

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

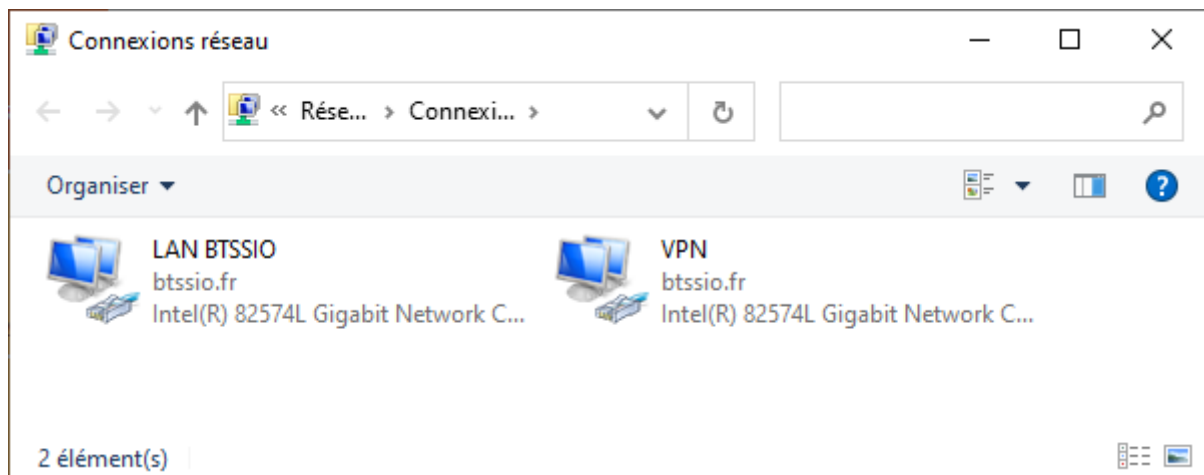
- 1 Active Directory
- 1 Serveur VPN
- Mot de passe Administrateur du domaine

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.

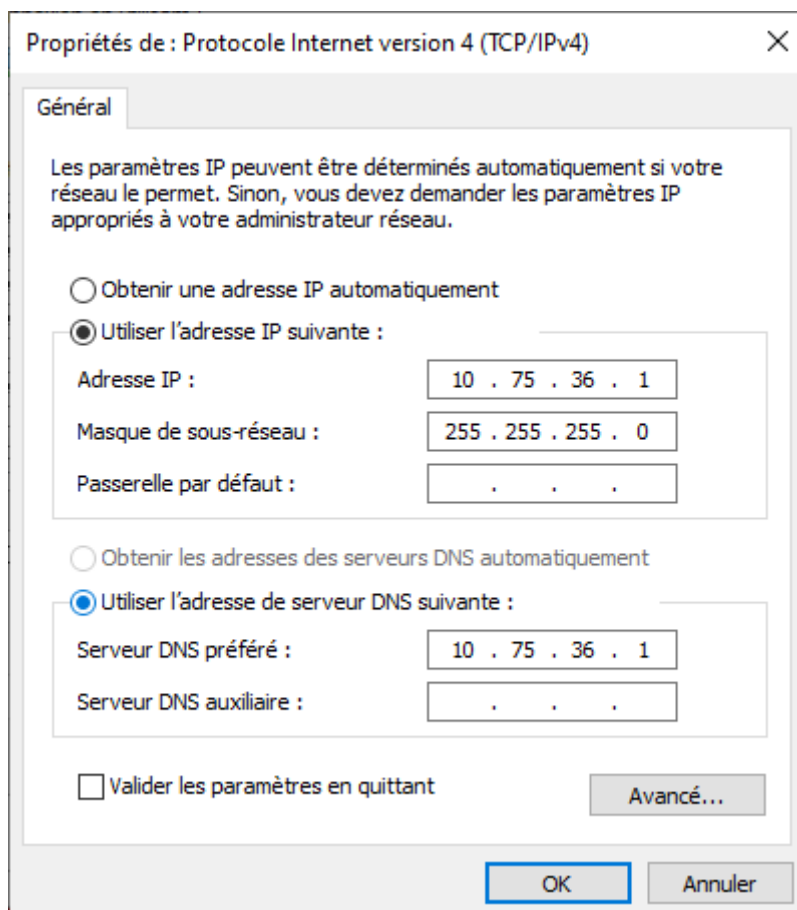
III – Préparation du serveur

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

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 115 . 254

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 115 . 2

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 10 . 75 . 36 . 1

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

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** »

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window. The title bar includes the application icon and name. The window has a standard Windows title bar with minimize, maximize, and close buttons. The main content area is titled 'Avant de commencer' in blue. On the right, it says 'SERVEUR DE DESTINATION dc1.btssio.fr'. On the left, there is a vertical list of steps: 'Avant de commencer' (highlighted in blue), 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'Confirmation', and 'Résultats'. The main text area contains the following information:

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
[Démarrer l'Assistant de Suppression de rôles et de fonctionnalités](#)

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

☐ Ignorer cette page par défaut

At the bottom, there are four buttons: '< Précédent', 'Suivant >' (highlighted with a dashed border), 'Installer', and 'Annuler'.

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

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window at the 'Sélectionner le type d'installation' step. The title bar and window controls are the same. The main content area is titled 'Sélectionner le type d'installation' in blue. On the right, it says 'SERVEUR DE DESTINATION dc1.btssio.fr'. On the left, the vertical list of steps is: 'Avant de commencer', 'Type d'installation' (highlighted in blue), 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'Confirmation', and 'Résultats'. The main text area contains the following information:

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

☒ **Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

☐ **Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

At the bottom, there are four buttons: '< Précédent', 'Suivant >' (highlighted with a dashed border), 'Installer', and 'Annuler'.

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

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER le serveur de destination

SERVEUR DE DESTINATION
dc1.btssio.fr

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
dc1.btssio.fr	10.75.36.1,192.168.115.254	Microsoft Windows Server 2022 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

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

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER des rôles de serveurs

SERVEUR DE DESTINATION
dc1.btssio.fr

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Accès à distance
Services de rôle
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

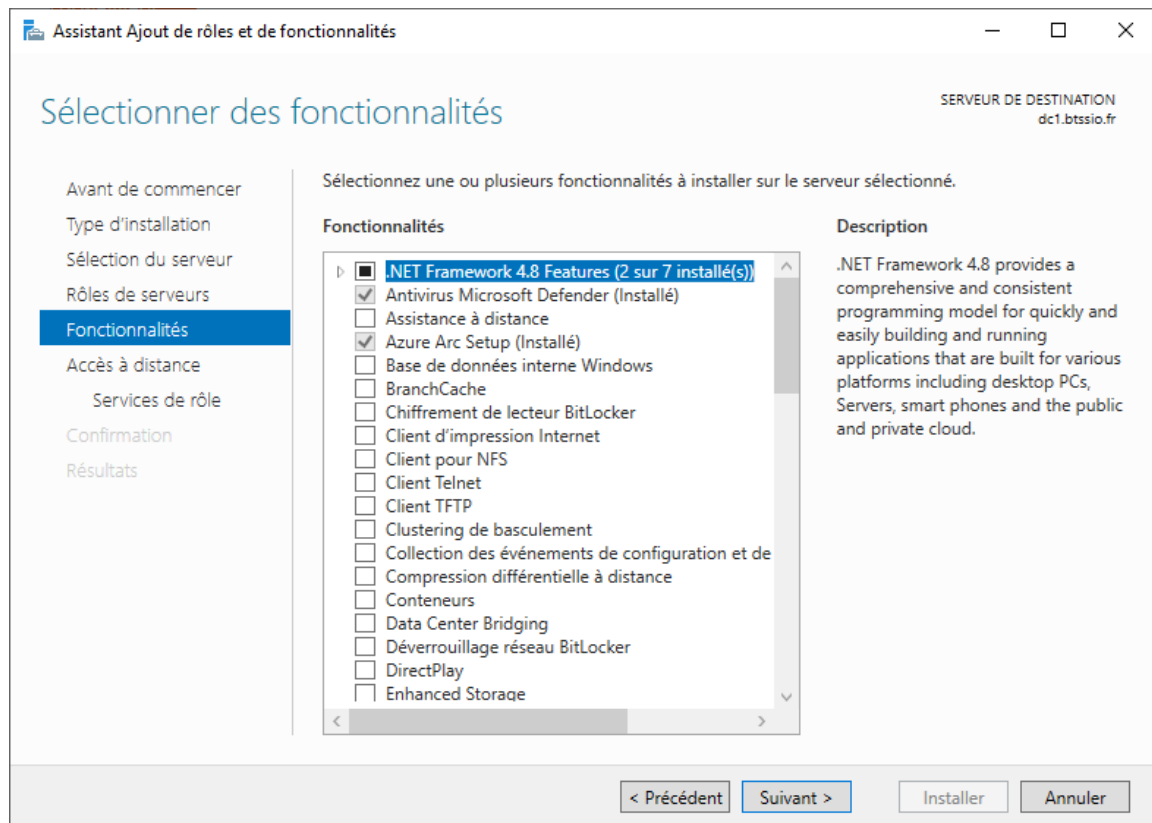
- ☒ Accès à distance
- ☐ Attestation d'intégrité de l'appareil
- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☒ Serveur DHCP (Installé)
- ☒ Serveur DNS (Installé)
- ☒ Serveur Web (IIS) (8 sur 43 installé(s))
- ☐ Service Guardian hôte
- ☒ Services AD DS (Installé)
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☐ Services de certificats Active Directory
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (2 sur 12 installés)
- ☐ Services de stratégie et d'accès réseau
- ☐ Services WSUS (Windows Server Update Services)

Description

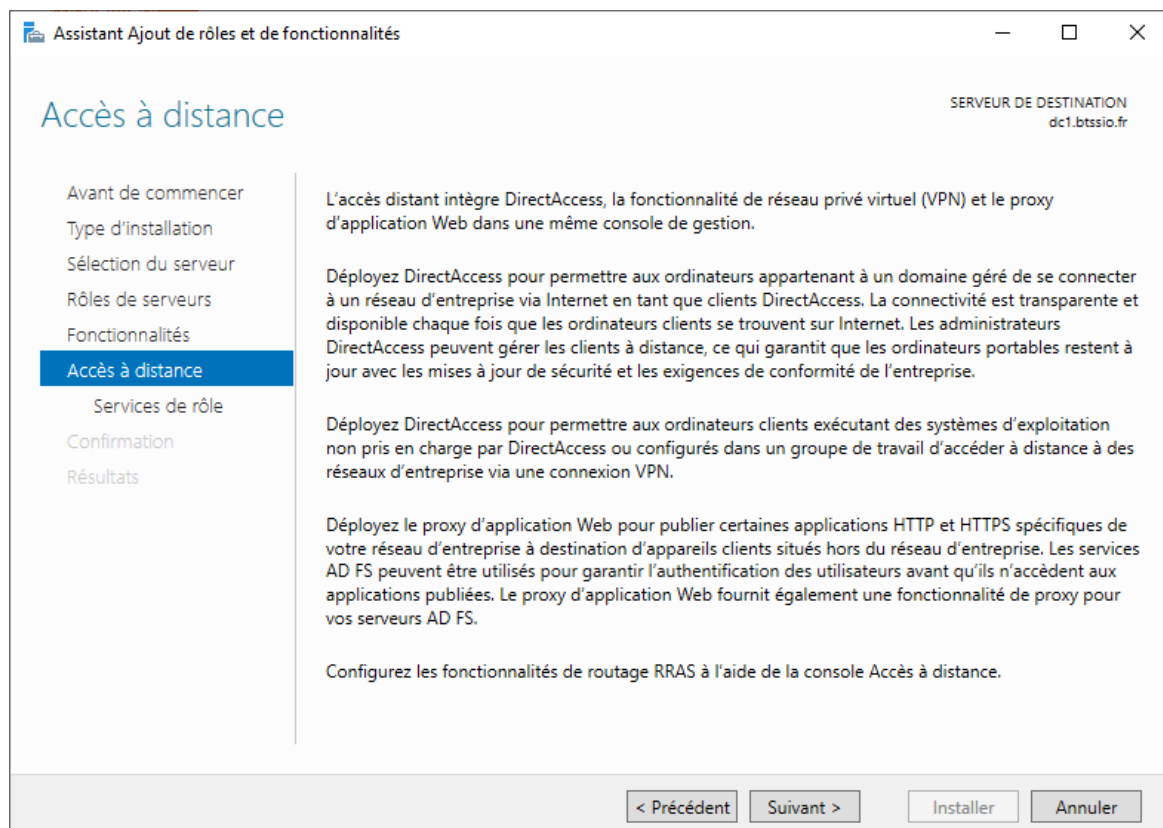
L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.

