

TP1 – Mise en œuvre d'une infrastructure 802.1x : connexions câblées

Sommaire :

1. Configuration Switch

2.1/ Situation de départ

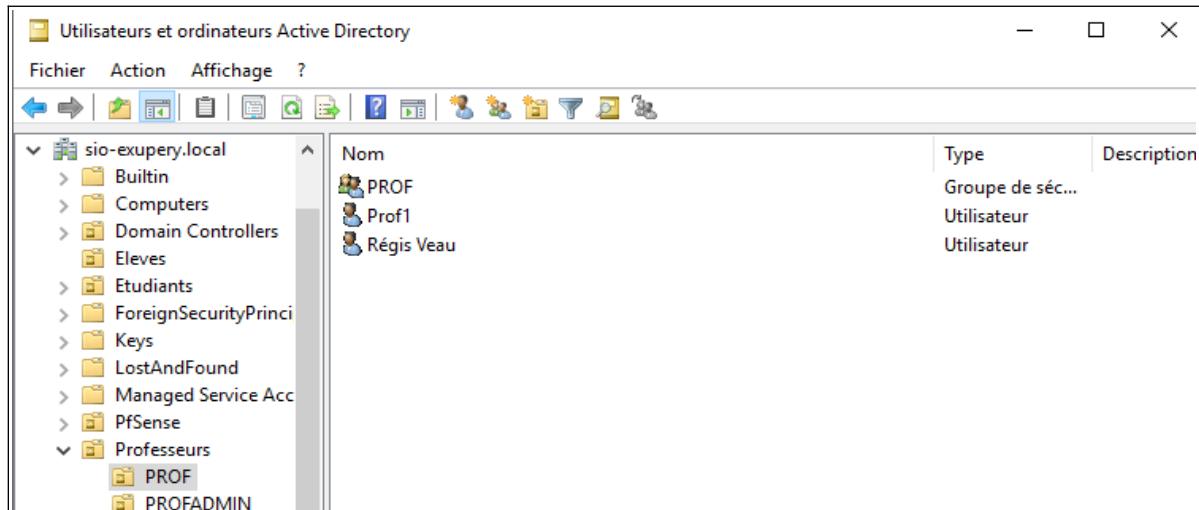
2.2/ Ajout du rôle Services de certificats Active Directory

2.3/ Installation du service NPS

2.4/ Configuration du serveur RADIUS NPS

1./ Configuration Switch

```
S1(config)#aaa new-model
S1(config)#aaa authentication dot1x default group radius
S1(config)#aaa authorization network default group radius
S1(config)#dot1x system-auth-control
```

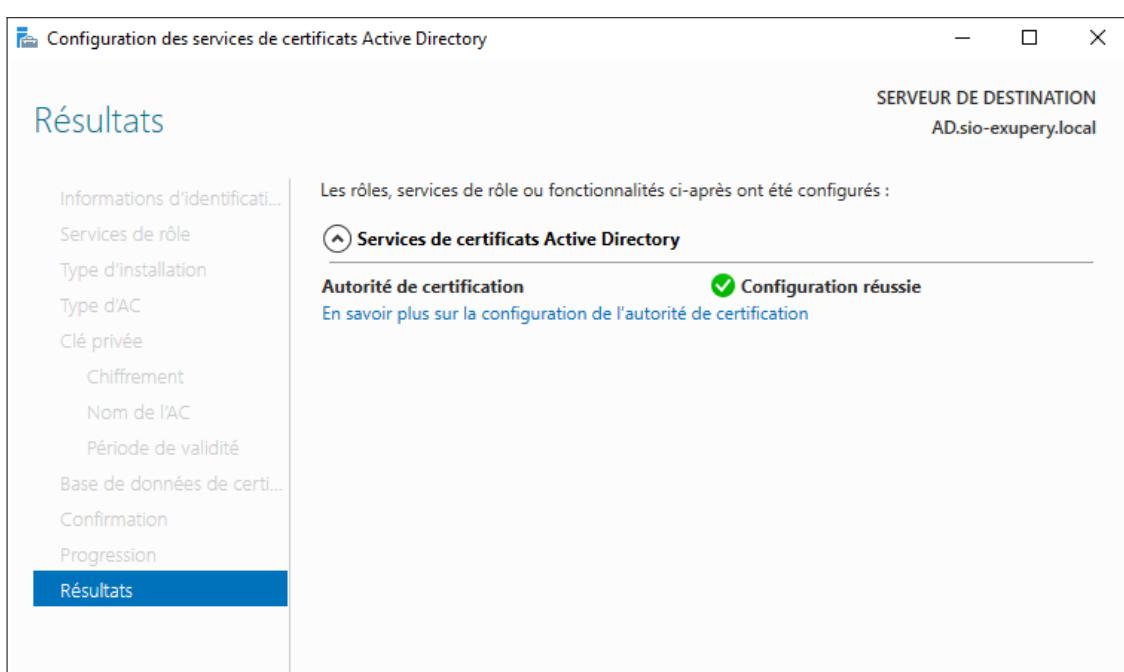
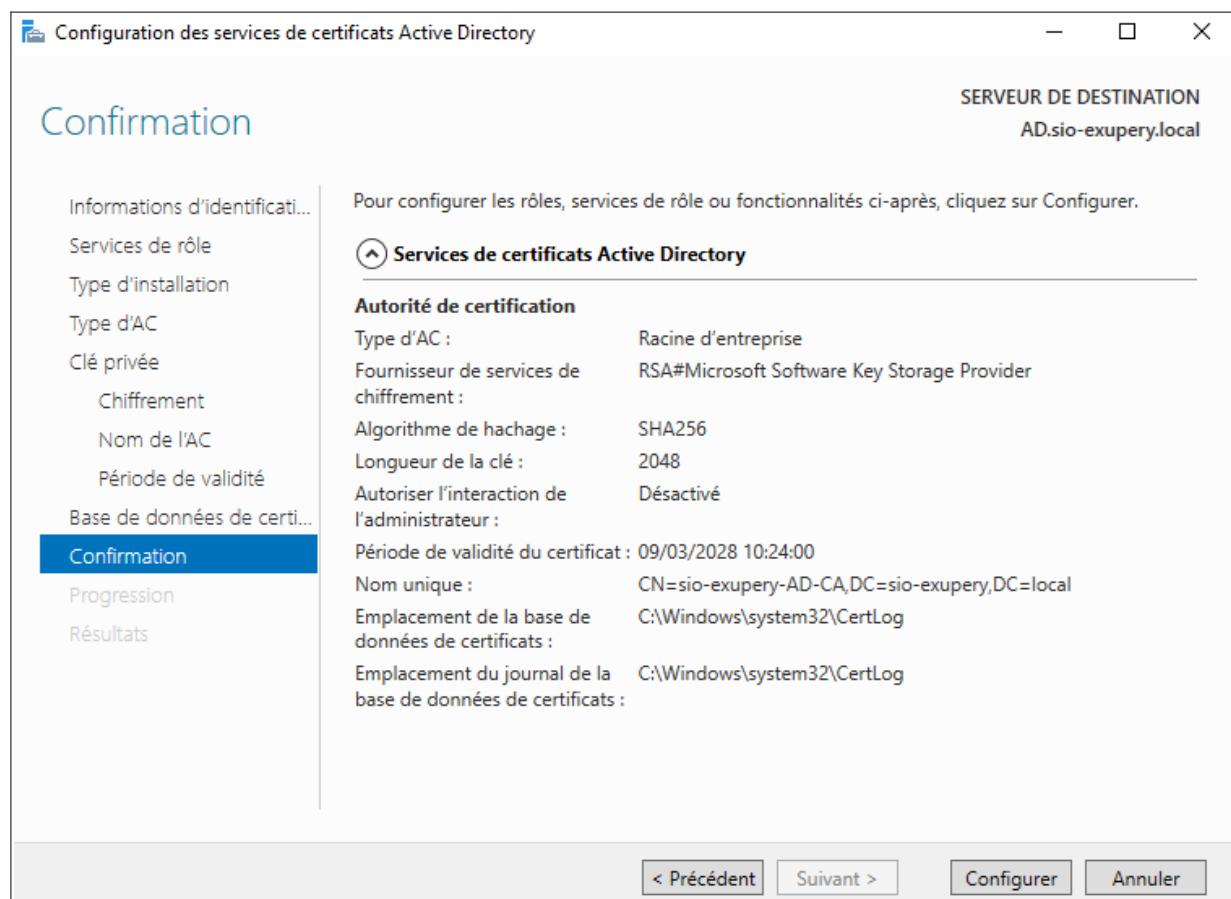


