

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



II. Dans outils accéder au Routage et accès distant

_		listance 1		DC	
Routage et accès	distant		-	· □ >	<
chier Action A	Affichage ?				
• 🔿 🖄 📰 🤅	🗐 🔂 📑 🚺				
Routage et accè	; distant	Ports	_	_	
Statut du serveur	veur	Nom		Dérinhérique	
WIN-L6	Configurer et activer le routage e	t l'accès à distance	PN1-1)	VPN	
Port	Désactiver le routage et l'accès à	distance	PN1-0)	VPN	
🚊 Clie	Activer DirectAccess		(PN4-1)	VPN	
Con	Toutes les tâches	>	(PN4-0)	VPN	
> <u>⊜</u> IPv4 > <u>⊜</u> IPv6	Supprimer		(PPP0E3-0) (PN2-1)	VPN	
<u>a</u> (Actualiser		(PN2-0)	VPN	
	Dronsiétés		RE6-1)	GRE	
	Proprietes		(ED-U)	GRE	
	Aide				
			_		>
					-
					_

- 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
 Mettre 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...

Condition	Valeur	
₹2		
ription de la conditio	n :	

Puis Groupes Windows

électio	inter une condition	×
électio	nnez une condition, puis cliquez sur Ajouter.	
Group	es	^
U ¢	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.	
R	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.	
Restri	ctions relatives aux jours et aux heures	
P	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)	~

Puis ajouter des groupes

stratégie.	mance aux groupes ne	cessaire pour corres	pondre à cette	
Groupes				on
				art
				arte
	Ajouter des groupes	Sur	oprimer	tati

Puis ajouter le groupe précédemment crée

un groupe	Types d'objets
A partir de cet emplacement :	
tim.local	Emplacements.
Entrez le nom de l'objet à sélectionner (<u>exemples</u>)	
Entrez le nom de l'objet à sélectionner (exemples)	
Entrez le nom de l'objet à sélectionner (<u>exemples</u>) <mark>vpn_user</mark>	Vérifier les nome
Entrez le nom de l'objet à sélectionner (<u>exemples</u>) v <u>pn user</u>	Vénfier les noms

puis Accès accordé

in		Spécifier l'autorisation d'accès
er		Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion corr à cette stratégie.
2	Accès acce	ardé
' 9	Accordez l'a	accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.
	O Accès refus	vé
19	Refusez l'a	ccès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.
10	L'accès est Choisissez s	déteminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS) elon les propriétés de numérotation utilisateur si les teritatives de connexion des clients répondent aux conditions de la

VII. Puis suivant faire ajouter dans Types de protocoles EAP

	Ajouter des protocoles EAP	×
	Méthodes d'authentification :	
	Microsoft: Carte à puce ou autre certificat Microsoft: PEAP (Protected EAP)	
Ajouter	Microsoft: Mot de passe sécurisé (EAP-MSCHAN	^o version 2)
Athodes d'authentification	<	>
Aéthodes d'authentification Authentification chiffrée Micros L'utilisateur peut modifier le r	<	Annuler
Aéthodes d'authentification Authentification chiffrée Micros L'utilisateur peut modifier le r Authentification chiffrée Micros L'utilisateur peut modifier le r		> Annuler
Méthodes d'authentification Authentification chiffrée Micros L'utilisateur peut modifier le Authentification chiffrée Micros L'utilisateur peut modifier le n Authentification chiffrée ("CHAP)	<	Annuler
Méthodes d'authentification Authentification chiffrée Micros L'utilisateur peut modifier le Authentification chiffrée Micros L'utilisateur peut modifier le r Authentification chiffrée (CHAP) Authentification pon chiffrée (PA	C OK	Annuler

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

	Stratégies réseau			
Clients et serveurs RADIUS	Les stratégies réseau vous permettent d'autoriser les con d'indiquer les circonstances dans lesquelles ces connexi	nexions au r ons peuvent	éseau de manière séle s'effectuer ou non.	ctive, et
Gestion	Nom de la stratégie	État	Ordre de traitement	Type d'accès
Gestion des modèles	VPN_PPTP_User	Activé	1	Accorder l'accès
	Connexions au serveur Microsoft de Routage et Accès distant	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/vpp user			
	Groupes Windows The optimized			
	Paramètres - Les paramètres suivants sont appliqués :			

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