< Précédent Suivant > Installer Annuler

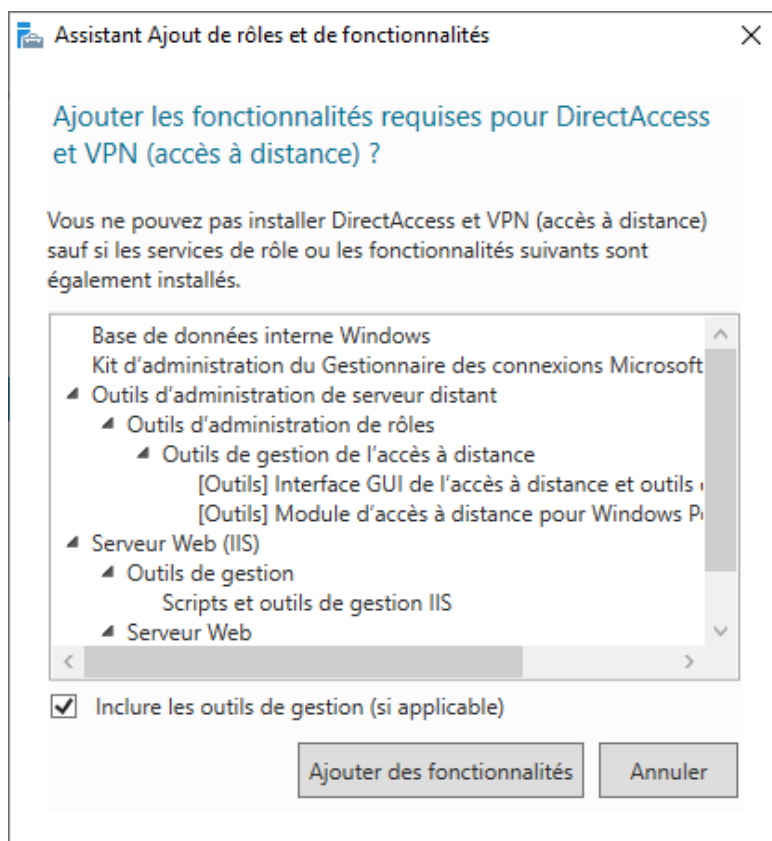
Laissez les fonctionnalités choisies par défaut et cliquez sur « **Suivant** »



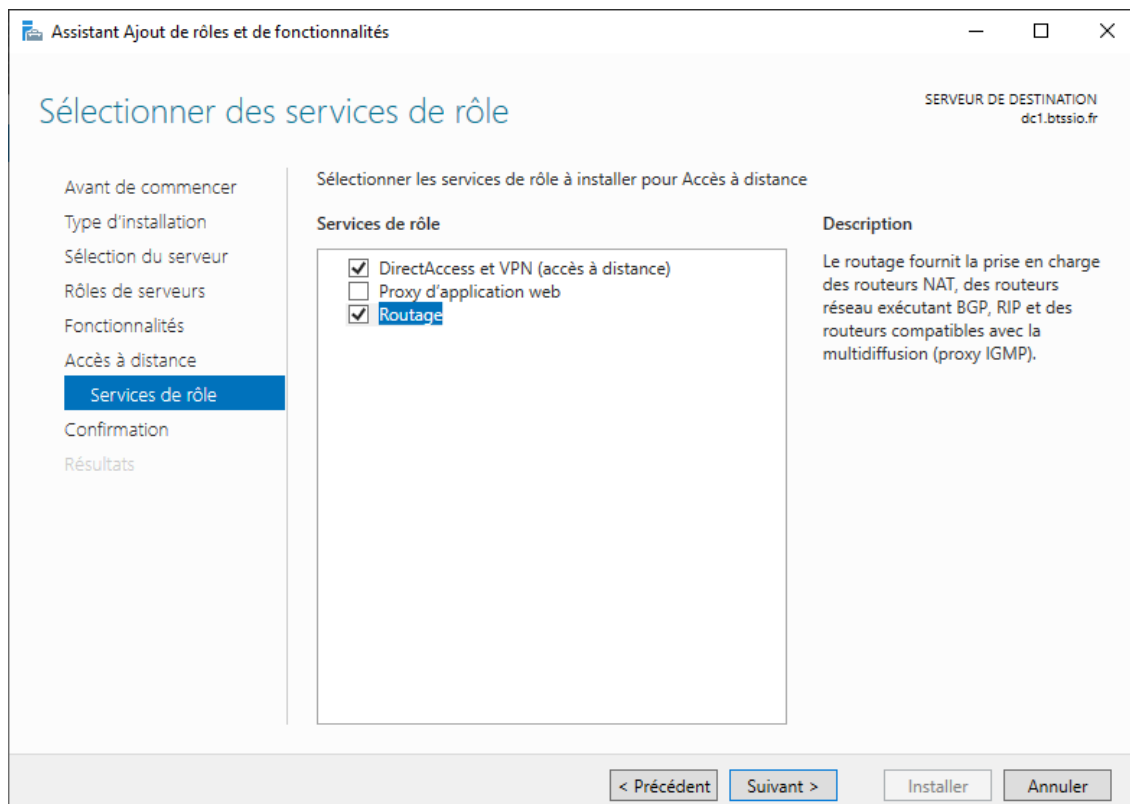
Cliquez sur « **Suivant** »



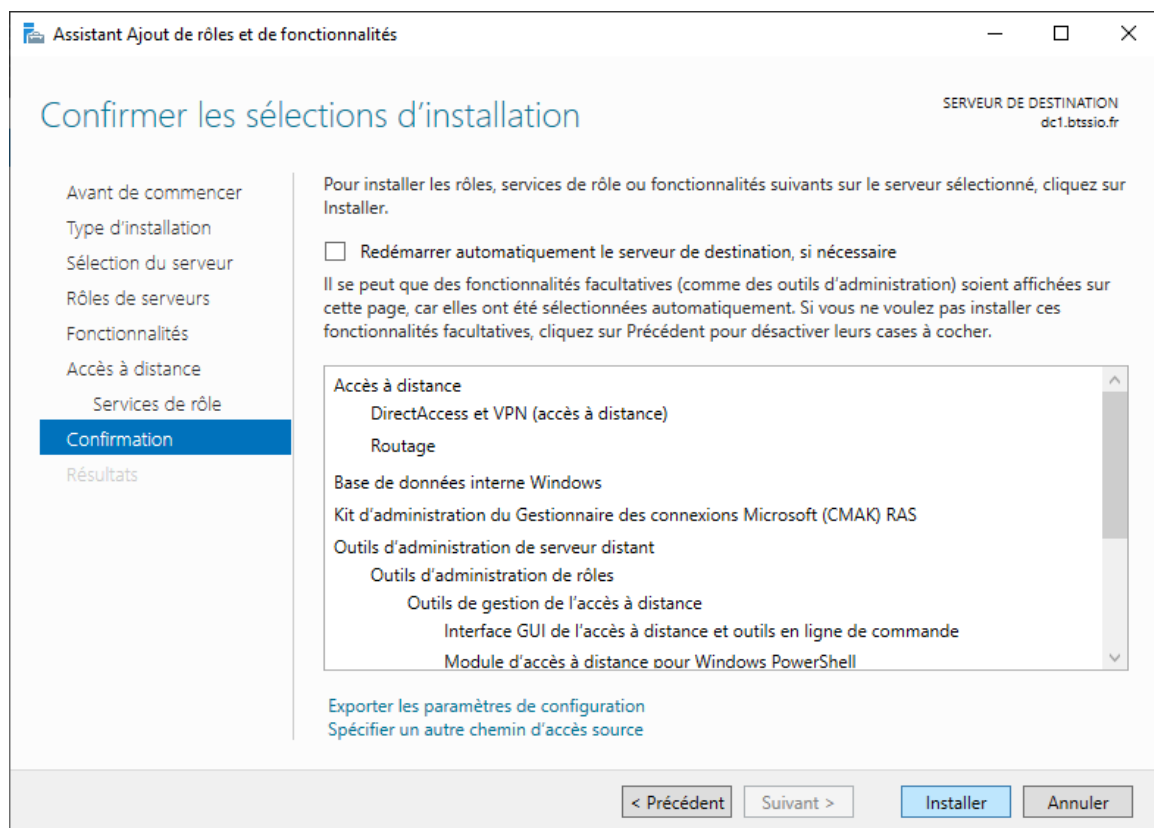
Cliquez sur « **Ajouter les fonctionnalités** »