Nom	Type	Description
Direction	Groupe de sécurité	
Corinne Geley	Utilisateur	

Deux unités d'organisation sont présentes :

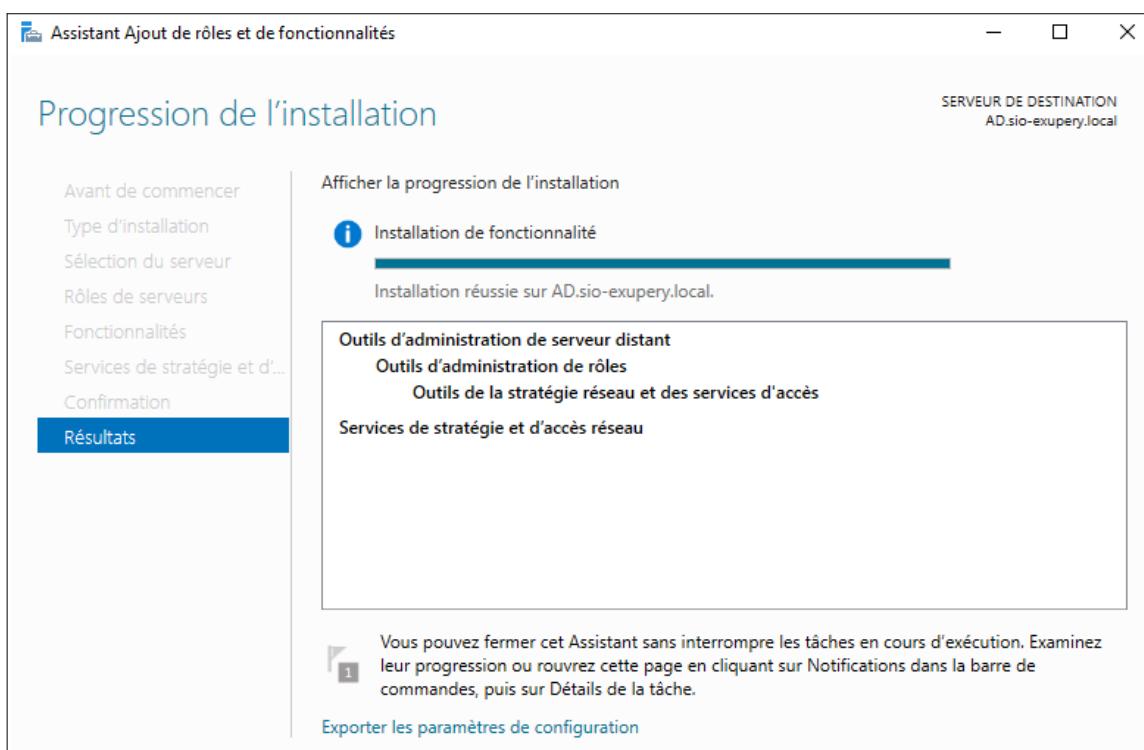
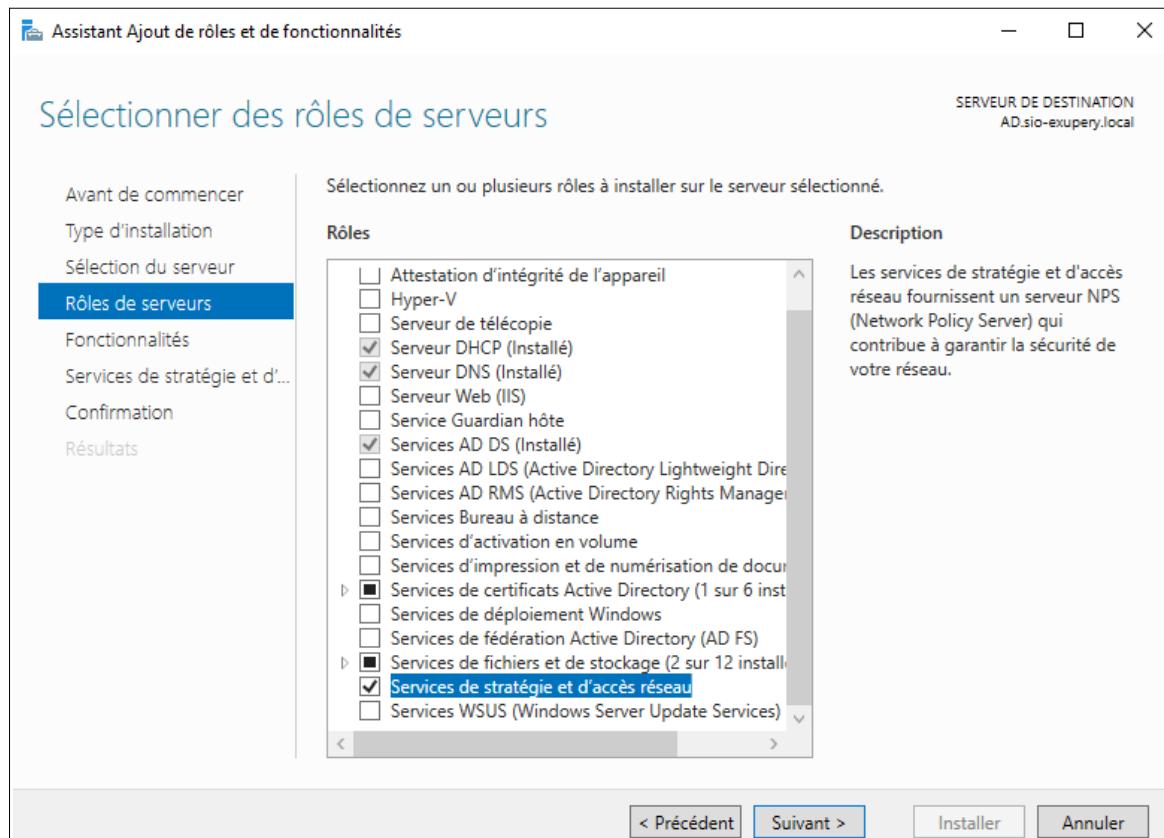
- Professeurs/Prof avec l'utilisateur Régis Veau dans le groupe Prof.
- Administration/Direction avec l'utilisateur Corinne Geley dans le groupe Direction.

2.2/ Ajout du rôle Services de certificats Active Directory



1ère étape : Nous ajoutons le rôle **Service de certificats Active Directory**.

2.3/ Installation du service NPS



1ère étape : Nous ajoutons le rôle **Services de stratégie et d'accès réseau**.

