sert de tableau de bord et permet de rapidement vérifier le bon fonctionnement des différents services ainsi que d'apporter des modifications aux paramètres du serveur.

2.2.2 Assistant Ajout de Rôles et de Fonctionnalités

Ce wizard permet d'installer des rôles et des fonctionnalités à Windows Server à travers une interface graphique. Il suffit de choisir le service à installer dans la liste puis de procéder à l'installation. C'est grâce à cet outil que nous pourrons installer notre service VPN durant le TP.

2.2.3 Routage et Accès Distant

Ce service permet de mettre en place et de configurer des accès distants à des réseaux privés. A travers son interface graphique, il est possible de modifier nos paramètres d'accès à distance ainsi que d'ajouter d'autres serveurs.

2.2.4 Gestion de l 'Ordinateur

Ce service rassemble de nombreux outils administratifs et permet aux utilisateurs de paramètres une multitude de services au même endroit. En effet, Gestion de l'ordinateur permet d'accéder rapidement à de nombreux outils tels que Event Viewer, Gestionnaire de Périphériques et Gestionnaire des Tâches sans avoir besoin d'ouvrir chaque service individuellement.

2.2.5 Pare-feu Windows Defender

Le pare-feu Windows Defender est le firewall par défaut de Windows Server. Il sert à filtrer les communications entre notre serveur et les autres réseaux. Son interface permet de créer, modifier et supprimer les règles de trafic entrant et sortant. Ces règles peuvent être paramétrées pour autoriser ou bloquer la connexion entre un programme ou un port spécifique et un réseau externe.

3 Qu'est-ce qu'un VPN ?

3.1 Définition VPN

Un VPN ou Virtual Private Network est un outil réseau qui permet à une machine de se connecter à un réseau distant à travers un tunnel privé. En réalité, ce tunnel est un réseau privé qui permet aux différents appareils autorisés de communiquer entre eux de façon sécurisée.

Un VPN redirige les données à travers un serveur distant, en les chiffrant au passage. En général, lorsque l'on accède à un site Web, notre FAI (fournisseur d'accès Internet) reçoit la demande et nous redirige vers notre destination. Mais lorsque l'on se connecte à un VPN, ce dernier redirige les données Internet à travers un serveur distant avant de les envoyer à notre destination.

Le VPN permet donc de masquer les données. Le chiffrement est important lorsque l'on souhaite protéger nos données et minimiser notre empreinte en ligne.

En se connectant à un VPN, l'adresse IP de notre machine est masquée. En effet, une nouvelle adresse IP appartement au serveur VPN est utilisée ce qui permet un certain niveau d'anonymité. Cela rend donc la navigation en ligne plus sécurisée et garantit une confidentialité accrue.

Ainsi, cet outil peut être utile dans de multiples cas de figure, mais généralement un VPN sert à deux choses :

- Se connecter à un réseau distant pour pouvoir accéder à ses ressources de façon relativement sécurisée
- Modifier ou dissimuler l'adresse IP d'une machine, lorsqu'elle se connecte à internet ou n'importe quel autre réseau

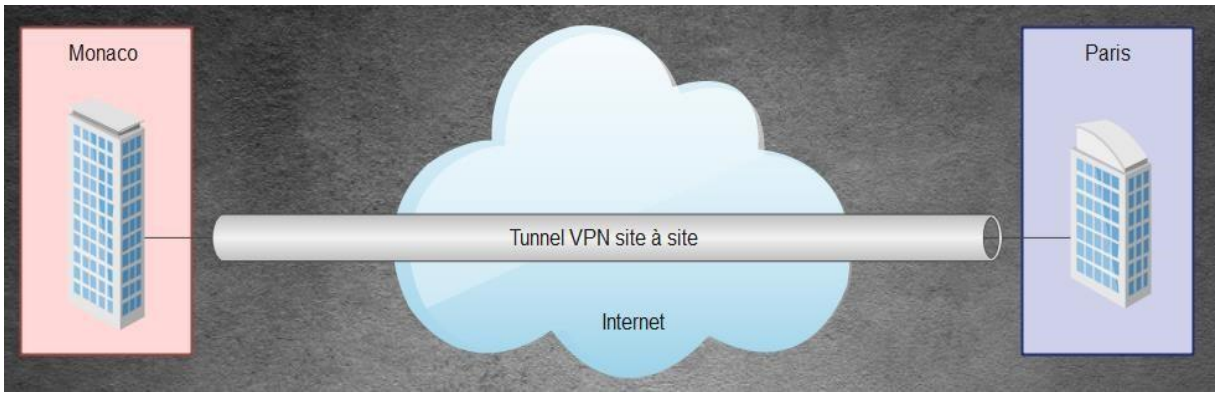
3.2 Service VPN Windows Server

Windows Server propose par défaut un service VPN. Ce dernier doit cependant être installé à travers l'interface Rôles et fonctionnalités avant de pouvoir être utilisé. Cet outil VPN fait parti du système d'Accès à Distance de Windows Server qui permet aux utilisateurs distants de se connecter de façon sécurisée au réseau du serveur et d'accéder aux ressources hébergées sur ce dernier. Ces fonctionnalités sont disponibles sur tous les systèmes d'exploitation Windows Server depuis WS2012.

Le VPN Remote Access de Windows Server peut être utilisé de deux façons différentes : pour mettre en place un réseau VPN site à site, ou pour mettre en place un réseau VPN client à site.

Le VPN site à site :

Un VPN site à site relie deux sites distants à travers une infrastructure réseau publique, par exemple en utilisant le réseau Internet. Si deux sites d'une même entreprise souhaitent communiquer entre eux tout en protégeant leurs échanges, ils peuvent alors faire recours à un VPN. D'un point de vue réseau, ces sites seront donc virtuellement interconnectés par un routeur géant : Internet. Dans ce cas, les échanges sont chiffrés pour empêcher que l'interception de données ne compromette la sécurité. On parle alors de tunnel VPN et deux équipements intermédiaires (un de chaque côté) appelés terminaisons VPN. Ces derniers assurent le bon fonctionnement du tunnel VPN ; il peut s'agir d'un routeur ou encore d'un firewall.

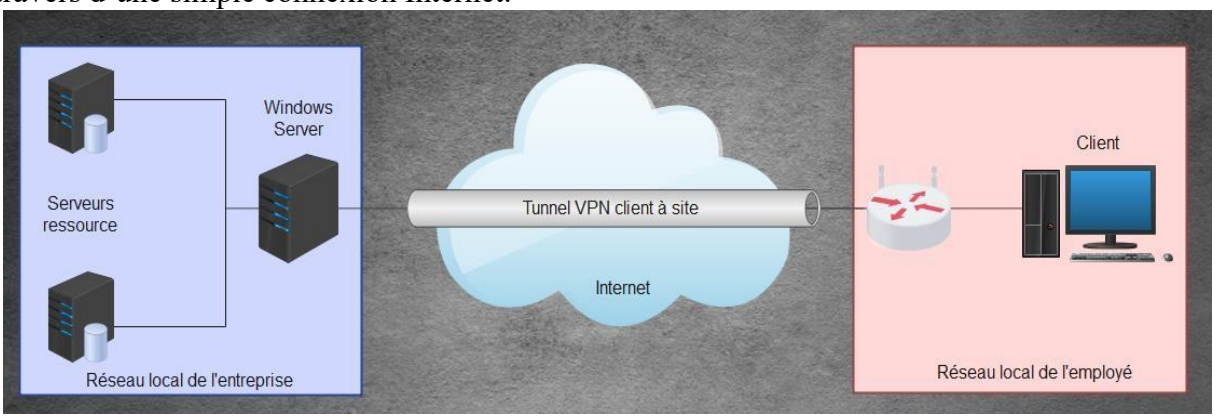


Le VPN MPLS (Multiprotocol Label Switching) est un type de réseau privé virtuel (VPN) basé sur une infrastructure MLPS. Il utilise des étiquettes pour acheminer les données sur le réseau, permettant ainsi une communication sécurisée et fiable entre les sites distants d'une entreprise ou d'une organisation. Avec le MPLS, la première fois qu'un paquet entre dans le réseau, il est affecté à une classe d'équivalence de transmission (FEC : Forwarding equivalence class) spécifique. Elle est indiquée en ajoutant une courte séquence de bits (l'étiquette) au paquet.

Chaque routeur du réseau dispose d'un tableau indiquant comment traiter les paquets d'un type de FEC spécifique. Ainsi, lorsque le paquet est entré dans le réseau, les routeurs n'ont pas besoin d'effectuer une analyse d'en-tête. Les routeurs suivants utilisent plutôt l'étiquette comme un index dans une table qui leur fournit un nouveau FEC pour ce paquet. Le VPN MPLS est également connu pour sa fiabilité, car il utilise une infrastructure hautement redondante pour acheminer les données sur le réseau. Les informations circulent par le biais de plusieurs liens de connexion, ce qui rend le réseau plus stable et moins susceptible aux interruptions.

Le VPN client à site :

Les VPN client à site ont pour but de fournir à un poste situé à l'extérieur de l'entreprise (sur un réseau partenaire ou domestique) un accès sécurisé au réseau de l'entreprise ; de cette manière le client ou l'employé peut obtenir un accès réseau aux ressources de l'entreprise au travers d'une simple connexion Internet.



Ce type de service est de plus en plus utilisé car il offre la possibilité aux employés qui sont souvent en déplacement d'accéder directement aux ressources nécessaires. Il est également utile

lorsque l'entreprise désire offrir des possibilités de télétravail à ses employés. La mise en place d'une telle solution nécessite de faire l'inventaire des exigences de sécurité car elle fournit un accès réseau à l'entreprise depuis des postes et de réseaux qui peuvent ne pas être considérés comme sécurisés.

La principale différence entre un VPN site à site et un VPN client à site est que le premier relie deux réseaux locaux distincts, tandis que le second permet à un individu de se connecter à un réseau privé virtuel à partir d'un appareil distant.

3.3 Protocoles de Tunneling VPN

Pour assurer le bon paramétrage d'une infrastructure d'accès à distance par VPN, il est essentiel de développer une certaine compréhension des protocoles de tunneling proposés. Cela nous permettra par la suite de pouvoir choisir le protocole le plus adapté à notre situation.

Windows Server offre une remarquable flexibilité en termes de configuration du service VPN en nous proposant un choix varié de protocoles de tunneling et d'authentification. Nous allons donc étudier le fonctionnement de ces protocoles pour déterminer dans quels scénarios ils peuvent être mis en place.

3.3.1 PPTP

PPTP : Point to Point Tunneling Protocol, est l'un des plus anciens protocoles de Microsoft. Il est également très rapide et simple à configurer. PPTP utilise le port TCP 1723, pour la communication qui utilise le protocole GRE (Generic Routing Encapsulation) permettant d'envelopper des paquets de données à l'intérieur de paquets de données secondaires afin d'établir une connexion réseau direct point à point.

Avantages :

- Configuration simple
- Compatible avec la plupart des systèmes d'exploitation
- Bonne vitesse de connexion

Inconvénients :

- Limite chiffrement de 128 bits (chiffrement des données n'est pas recommandé)
- Pas de garantit d'intégrité (ne vérifie pas si les données n'ont pas été modifiées en transit)
- Problèmes de performances sur les réseaux instables

3.3.2 SSTP

SSTP : Secure Socket Tunneling Protocol, est un protocole créé par Microsoft qui transporte le trafic VPN en l'encapsulant via un lien SSL (Secure Sockets Laye) à travers le port HTTPS

(HyperText Transfer Protocol Secure). Ce port TCP 443 est rarement bloqué car la plupart des navigations Web ne fonctionneraient pas sans lui. Par conséquent, non seulement SSTP passe à travers 99% des pare-feux, mais il garantit également que votre VPN est chiffré.

Avantages :

- Facile à utiliser
- Peut contourner la plupart des pare-feux Haut niveau de sécurité
- Intégré à l'environnent Windows
- Peut supporter une large gamme d'algorithmes de chiffrement

Inconvénient :

- Détenue et maintenue à 100% par Microsoft
- Compliqué à mettre en place sur les plateformes autres que Windows

3.3.3 L2TP

L2TP : Layer 2 Tunneling Protocol, est un protocole qui ne fournit aucun chiffrement par luimême. Le VPN L2TP utilise généralement un protocole d'authentification tel que IPSec (Internet Protocol Security) pour un chiffrement fort, ce qui lui donne un avantage sur les autres protocoles. Les données transmises via le protocole L2TP/IPsec utilisent les ports UDP 500, 1701, 4500. Ces données sont généralement authentifiées deux fois, ce qui ralentit les performances mais offre le plus haut niveau de sécurité.

Avantages :

- Facile à configurer (sur les systèmes exploitation Mac et Windows)
- Haut niveau de chiffrement et de sécurité
- Double encapsulation des données, ce qui signifie une double vérification des données
- Disponible non seulement sur ordinateur de bureau mais aussi sur les systèmes d'exploitation mobile

Inconvénient :

- Performances lentes en raison de la double authentification
- Certains pare-feux peuvent bloquer les ports du protocoles L2TP

3.3.4 IKEv2

IKEv2 : Internet Key Exchange version 2, est un protocole de chiffrement de requête et de réponse développé par Cisco et Microsoft. Il établit et gère l'attribut Security Association (SA), qui est utilisé pour prendre en charge une communication sécurisée entre deux entités de réseau. Il le fait dans une suite d'authentification, généralement IPsec qui permet d'assurer un trafic sécurisé. Il permet aux périphériques VPN situés aux deux extrémités du tunnel de chiffrer et de déchiffrer les paquets à l'aide des clés pré-partagées, de protocoles d'authentification (EAP) ou de signatures numériques.
Le chiffrement et le déchiffrement utilisent l'authentification asymétrique, ce qui signifie que les deux extrémités du tunnel n'ont pas besoin de s'entendre sur une seule méthode d'authentification.

Avantages :

- Protocole hautement sécurisé
- Connexion stable et fiable
- L'un des protocoles le plus rapide

Inconvénient :

- Prend en charge un nombre limité de plateformes
- Peut être bloqué par certains pare-feux

3.4 Protocoles d'Authentification VPN

3.4.1 PAP

PAP : Password Authentification Protocole, est un protocole d'authentification point à point (PPP) qui utilise un nom d'utilisateur et un mot de passe pour authentifier les utilisateurs. Ces données d'authentification ne sont cependant pas chiffrées, ce qui fait de PAP le protocole d'authentification le moins sécurisé parmi ceux proposés par Windows Server. En effet, lorsqu'un utilisateur essaye d'établir une session PPP avec un serveur, il lui envoie son nom d'utilisateur et son mot de passe en texte brut dans un paquet de requête d'authentification. Toute personne analysant les communications entre le serveur et ses utilisateurs peut donc facilement déterminer les identifiants et mots de passe de cet utilisateur.

Avantage :

- Compatible avec la plupart des OS

Inconvénient :

- Transmet les logins et mots de passe en clair

3.4.2 CHAP

CHAP : Challenge Handshake Authentication Protocol, est un protocole d'authentification point à point (PPP) qui utilise une méthode de défi-réponse pour vérifier l'identité de ses clients. Ainsi, le pair (l'authentificateur) défie l'appelant (l'authentifié) de prouver son identité. Pour ce

faire, l'appelant doit envoyer une réponse hash en utilisant MD5. Le pair résout ensuite son propre calcul et compare sa réponse avec celle envoyée par l'appelant pour déterminer si l'authentification est réussie ou non. De plus, CHAP est capable de réauthentifier ses utilisateurs de façon périodique en renvoyant des défis à un intervalle de temps paramétrable pour encore plus de sécurité.

Avantages :

- Compatible avec la plupart des OS
- Plus sécurisé que PAP

Inconvénient :

- Seule l'identité du client est vérifiée
- Ne protège pas contre les attaques man in the middle

3.4.3 MS-CHAPv2

MS-CHAPv2 : Microsoft Challenge Handshake Authentication Protocol Version 2, est un processus d'authentification mutuelle avec mot de passe chiffré à sens unique. Cette authentification mutuelle signifie que le serveur d'authentification et le client doivent vérifier leurs identités respectives avant que la connexion soit établie. Tout comme le protocole CHAP, MS-CHAPv2 utilise le principe de défi-réponse où le pair envoie un défi et l'appelant doit envoyer une réponse hash en utilisant MD5 qui est ensuite comparée à la réponse du pair. Cependant la particularité de MS-CHAPv2 est que la réponse du pair contient elle aussi un calcul hash qui est à son tour vérifié par l'appelant avant que la connexion soit autorisée.

Avantages :

- Protocole le plus utilisé pour l'authentification VPN
- Plus sécurisé que PAP et CHAP

Inconvénient :

- Ne protège pas contre les attaques man in the middle

3.4.4 EAP

EAP : Extensible Authentication Protocol, est un système comprenant plusieurs méthodes d'authentification. Contrairement aux options étudiées précédemment, EAP est bien plus qu'un simple protocole d'authentification : c'est une infrastructure permettant au serveur d'authentification et aux utilisateurs de négocier la méthode d'authentification utilisée pour établir la connexion. Par défaut, la méthode d'authentification utilisée sera EAP-TLS (Transport Layer Security), une méthode d'authentification mutuelle qui requiert un certificat d'authentification coté client. De ce fait, EAP-TLS est l'une des méthodes d'authentification les plus sécurisées proposées par EAP.

Avantages :

- Méthode d'authentification flexible
- Plus sécurisé que PAP et CHAP

Inconvénient :

- Pas aussi simple à mettre en place que PAP et CHAP

4 Mise en Place d'un Service VPN Windows Server

4.1 Présentation du TP

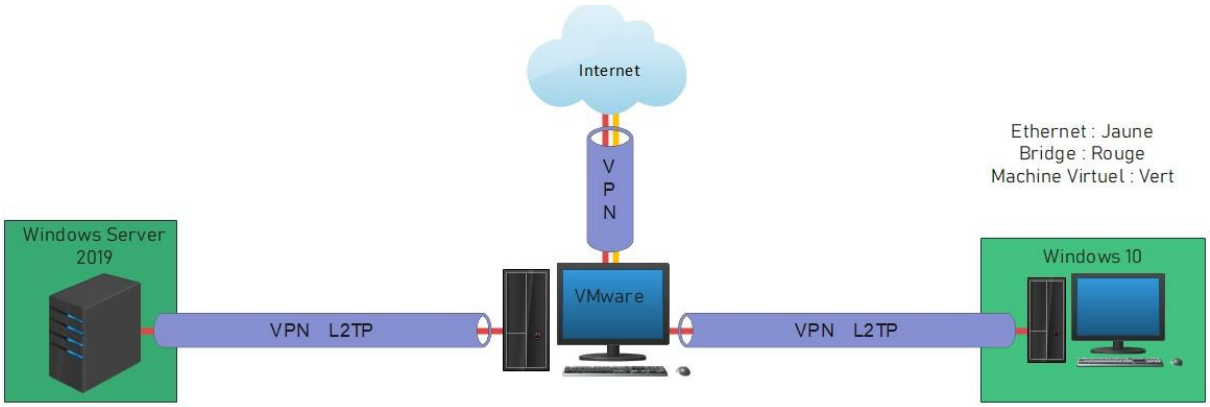
Afin de mieux comprendre le fonctionnement du service VPN sous Windows Server, nous allons maintenant détailler la mise en place d'un tunnel VPN entre un serveur et un client. Pour cette démonstration, nous avons décidé de mettre en place un VPN L2TP avec certificat depuis un Windows Server. Cette configuration nous permet d'étudier L2TP, un protocole couramment utilisé et relativement simple à mettre en place. De plus, cette configuration nous permet de mettre en place le protocole IPsec avec un certificat d'authentification pour sécuriser notre tunnel.

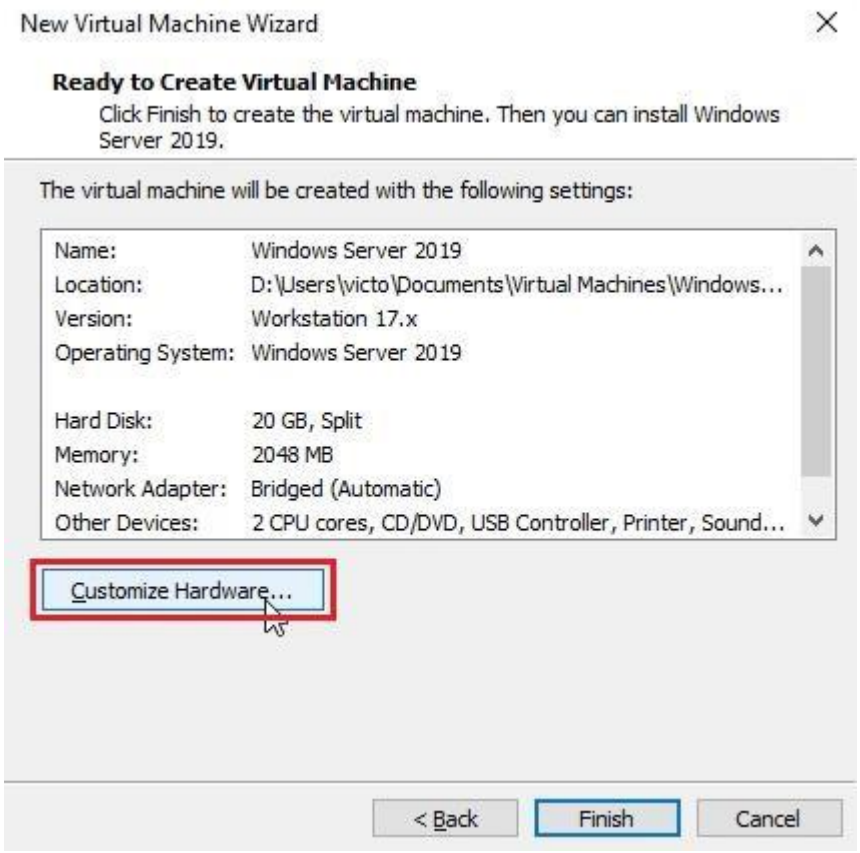
4.2 Mise en Place des Machines Virtuelles

Par souci d'efficacité, nous avons décidé de réaliser notre démonstration avec des machines virtuelles. Pour ce faire, nous allons installer Windows Server 2019 et Windows 10 version 21H2 sur VMware Workstation Pro 17.

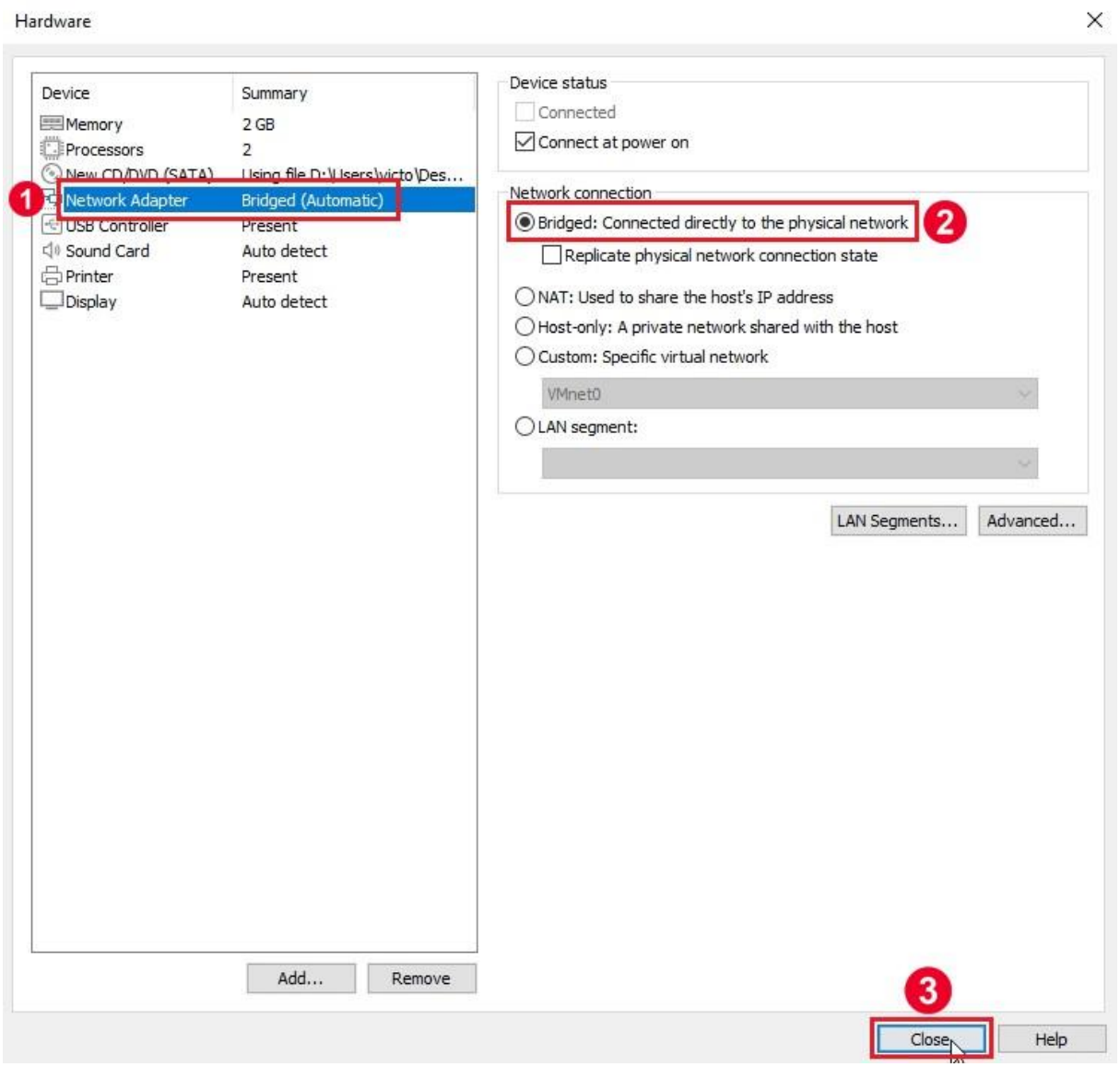
Pour assurer le bon fonctionnement de notre VPN par la suite, nous aurons besoin que nos deux machines virtuelles soient capables d'accéder à Internet et de communiquer entre elles à travers Internet. Afin d'assurer ces fonctionnalités, nous allons donc configurer nos 2 VM en mode Bridged dans VMware.