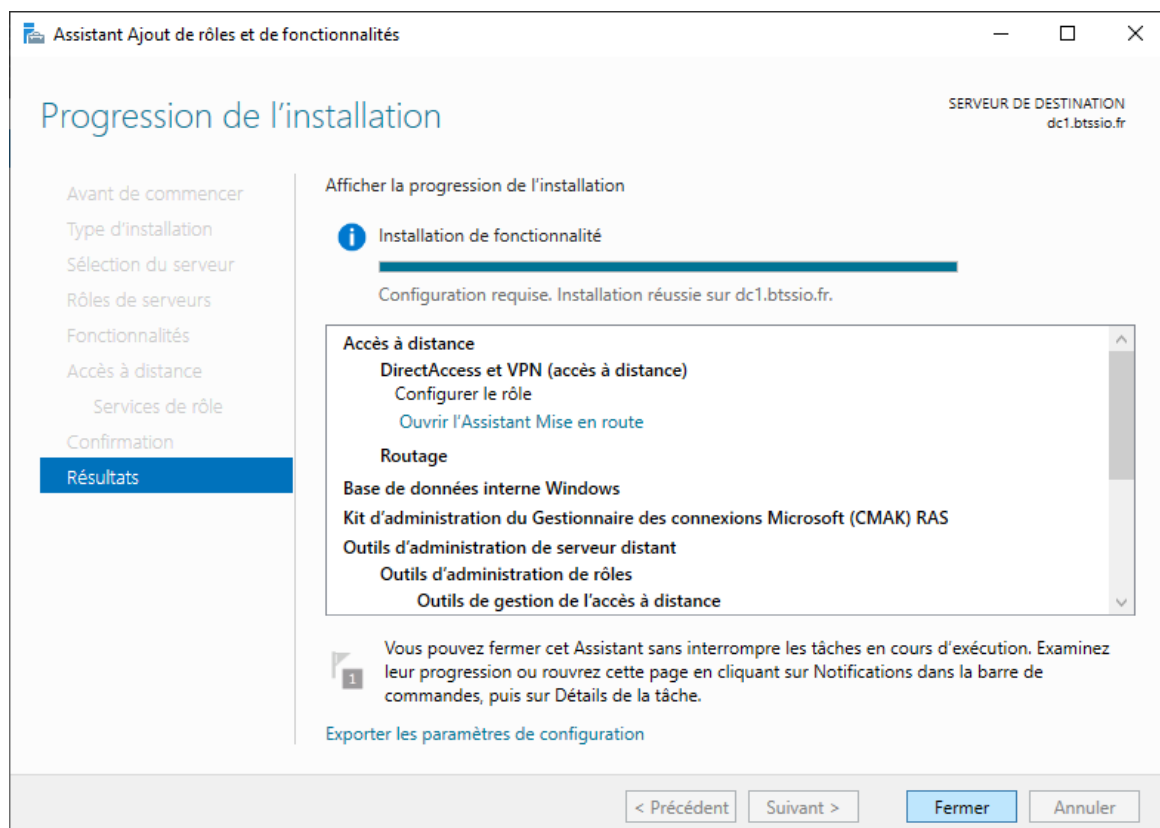
Cochez « **DirectAccess et VPN** » et « **Routage** » puis cliquez sur « **Suivant** »



Cliquez sur « **Installer** »



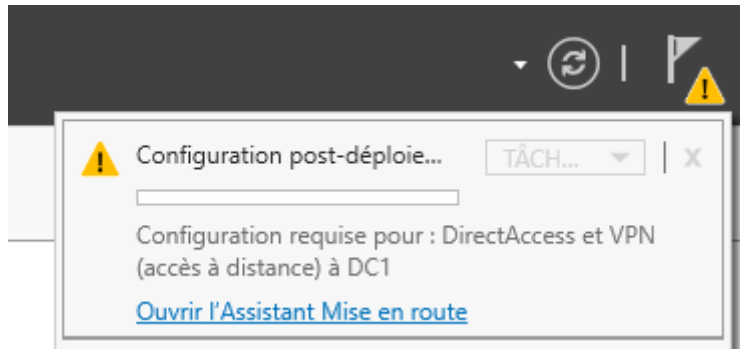
Une fois l'installation terminée, cliquez sur « **Fermer** »



III – Configuration du service VPN

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

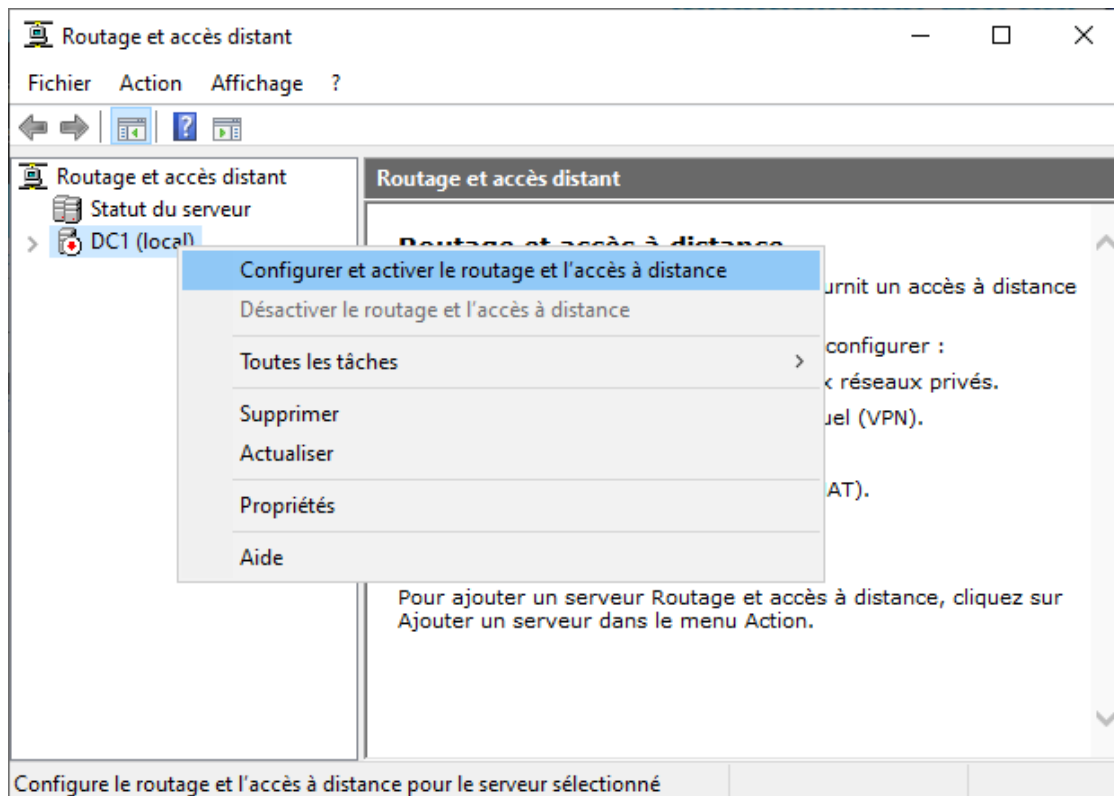
Rendez-vous dans le centre de notification du Gestionnaire de serveur et cliquez sur « **Ouvrir l'Assistant Mise en route** »



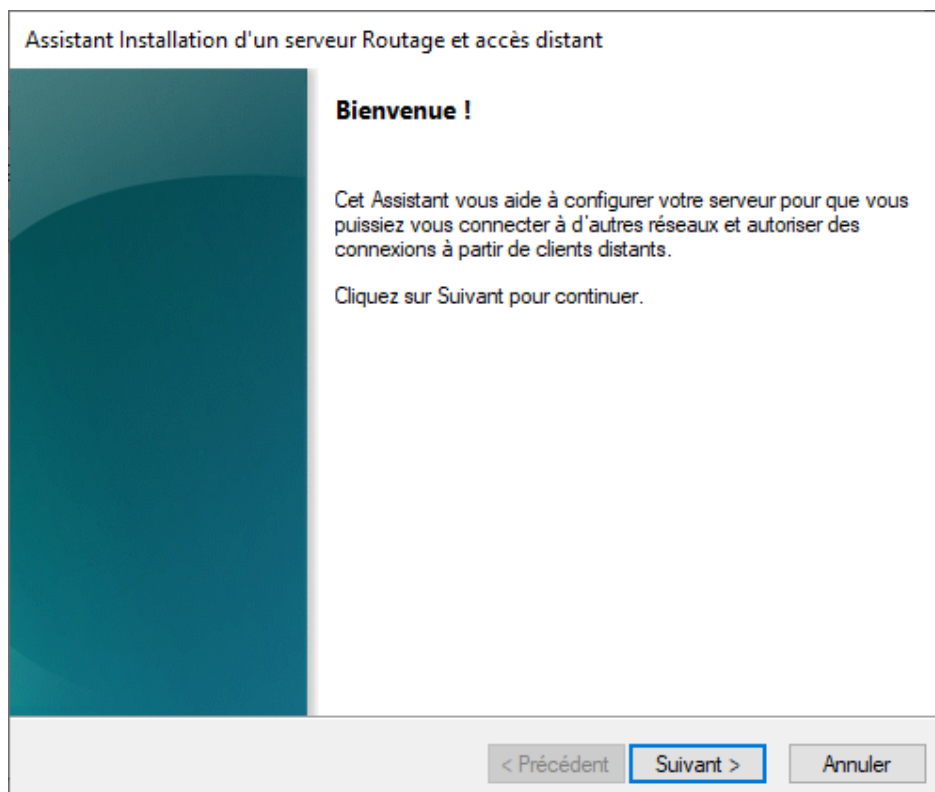
Une fois l'assistant lancé, cliquez sur « **Déployer VPN uniquement** »



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** »

Assistant Installation d'un serveur Routage et accès distant

Configuration

Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.

- ☐ Accès à distance (connexion à distance ou VPN)
Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).
- ☐ NAT (Network address translation)
Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.
- ☒ Accès VPN (Virtual Private Network) et NAT
Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.
- ☐ Connexion sécurisée entre deux réseaux privés
Connecter ce réseau à un réseau distant tel que celui d'une succursale.
- ☐ Configuration personnalisée
Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.

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

Assistant Installation d'un serveur Routage et accès distant

Connexion VPN

Au moins une interface réseau doit être connectée à Internet afin de permettre aux clients VPN de se connecter à ce serveur.

Sélectionnez l'interface réseau qui connecte ce serveur à Internet.

Interfaces réseau :

Nom	Description	Adresse IP
LAN BTSSIO	Intel(R) 82574L Gigabit Ne...	10.75.36.1
VPN	Intel(R) 82574L Gigabit Ne...	172.16.1.253

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

Assistant Installation d'un serveur Routage et accès distant

Attribution d'adresses IP

Vous pouvez sélectionner la méthode d'assignation des adresses IP aux clients.

Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?

☒ **Automatiquement**
Si vous utilisez un serveur DHCP pour attribuer des adresses, vérifiez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.

☐ À partir d'une plage d'adresses spécifiée

< Précédent Suivant > Annuler

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

Assistant Installation d'un serveur Routage et accès distant

Gestion de serveurs d'accès à distance multiples

Des demandes de connexion peuvent être authentifiées localement ou transférées à un serveur RADIUS (Remote Authentication Dial-In User Service) pour être authentifiées.

Bien que le Routage et l'accès à distance permettent l'authentification de demandes de connexion, des réseaux de grande taille incluant plusieurs serveurs d'accès à distance utilisent souvent un serveur RADIUS pour centraliser l'authentification.

Si vous utilisez un serveur RADIUS sur votre réseau, vous pouvez paramétrer ce serveur pour transférer les requêtes d'authentification au serveur RADIUS.