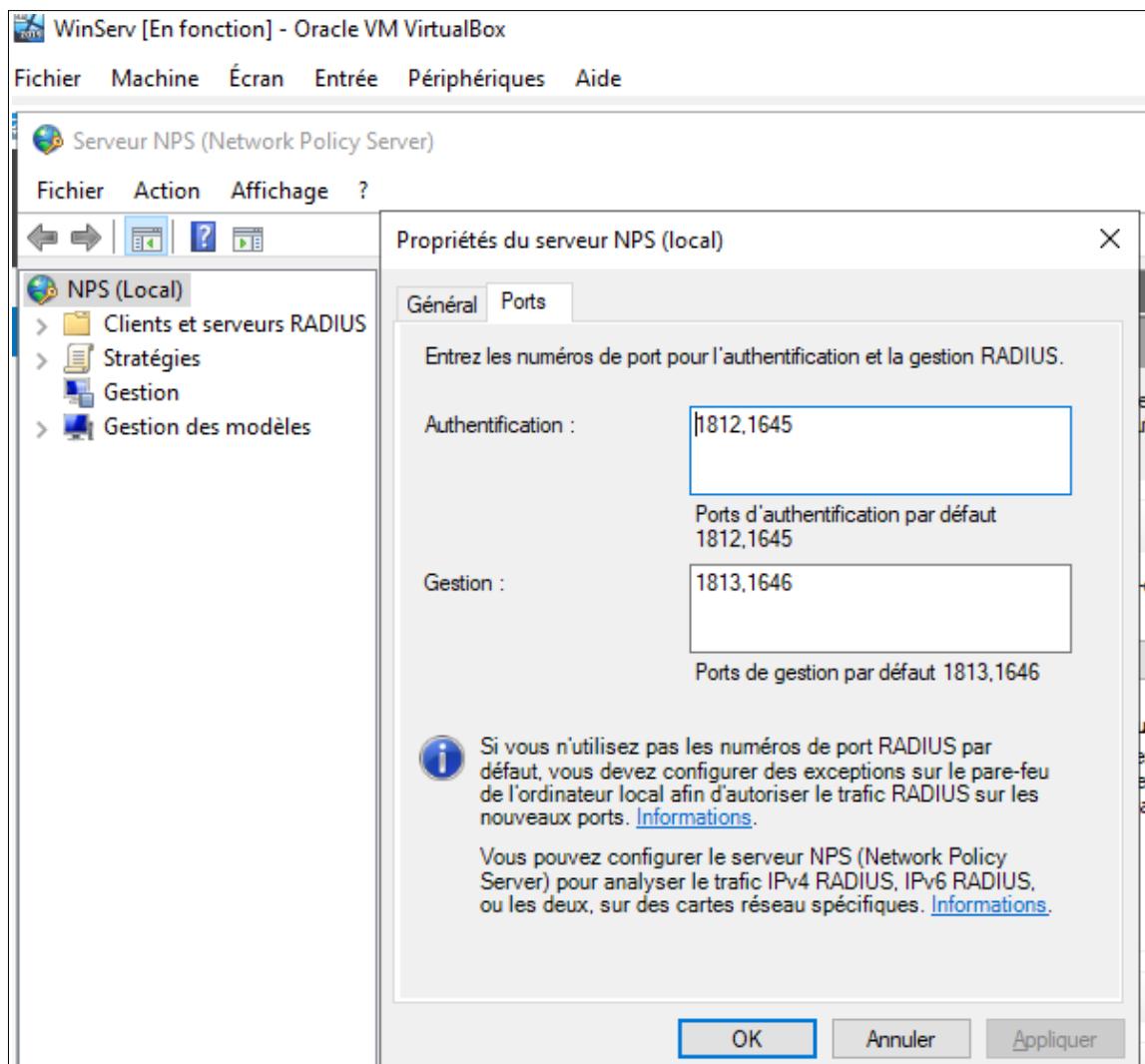
```

    UDP  [fe80::7dff:791:c3aa:b7b3%8]:53  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:88  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:464  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:1645  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:1646  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:1812  *:*
    UDP  [fe80::7dff:791:c3aa:b7b3%8]:1813  *:*

```

C:\Users\Administrateur>

2ème étape : Nous affichons les **ports en écoute** afin de vérifier le bon fonctionnement du service NPS.



3ème étape : Nous pouvons également retrouvé ces ports dans la console **Serveur NPS**.

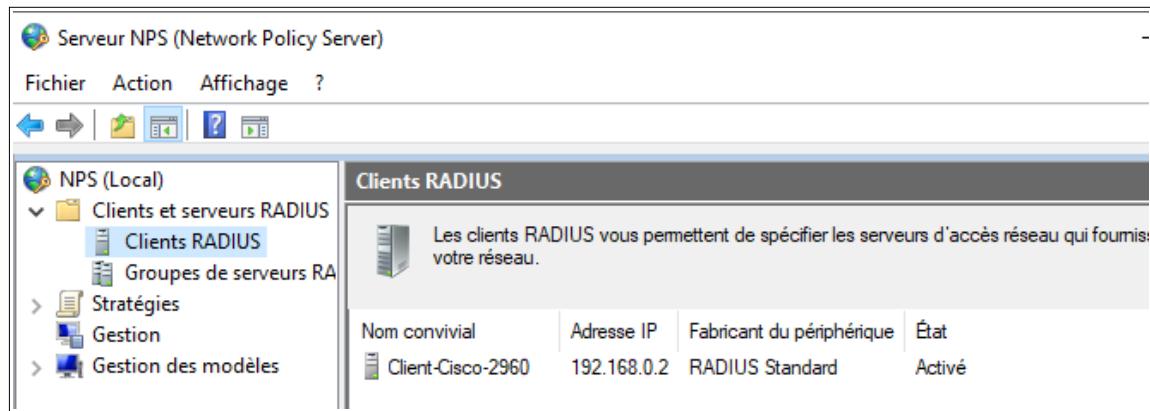
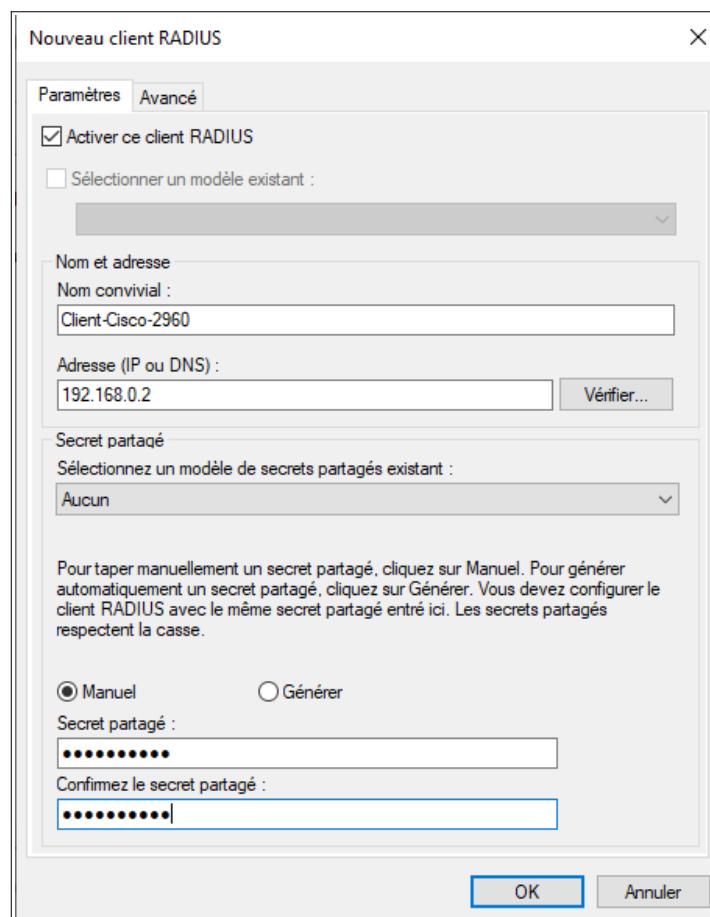
```

C:\> netstat -an | find "192.168.1.50"
  UDP  192.168.1.50:1645      *:*
  UDP  192.168.1.50:1646      *:*
  UDP  192.168.1.50:1812      *:*
  UDP  192.168.1.50:1813      *:*
C:\> Administrateur>

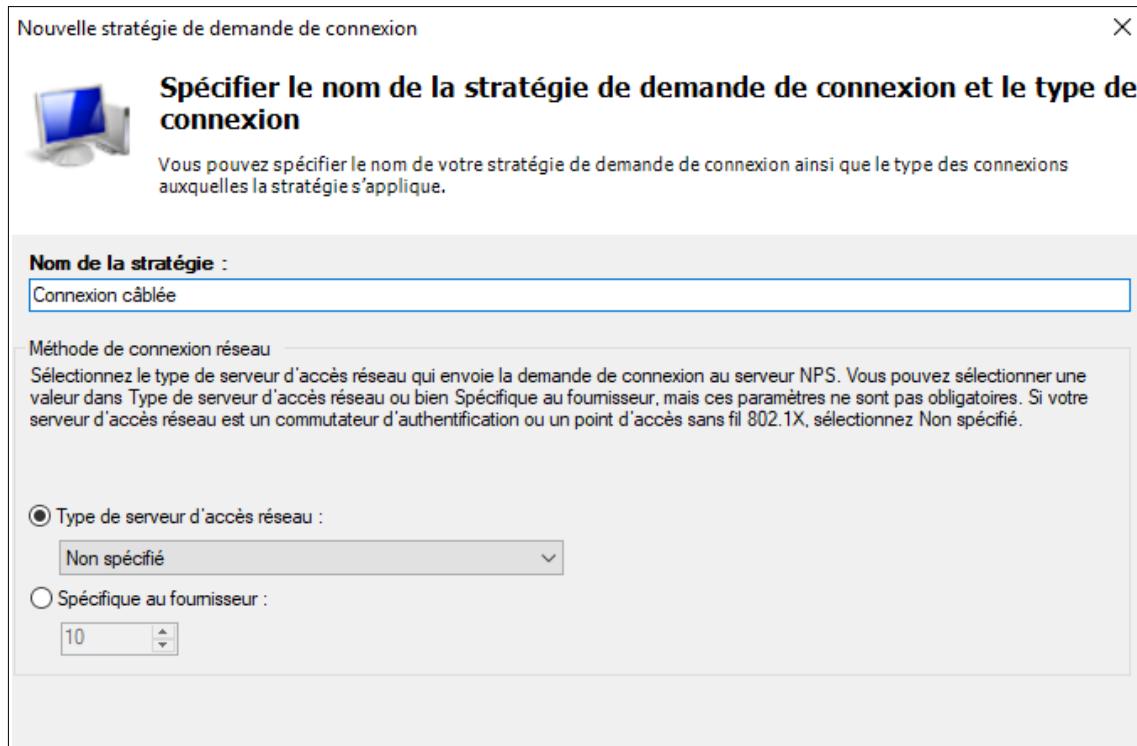
```

