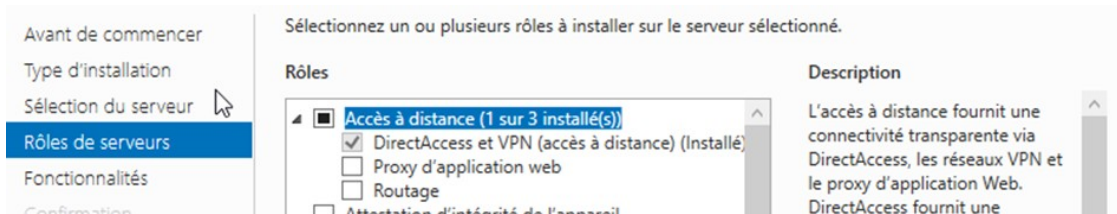


Microsoft
Windows
Server standard
2022

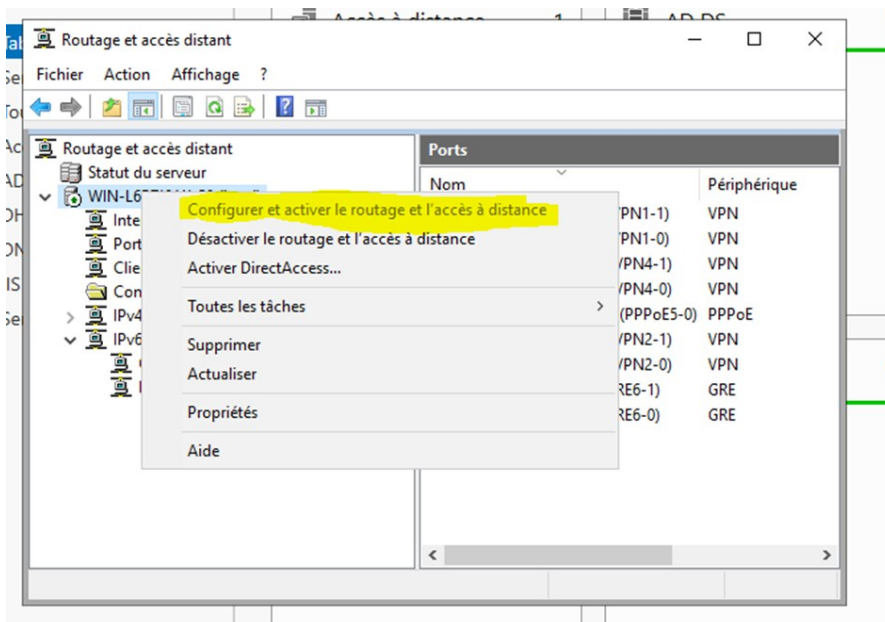
Procédure : VPN

Objectif : VPN

I. Installer Accès à distance grâce à Gérer, dans le gestionnaire de serveur



II. Dans outils accéder au Routage et accès distant

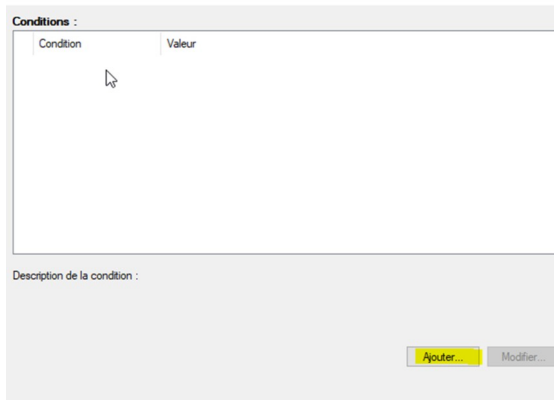


III. Clic droit sur le serveur puis configurer et activer le routage et l'accès à distance
Cliquer sur custom configuration puis VPN access