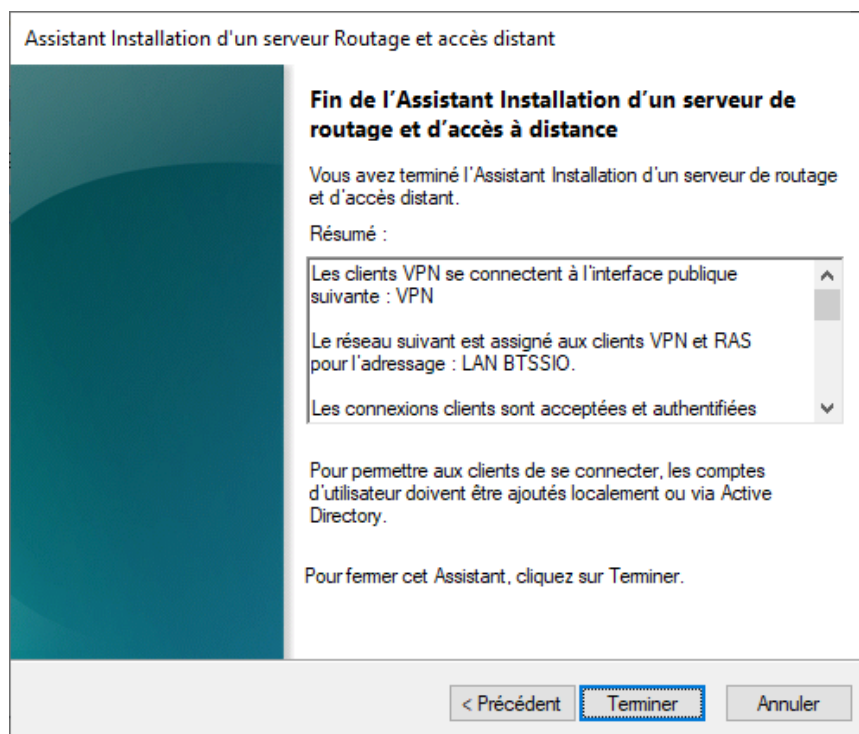
Voulez-vous configurer ce serveur pour qu'il interagisse avec un serveur RADIUS ?

☒ **Non, utiliser Routage et accès distant pour authentifier les demandes de connexion**

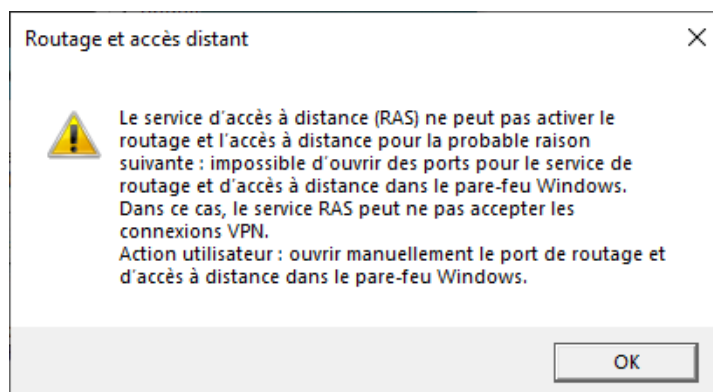
☐ Oui, configurer ce serveur pour travailler avec un serveur RADIUS

< Précédent Suivant > Annuler

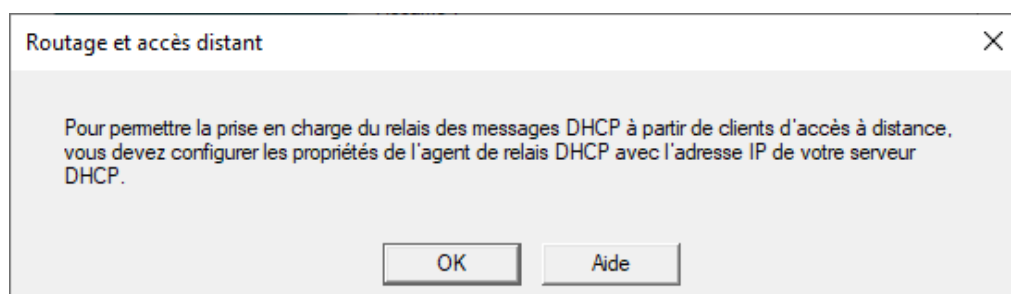
L'assistant affiche un résumé des configurations, cliquez sur « **Terminer** »



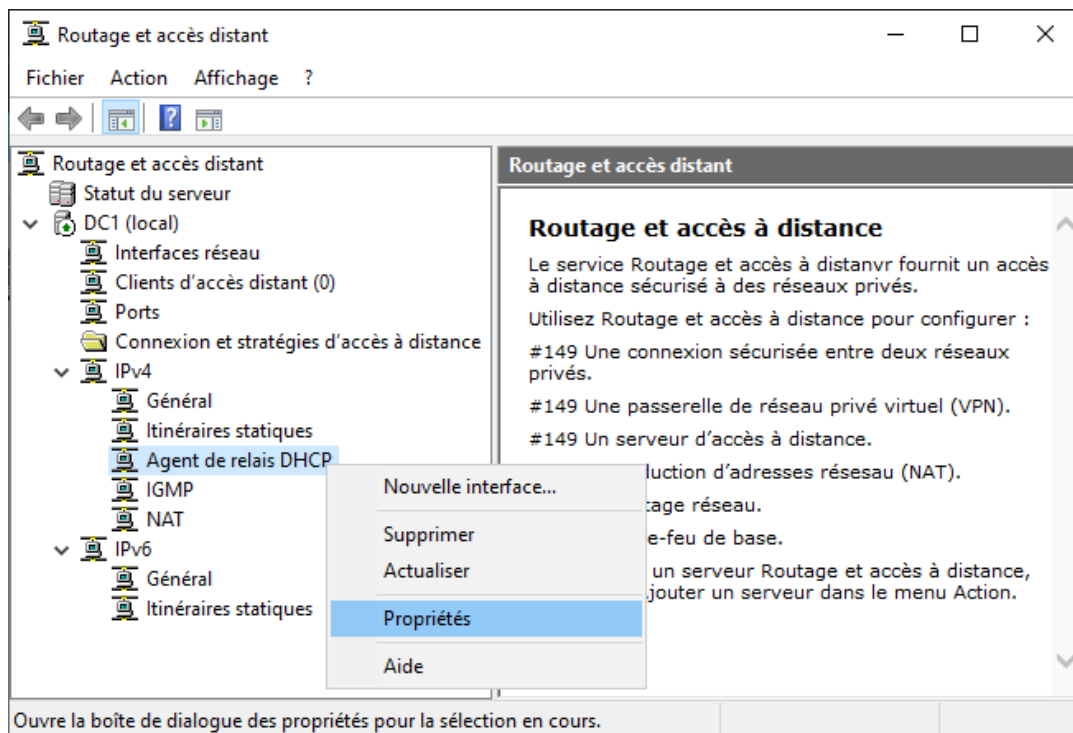
Pour l'avertissement concernant l'ouverture des ports, nous ouvriront ces ports manuellement. Cliquez sur « **OK** »



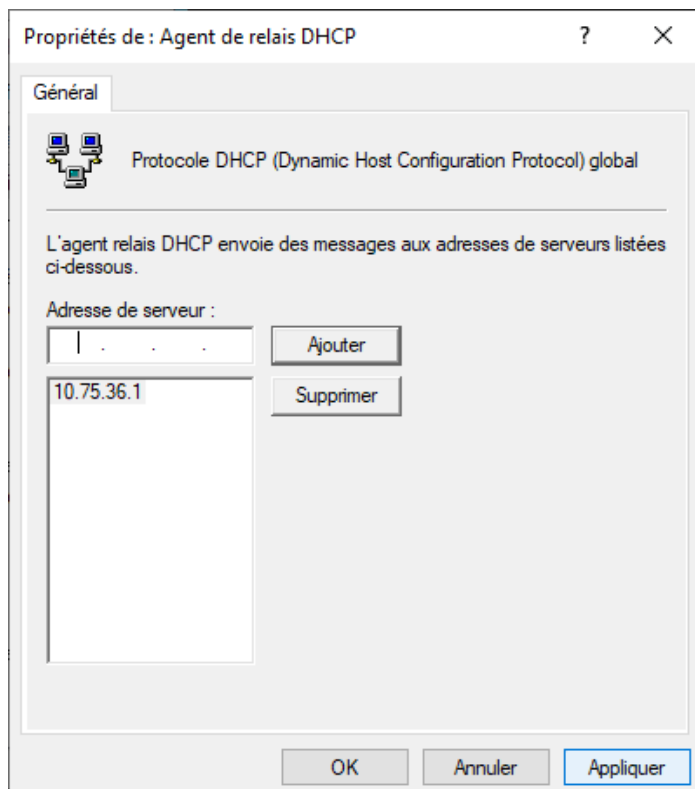
En ce qui concerne l'agent relais DHCP cliquez sur « **OK** » et nous allons configurer dans la partie tout juste après.



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** »

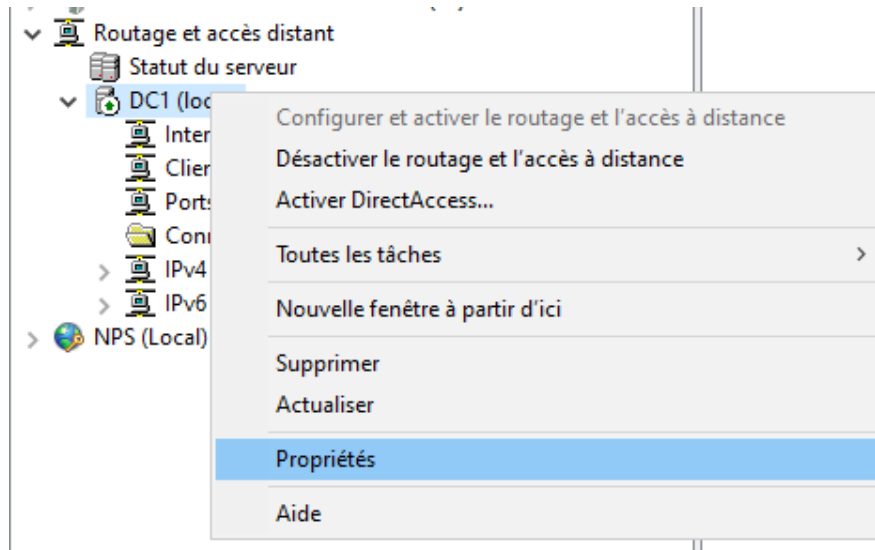


Préciser ici l'adresse IP du serveur DHCP (dans mon cas ici c'est l'adresse de mon contrôleur de domaine) puis cliquez sur « **Appliquer** »

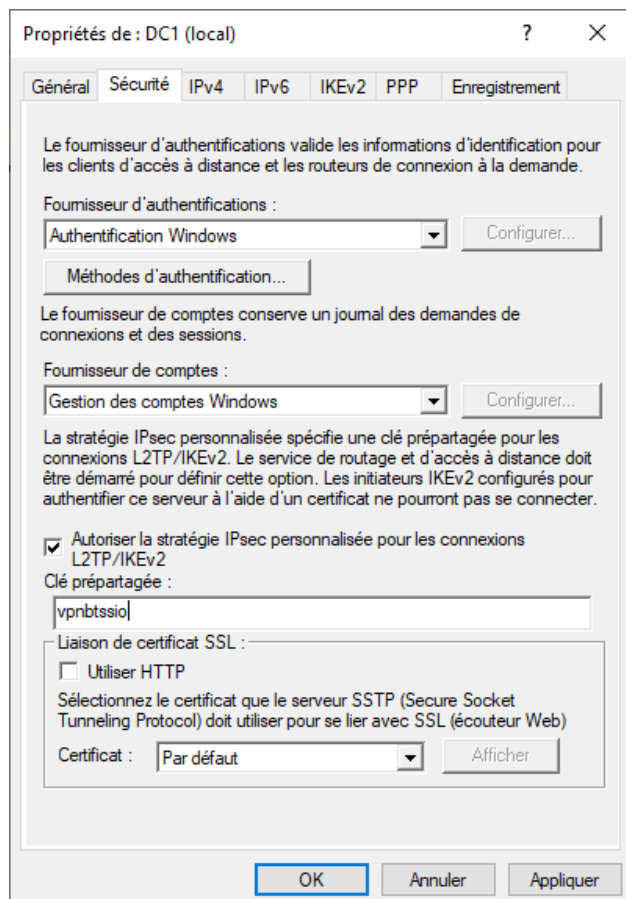


Actuellement avec le service VPN installé, il est par défaut en **PPTP (Point-to-Point Tunneling Protocol)**, nous allons activer le protocole **L2TP (Layer 2 Tunneling Protocol)** avec une clé prépartagée.