En effet, le mode de connexion Bridged de VMware assure une connexion internet aux VM puisqu'elles se greffent virtuellement sur le même réseau que la machine physique. Le schéma ci-dessous explique cette connexion, et illustre le chemin que prendra notre VPN pour atteindre chaque machine.





Pour configurer nos machines virtuelles en mode Bridged, nous allons tout d'abord réaliser une installation standard en utilisant les paramètres par défaut jusqu'à arriver à la dernière page. Sur cette page nous allons cliquer sur Customize Hardware.



C'est ici que nous allons pouvoir configurer les paramètres réseau de nos VM. Nous allons donc cliquer sur Network Adapter puis sélectionner l'option Bridged avant de fermer la page en cliquant sur Close.
Nous pouvons ensuite terminer l'installation en cliquant sur Finish.

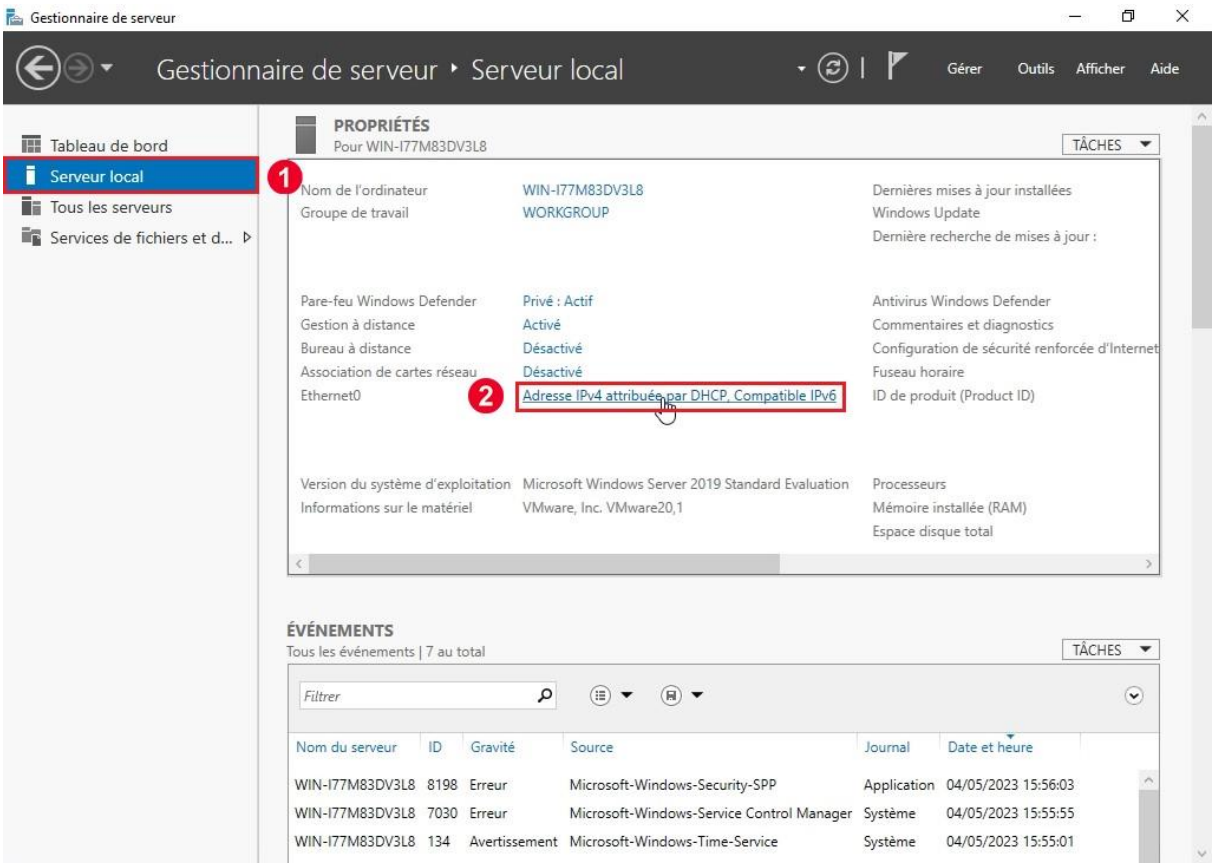
Il faudra répliquer cette configuration sur notre seconde machine virtuelle pour assurer le bon fonctionnement de notre VPN.

Une fois que nos deux machines sont installées et configurées en mode Bridge dans VMware, nous pouvons donc commencer la configuration du VPN sur Windows Server.

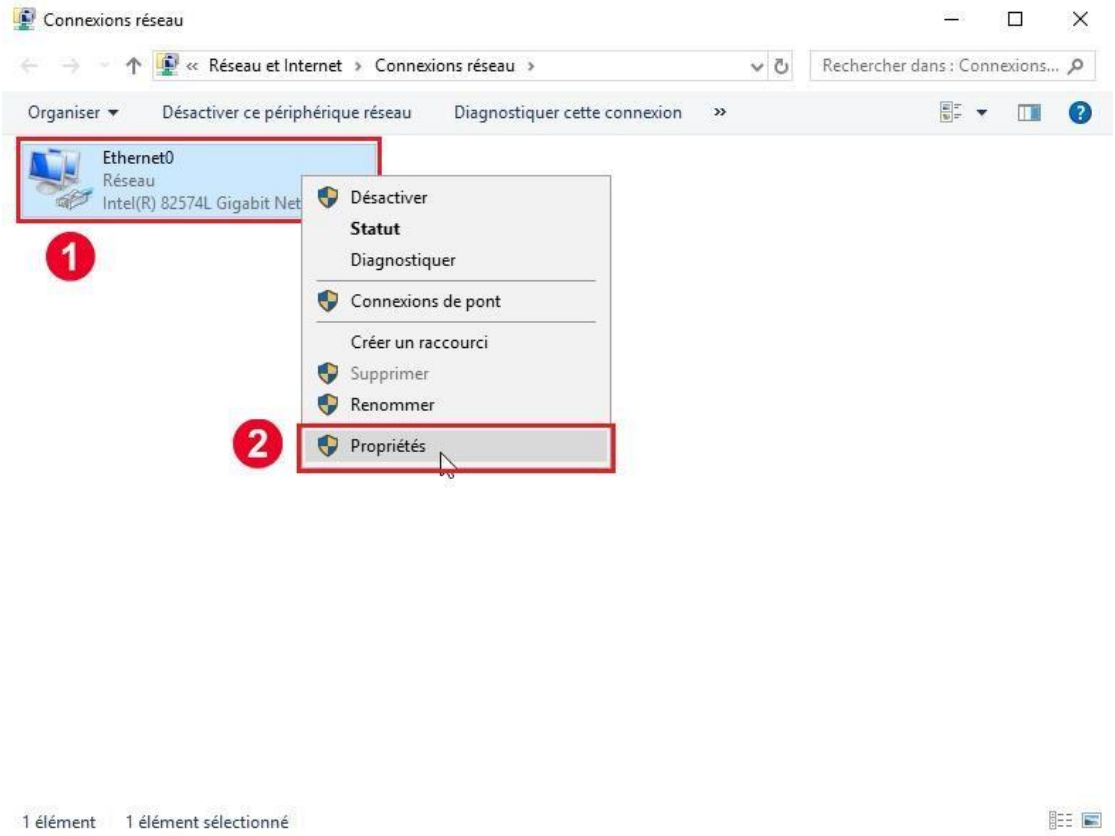
4.3 Configuration du Serveur VPN sur Windows Server

4.3.1 Adressage IP Statique

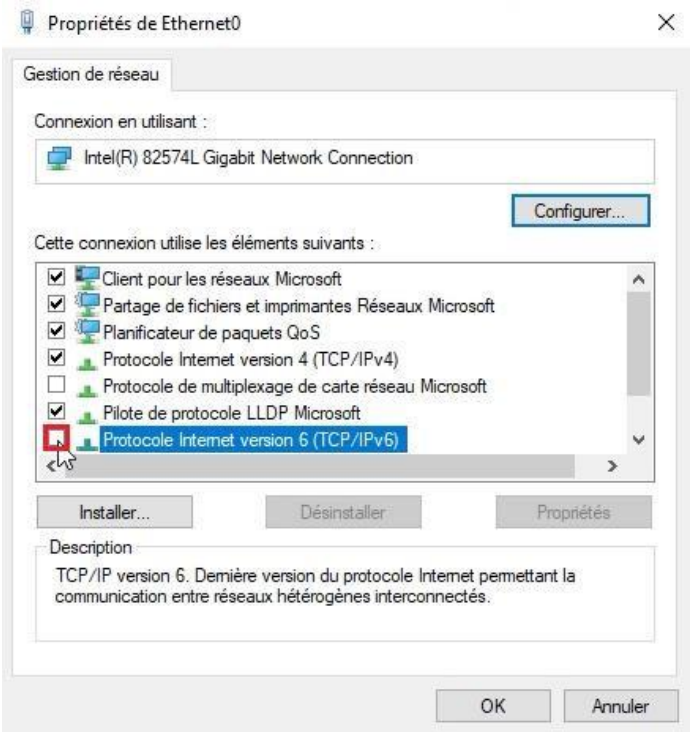
Si ce n'est déjà fait, nous vous recommandons d'assigner une adresse IPv4 statique au serveur de manière à ce qu'il soit plus facilement joignable par le client.



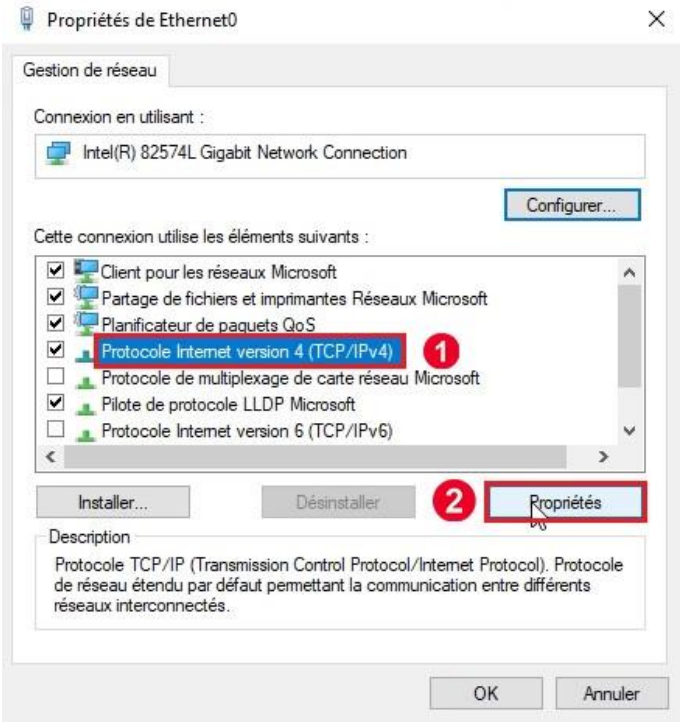
Pour ce faire, il nous suffit de nous rendre dans le gestionnaire de serveur, de cliquer à gauche sur Serveur Local, puis sur Adresse IPv4 attribuée par DHCP. (Cette page peut aussi être atteinte depuis le panneau de configuration en allant dans les options réseau.)



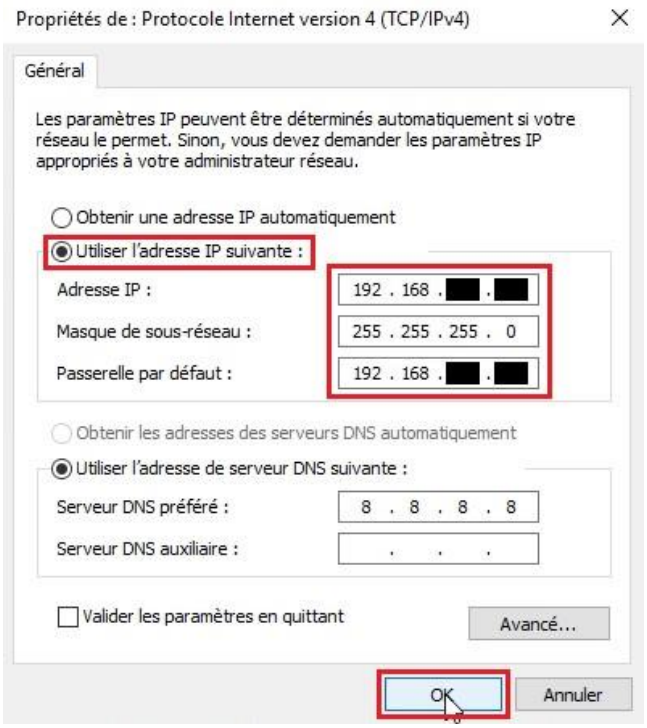
Ici, nous choisissons l'adaptateur réseau connecté à internet (Ethernet0 dans notre cas) et nous faisons un clic droit dessus pour ouvrir ses Propriétés.



Sur cette page, nous pouvons désactiver IPv6 en décochant la case Protocole internet version 6 car nous utiliserons uniquement IPv4 pour notre VPN.



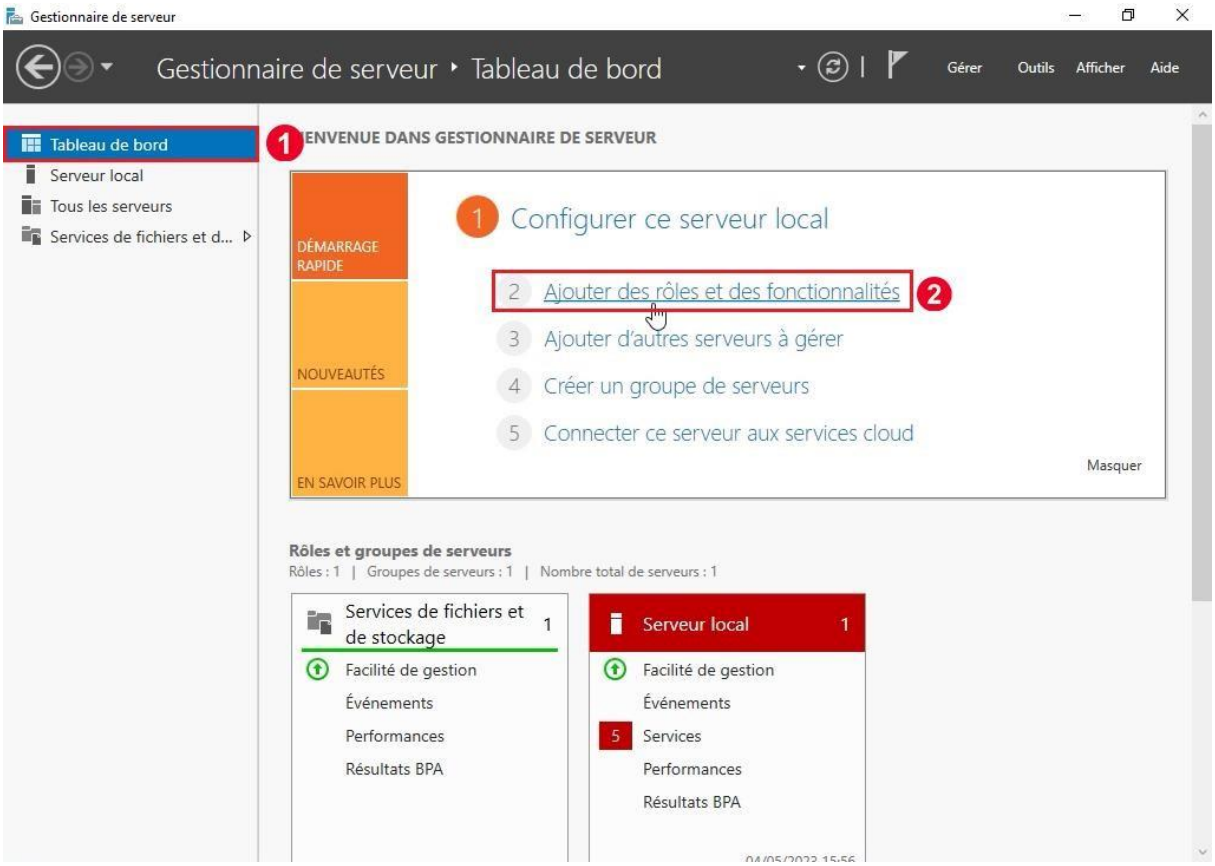
Enfin, nous pouvons sélectionner sur la ligne Protocole internet version 4 puis cliquer sur Propriétés pour passer modifier notre adresse IPv4.



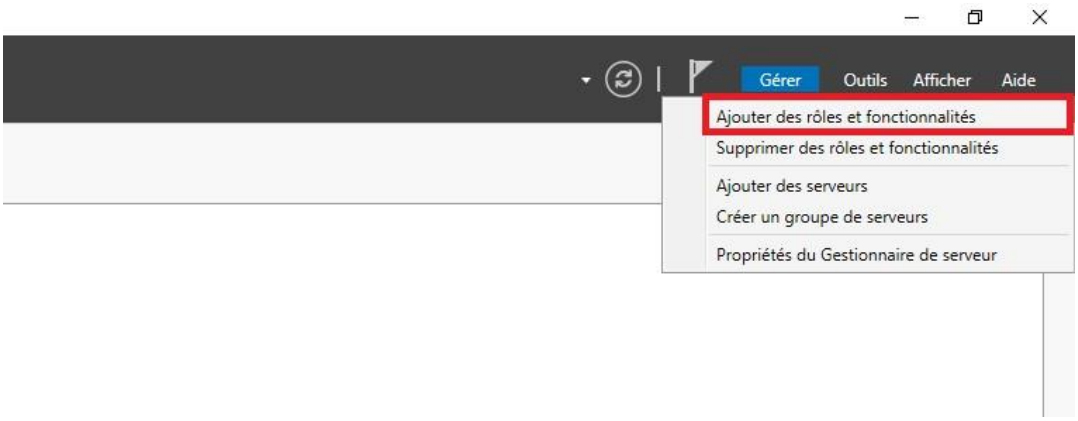
Nous pouvons maintenant cliquer sur Utiliser l'adresse IP suivante puis renseigner l'adresse IP statique désirée avec son masque de sous-réseau et sa passerelle par défaut. Nous pouvons ensuite cliquer sur OK pour confirmer nos modifications.

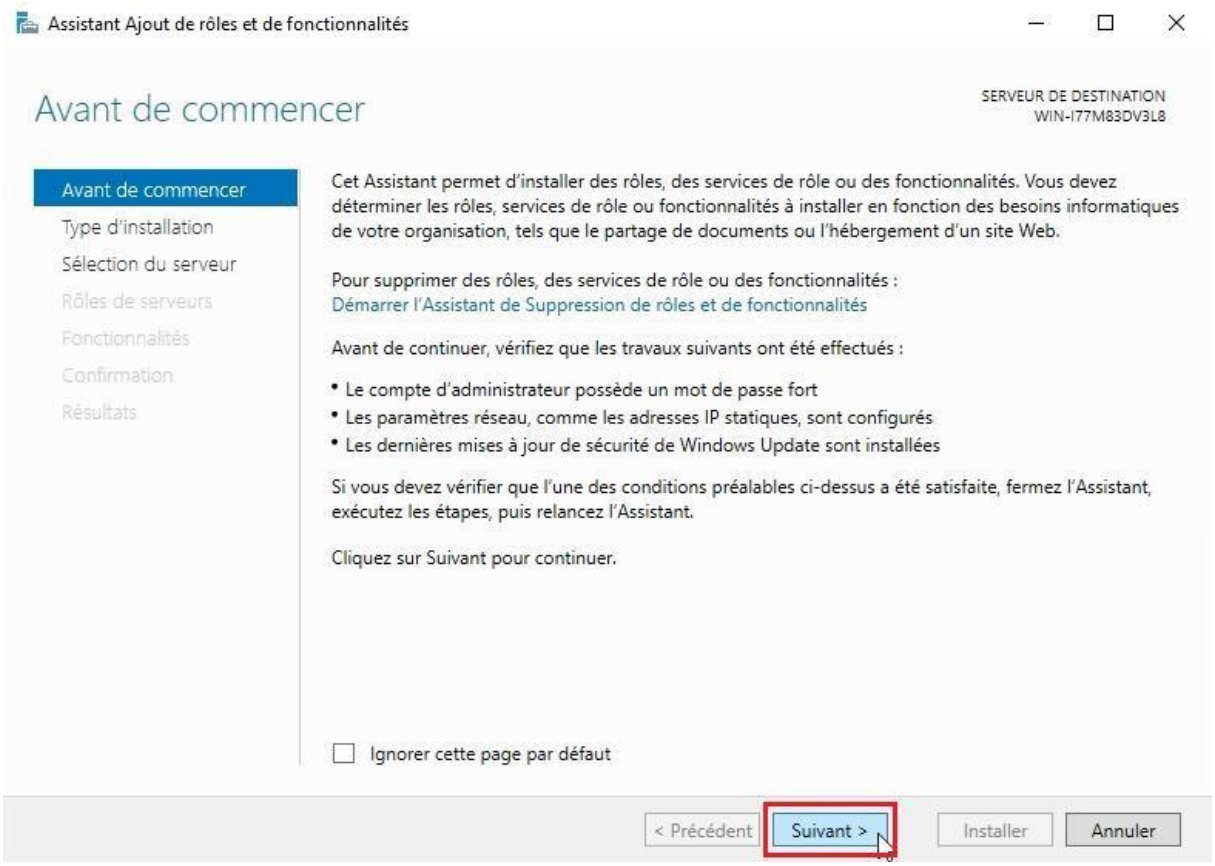
4.3.2 Installation du Service VPN

Pour commencer notre installation, nous avons tout d'abord besoin d'installer le service VPN. Il est possible de l'installer en lignes de commandes avec PowerShell ou avec l'interface graphique de Rôles et Fonctionnalités. Cependant, nous utiliserons l'interface graphique pour ce TP.