4ème étape : Nous vérifions le **sockets associés** aux ports d'écoute du serveur Radius. Nous observons que l'adresse IP concorde bien.

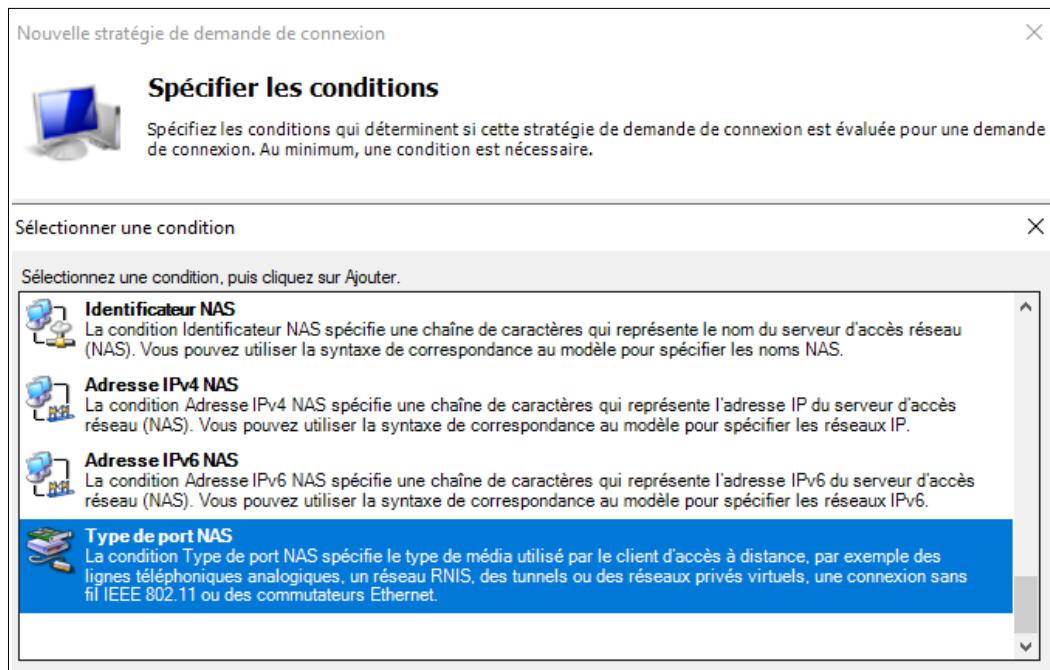
2.4/ Configuration du serveur RADIUS NPS



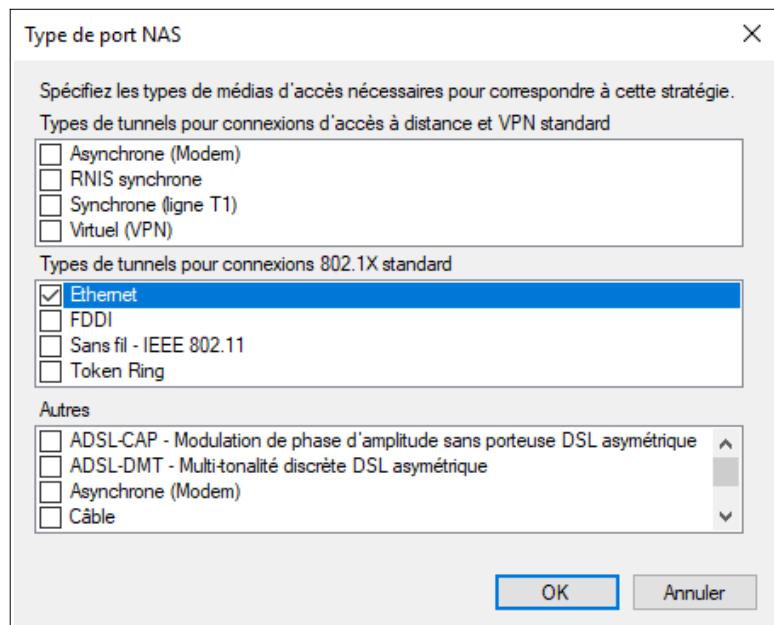
1ère étape : Création d'un nouveau **client Radius** avec son nom convivial, adresse IP et secret partagé.