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

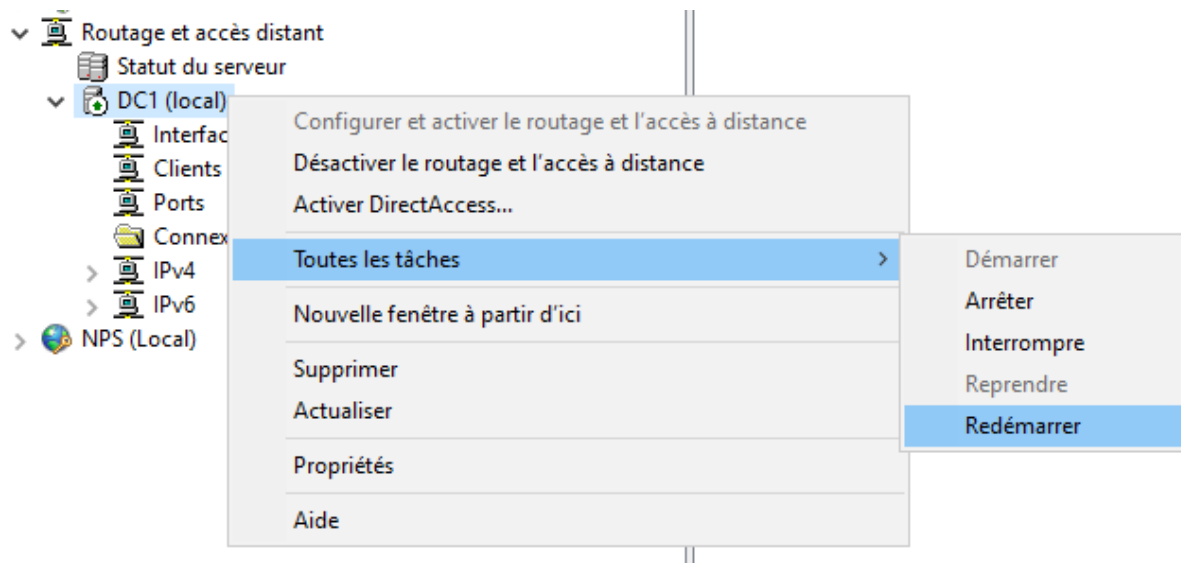


Allez dans l'onglet « **Sécurité** » et cochez la case pour autoriser le protocole L2TP et saisissez votre clé pré-partagée.



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

A screenshot of the 'Nouvel objet - Utilisateur' dialog box in Active Directory. The title bar says 'Nouvel objet - Utilisateur'. The 'Créer dans' field shows 'btssio.fr/BTSSIO/Utilisateurs/VPN'. The form has several fields: 'Prénom' with 'Chéridanh', 'Initiales' (empty), 'Nom' with 'TSIELA', 'Nom complet' with 'Chéridanh TSIELA', 'Nom d'ouverture de session de l'utilisateur' with 'cheridanh' and a dropdown showing '@btssio.fr', and 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' with 'BTSSIO\' and 'cheridanh'. At the bottom, there are three buttons: '< Précédent', 'Suivant >' (highlighted), and '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

Propriétés de : Chéridanh TSIELA

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+
Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Autorisation d'accès réseau

☐ Autoriser l'accès

☐ Refuser l'accès

☒ Contrôler l'accès via la Stratégie d'accès à distance

☐ Vérifier l'identité de l'appelant :

Options de rappel

☒ Pas de rappel

☐ Défini par l'appelant (service de routage et d'accès à distance uniquement)

☐ Toujours rappeler :

☐ Attribuer des adresses IP statiques

Définissez les adresses IP à activer pour cette connexion d'appel entrant.

☐ Appliquer les itinéraires statiques

Définir les itinéraires à activer pour cette connexion d'appel entrant.

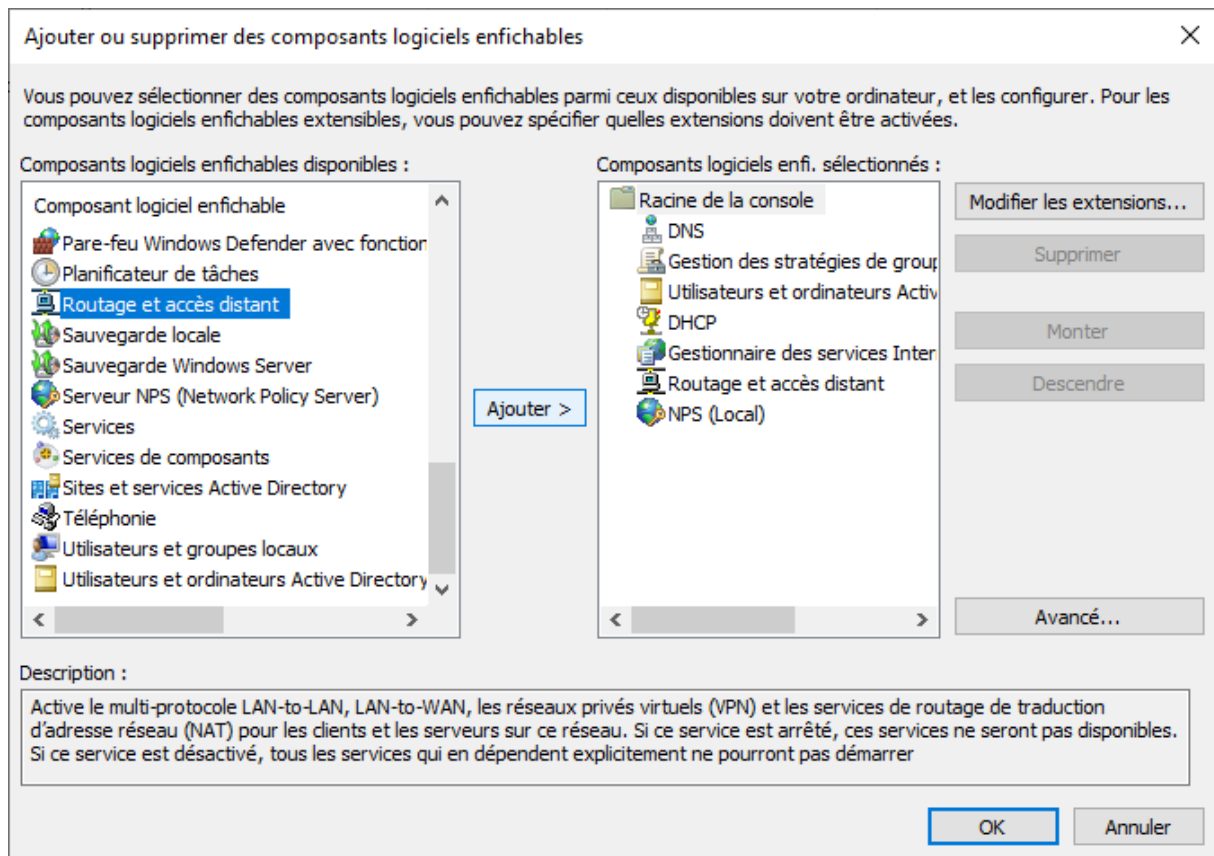
OK Annuler Appliquer Aide

III – Stratégie d'accès réseau

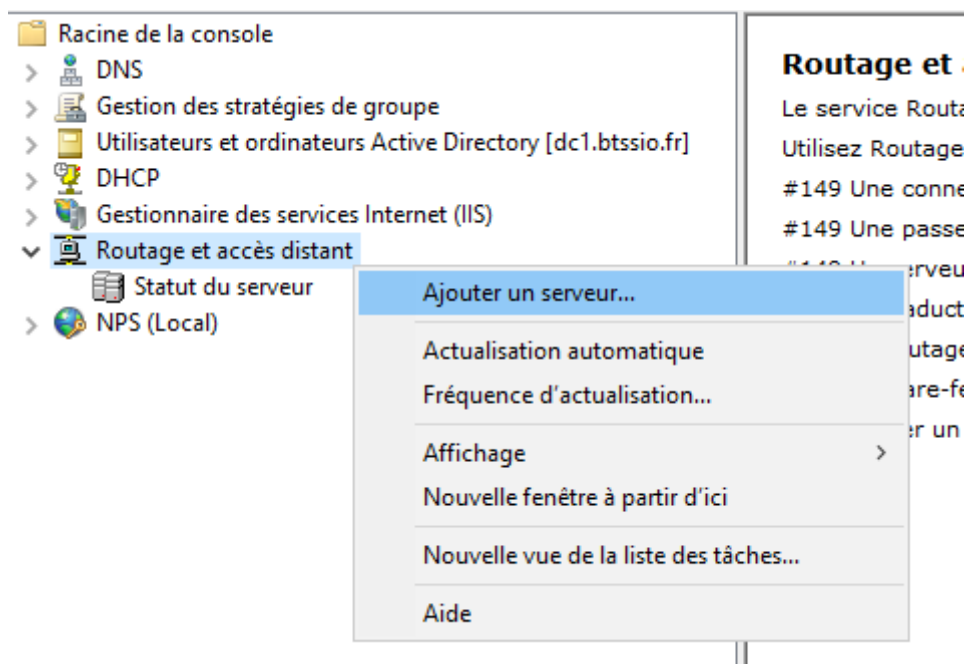
Commencez par ajouter les consoles d'administration créées lors de notre installation du service VPN.