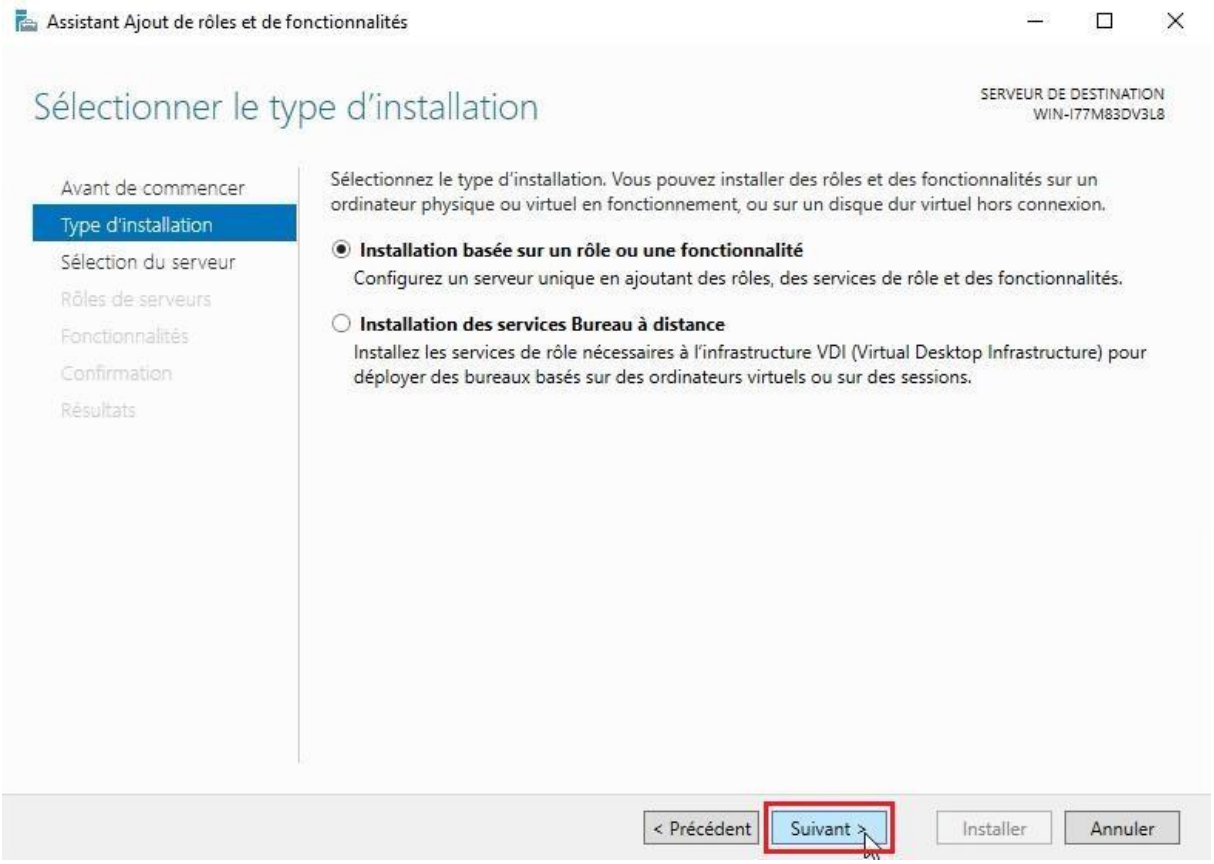


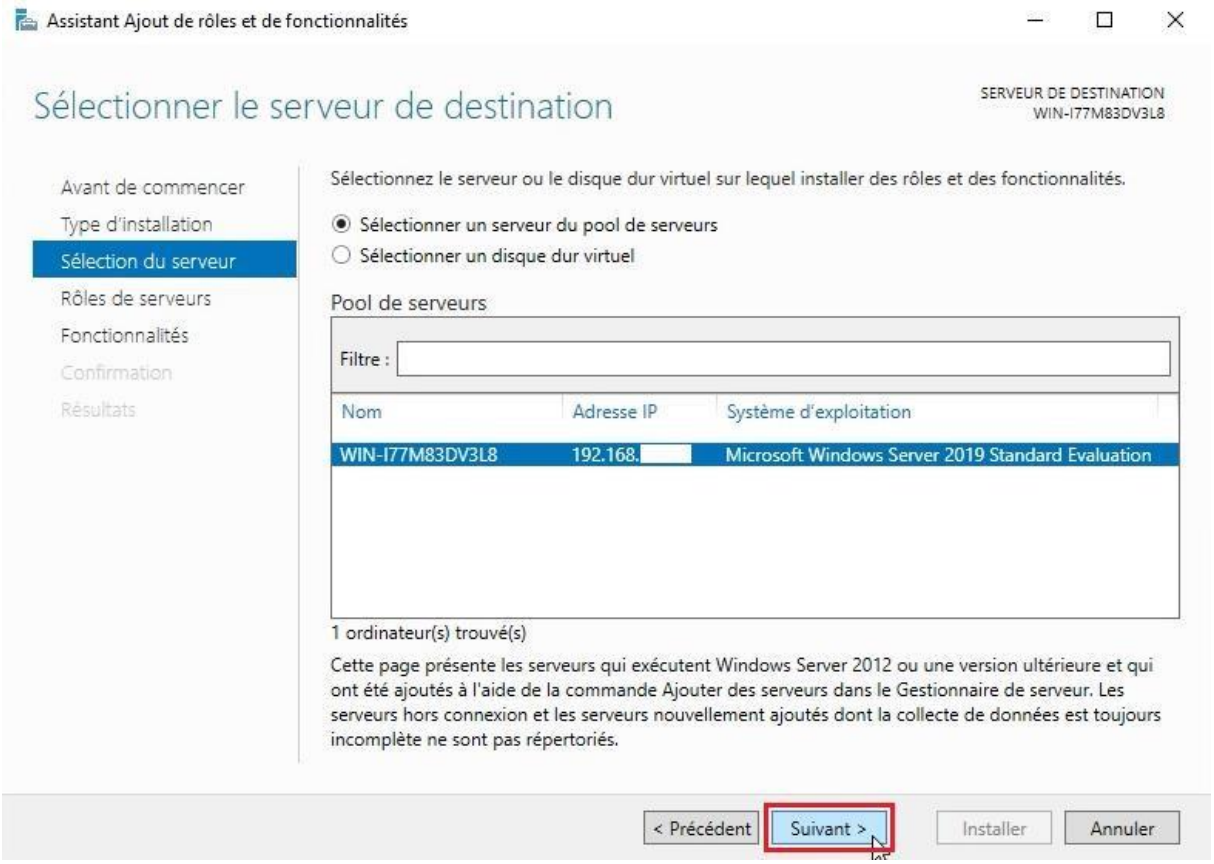
Nous allons donc ouvrir le Gestionnaire de serveur et cliquer sur l'option 2 Ajouter des rôles et fonctionnalités (cette page peut aussi être atteinte en cliquant sur Gérer en haut à droite puis sur Ajouter des rôles et fonctionnalités).

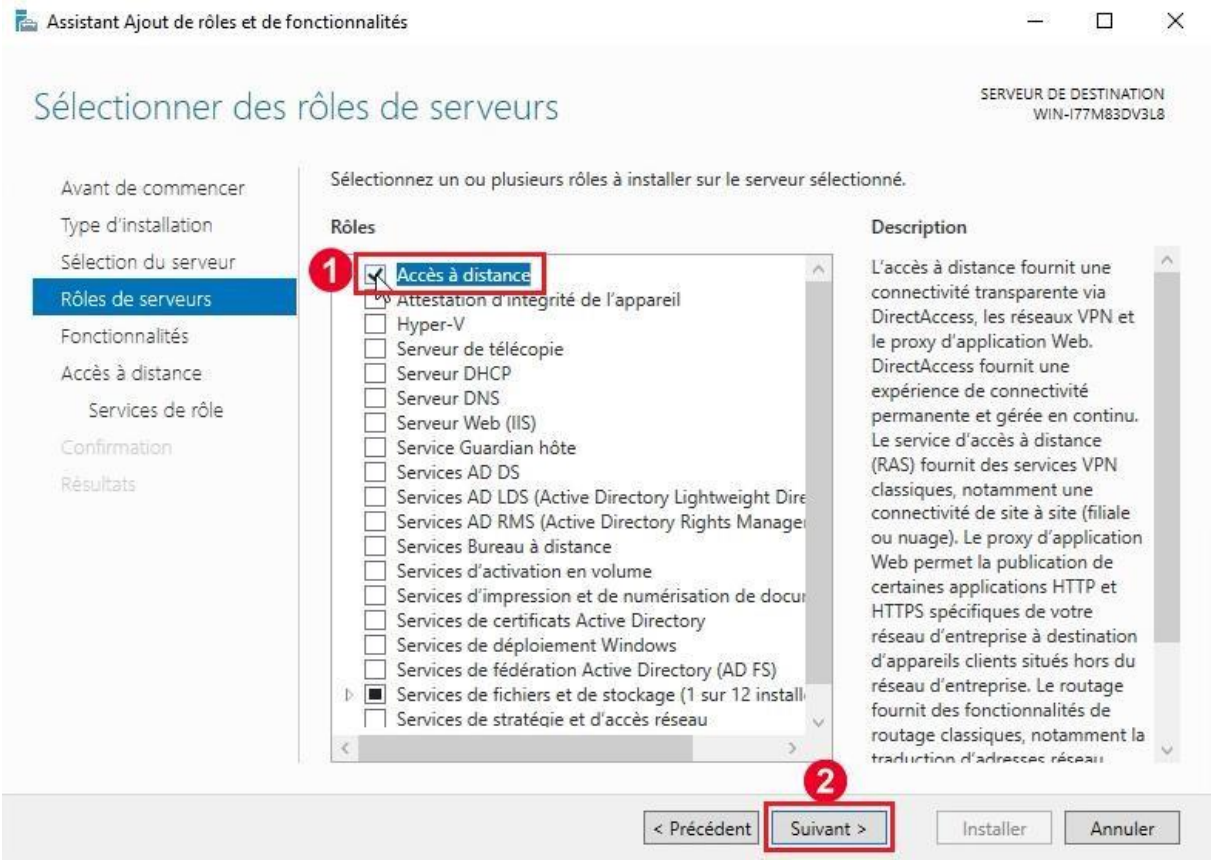




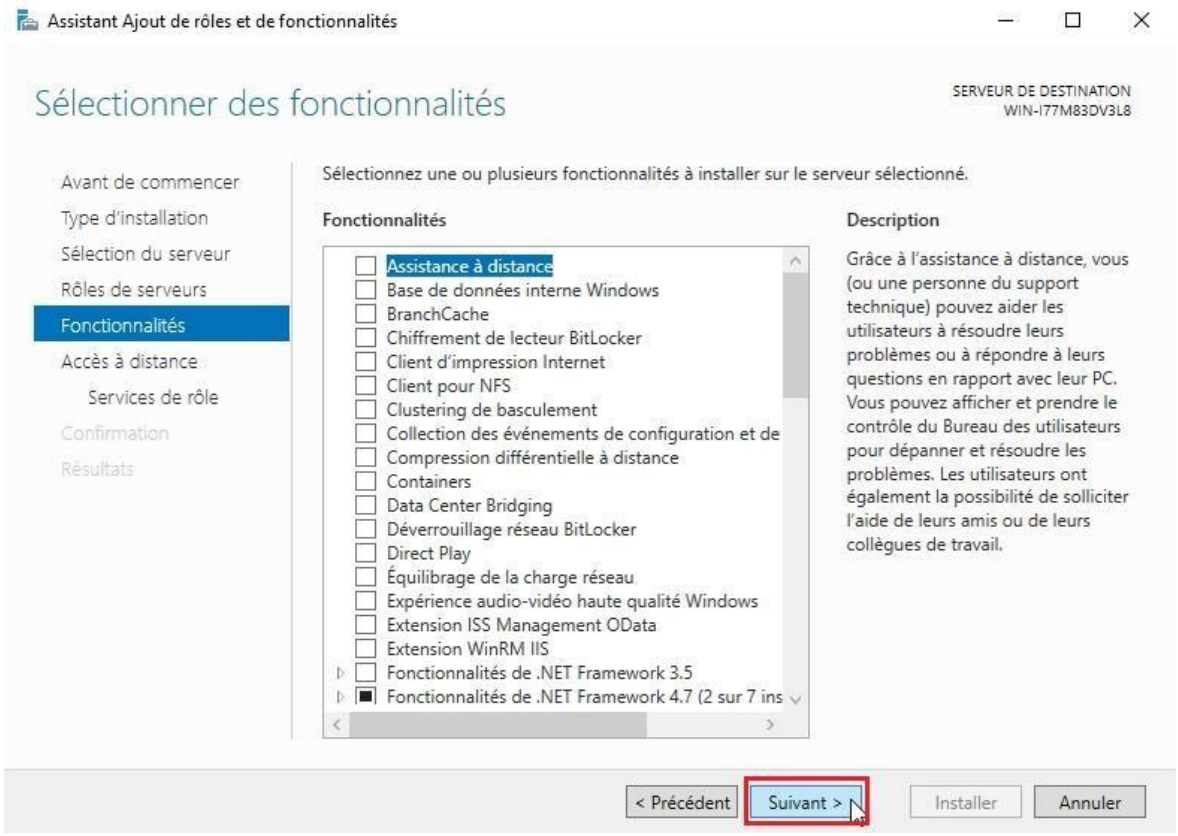
Pour notre installation, nous allons laisser les paramètres par défaut et donc cliquer sur Suivant jusqu'à ce que nous atteignions la page Rôles de serveurs.



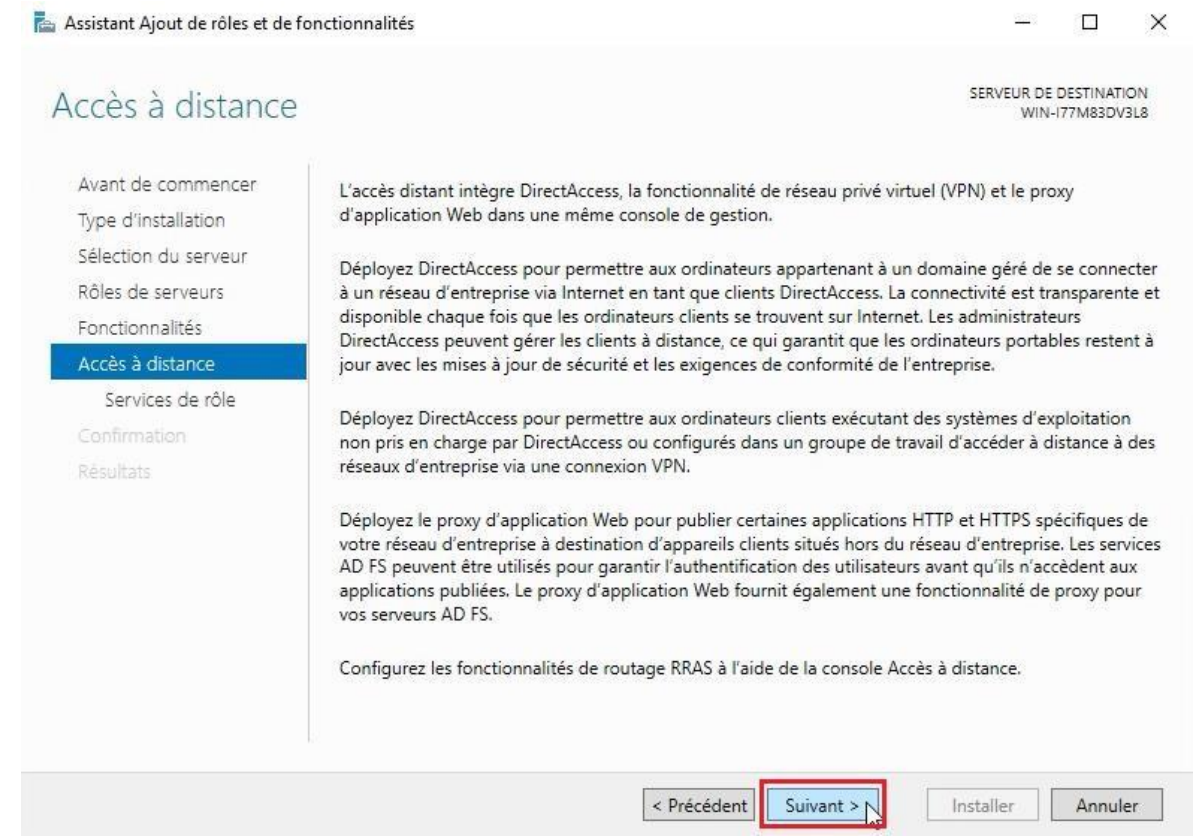


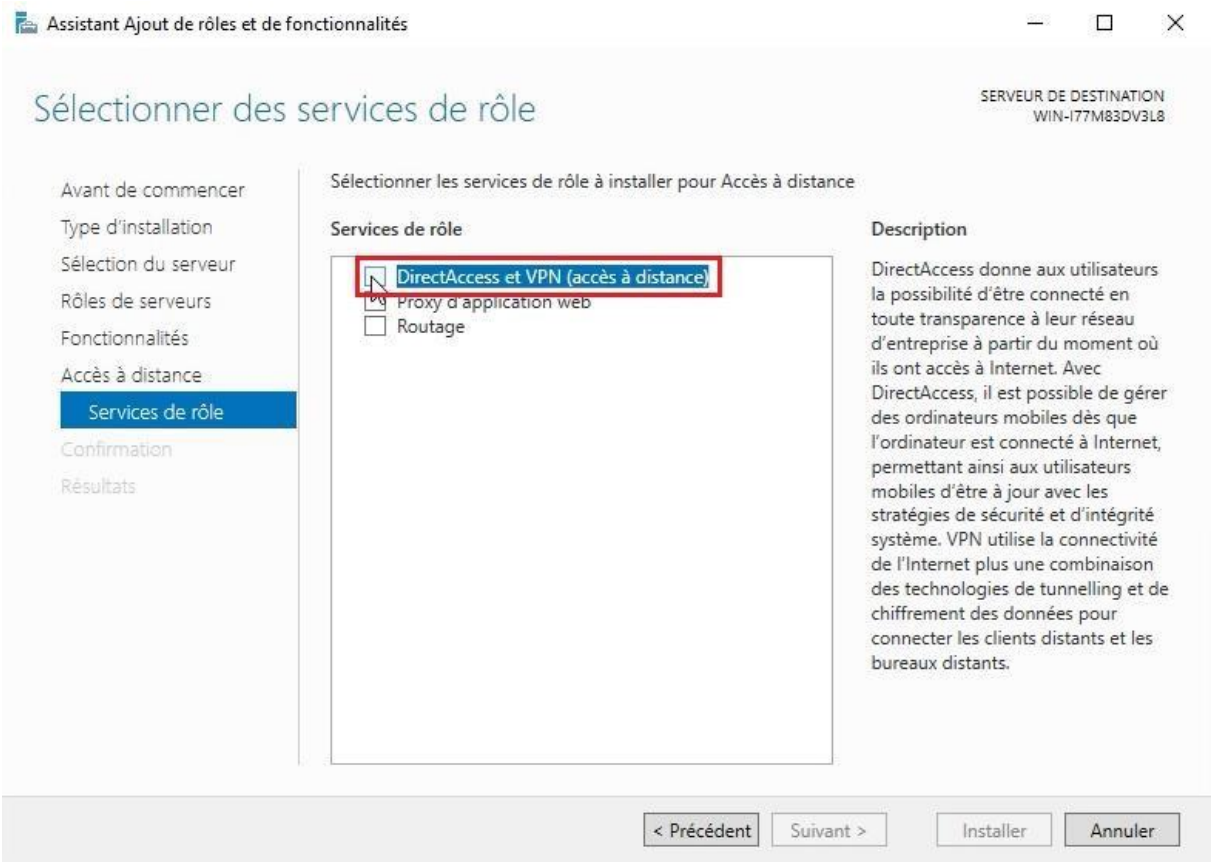


Ici nous allons sélectionner la case Accès à distance puis cliquer sur Suivant.

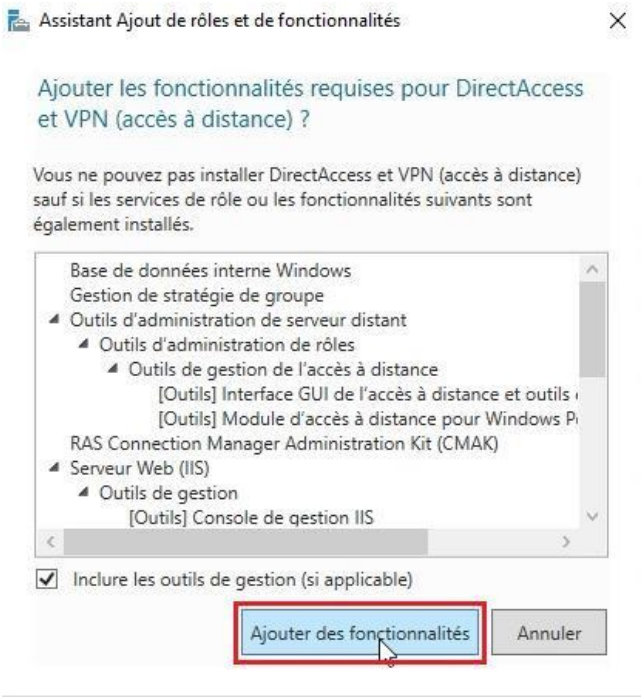


Nous pouvons laisser ces deux prochaines pages par défaut et cliquer Suivant jusqu'à arriver sur la page Services de rôle.

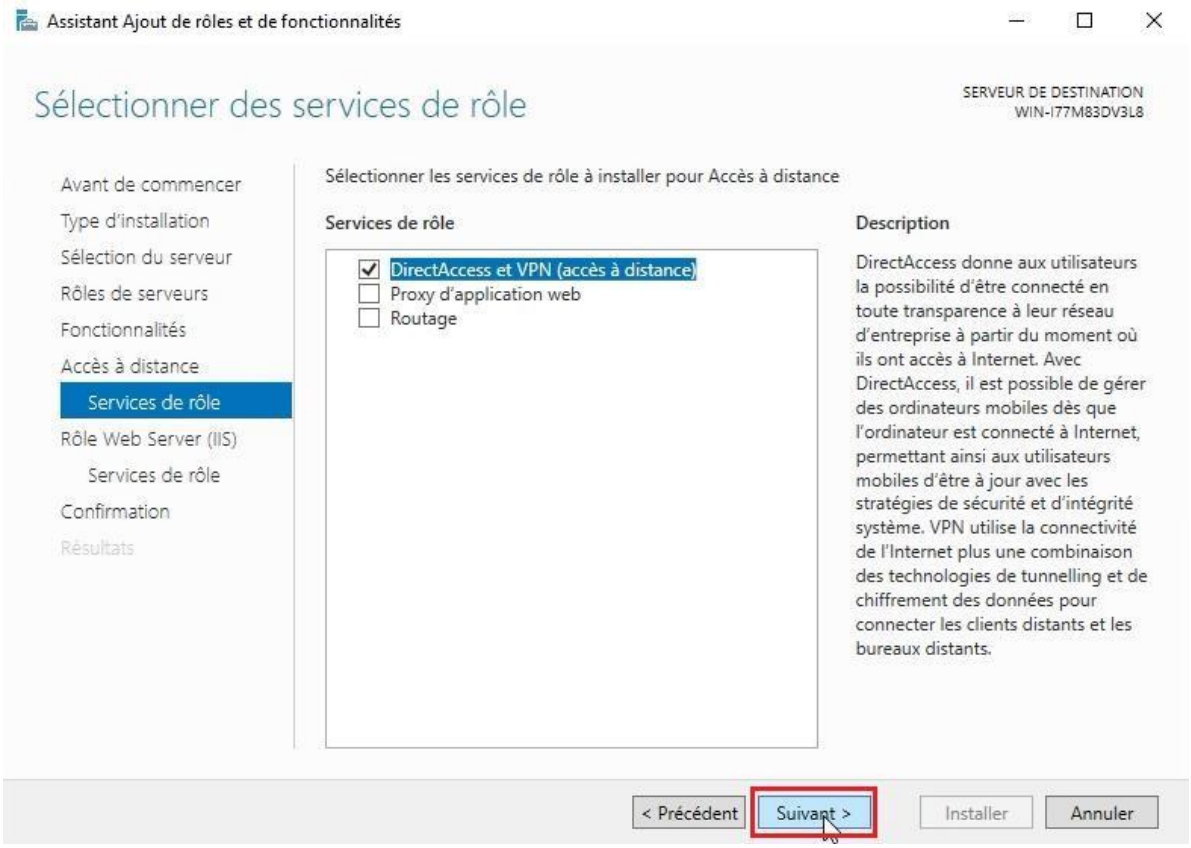




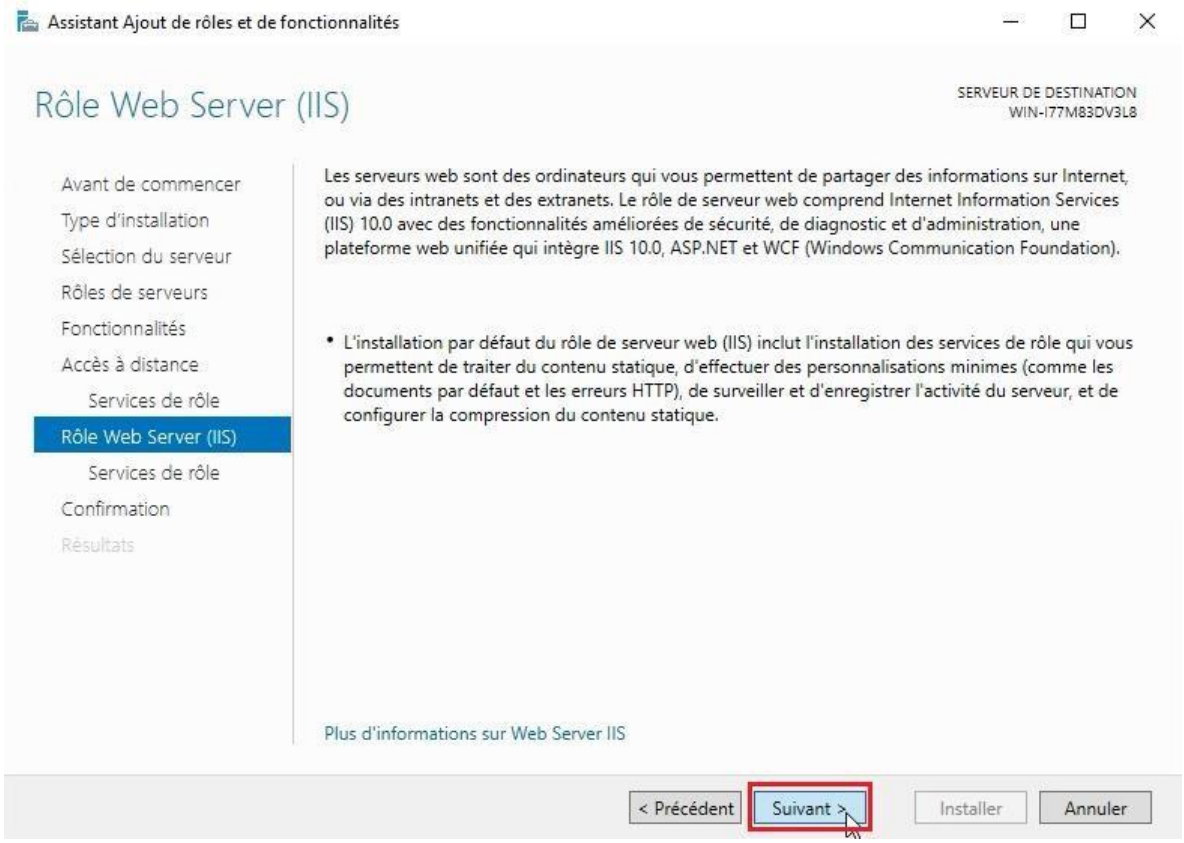
C'est ici que nous allons installer le service VPN en sélectionnant la case DirectAccess et VPN (accès à distance).