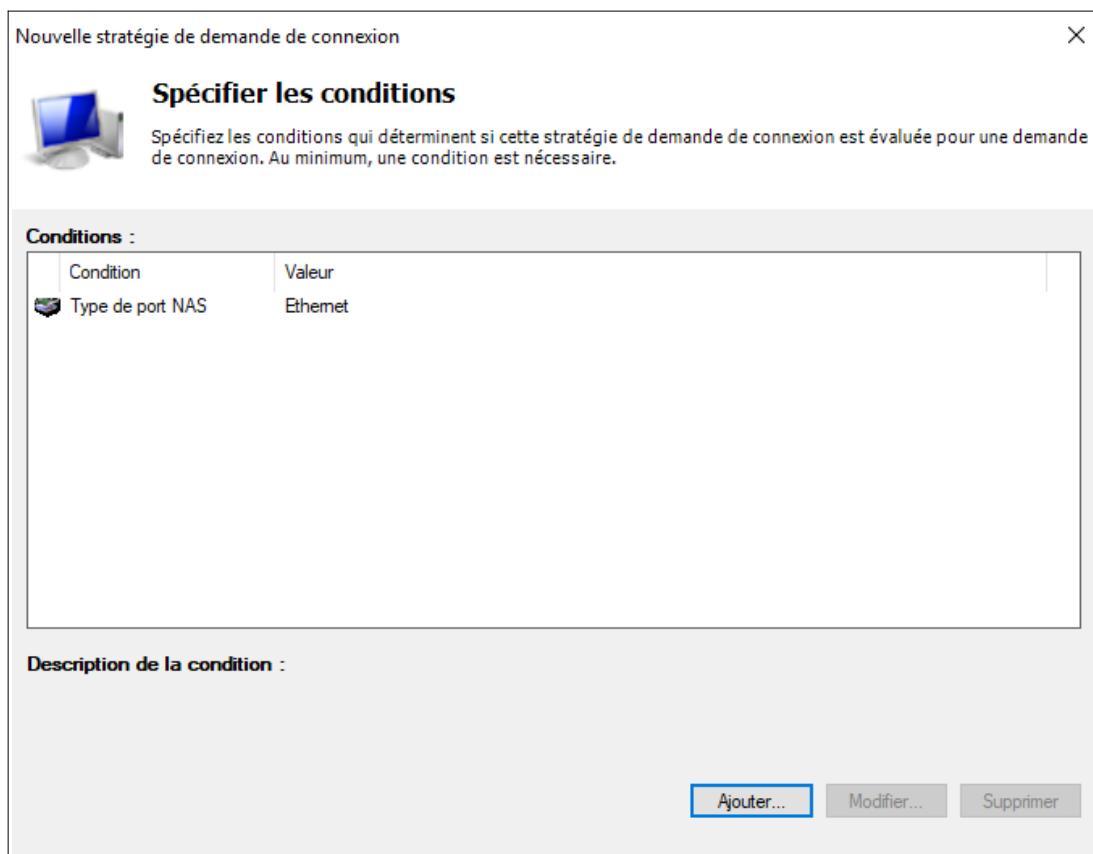
2ème étape : Nous ajoutons une nouvelle **stratégie de demande de connexion** nommée « **connexion câblée** »



3ème étape : Nous spécifions les conditions, notamment avec **type de port NAS**.



4ème étape : Nous cochons par la suite **Ethernet** dans la catégorie types de tunnels pour connexion 802.1X.



5ème étape : Notre condition est bien présente nous pouvons désormais faire suivant.

Nouvelle stratégie de demande de connexion

Spécifier le transfert de la demande de connexion



La demande de connexion peut être authentifiée par le serveur local ou être transférée aux serveurs RADIUS d'un groupe de serveurs RADIUS distants.

Si la demande de connexion correspond aux conditions de la stratégie, ces paramètres sont appliqués.

Paramètres :

Transfert de la demande de connexion

Authentification

Gestion

Spécifiez si les demandes de connexion sont traitées localement, si elles sont transférées à des serveurs RADIUS distants pour authentification, ou si elles sont acceptées sans authentification.

Authentifier les demandes sur ce serveur

Transférer les demandes au groupe de serveurs RADIUS distants suivant pour authentification :

<non configurée>

Nouveau...

Accepter les utilisateurs sans validation des informations d'identification

6ème étape : Nous demandons que les **demandes** soit **authentifier sur ce serveur**.

Nouvelle stratégie de demande de connexion

Spécifier 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.

Remplacer les paramètres d'authentification de stratégie réseau

Ces paramètres d'authentification sont utilisés à la place des contraintes et des paramètres d'authentification de la stratégie réseau.

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.