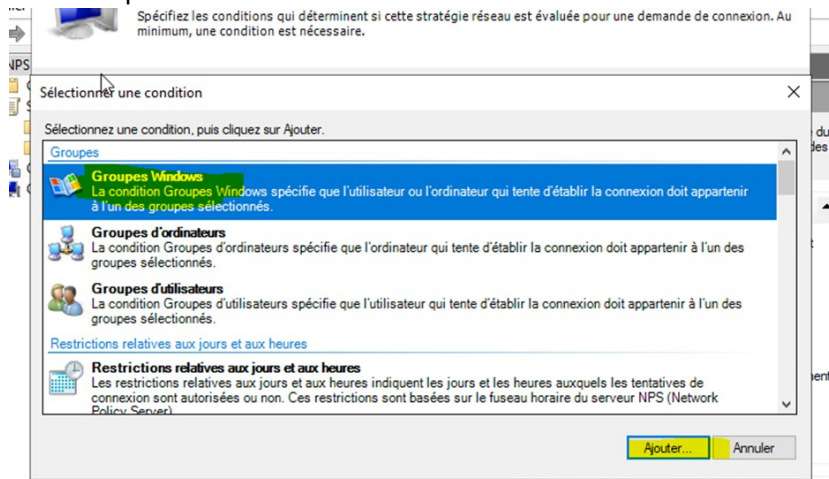
IV. Crée un groupe utilisateur dans l'AD VPN_users
Mette les users que vous voulez dans le groupe
Bien vérifier dans les propriétés de l'user dans Appel entrant que l'option Contrôler l'accès via la Stratégie d'accès à distance est coché

V. Dans la barre de recherche google taper NPS puis ouvrir serveur NPS

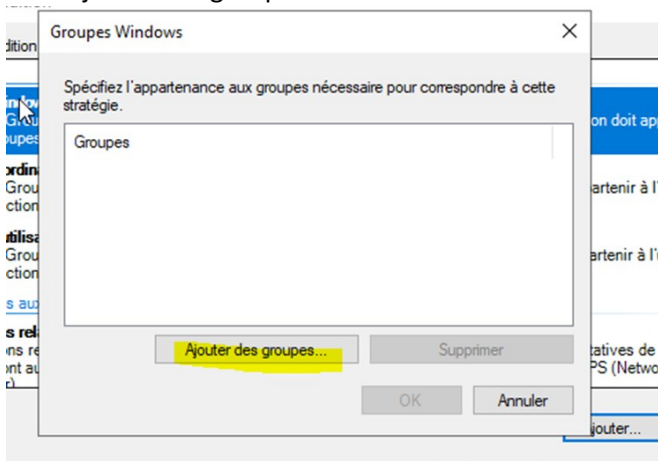
- VI. Dans Stratégies réseau, clic droit nouveau
Donner un nom puis type de serveur mettre Serveur d'accès à distance
Dans condition faire ajouter...



Puis Groupes Windows



Puis ajouter des groupes



Puis ajouter le groupe précédemment créé

Sélectionnez le type de cet objet :
un groupe
Types d'objets...

À partir de cet emplacement :
tim.local
Emplacements...

Entrez le nom de l'objet à sélectionner (exemples) :
vpn_user
Vérifier les noms

Avancé... OK Annuler

puis Accès accordé

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

VII. Puis suivant faire ajouter dans Types de protocoles EAP

Types de protocoles EAP :

Ajouter des protocoles EAP

Méthodes d'authentification :

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

OK Annuler

Méthodes d'authentification

- Authentification chiffrée Microsoft
- L'utilisateur peut modifier le mot de passe
- Authentification chiffrée Microsoft
- L'utilisateur peut modifier le mot de passe
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification.

VIII. On peut rajouter un délai d'inactivité, des restrictions relatives

Stratégies réseau

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

Nom de la stratégie	État	Ordre de traitement	Type d'accès
VPN_PPTP_User	Activé	1	Accorder l'accès
Connexions au serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès
Connexions à d'autres serveurs d'accès	Activé	3	Refuser l'accès

VPN_PPTP_User

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Groupes Windows	TIM\vpn_user

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
-----------	--------

Sur le client, être en IP fixe et essayer de ping le serveur ensuite dans la barre de recherche google aller sur parametre VPN → ajouter un VPN → puis saisir les informations demandé mettre le type de réseau en Protocole PPTP puis se connecter au VPN