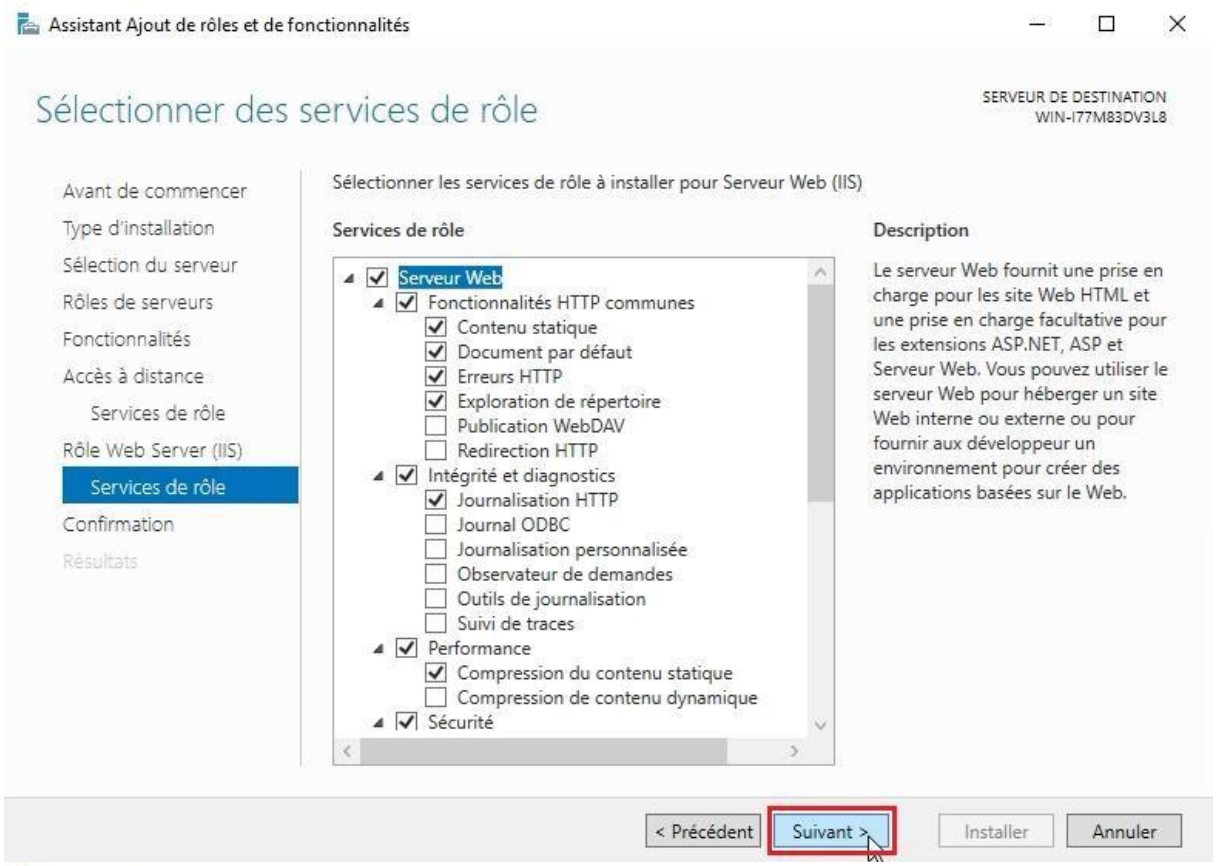
Suite à cela, une page devrait s'ouvrir nous demandant de confirmer notre installation, nous allons donc cliquer sur Ajouter des fonctionnalités.

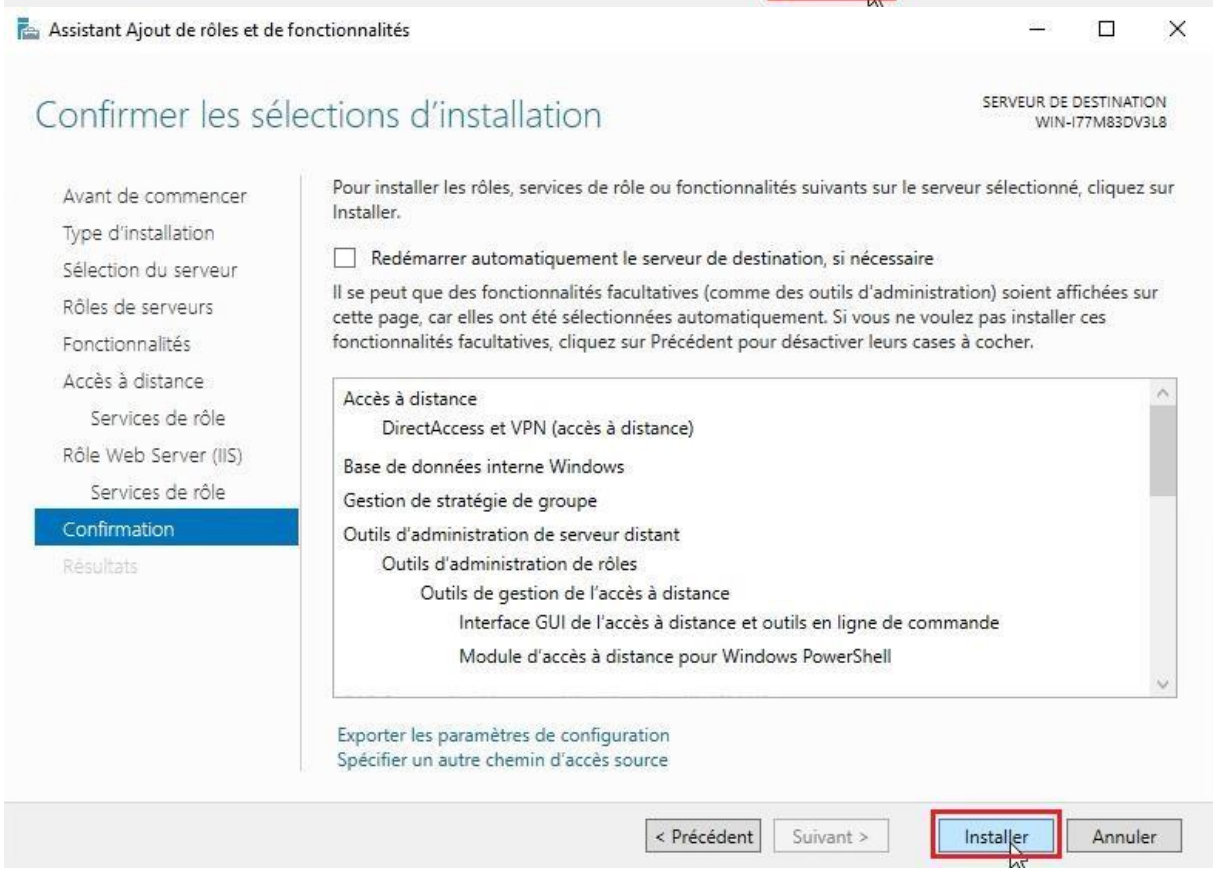


Après cela, il nous suffit de cliquer sur Suivant jusqu'à arriver à la page Confirmation.



Windows Server

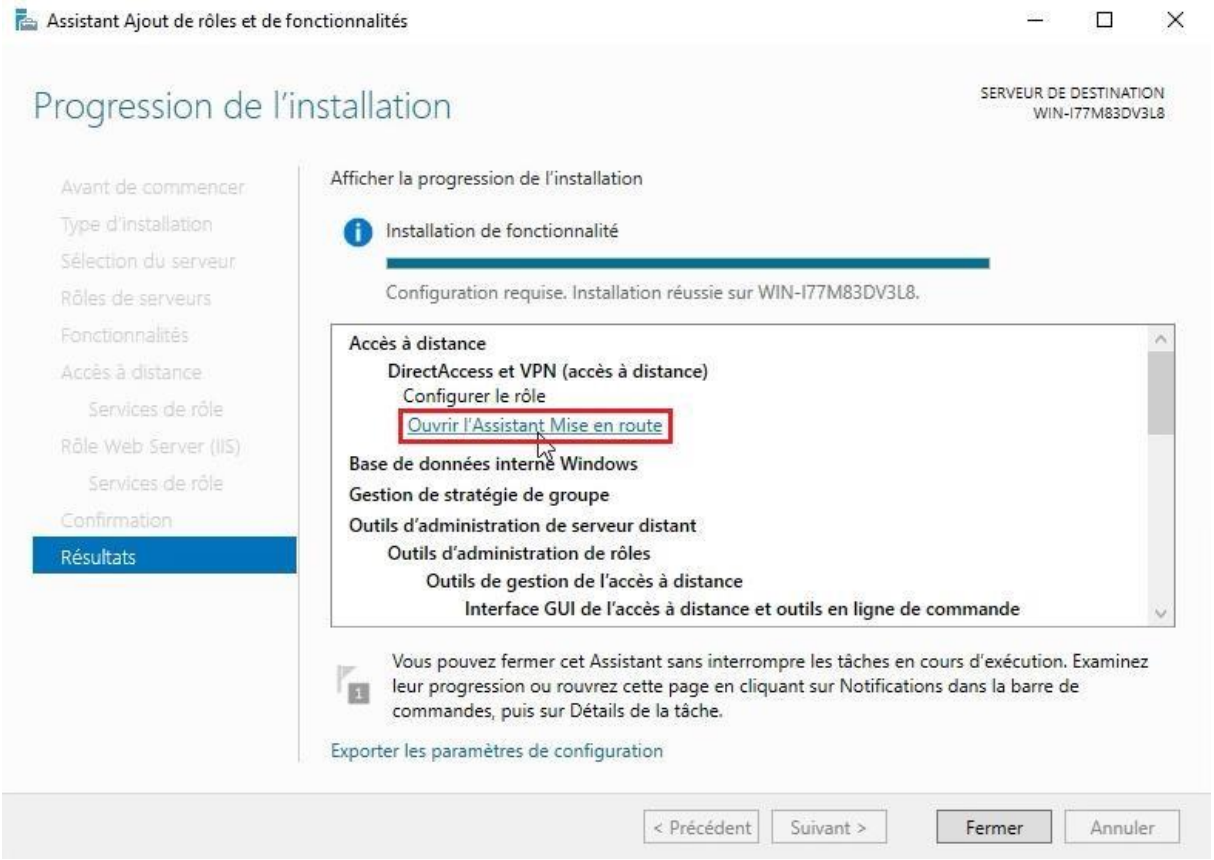


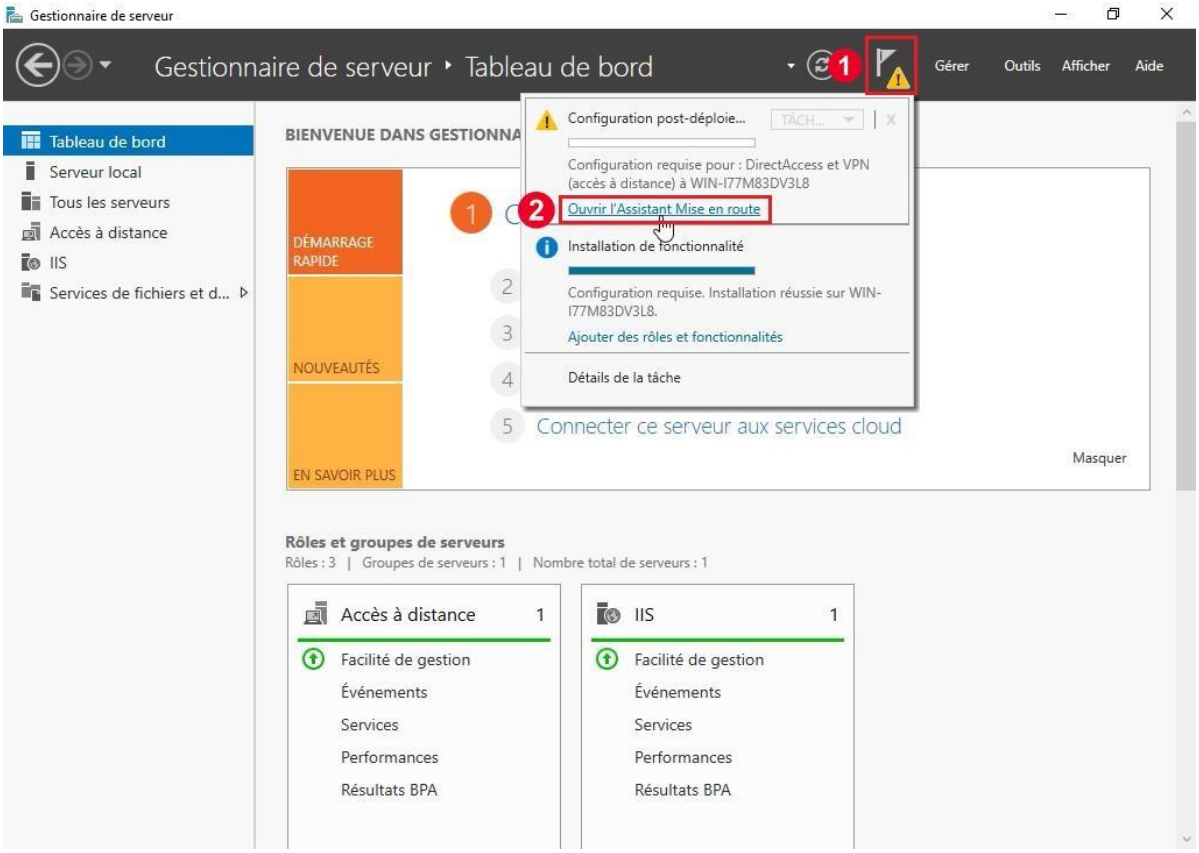


Sur cette page il ne nous reste plus qu'à cliquer sur Installer pour lancer l'installation.

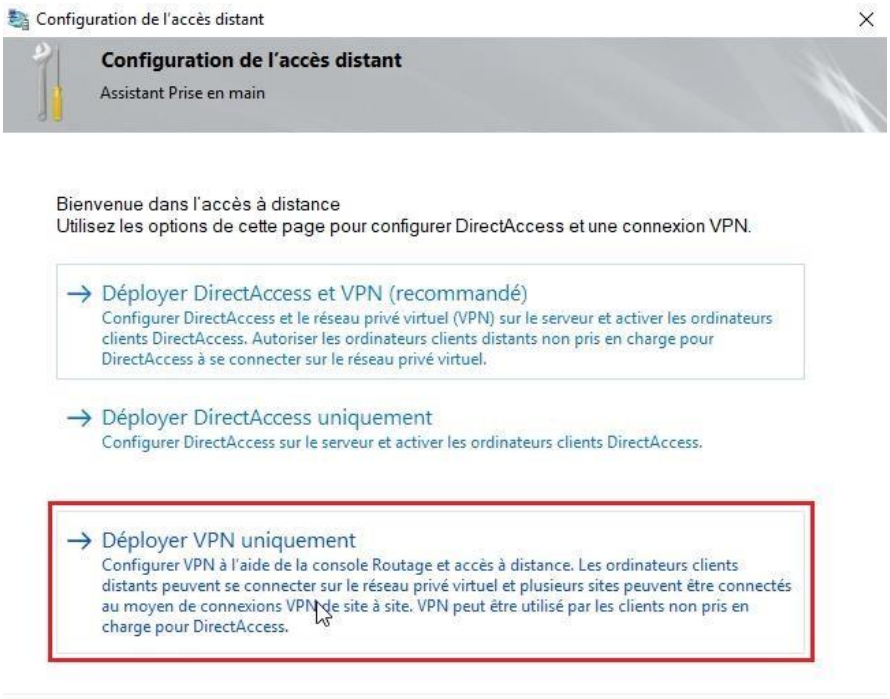
4.3.3 Configuration du Routage et Accès Distant

Une fois l'installation terminée, nous allons pouvoir configurer le service Routage et accès distant.
Pour ouvrir ce service, nous pouvons cliquer sur Ouvrir l'Assistant Mise en route dans la fenêtre d'installation que nous venons d'utiliser. (Cette page peut mettre un certain temps à charger).

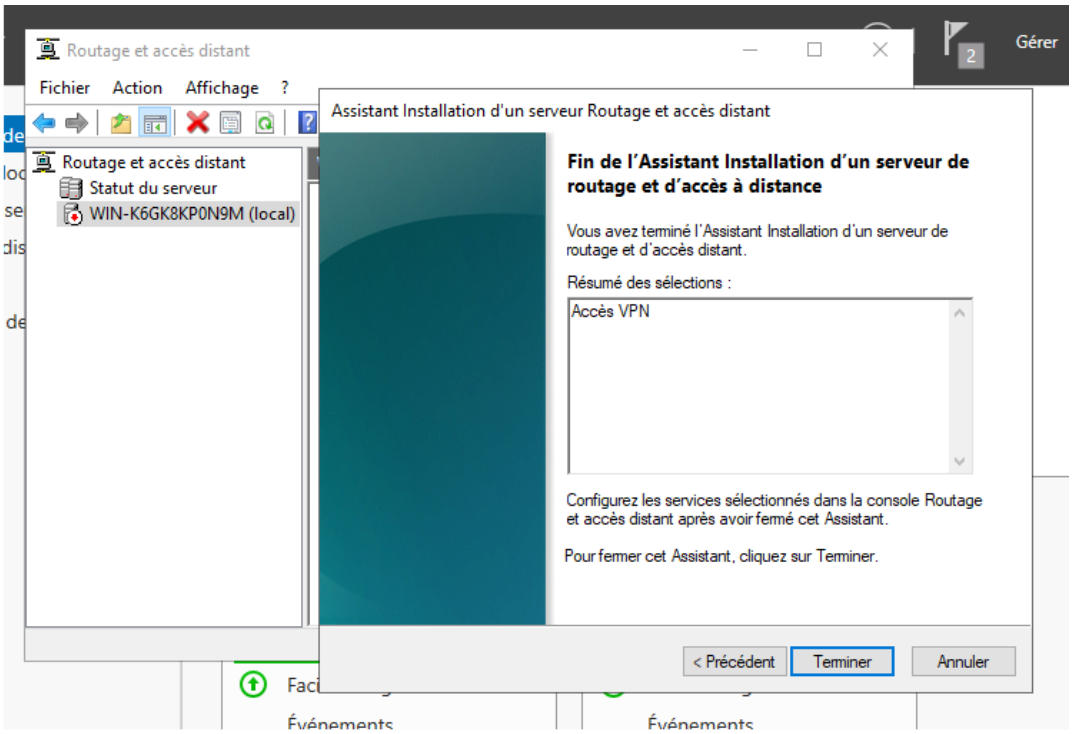




(Nous pouvons aussi retrouver cet outil en cliquant sur le drapeau en haut à droite du Gestionnaire de serveur, puis sur le message Ouvrir l'Assistant Mise en route.)

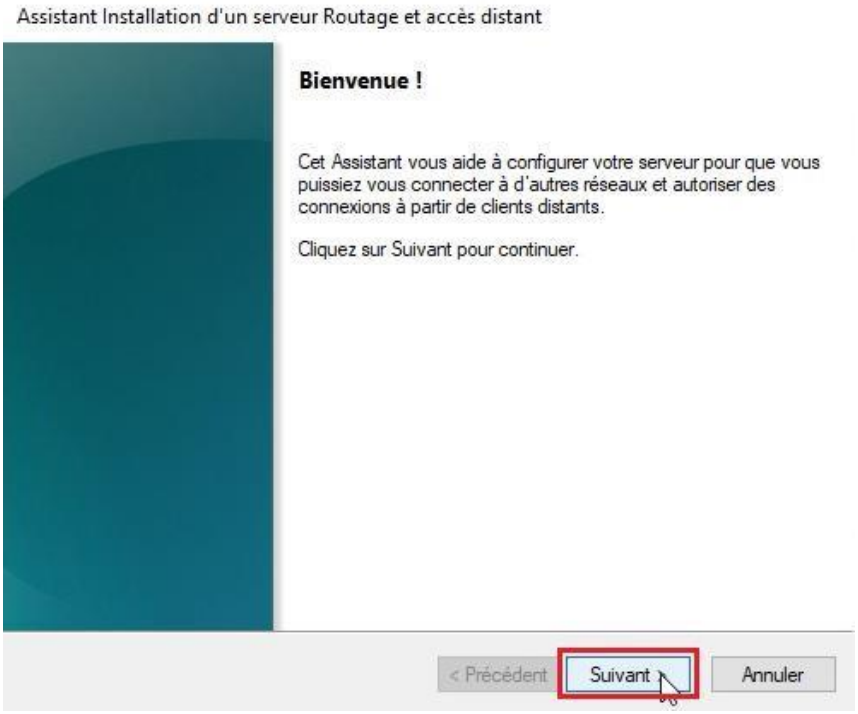


Une fenêtre de Configuration de l'accès distant devrait s'ouvrir. Dans notre cas, nous allons sélectionner Déployer VPN uniquement car nous n'aurons pas besoin de DirectAccess durant notre TP.

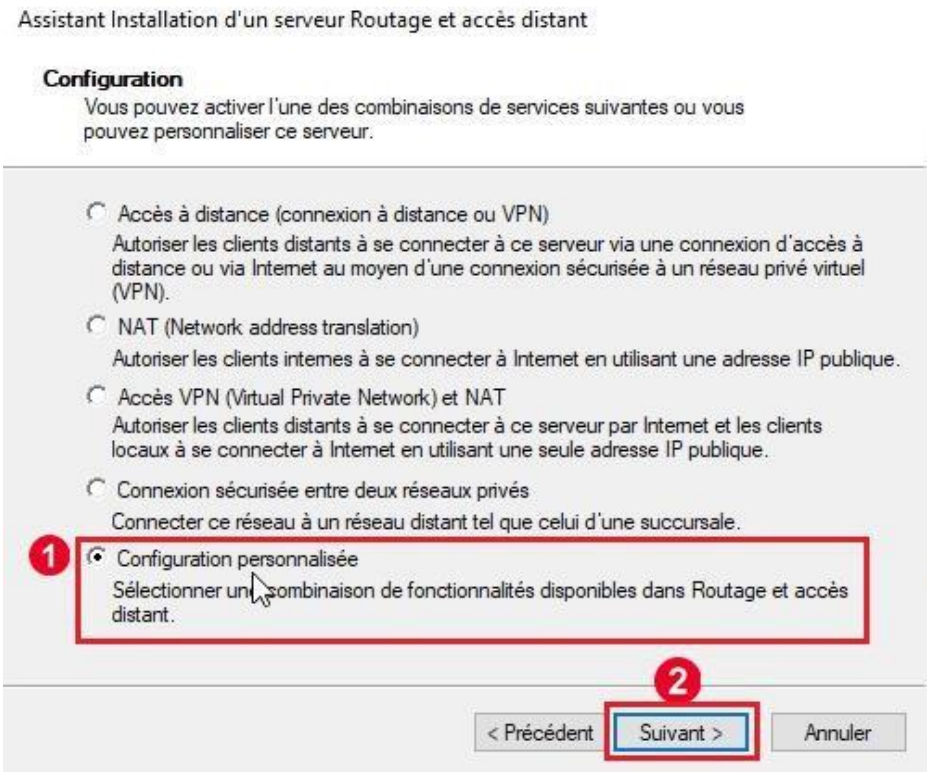


.