Dans notre console MMC ajoutez les composants suivants :

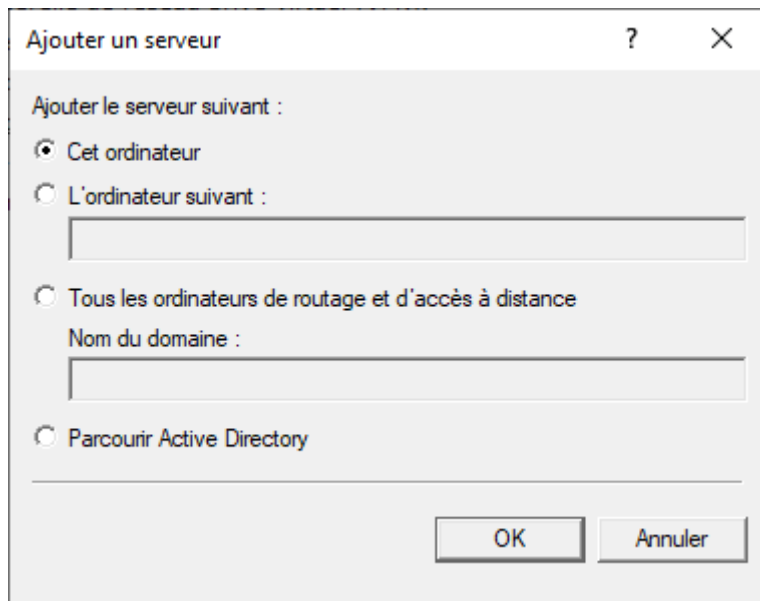
Routage et accès distant et NPS



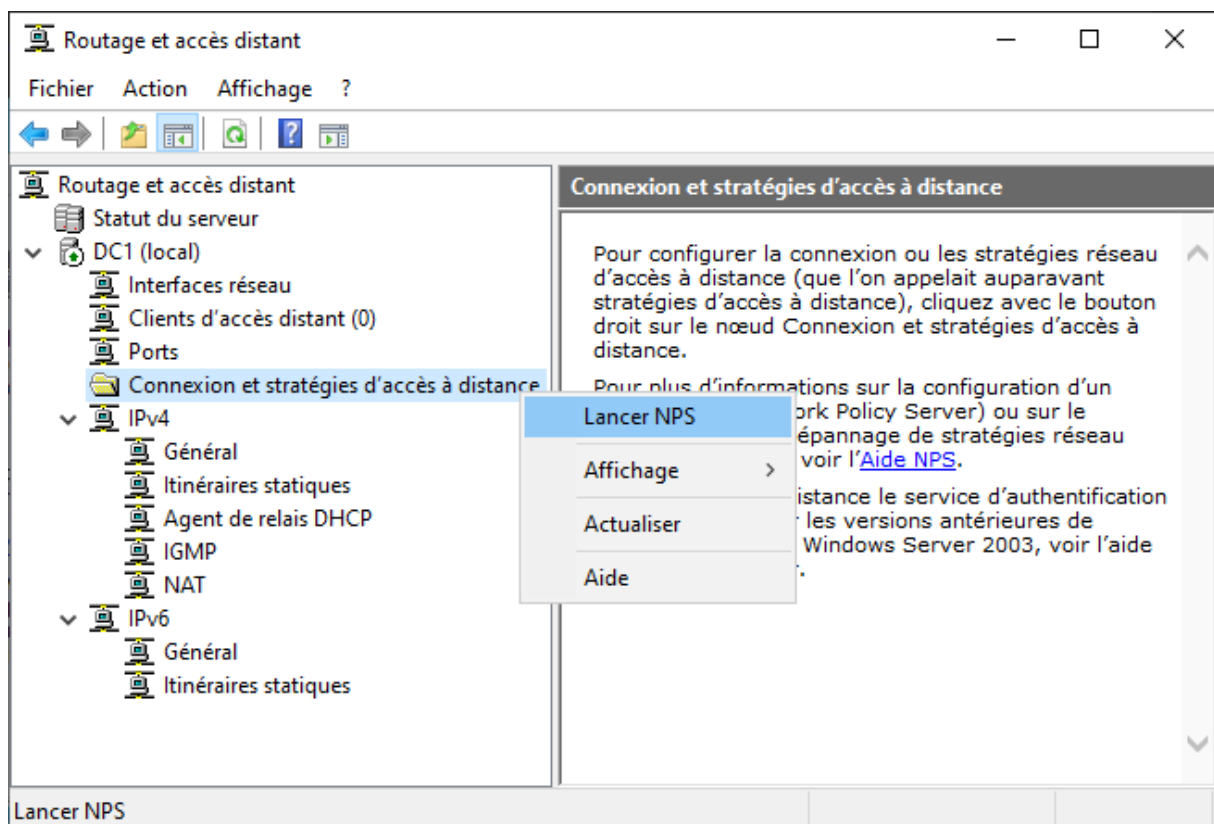
Une fois les composants ajoutés, clic droit sur routage et accès distant et cliquez sur « **Ajouter un serveur** »



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



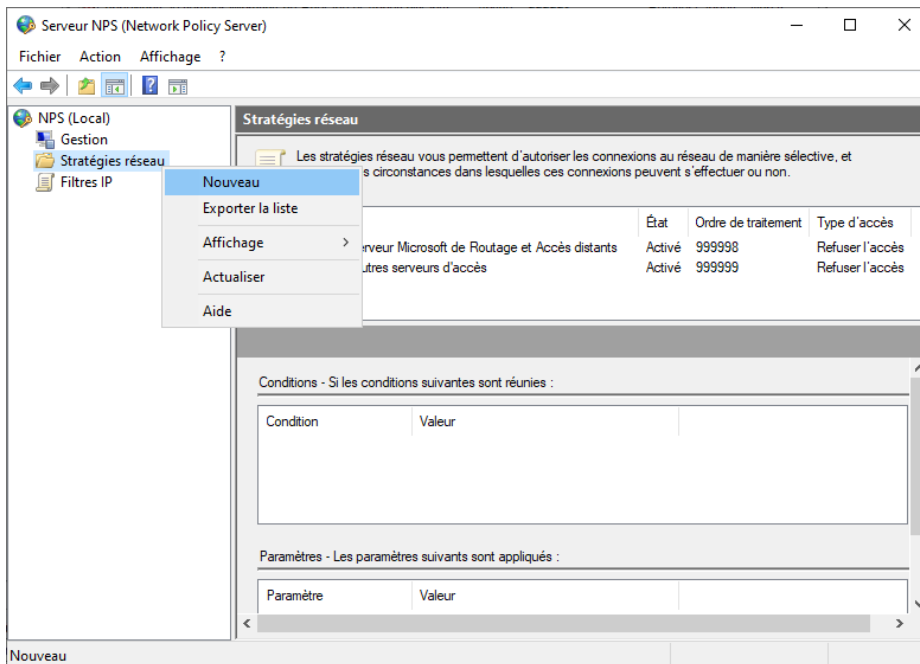
Faites un clic droit sur « **Connexion et stratégies d'accès à distance** » puis cliquez sur « **Lancer NPS** »



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)** »

Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :
VPN BTSSIO

Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

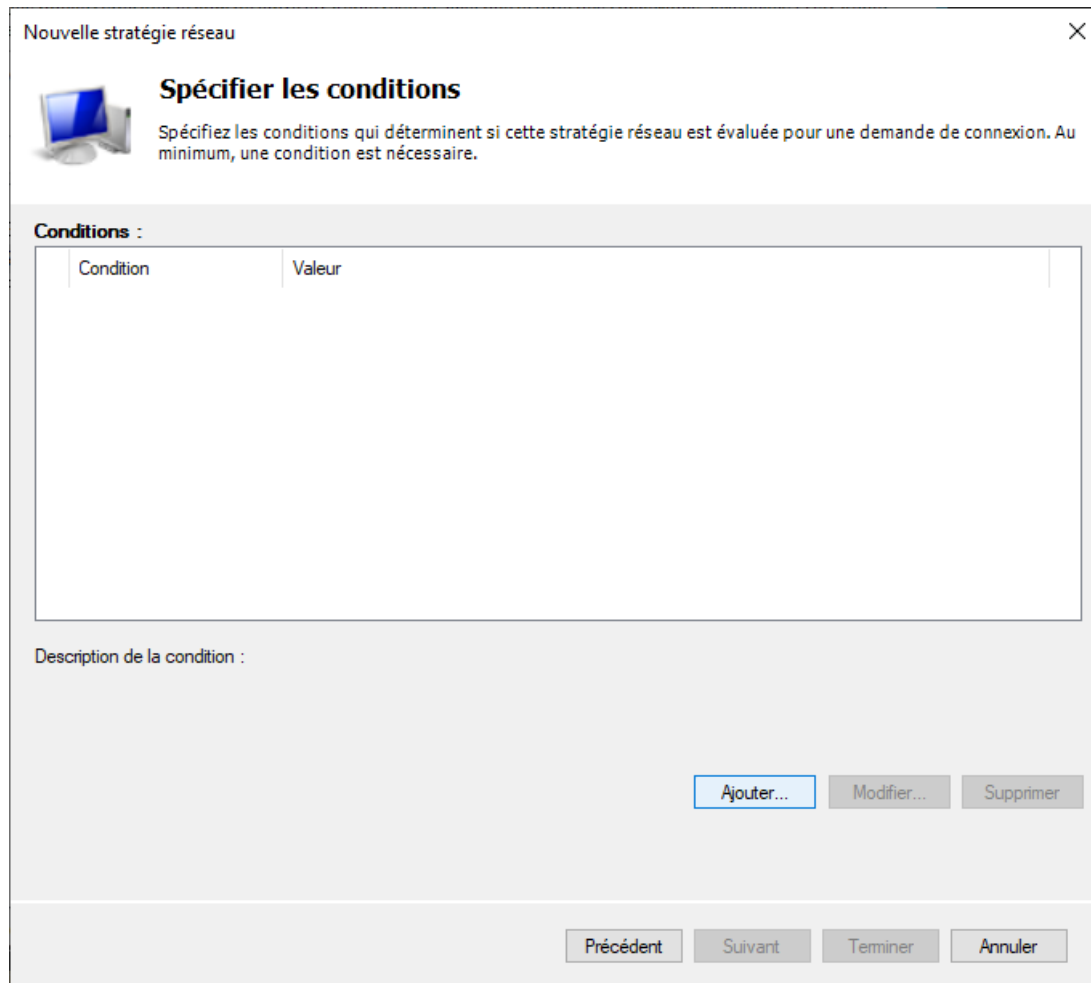
☒ Type de serveur d'accès réseau :
Serveur d'accès à distance (VPN-Dial up)

☐ Spécifique au fournisseur :
10

Précédent Suivant Terminer Annuler

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

Cliquez sur « **Ajouter** »



Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

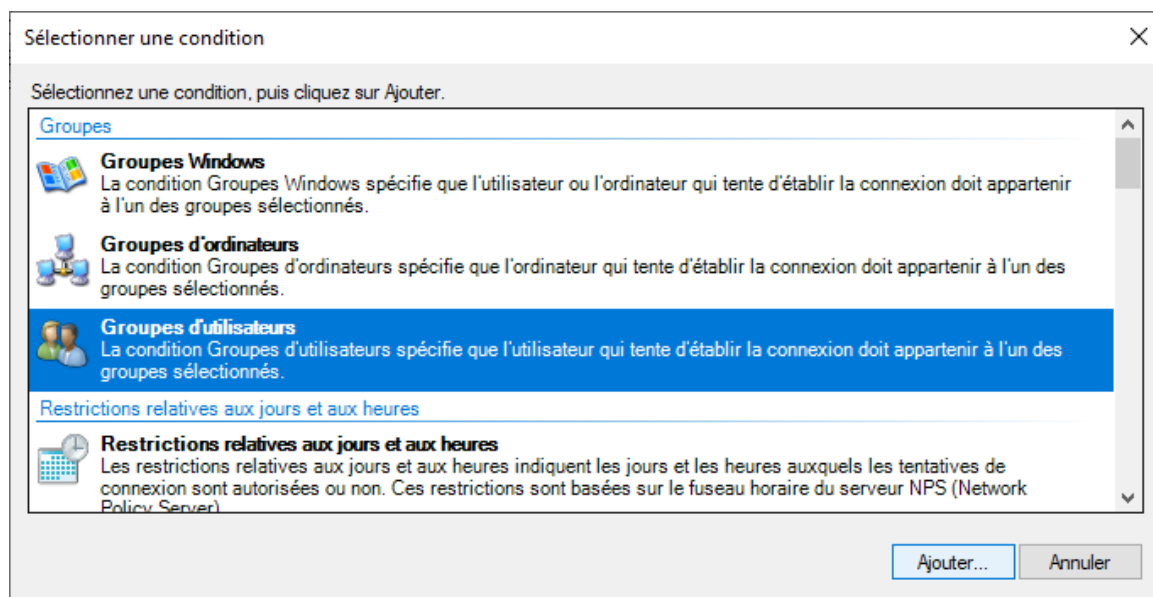
Condition	Valeur
-----------	--------

Description de la condition :

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Sélectionner « **Groupe d'utilisateurs** »



Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

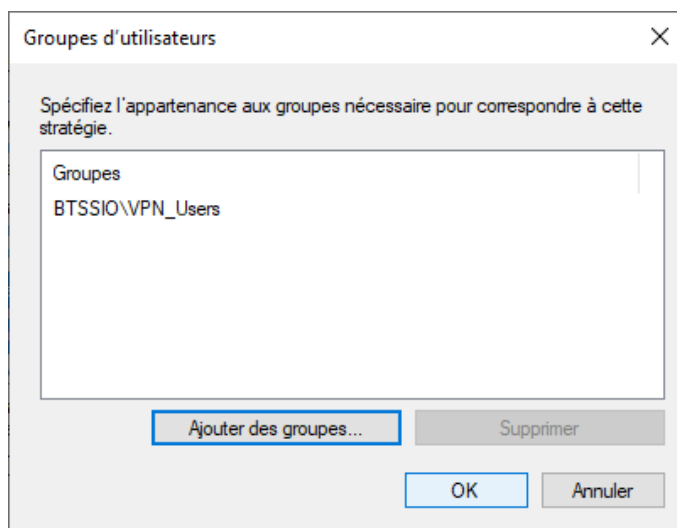
- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

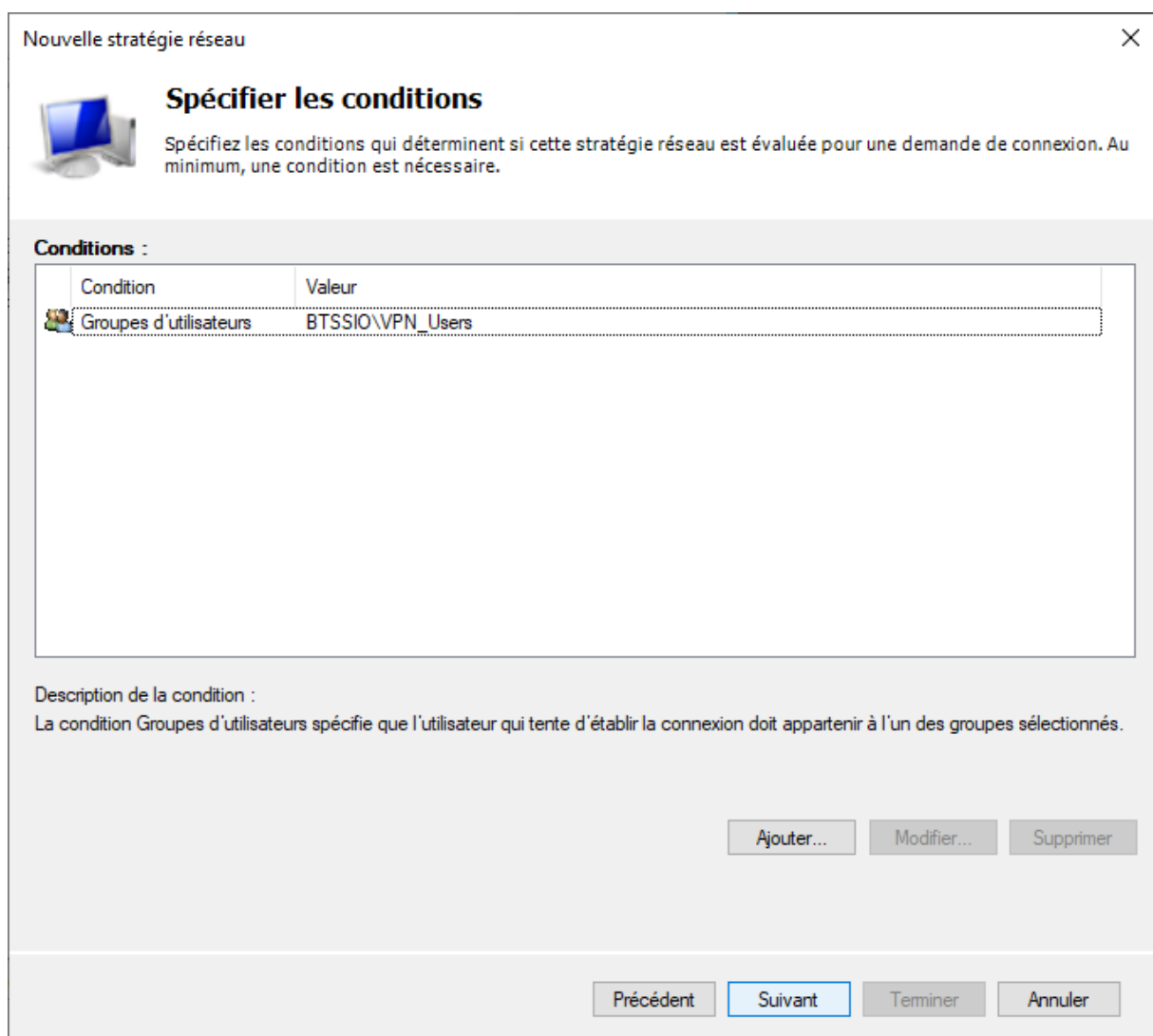
- Restrictions relatives aux jours et aux heures**
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter... Annuler

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




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



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

Nouvelle stratégie réseau

 **Spécifier l'autorisation d'accès**

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ **Accès accordé**
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.


☐ **Accès refusé**
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie

Précédent Suivant Terminer Annuler

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

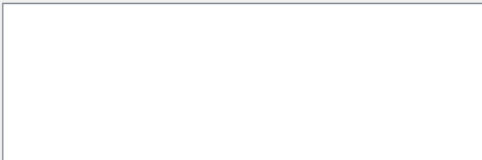
Nouvelle stratégie réseau

 **Configurer les méthodes d'authentification**

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :



Monter
Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
☒ L'utilisateur peut modifier le mot de passe après son expiration

☒ Authentification chiffrée Microsoft (MS-CHAP)
☒ L'utilisateur peut modifier le mot de passe après son expiration

☐ Authentification chiffrée (CHAP)

☐ Authentification non chiffrée (PAP, SPAP)

☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

Précédent Suivant Terminer Annuler

Ajouter les méthodes d'authentification comme ci-dessous :

Nouvelle stratégie réseau

Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

- Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)
- Microsoft: Carte à puce ou autre certificat

Monter
Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

Précédent Suivant Terminer Annuler

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

Nouvelle stratégie réseau

Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

- Contraintes
 - Délai d'inactivité**
 - Délai d'expiration de session
 - ID de la station appelée
 - Restrictions relatives aux jours et aux heures
 - Type de port NAS

Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

☐ Déconnecter au-delà de la durée d'inactivité maximale

1

Précédent Suivant Terminer Annuler

Cliquez sur « Suivant »

Nouvelle stratégie réseau

Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

☒ Standard

☐ Spécifiques au fournisseur

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Cliquez sur « Terminer »

Nouvelle stratégie réseau

Fin de la configuration de la nouvelle stratégie réseau

Vous avez correctement créé la stratégie réseau suivante :

VPN BTSSIO

Conditions de la stratégie :

Condition	Valeur
Groupes d'utilisateurs	BTSSIO\VPN_Users

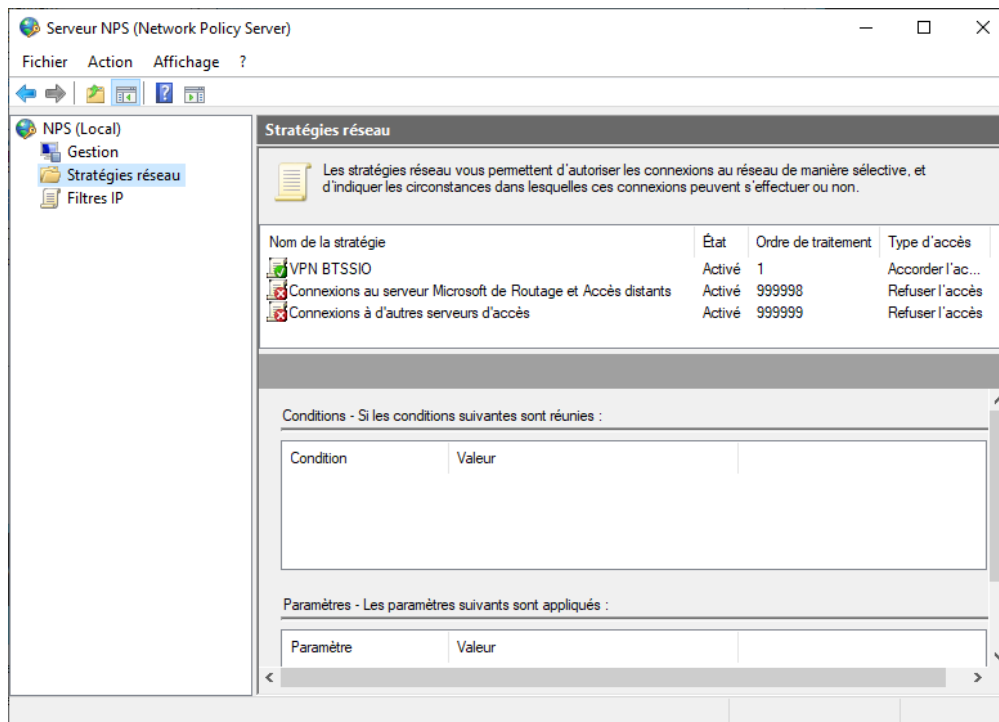
Paramètres de la stratégie :

Condition	Valeur
Méthode d'authentification	Protocole EAP OU MS-CHAP v1 OU MS-CHAP v1 (l'utilisateur peut modifie...
Autorisation d'accès	Accorder l'accès
Framed-Protocol	PPP
Service-Type	Framed
Ignorer les propriétés de numérotation des utilisateurs	Faux
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP) OU Microsoft: Mot de passe sécurisé (EA...

