Colombelle Malone
Bardet Arthur
BTS SIO 2

Document de validation de compétences

RADIUS

Dates du projet : 15/10

Equipe 4

1. Présentation du contexte d'entreprise

L'entreprise PRESBOIS possède des open Space et des endroits cloisonnées, ils veulent désormais ne plus être dépendant de vlan soit que tout le monde ait accès à un vlan en particulier en fonction du port dans lequel il se branche.

2. Objectifs attendus

On doit désormais pouvoir grâce au port Ethernet ou wifi de l'entreprise à partir de l'authentification depuis un poste de l'entreprise attribué un vlan et les autorisations qui vont avec directement à la connexion.

3. Plan de travail

Activité 1 : Installation de deux nouveaux services sur le serveur Windows 2025

- Installation d'une autorité de certification
- Installation du service NPS – Serveur Radius

Activité 2 : Paramétrage du service NPS

- Déclaration d'un client Radius : le commutateur
- Déclaration d'une stratégie de connexion
- Déclaration d'une stratégie d'accès réseau

Activité 3 : Paramétrer le commutateur Client Radius

- Paramétrage général 802.1x – déclaration du serveur RADIUS
- Paramétrage des ports contrôlés 802.1x

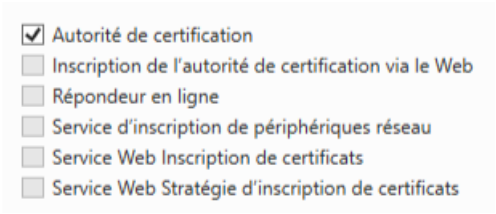
Activité 4 : Configurer le client final en 802.1x

- Service Configuration automatique de réseau câblé
- Onglet « Authentification » des propriétés de la carte réseau
- Réglage des paramètres avancés

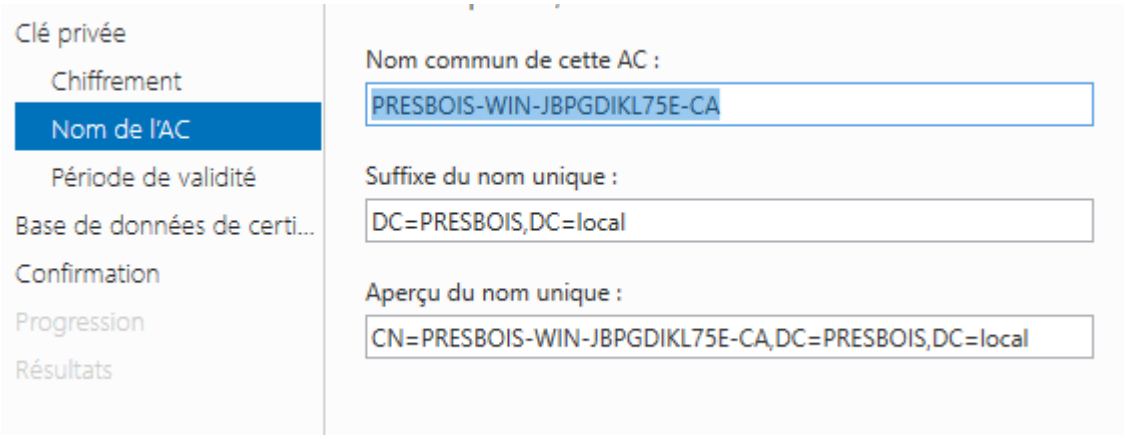
4. Réalisation

<u>Activité 1 : Installation de deux nouveaux services sur le serveur Windows 2025 :</u>

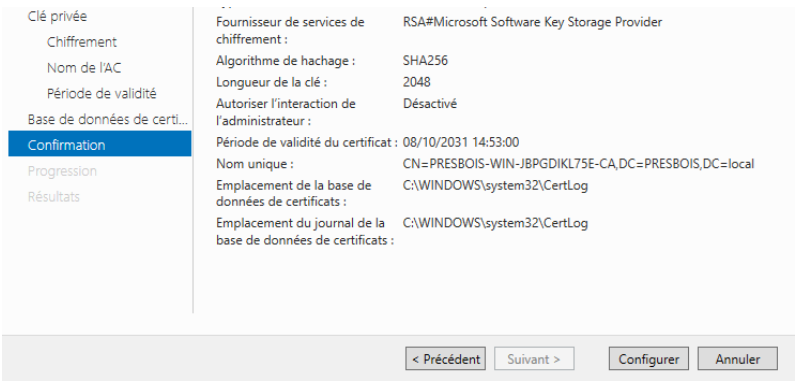
Lors de l'installation Vous cocher le service de rôle « Autorité de certification »



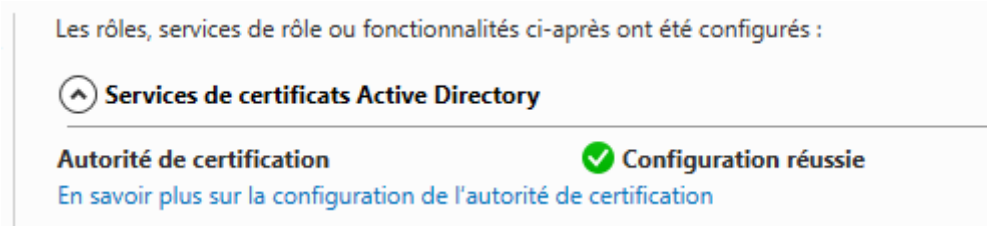
Ensuite nous allons mettre ensuite les paramètres suivants :