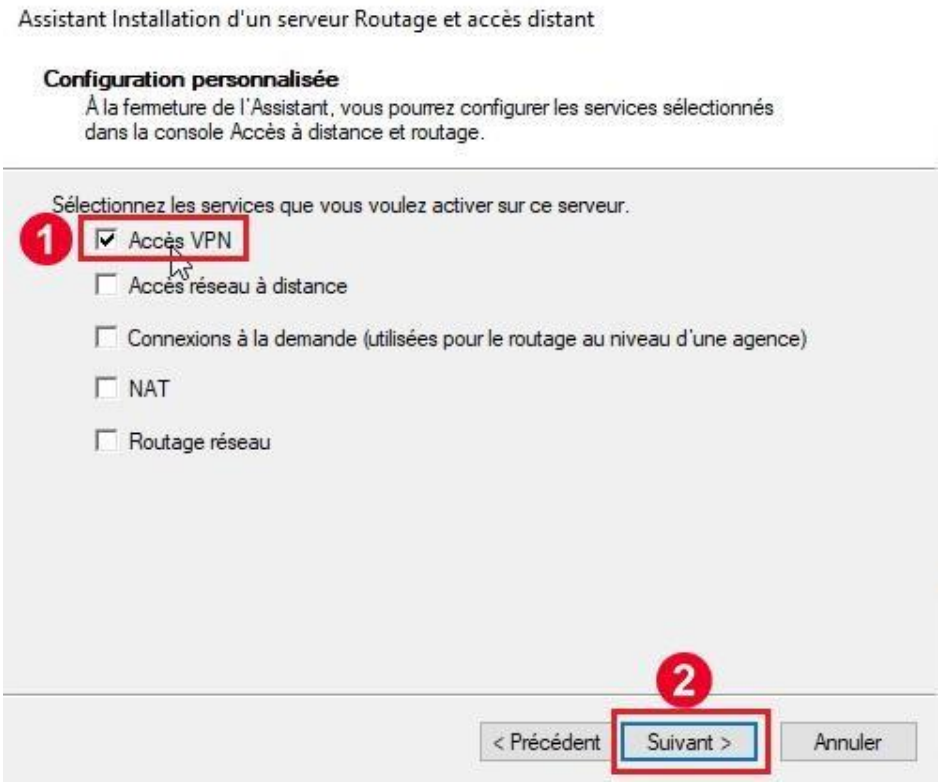
Une fois l'option sélectionner, le gestionnaire Routage et accès distant devrait s'ouvrir automatiquement. Ici, nous allons configurer notre accès à distance en faisant un clic droit sur notre serveur local, puis en cliquant sur Configurer et activer le routage et l'accès à distance.



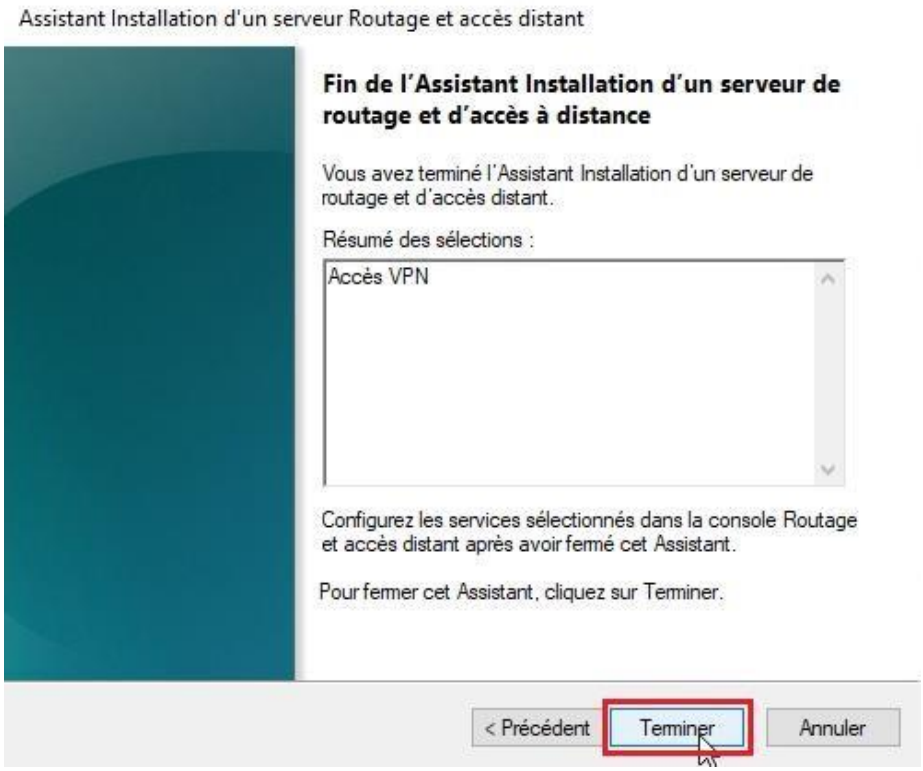
Dans cet Assistant d'installation nous pouvons faire Suivant sur la première page.



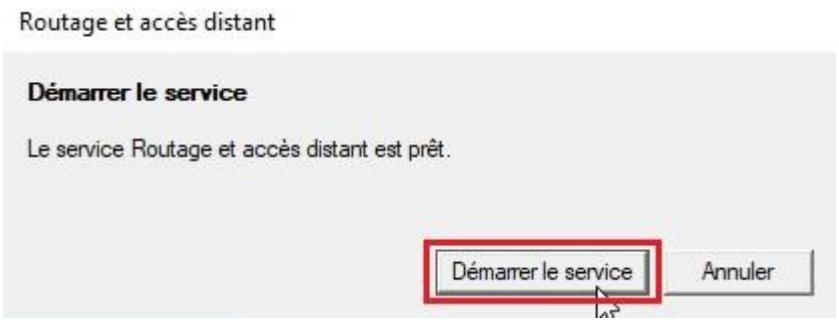
Ensuite, sur la page configuration, nous allons sélectionner la Configuration personnalisée avant de faire Suivant.



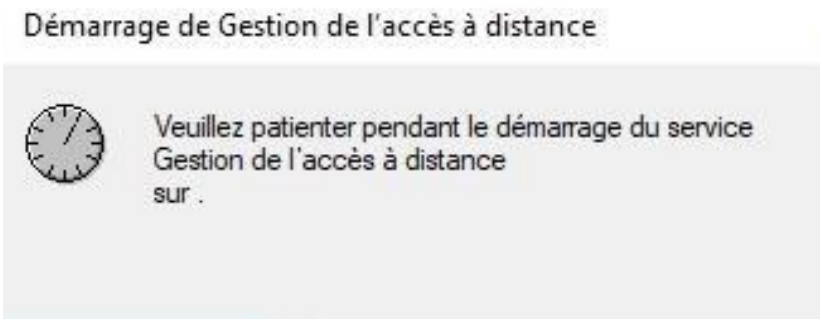
Sur la page Configuration personnalisée, nous allons sélectionner Accès VPN, puis cliquer sur Suivant.



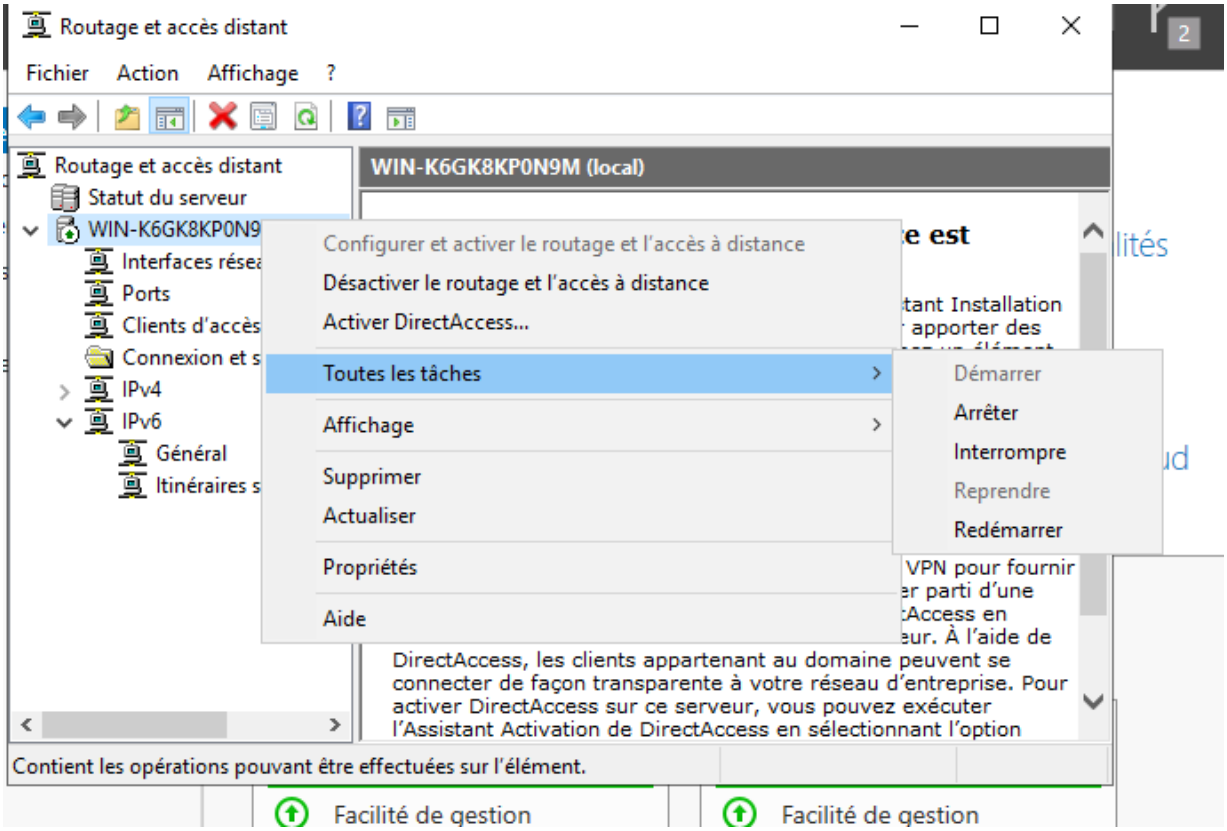
Enfin, nous allons cliquer sur Terminer pour confirmer notre installation.



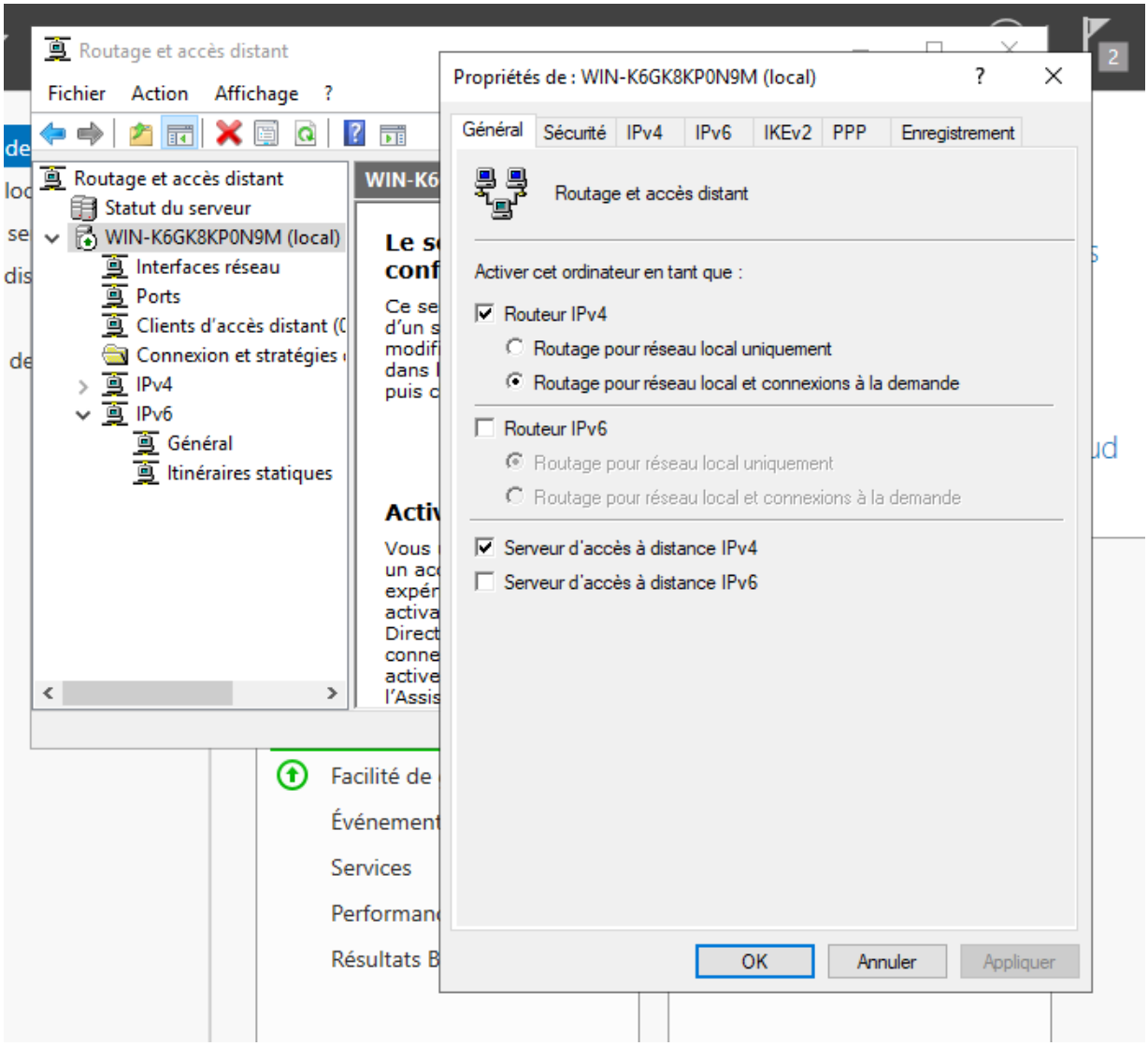
Une fenêtre nous indiquant que le service est prêt au démarrage devrait s'ouvrir. Nous allons donc cliquer sur Démarrer le service.

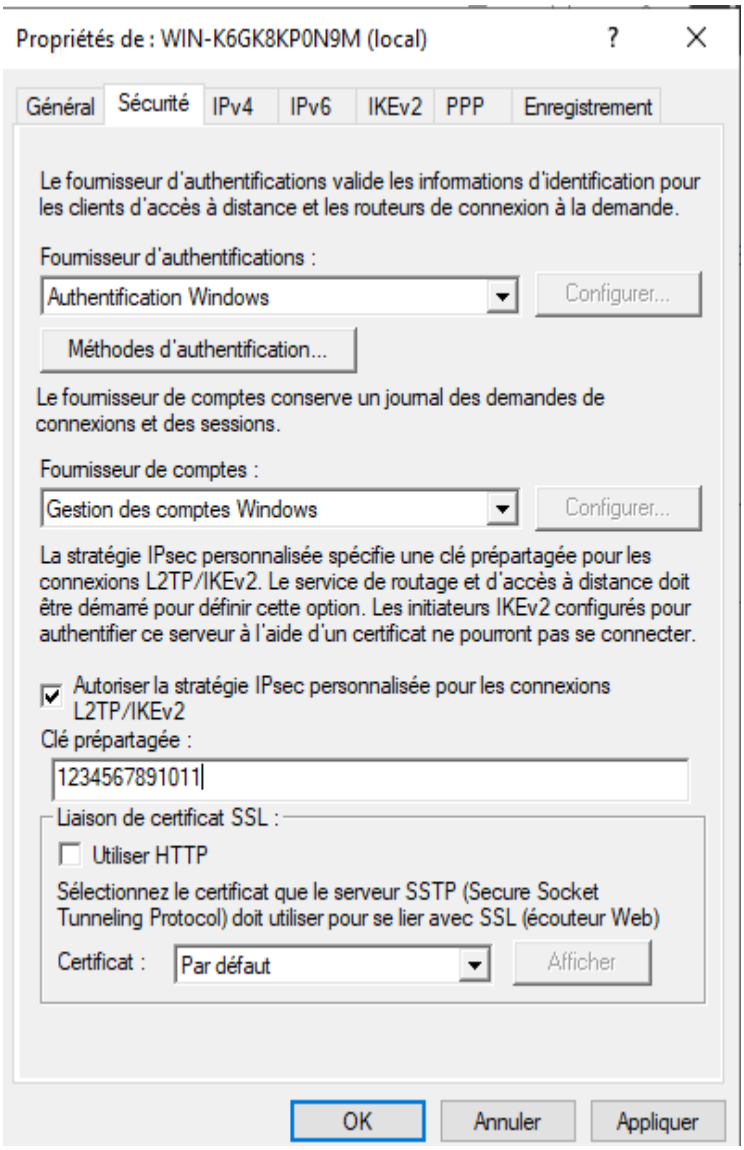


Après un court chargement, notre service Routage et accès à distance devrait se lancer.



Pour finaliser notre configuration du service, nous pouvons faire un clic droit sur notre serveur local puis cliquer sur Propriétés.

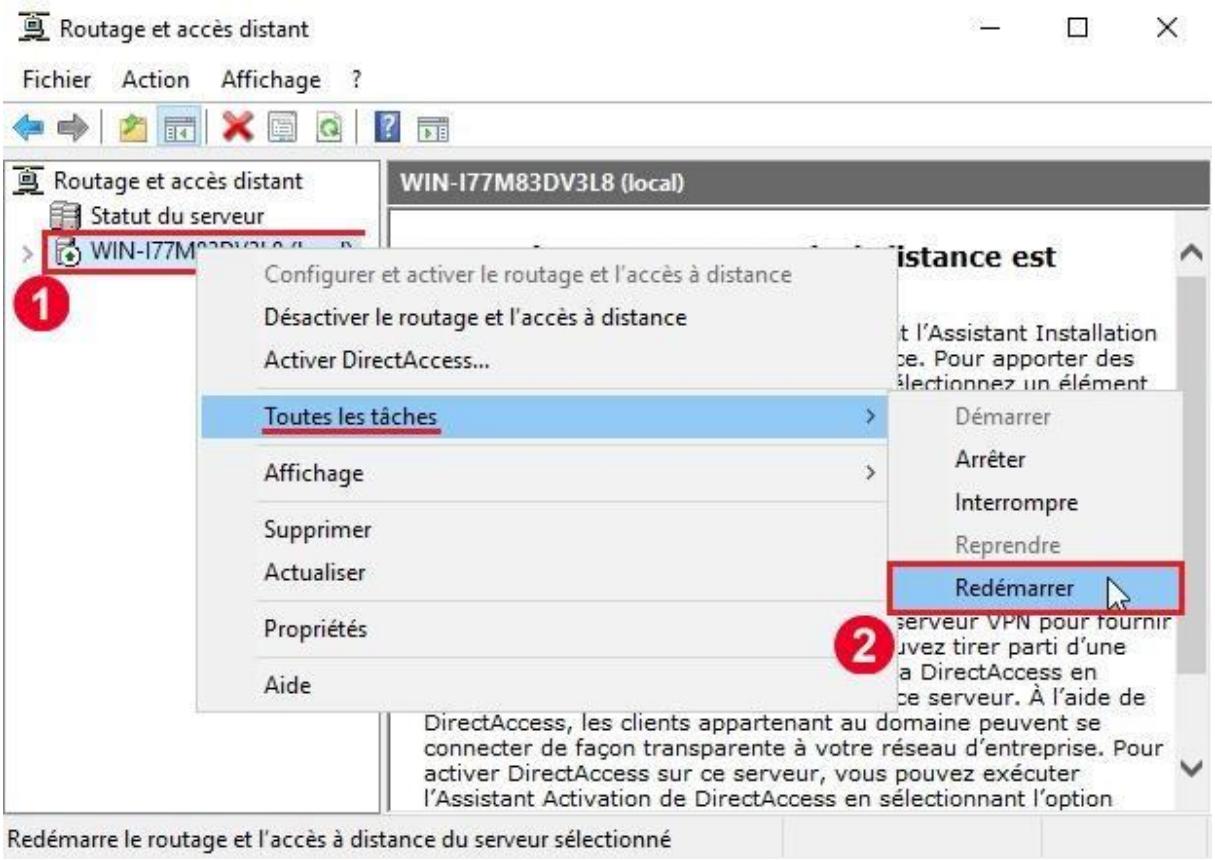




Ici, nous allons nous intéresser à l'onglet Sécurité.

Pour notre TP nous avons décidé de mettre en place une clé pré-partagée pour sécuriser notre VPN.
Pour ce faire, il nous suffit de cocher la case Autoriser la stratégie IPsec personnalisée pour les connexions L2TP/IKEv2 et de taper la clé de notre choix dans le champ Clé prépartagée. (Il faudra mémoriser cette clé pour la renseigner par la suite sur le client VPN) Nous pouvons ensuite cliquer sur Appliquer.

Une fenêtre devrait s'ouvrir pour nous demander de redémarrer le service, nous allons donc cliquer sur OK.

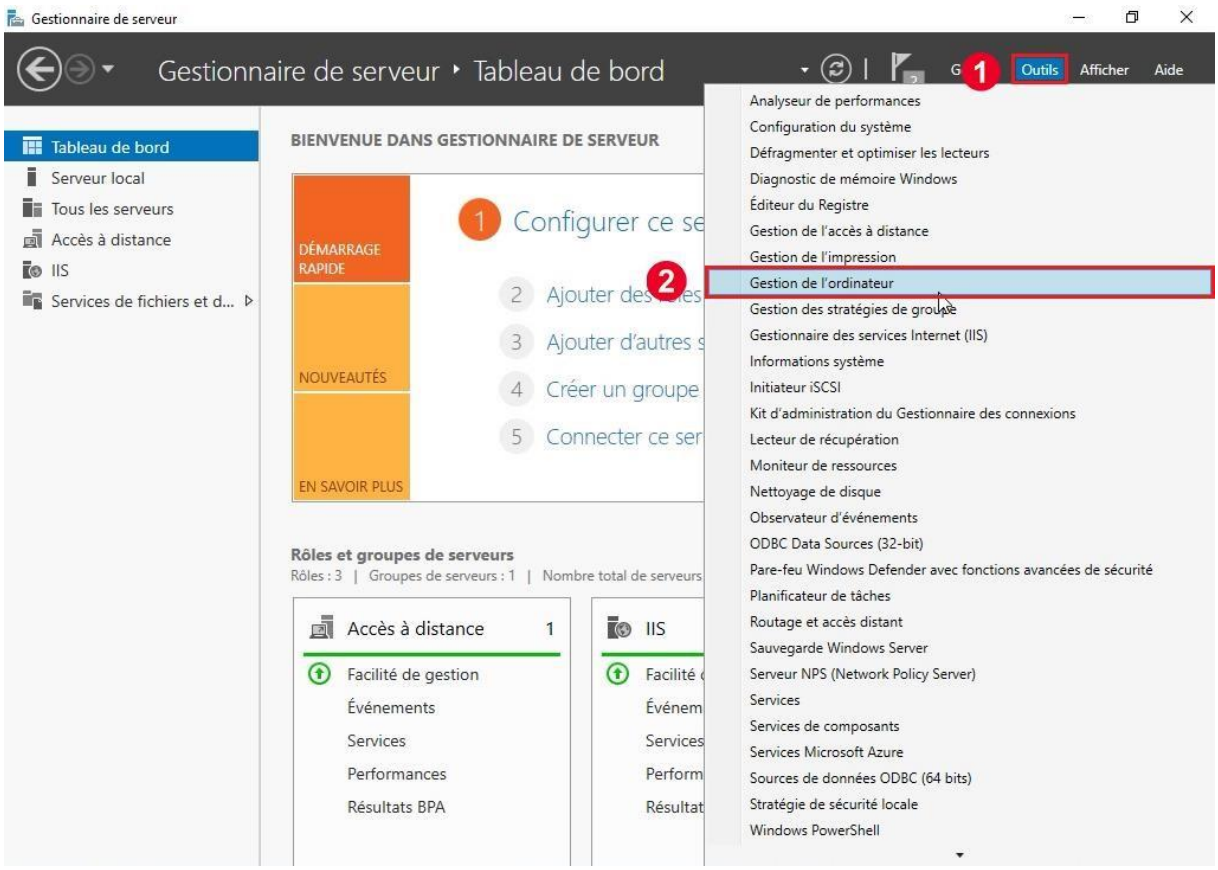


Pour redémarrer le service et appliquer nos modifications, nous allons donc faire un clic droit sur notre serveur local, puis naviguer dans Toutes les tâches et cliquer sur Redémarrer.