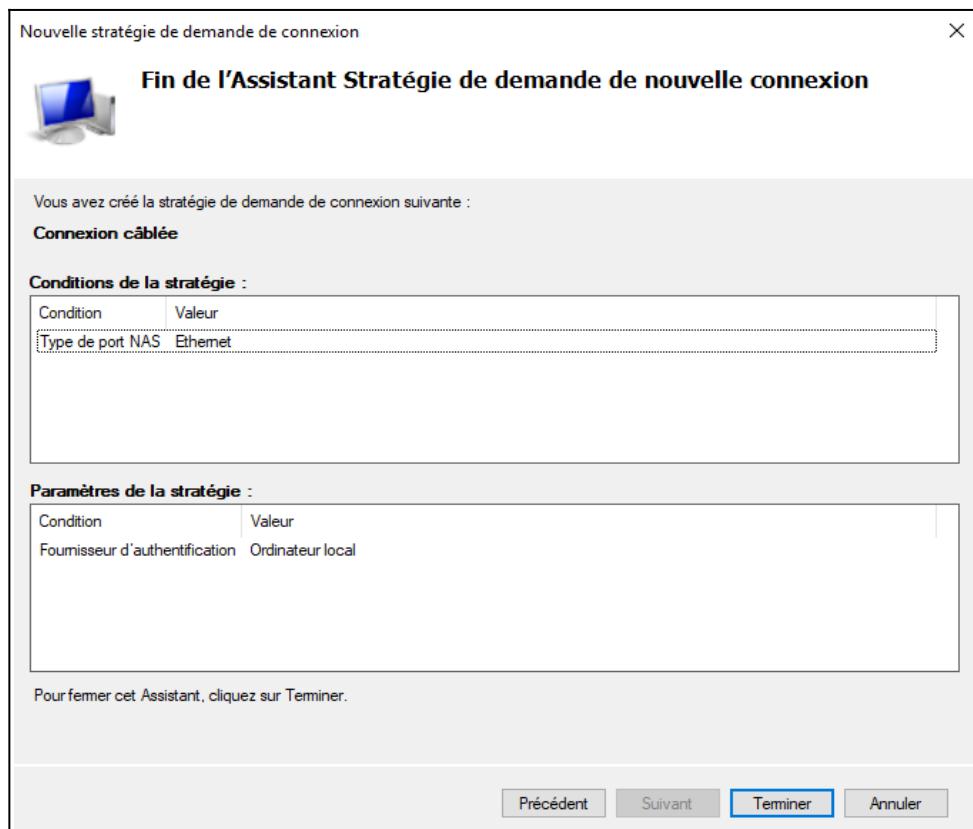
Précédent

Suivant

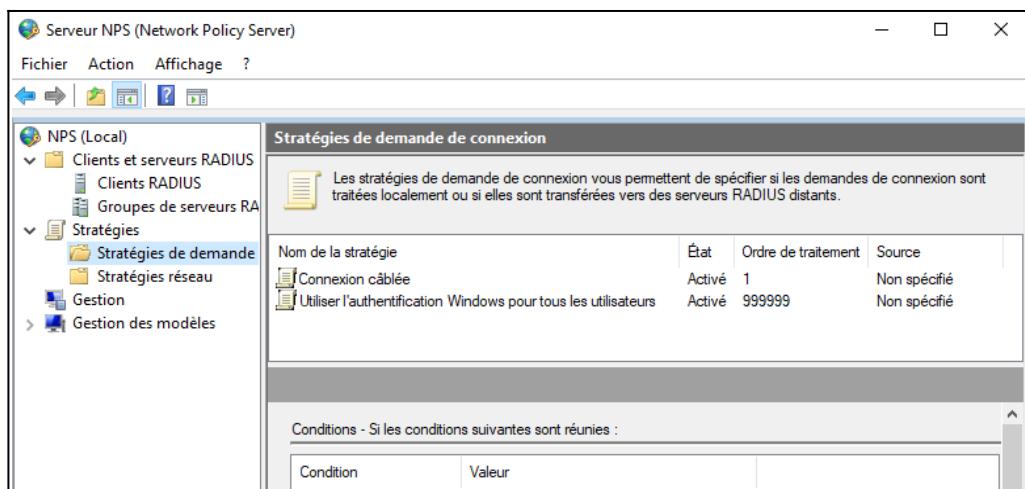
Terminer

Annuler

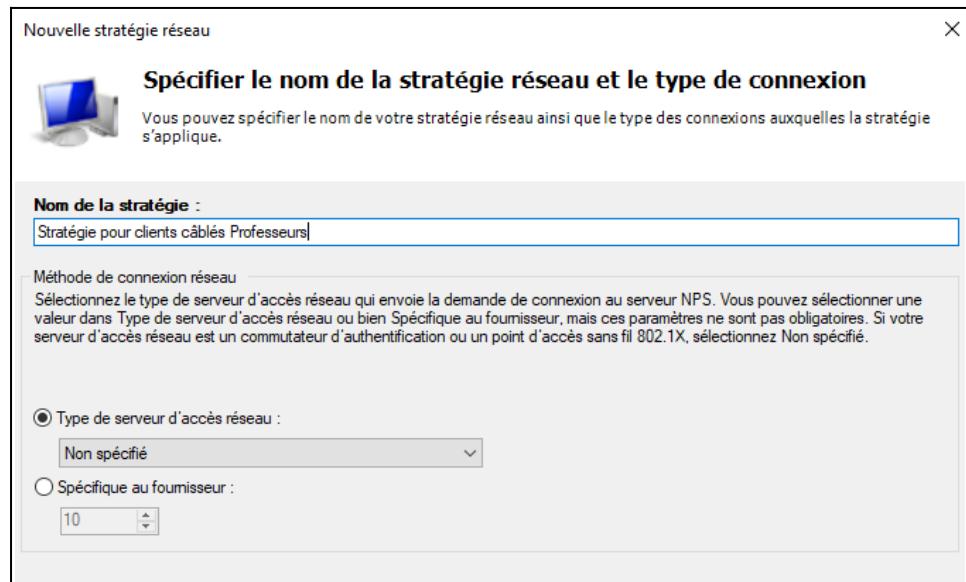
7ème étape : Ici nous ne modifions aucun paramètre.



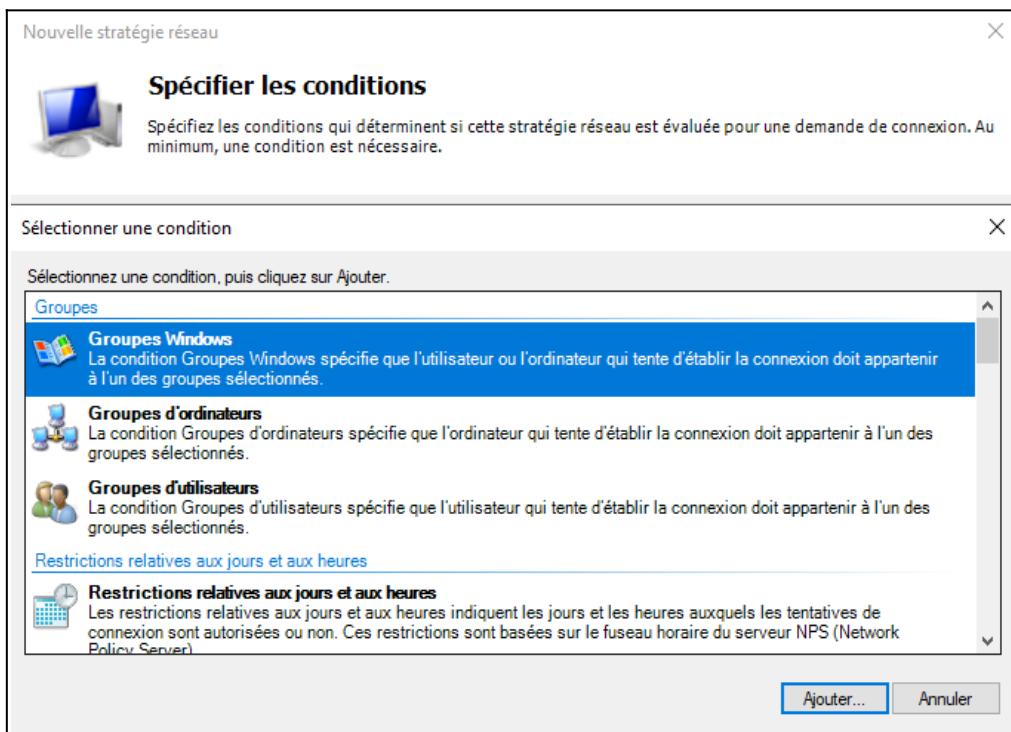
8ème étape : Nous pouvons désormais terminer la **stratégie de demande de connexion**.



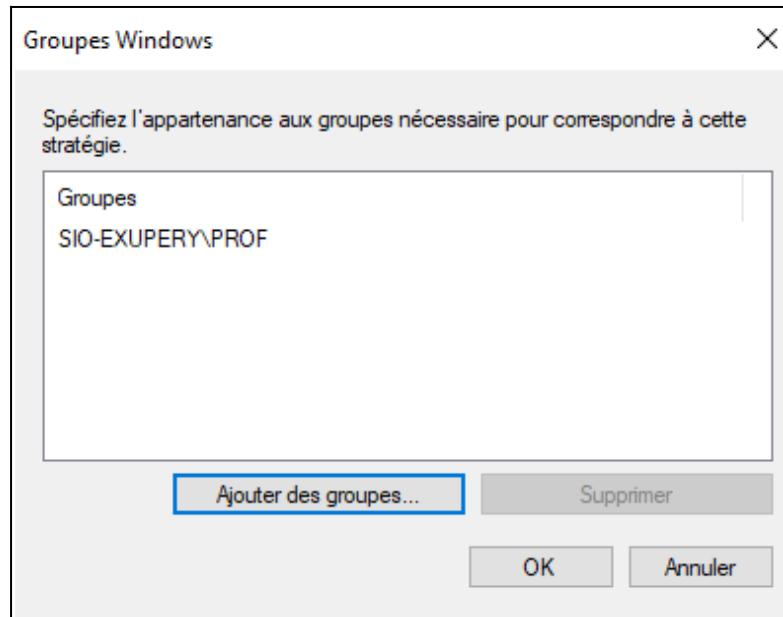
9ème étape : Nous observons que notre stratégie est bien présente.



10ème étape : Nous souhaitons désormais créer une nouvelle **stratégie réseau** pour les membres du **groupe Professeurs**.