Pour fermer cet Assistant, cliquez sur Terminer.

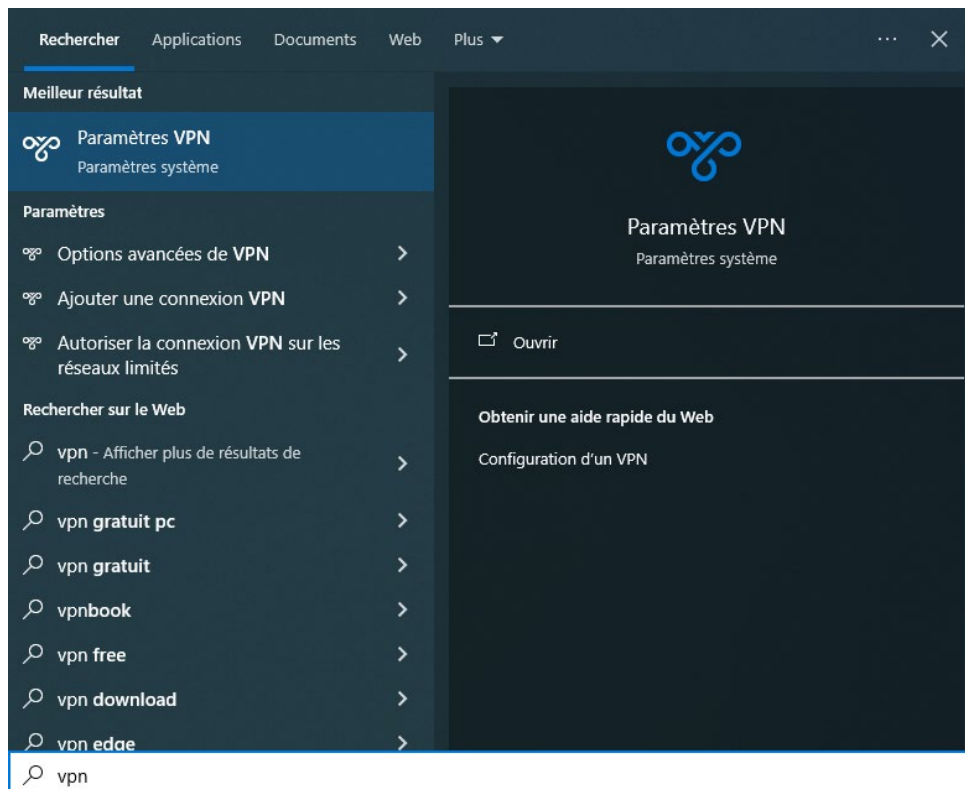
Précédent Suivant Terminer Annuler

Notre stratégie réseau a bien été créé avec succès !



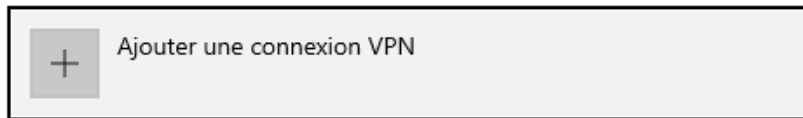
III – Test de connexion

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



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

VPN



Options avancées

Autoriser les connexions VPN sur des réseaux limités

☒ Activé

Autoriser les connexions VPN en itinérance

☒ Activé

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



Ajouter une connexion VPN



VPN BTSSIO

Connecter

Options avancées

Supprimer

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.

Sécurité Windows

Se connecter

BTSSIO\cheridanh

••••••••

Domaine : BTSSIO

Le nom d'utilisateur ou le mot de passe est incorrect.

OK Annuler

La connexion s'est effectuée avec succès !

VPN



Ajouter une connexion VPN

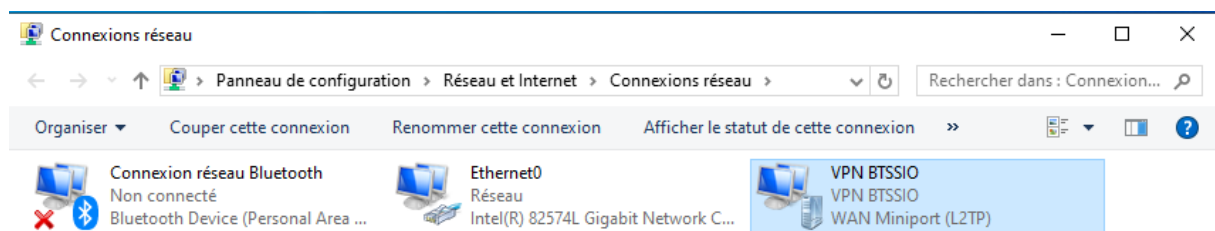


VPN BTSSIO
Connecté

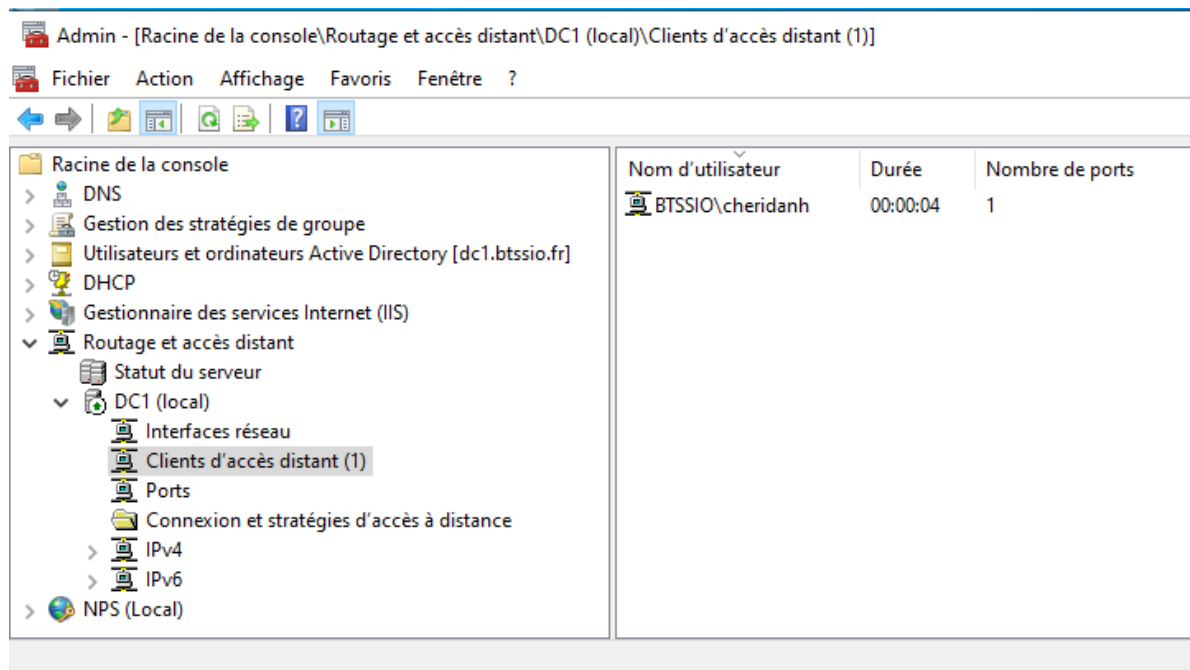
Options avancées

Déconnecter

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

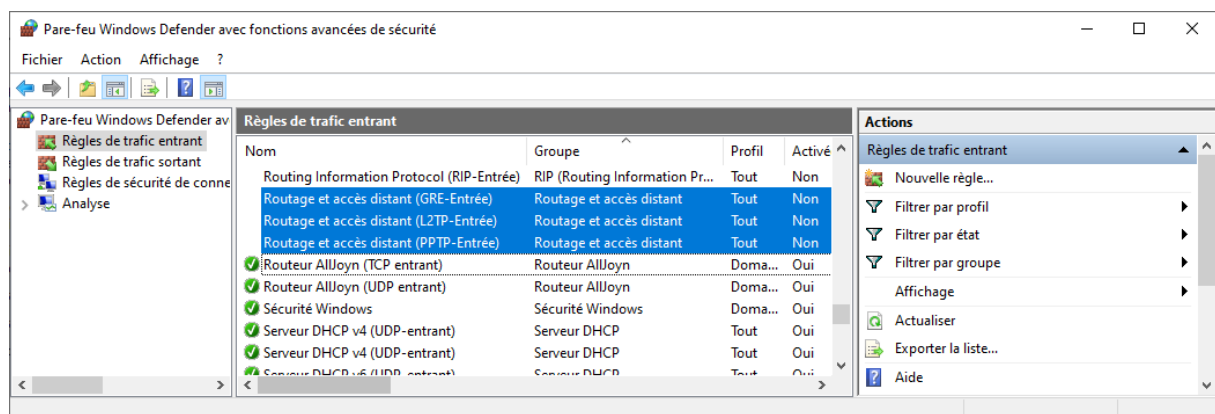


Au niveau de notre serveur VPN, on peut voir les utilisateurs connectés dans « **Clients d'accès distant** »

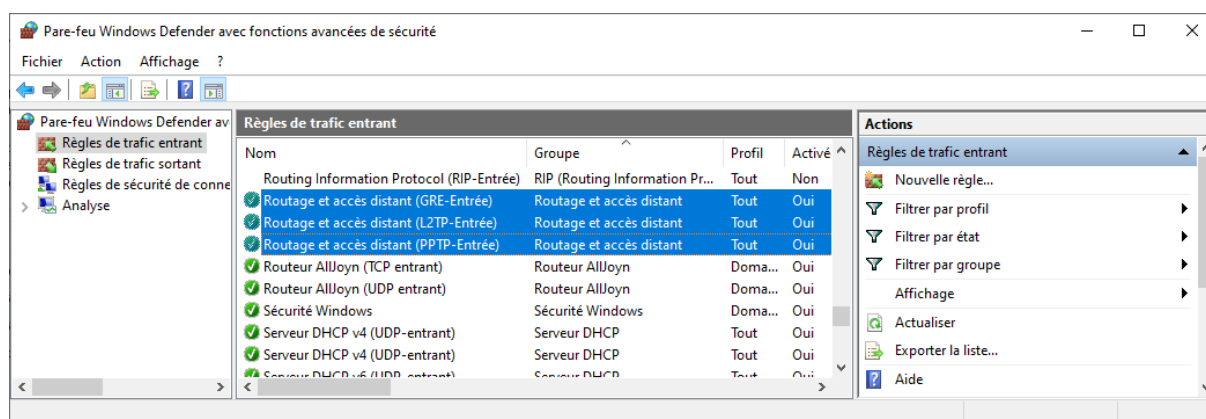


Rappelez-vous pendant la configuration de notre serveur, nous avons un avertissement concernant l'ouverture des ports.

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>