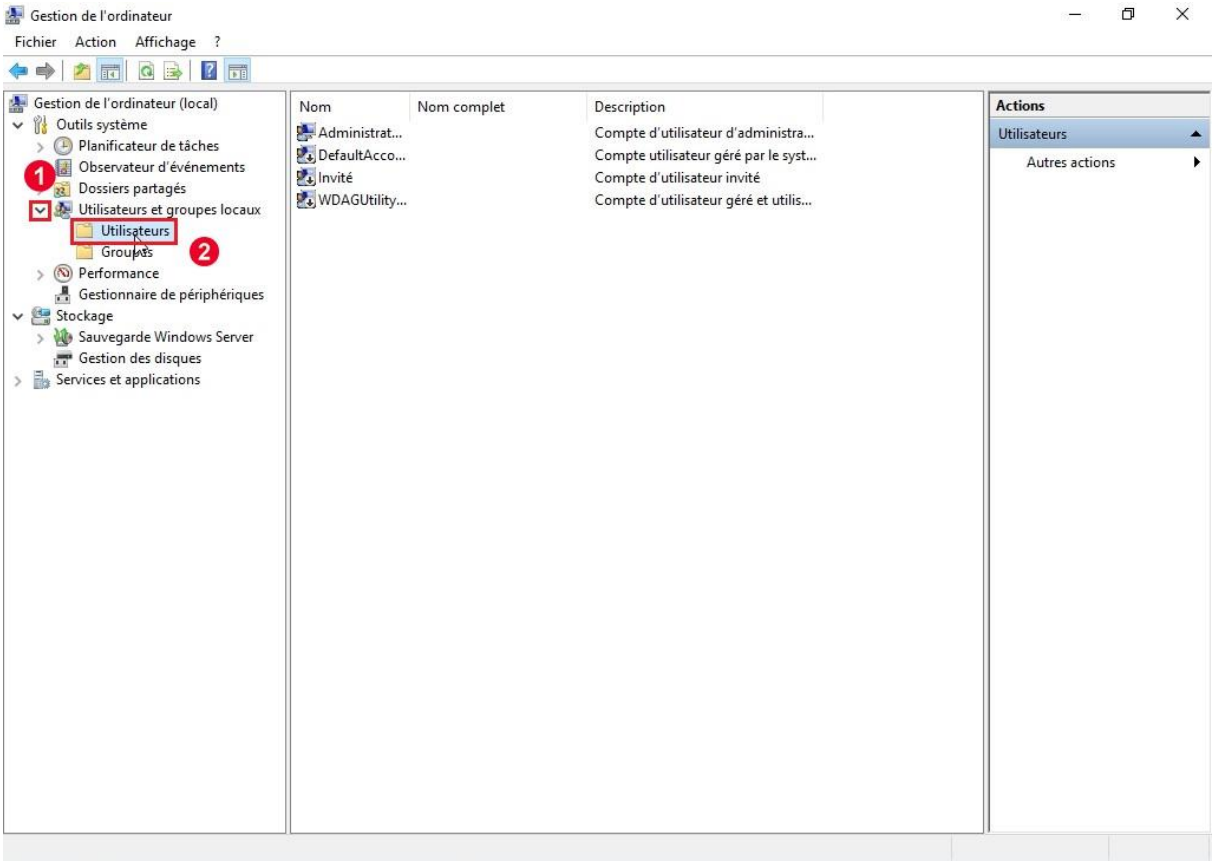
Nous avons maintenant terminé de configurer le service Routage et accès distant.

4.3.4 Mise en Place d'Autorisations dans Gestion de l'Ordinateur

Afin d'assurer qu'un PC utilisant notre VPN soit capable de se connecter à l'un de nos utilisateurs, nous allons maintenant autoriser notre compte Administrateur local à être contrôlé à distance.

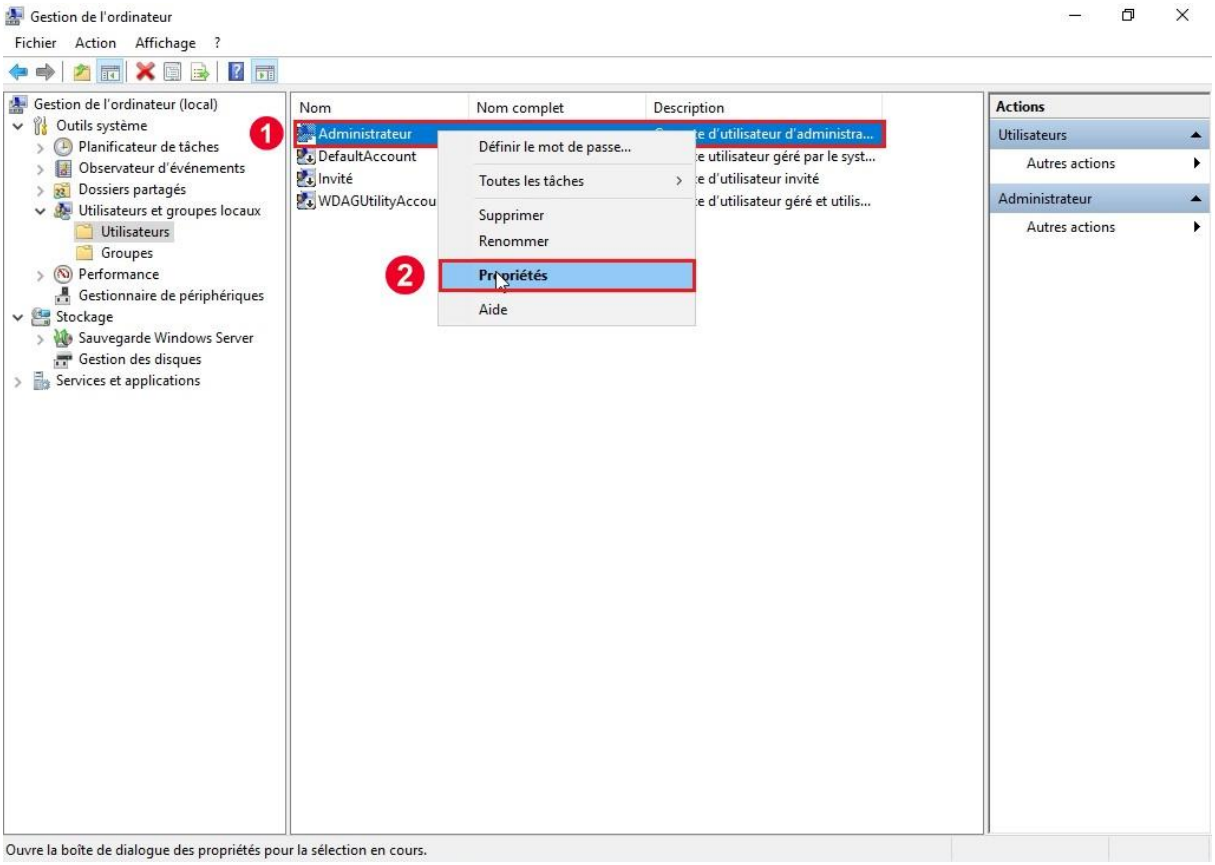


Pour ce faire, nous allons nous rendre dans le Gestionnaire de serveur, cliquer sur Outils, puis sur Gestion de l'ordinateur.

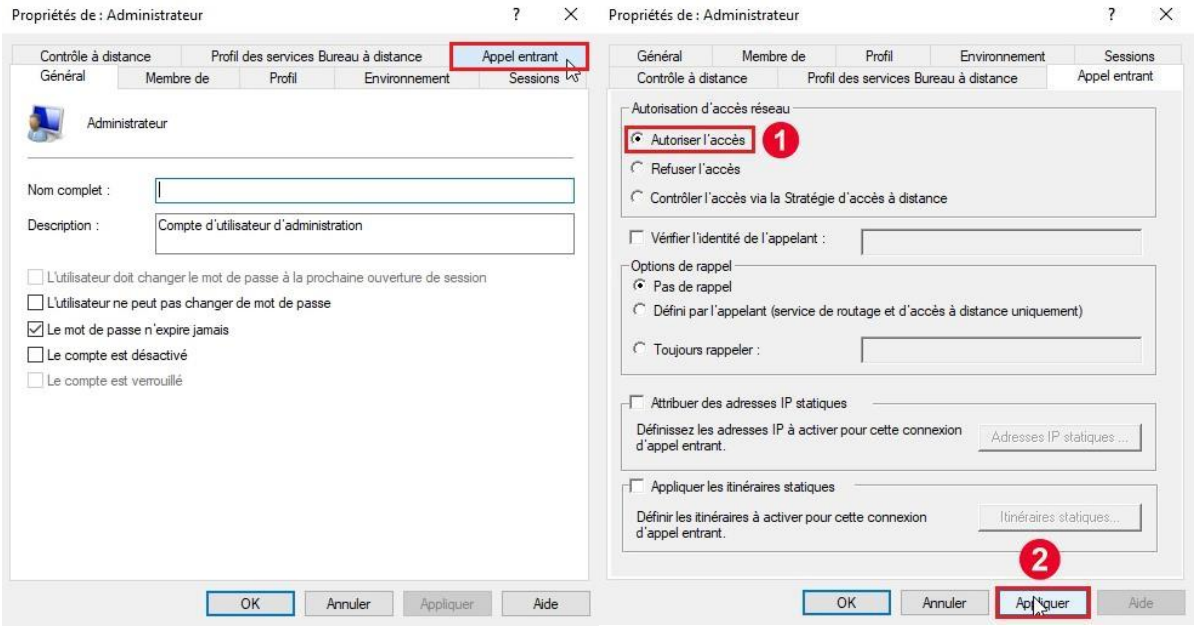


Ici, nous allons développer le dossier Utilisateurs et groupes locaux en cliquant sur >, puis nous allons cliquer sur le sous-dossier Utilisateurs.

Windows Server



Pour notre TP, nous avons choisi de donner accès aux utilisateurs VPN à notre compte Administrateur local. Nous allons donc faire un clic droit sur Administrateur puis cliquer sur Propriétés.



Ici, nous allons ouvrir l'onglet Appel entrant puis cocher la case Autoriser l'accès et Appliquer.

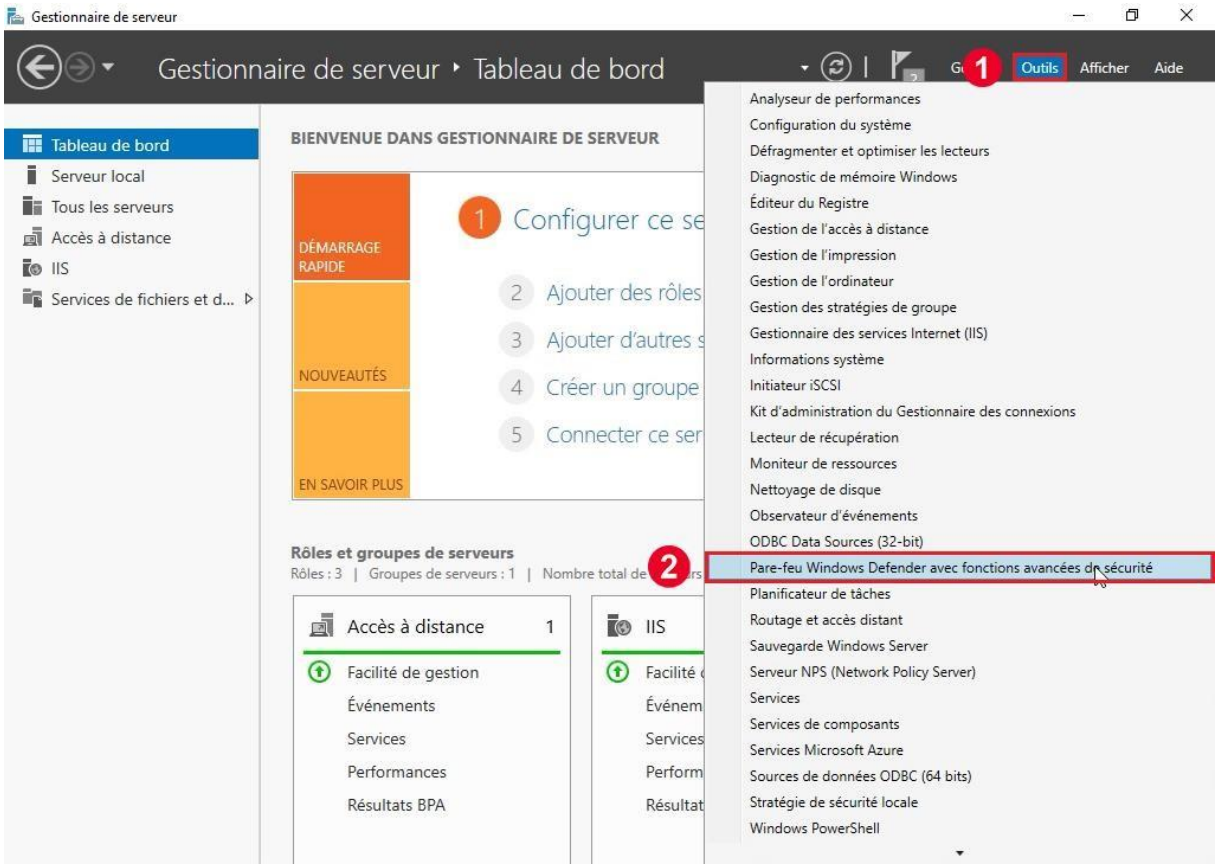
Nous pouvons maintenant fermer cette fenêtre et passer à l'étape suivante : l'ouverture des ports.

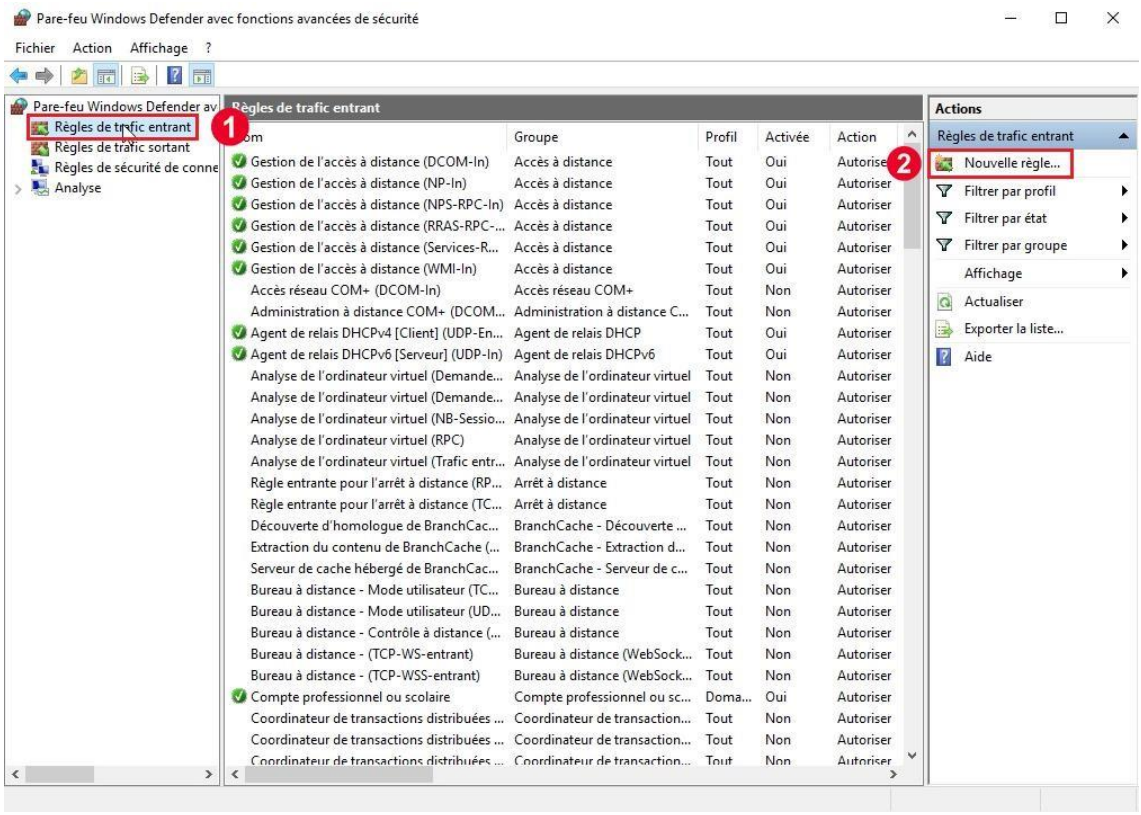
4.3.5 Ouverture des ports L2TP

A présent, il ne nous reste plus qu'à configurer notre firewall pour laisser passer notre VPN. Pour ce faire, nous pouvons soit créer des règles dans l'interface graphique Windows Defender, soit taper la commande suivante dans PowerShell :

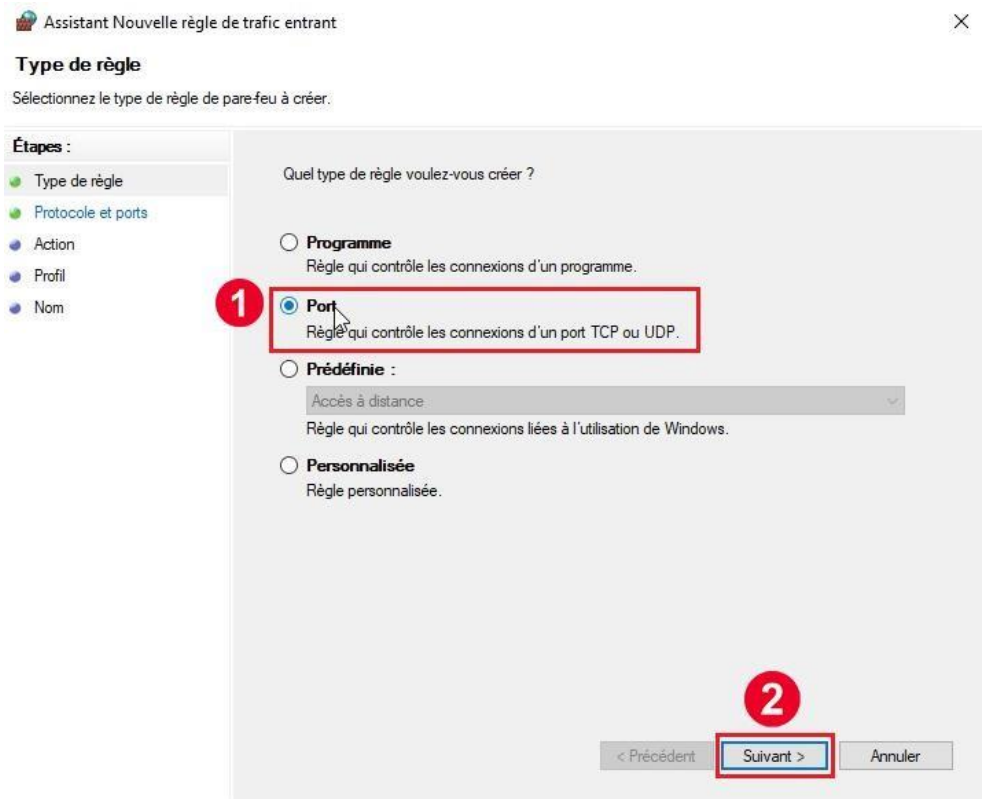
```
New-NetFirewallRule -DisplayName "VPNUDP" -Direction inbound -Profile Any -Action Allow -LocalPort 500, 1701, 4500 -Protocol UDP
```

Pour ajouter ces règles en interface graphique, nous pouvons ouvrir le Pare-feu Windows Defender en retournant dans le Gestionnaire de serveur, cliquer sur Outils puis sur Pare-feu Windows Defender avec fonctionnalités avancées de sécurité.

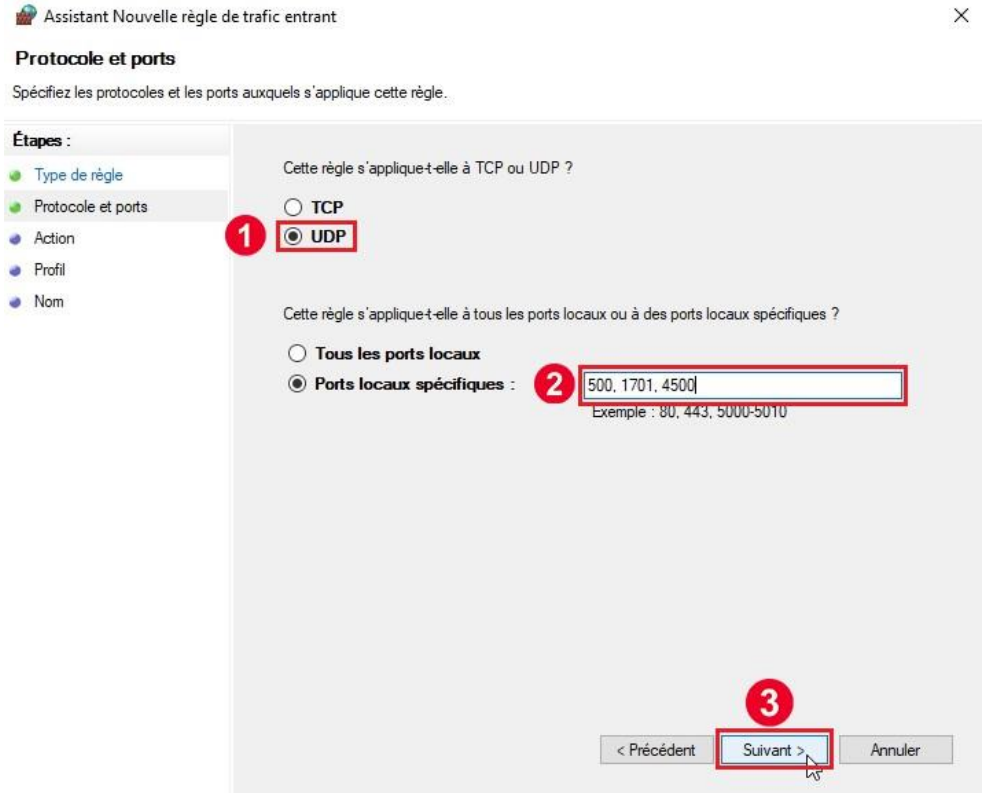




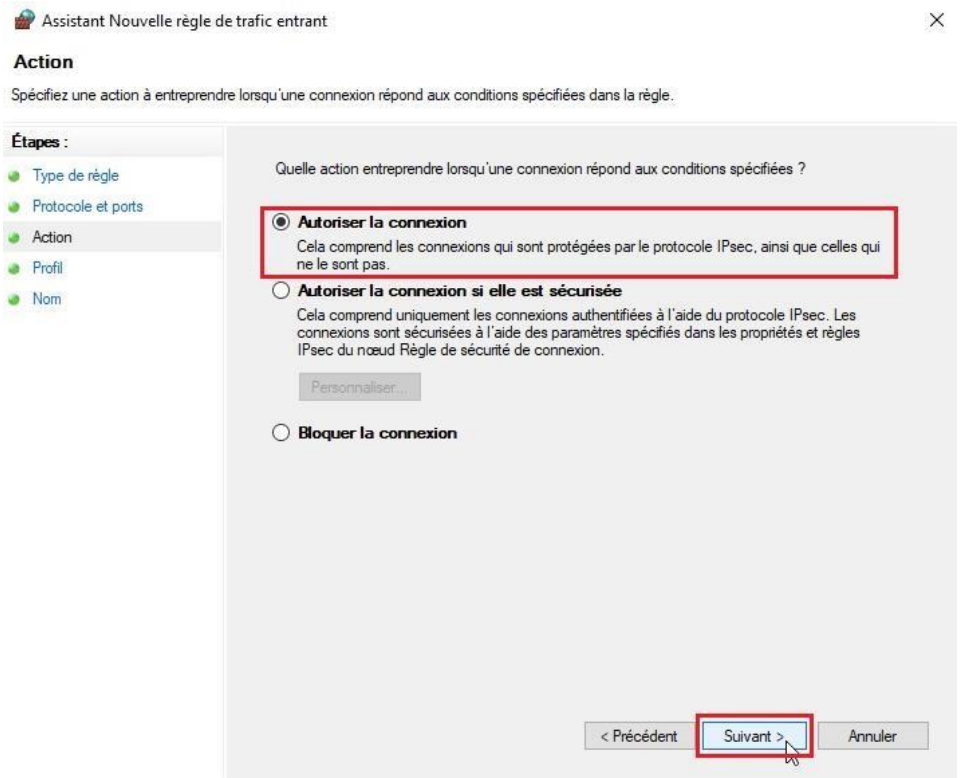
Sur la partie gauche de la fenêtre nous allons cliquer sur Règles de trafic entrant puis cliquer sur Nouvelle règle.



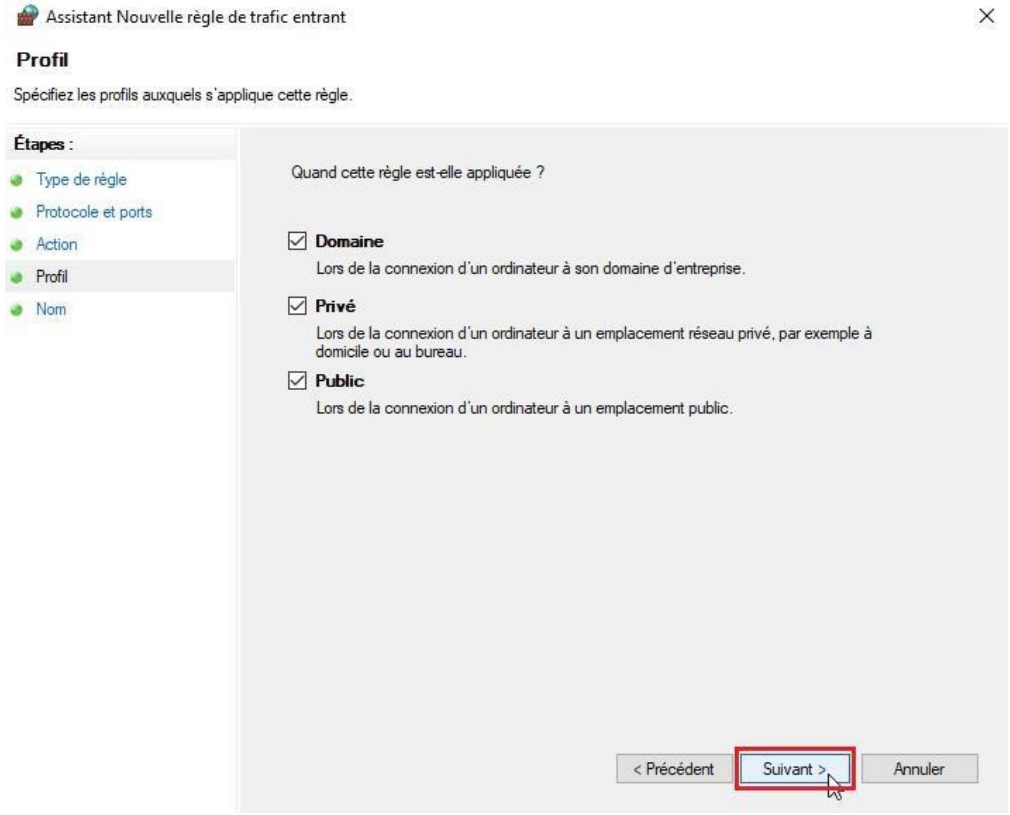
Ici, nous allons sélectionner l'option Port puis cliquer sur Suivant.