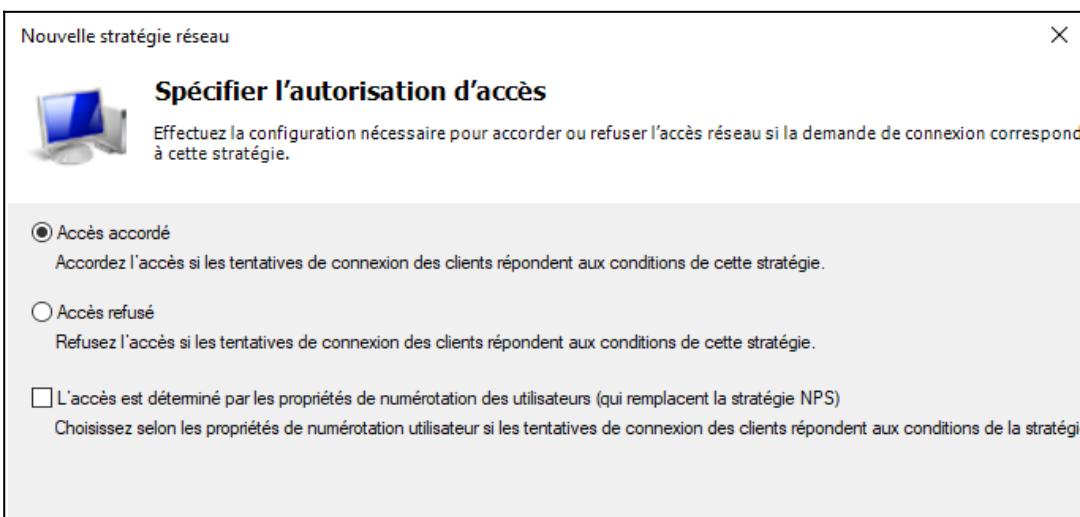
11ème étape : Nous ajoutons une **condition** en choisissant « **groupes Windows** ».



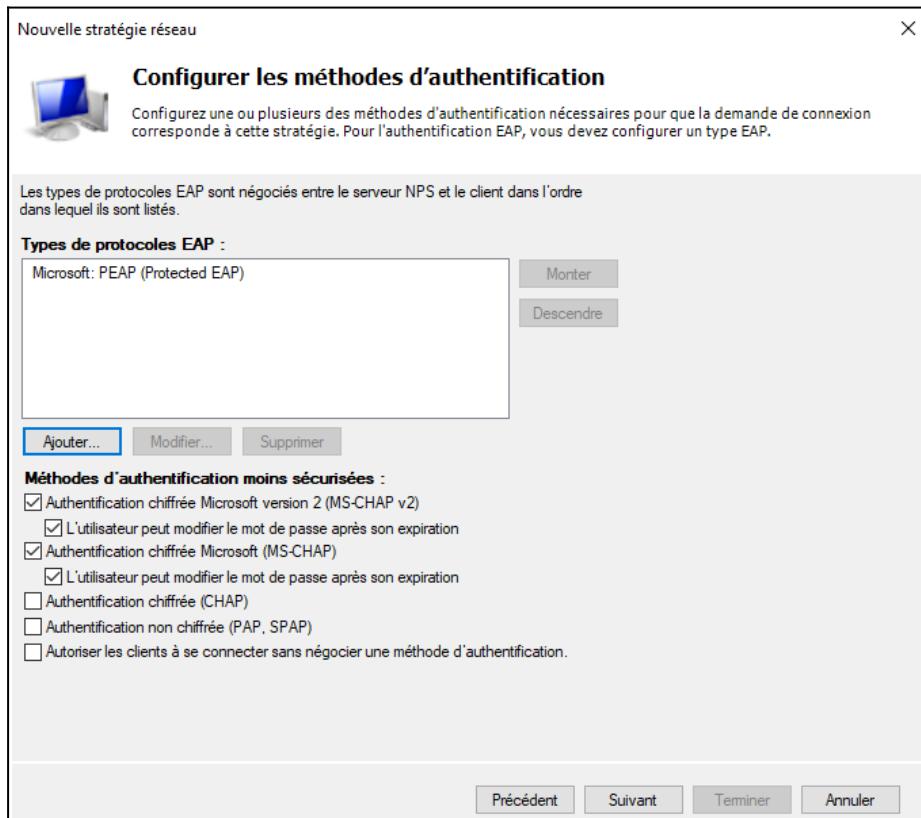
12ème étape : Bien évidemment dans celle-ci, le **groupe PROF** est ajouté.



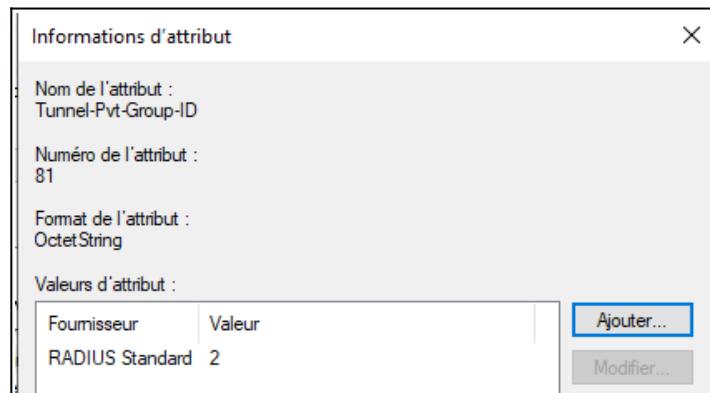
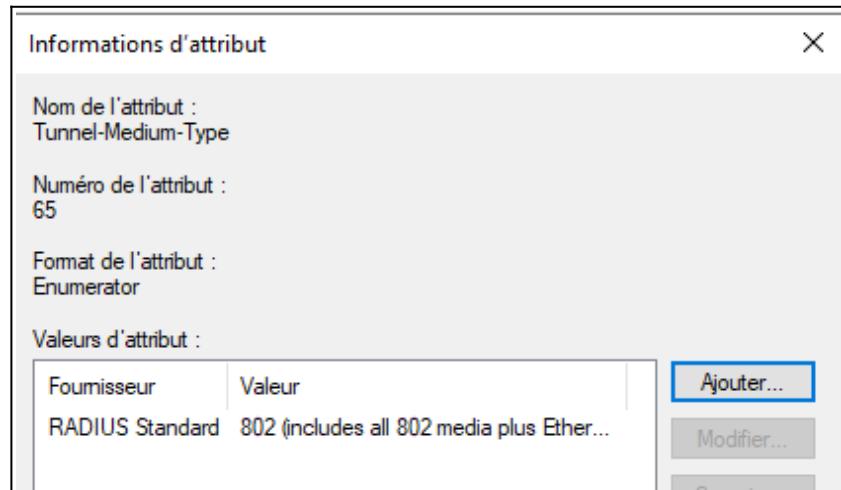
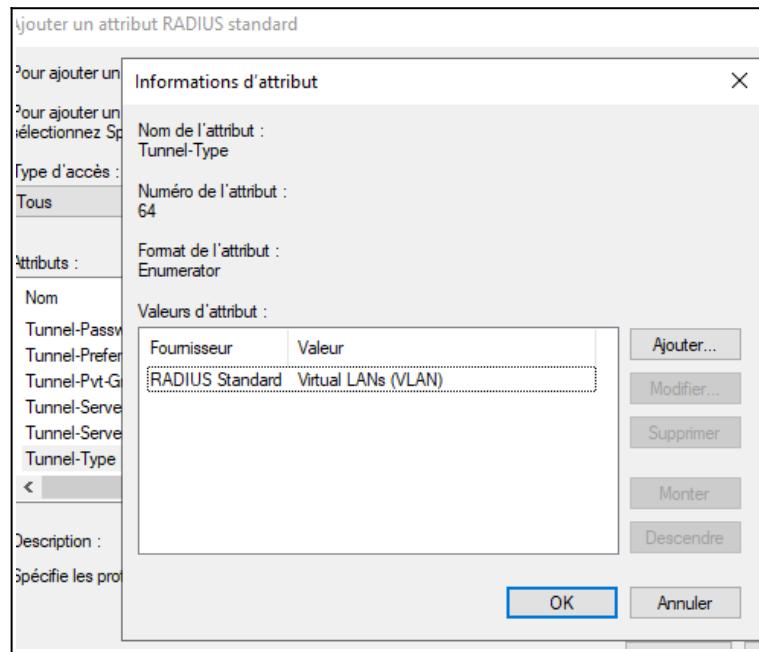
13ème étape : Nous ajoutons par ailleurs une deuxième condition pour spécifier le **type de port NAS** en cochant **Ethernet**.