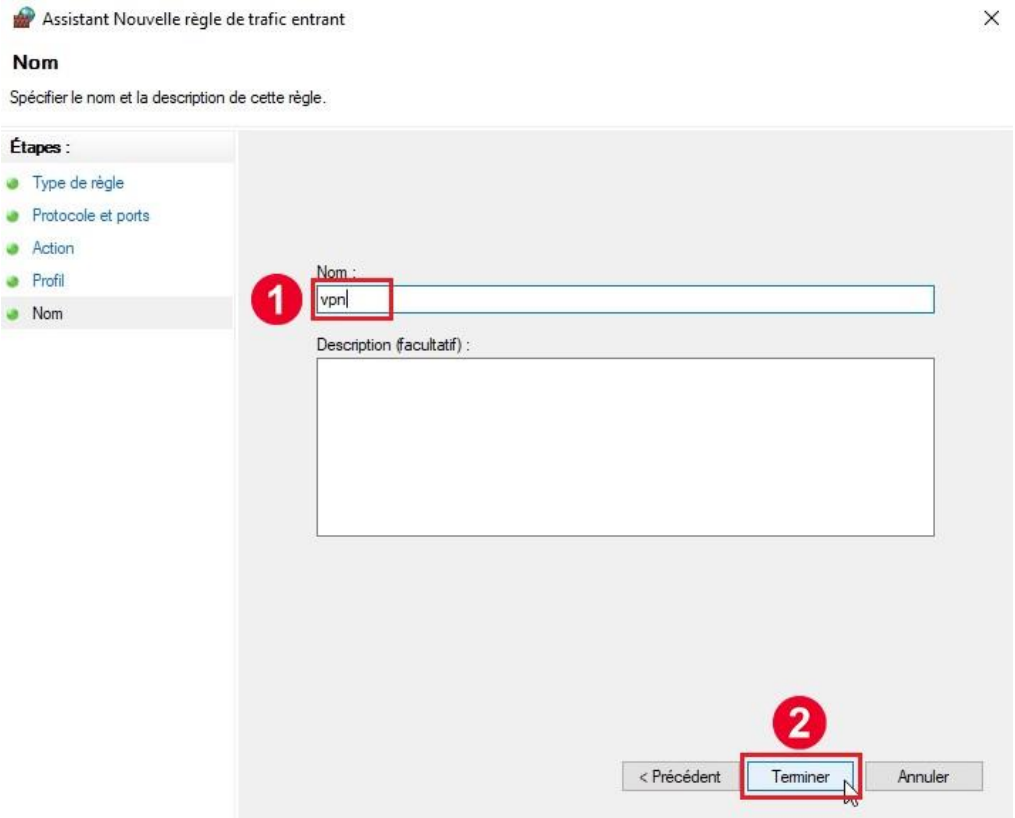
Nous allons ensuite sélectionner UDP puis dans Ports locaux spécifiques, nous allons rentrer les ports suivants séparés de virgules : 500, 1701, 4500 et cliquer sur Suivant.



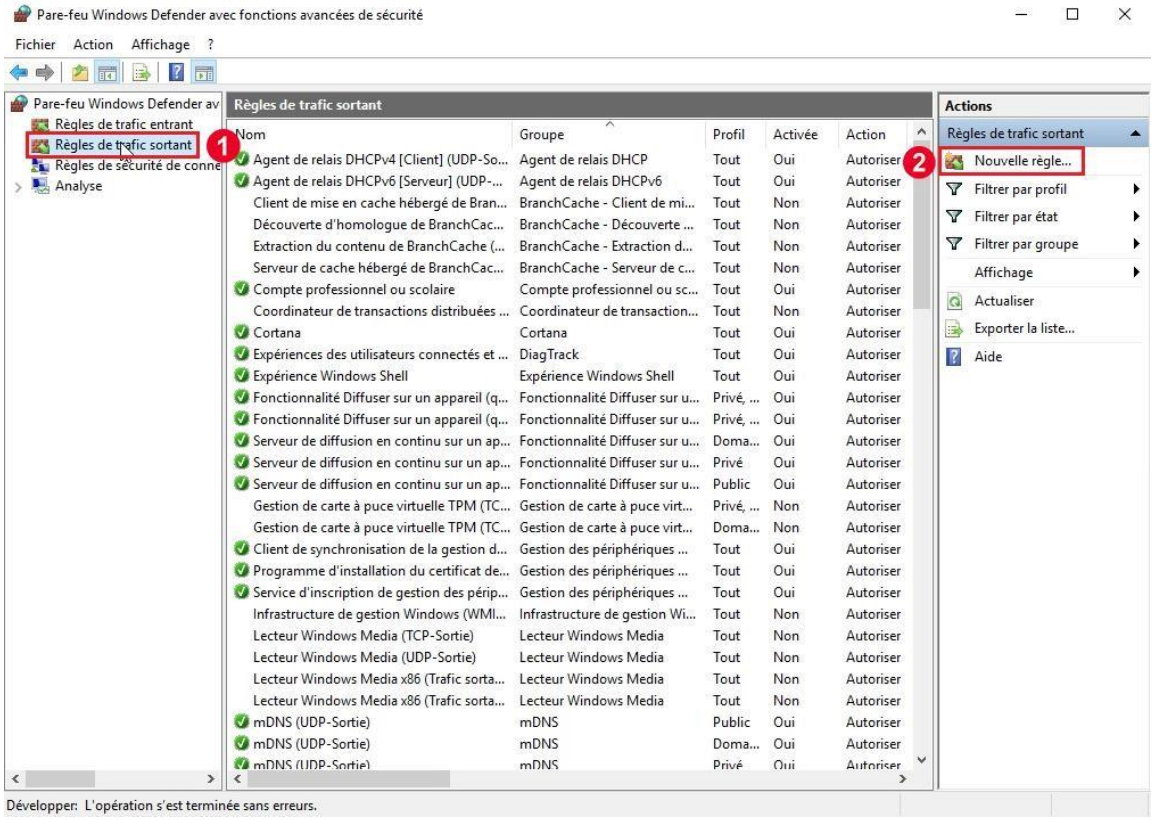
Dans la page Action, nous allons vérifier que l'option Autoriser la connexion est sélectionnée et cliquer sur Suivant.



Ici, nous pouvons laisser les options par défaut et cliquer sur Suivant.

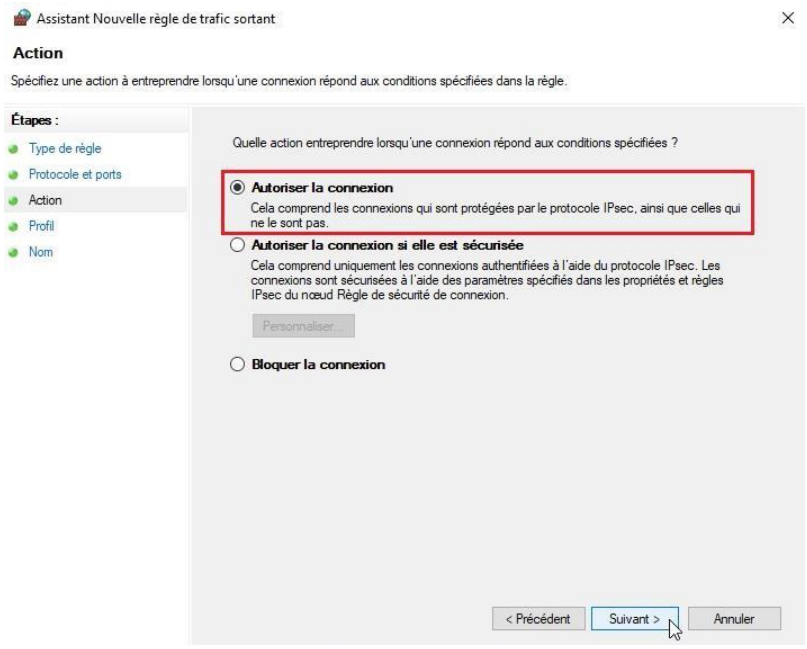


Enfin, nous devons donner un nom arbitraire à la règle et cliquer sur Terminer.



Nous pouvons maintenant cliquer sur Règles de trafic sortant puis sur Nouvelle règle.

Ici, nous allons reproduire les mêmes paramètres que pour la règle de trafic entrant (Ports ; UDP ; 500, 1701, 4500).
Il faudra cependant bien s'assurer que l'option Autoriser la connexion est sélectionnée dans la page Action.

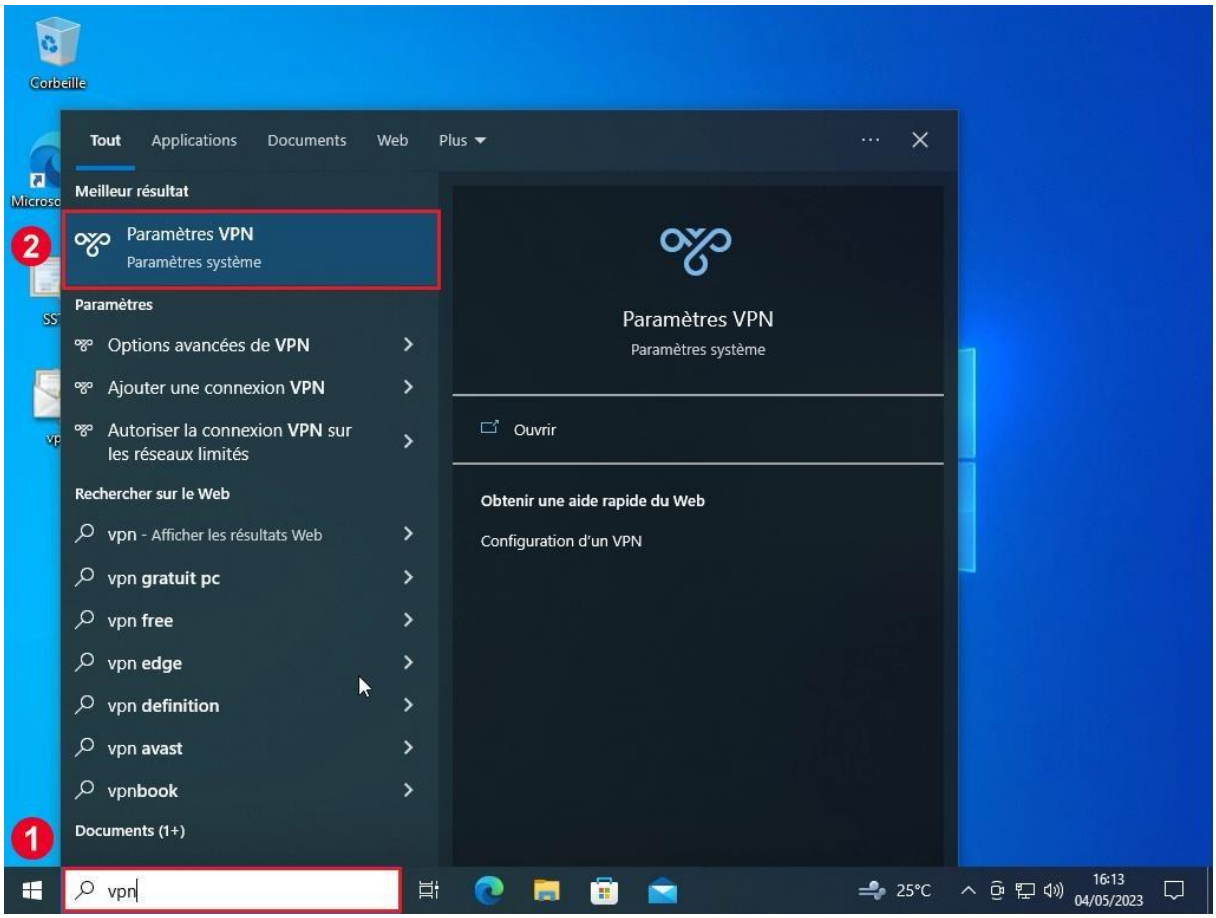


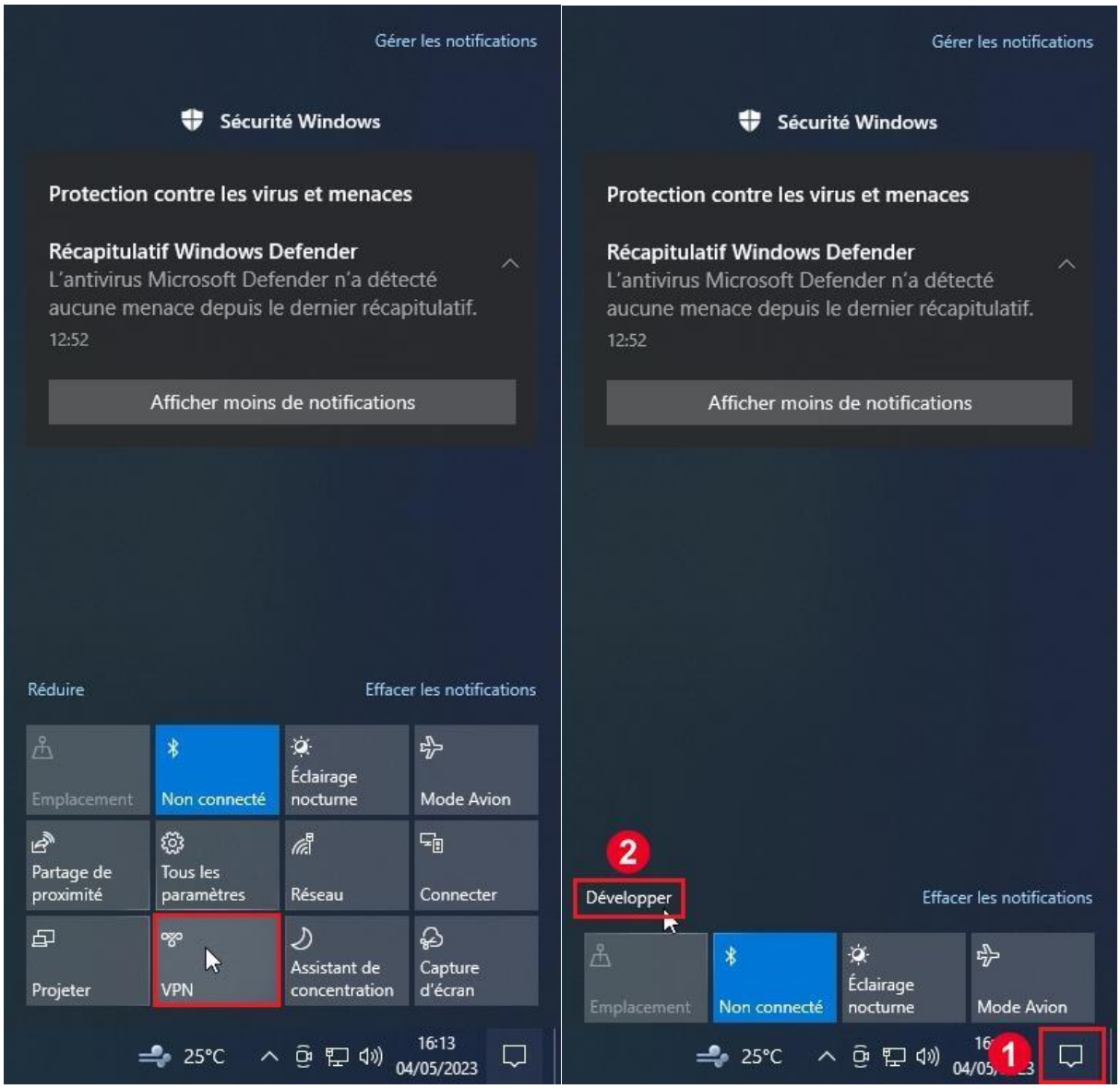
Une fois nos 2 règles créées, nous avons donc fini de configurer notre VPN coté serveur.

4.4 Configuration du Client VPN sur Windows 10

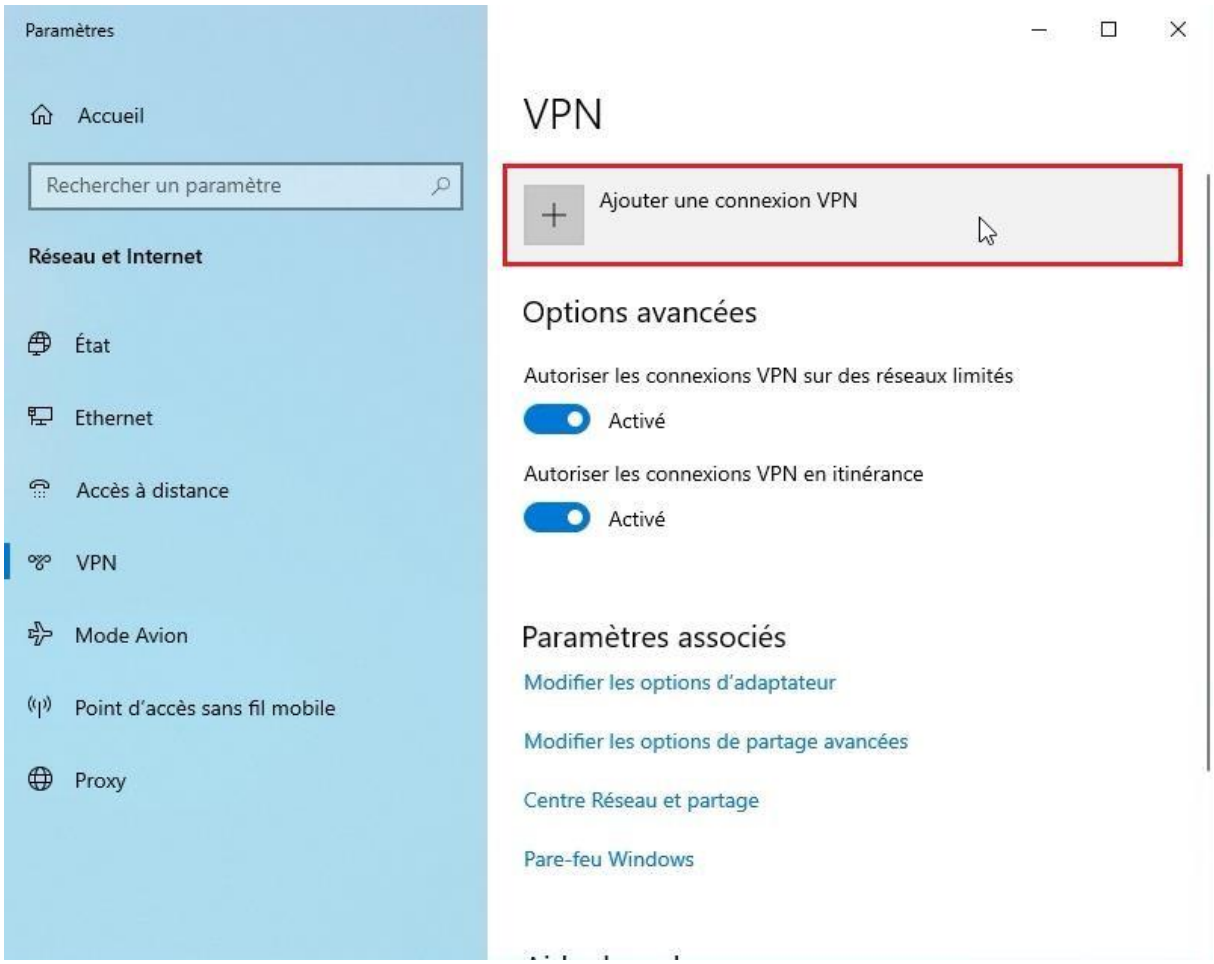
4.4.1 Options VPN

Nous allons donc passer à la configuration du VPN sur notre client Windows 10.
Une fois notre Windows 10 lancé, nous pouvons directement nous rendre dans les paramètres VPN pour configurer notre tunnel.
Pour ce faire, nous pouvons chercher VPN dans la barre de recherche Windows.





Il est aussi possible d'atteindre la configuration vpn en cliquant sur l'icône Notifications dans la barre de tâches puis sur l'icône VPN (vous aurez peut-être besoin de cliquer sur Développer pour voir toutes les icones)



Ici, il nous suffit de cliquer sur Ajouter une connexion VPN.

Enfin, nous devons remplir les informations suivantes puis cliquer sur Enregistrer :

Fournisseur VPN : Windows (intégré)

Nom de la connexion : *nom arbitraire*

Nom ou adresse du serveur : *adresse IPv4 du Windows Server*

Type de réseau privé virtuel : L2TP/IPsec avec clé pré-partagée

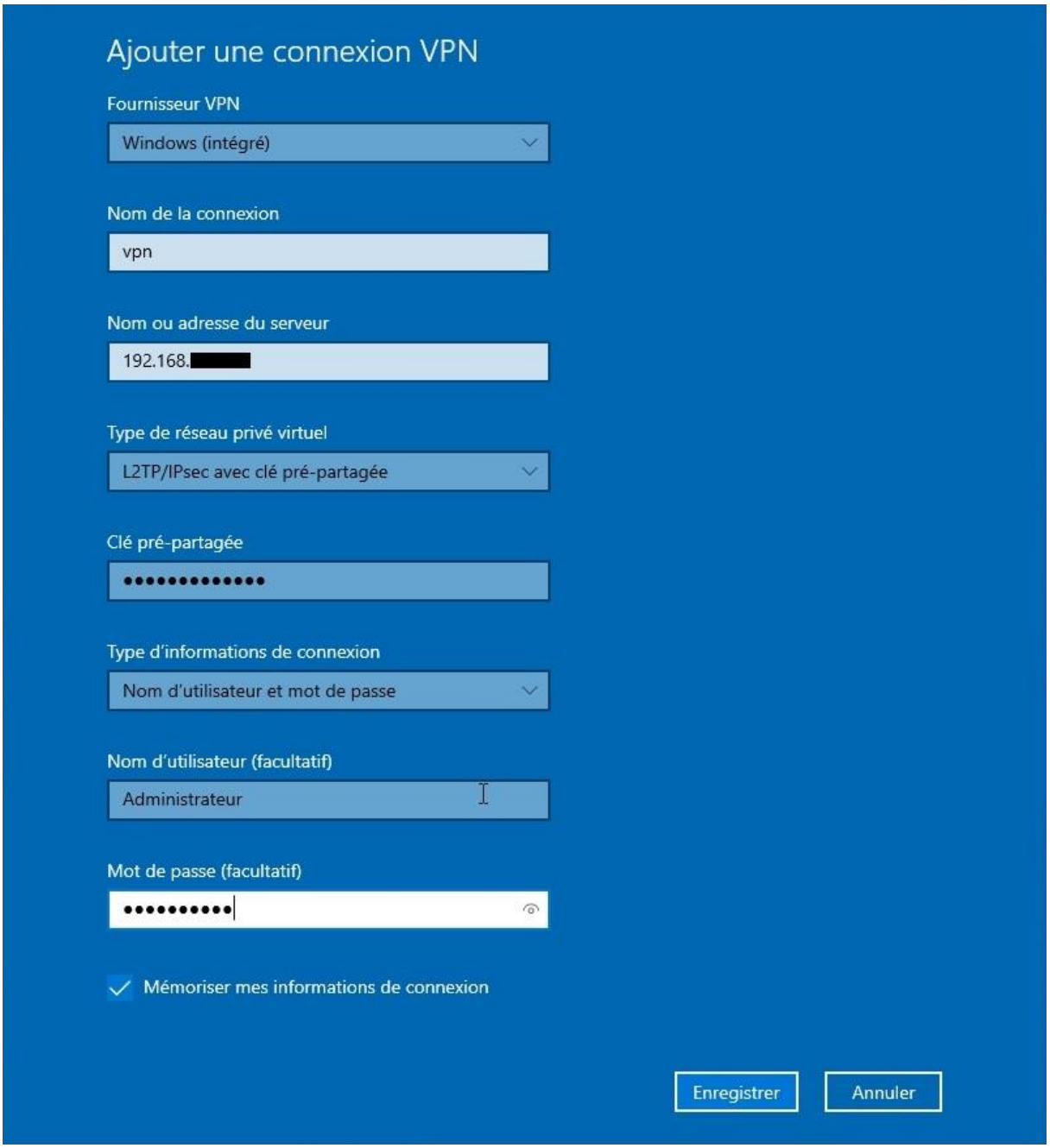
Clé pré-partagée : *clé pré-partagée créée sur Windows Server*

Type d'informations de connexion : Nom d'utilisateur et mot de passe

Nom d'utilisateur : Administrateur

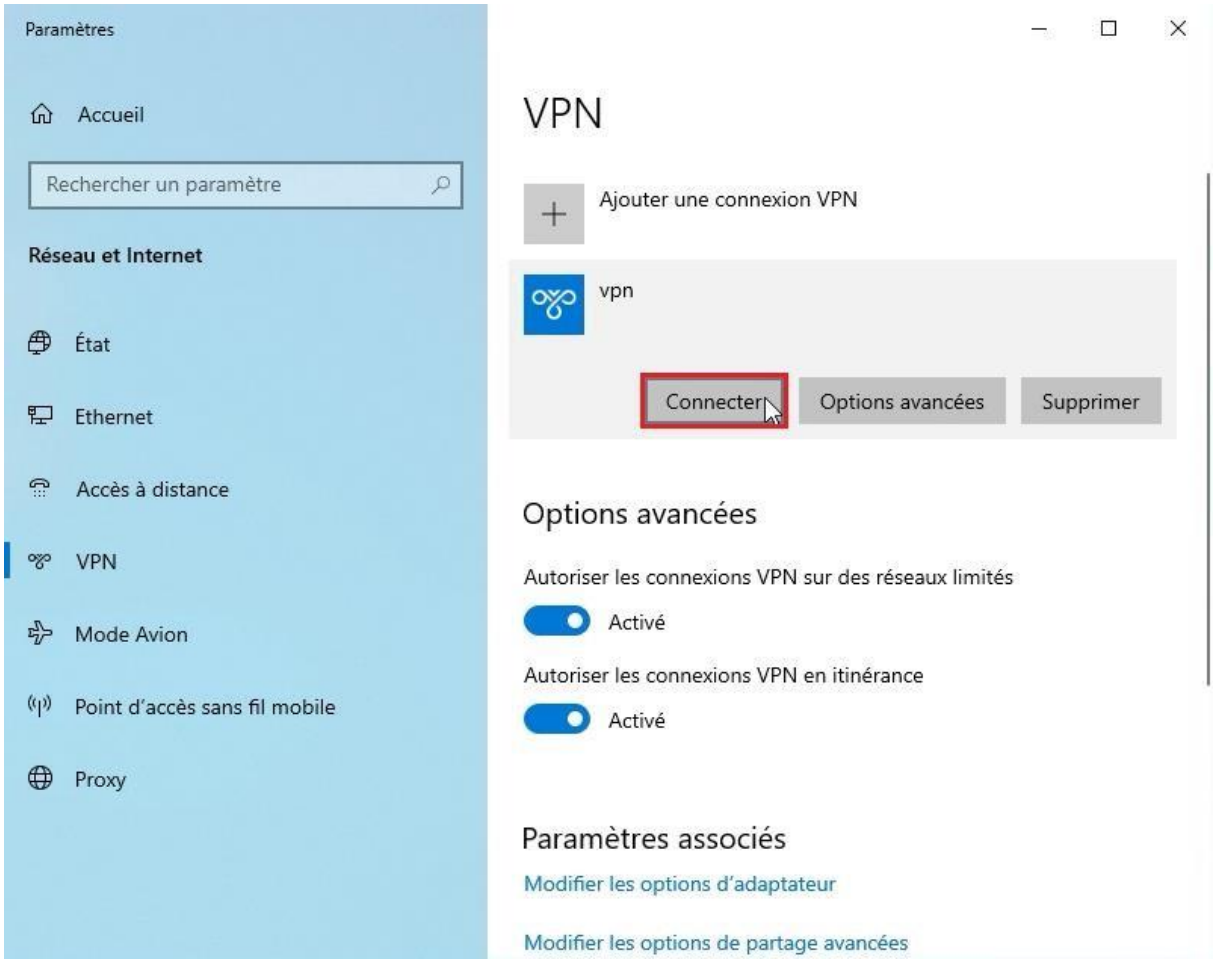
Mot de passe : *mdp du compte Administrateur*

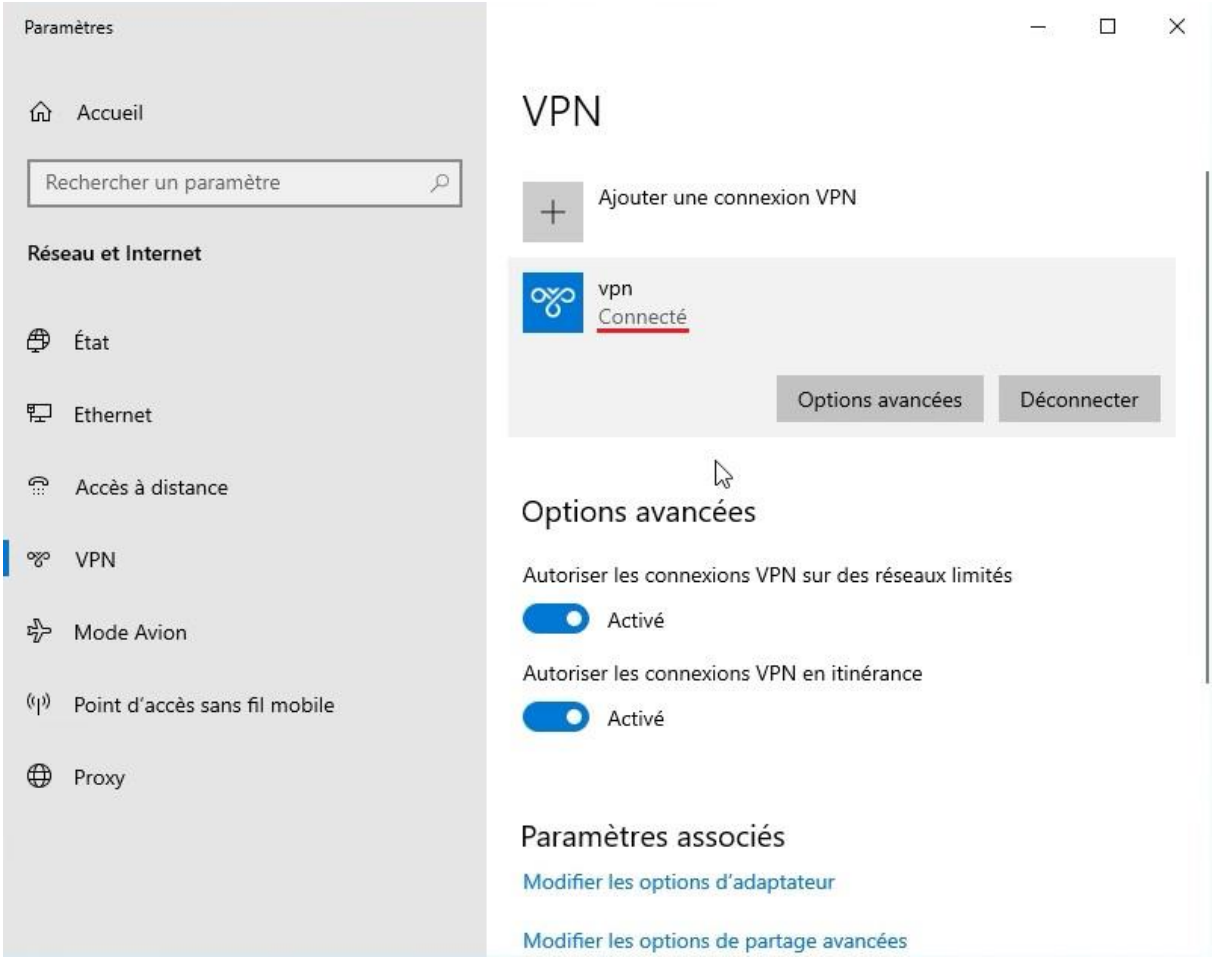
Une fois ces informations remplies, cette page devrait ressembler à cela :



4.4.2 Connexion VPN

Pour utiliser notre VPN, nous pouvons maintenant retourner sur la page de configuration VPN, sélectionner le VPN que nous avons créé et cliquer sur Connecter.





Après un cours chargement, le message Connecté devrait s'afficher en dessous du VPN utilisé.

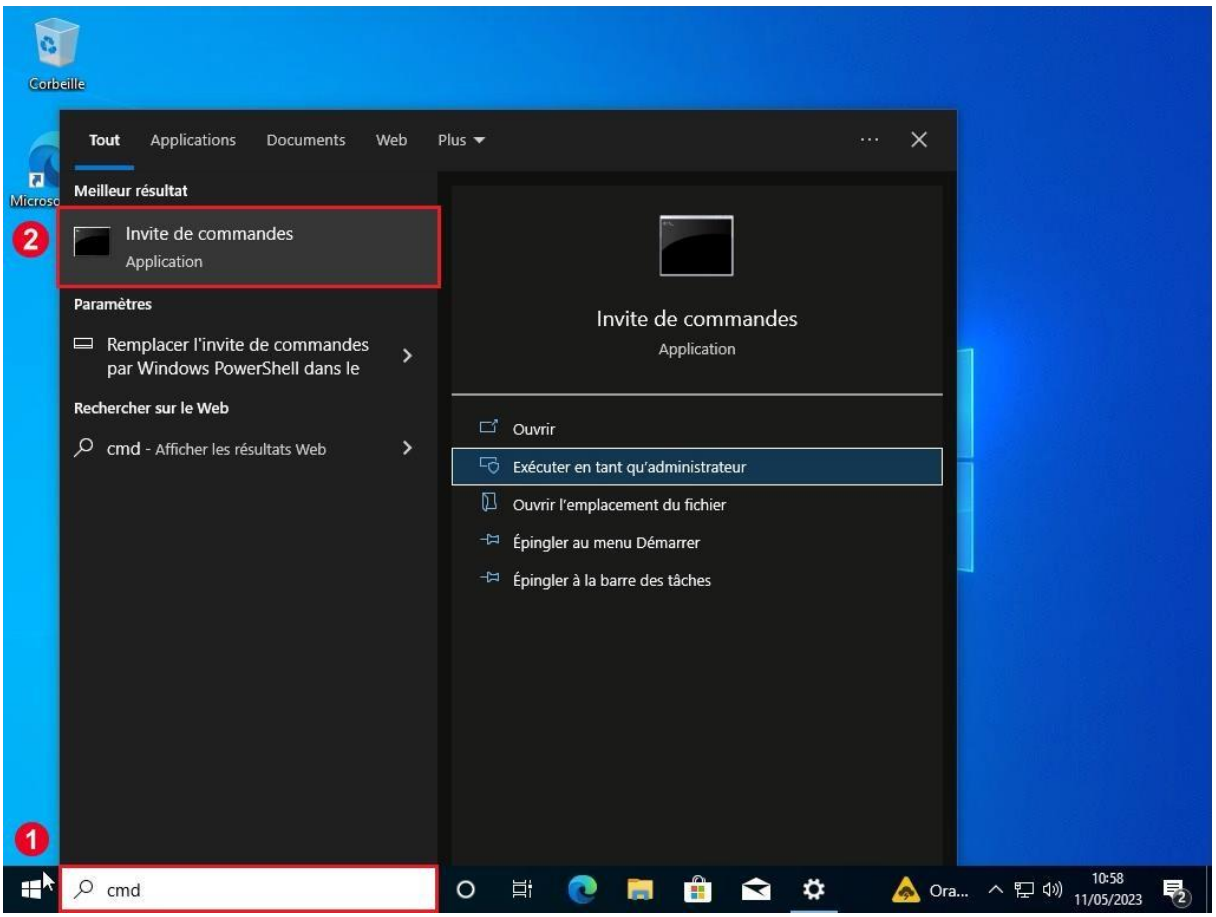
Nous venons ainsi de créer un tunnel VPN permettant à nos deux machines virtuelles de communiquer de façon sécurisée à travers Internet.

4.5 Vérification de l'Installation

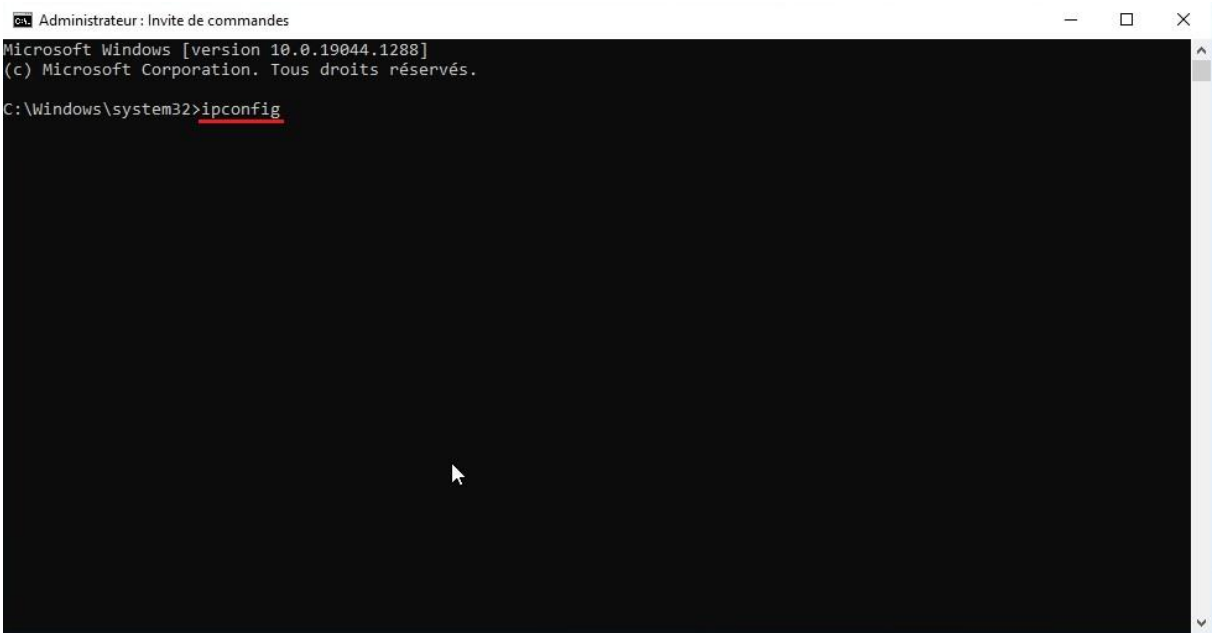
Afin de vérifier le bon fonctionnement de notre VPN nous allons maintenant utiliser plusieurs outils pour diagnostiquer notre réseau VPN.

4.5.1 Vérification Côté Client

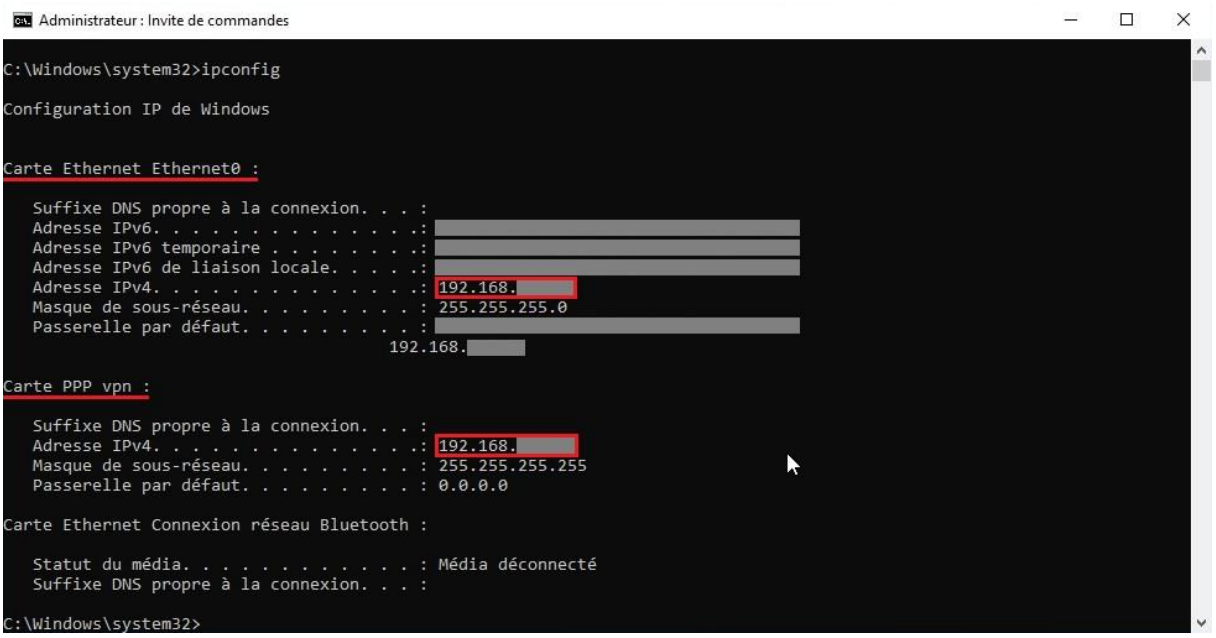
Une fois que notre VPN annonce qu'il est connecté sur notre client Windows 10, nous pouvons vérifier cette connexion grâce à la commande ipconfig.



Pour ce faire, nous allons ouvrir l'invite de commandes en tapant cmd dans la barre de recherche Windows, puis en cliquant sur l'application Invite de commandes.



Une fois l'invite de commande ouvert, nous allons taper la commande ipconfig puis appuyer sur la touche Entrée pour exécuter la commande.



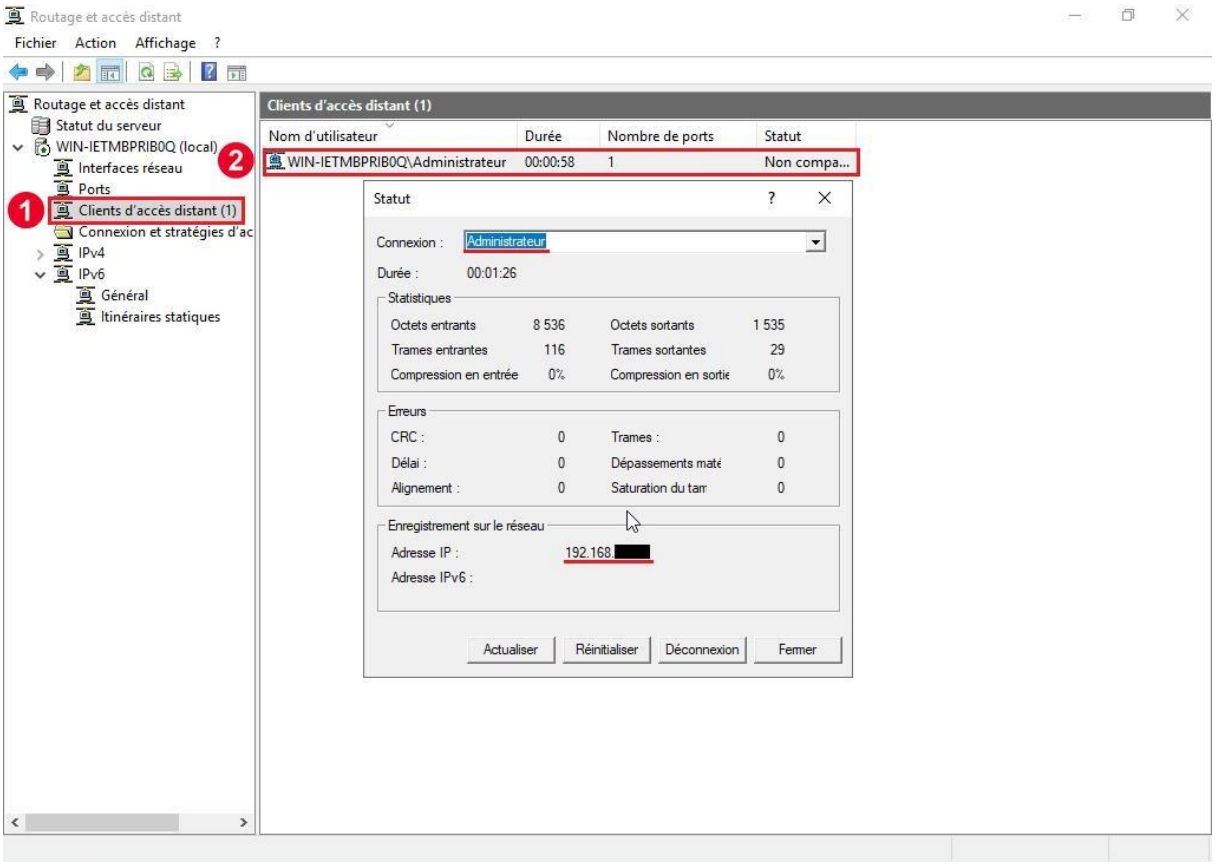
Si VPN est bien connecté, les informations suivantes devraient s'afficher :

- Carte Ethernet suivi de notre adresse IP locale
- Carte PPP vpn suivi de notre adresse IP vpn

Ici, nous pouvons voir que nous avons bien ces deux adresses IP sur deux cartes réseaux différentes. Nous pouvons donc en conclure que notre VPN est bien connecté.

4.5.2 Vérification Côté Serveur

Pour finir, nous allons vérifier que notre serveur VPN est bien capable d'identifier les clients VPN auxquels il est connecté.



Pour ce faire, nous allons retourner dans le service Routage et accès distant.

Ici, nous allons simplement cliquer sur le dossier Clients d'accès distant (1), puis vérifier que notre client Windows 10 est bien dedans. Nous pouvons même cliquer sur notre client pour avoir plus d'informations sur le compte et l'adresse IP utilisés pour établir cette connexion.

Dans notre cas, nous pouvons voir que l'utilisateur affiché correspond bien au client VPN que nous avons configuré. Nous pouvons donc en conclure que la connexion VPN entre notre client et notre serveur est bien établie.

5 Sources

https://blog.avast.com/fr/windows-server-vs-windows-quelle-est-la-difference
https://learn.microsoft.com/en-us/windows/win32/srvnodes/windows-server
https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-vpn-inwindows-server-essentials https://learn.microsoft.com/fr-fr/windows-server/remote/remote-access/get-startedinstall-ras-as-vpn?tabs=powershell
https://learn.microsoft.com/fr-fr/windows-server/remote/remote-access/tutorial-aovpndeploy-setup https://www.snel.com/support/how-to-set-up-an-l2tp-ipsec-vpn-on-windows-server-2019/#:~:text=A%20VPN%20or%20Virtual%20Private,connected%20over%20a%20private%20network. https://www.expressvpn.com/what-is-vpn/protocols/pptp
https://www.okta.com/identity-101/pap-security/
https://docs.oracle.com/cd/E56338_01/html/E53884/pppsvrconfig.reference-21.html
https://www.tutorialspoint.com/challenge-handshake-authentication-protocol-chap
https://learn.microsoft.com/fr-fr/windows-server/networking/technologies/extensibleauthentication-protocol/network-access
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
https://supporthost.in/how-to-setup-l2tp-vpn-on-windows-server-2019/
https://www.vpnmonami.com/vpn-pour-les-nuls/ https://www.le-vpn.com/fr/pptp/#:~:text=Protocole%20PPTP%20Le%20Protocole%20PPTP%20%28de%20l%E2%80%99anglais%20Point-to-Point,un%20tunnel%20GRE%20pour%20encapsuler%20des%20paquets%20PPP
https://fr.wizcase.com/blog/les-protocoles-de-securite-vpn-expliques-comprendre-lepptp/#:~:text=PPTP%20est%20%C3%A9conomique.-,Inconv%C3%A9nients,PPTP%20n'est%20pas%20recommand%C3%A9
http://www.ordinateur.cc/r%C3%A9seaux/R%C3%A9seau-Internet/67354.html
https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/pptp
https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-gre-tunneling/
https://4sysops.com/archives/how-to-setup-an-sstp-vpn-server-with-windows-server/
https://www.purevpn.fr/blog/openvpn-vs-sstp-vpn/#:~:text=Mais%20si%20vous%20%C3%AAtes%20un,pas%20sur%20les%20appareils%20mobiles

https://www.purevpn.fr/quest-ce-quun-vpn/protocoles/l2tp https://www.bicomm.fr/livebox-v3-redirection-de-ports-vpn-l2tp-ipsec/

https://www.vpnmonami.com/quest-ce-que-l2tp/#:~:text=L'acronyme%20L2TP%20signifie%20Layer,priv%C3%A9%20sur%20des%20r%C3%A9seaux%20publics https://rdr-it.com/serveur-vpn-windows-server-installation-configuration/4/ https://informerick.com/tutoriels-informatique/creer-vpn-server-windows/#:~:text=En%20bref%2C%20c'est%20un,Allez%20dans%20les%20param%C3%A8tres%20Windows https://4sysops.com/archives/how-to-setup-an-sstp-vpn-server-with-windows-server/