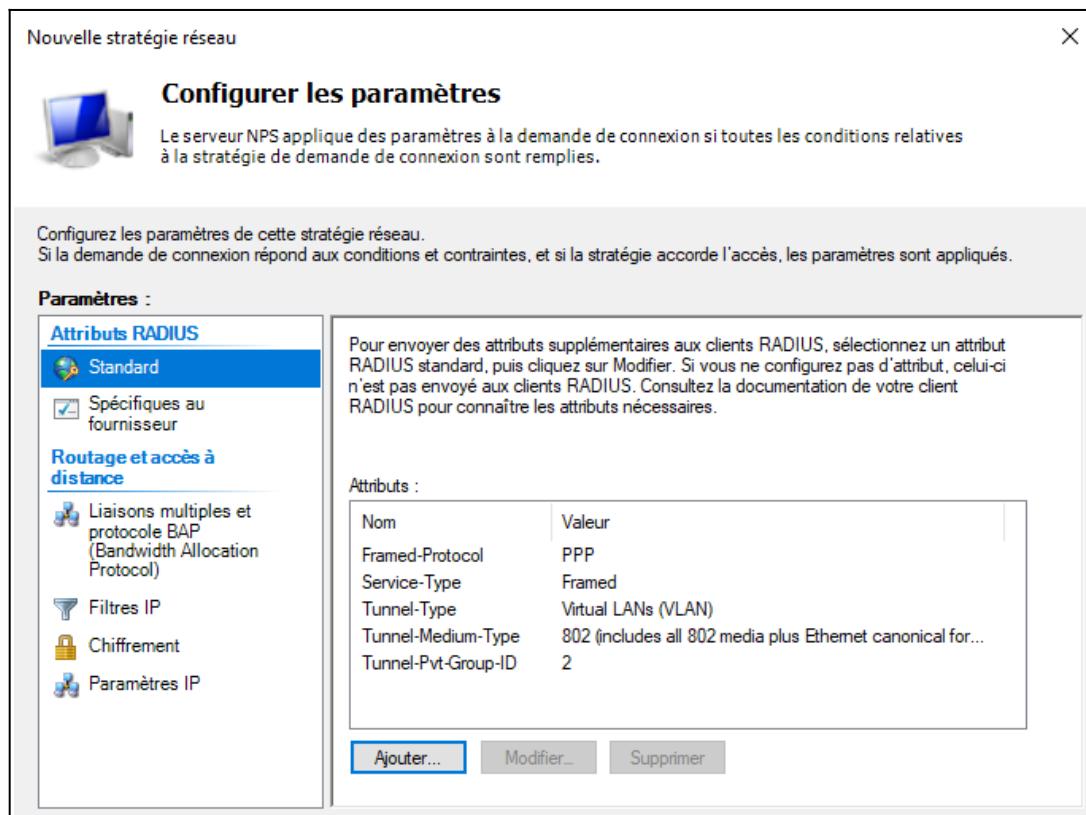
14ème étape : Nous accordons l'accès pour les membres du groupe.



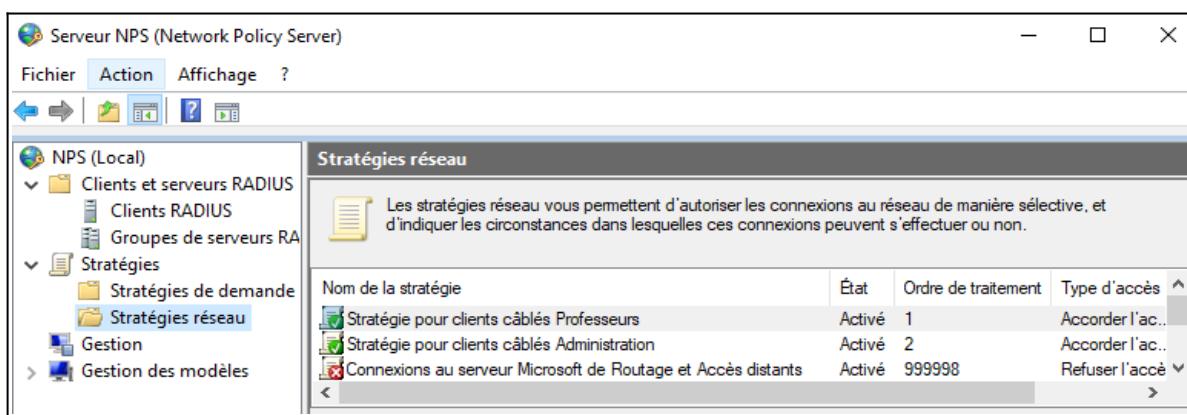
15ème étape : Nous déclarons le **type de protocole EAP (PEAP)** dans l'onglet pour configurer les **méthodes d'authentification**.



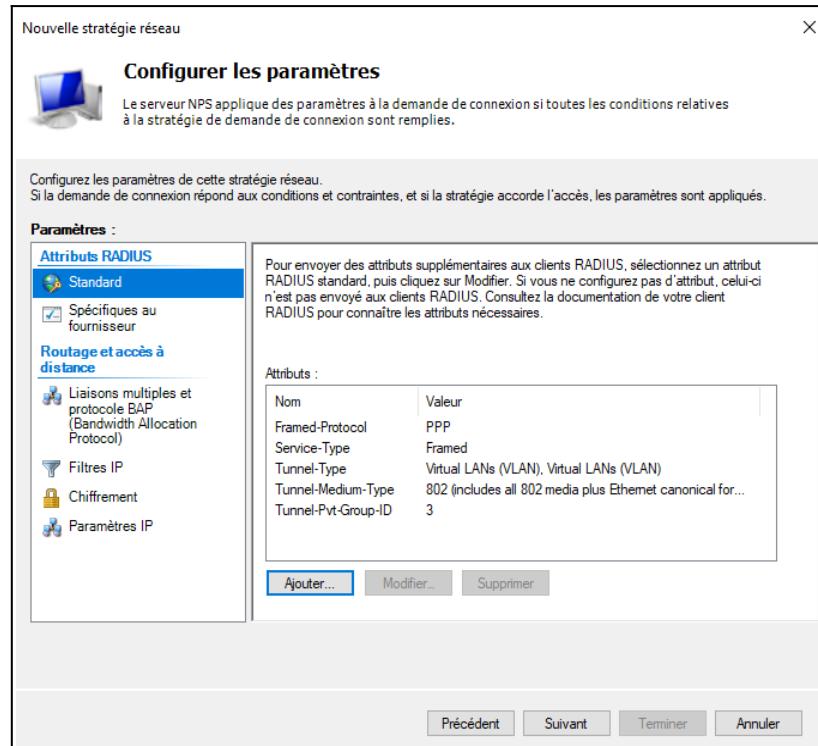
16ème étape : Dans l'onglet configurer les paramètres, nous ajoutons des nouvelles valeurs d'attribut pour le client Radius.



17ème étape : Nous pouvons observer les **attributs** que nous avons ajoutés.



18ème étape : Nous définissons désormais une stratégie d'accès réseau plaçant dans le VLAN3 les membres authentifiés comme faisant partie du groupe



19ème étape : Comme visualisé au-dessus, un récapitulatif des configurations nous est fourni.