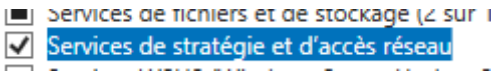
Puis vous cliquez sur suivant jusqu'à confirmation



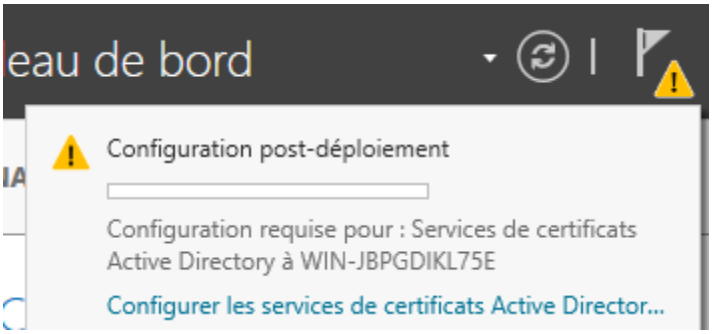
Puis après avoir appuyé sur « Configurer » vous obtenez cette fenêtre :



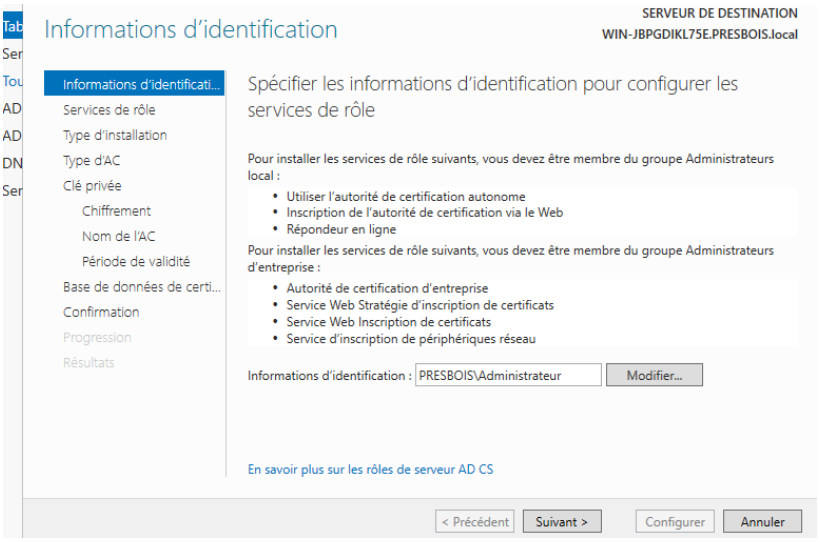
Nous avons fini avec la configuration de notre certification. Nous allons maintenant nous occupés d'installer le Service NPS, vous faites le même processus qu'avant sauf que nous allons choisir ce service :



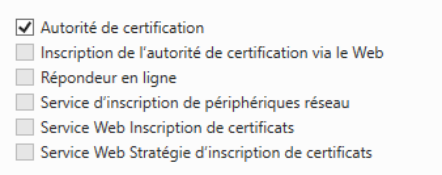
Puis vous appuyez sur suivant puis installer. Ensuite vous allez appuyer sur le drapeau et vous allez appuyer sur "Configurer les services de certificats Active Directory"



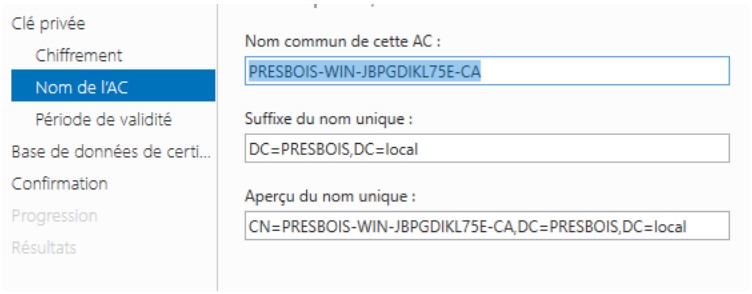
Vous allez atterrir sur cette page :



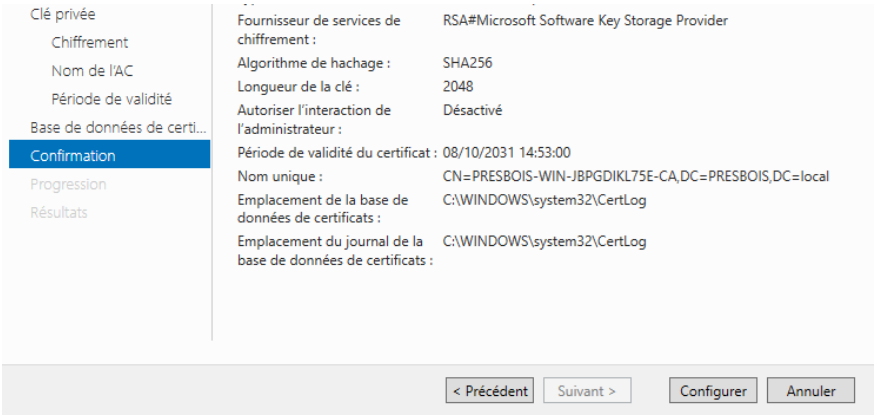
Vous cliquez sur Suivant et dans service de rôle vous allez cocher "Autorité de certification"



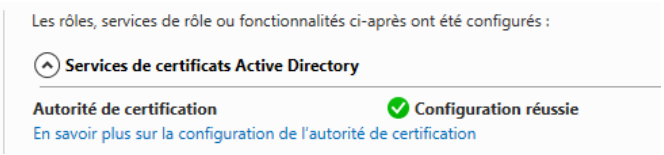
Vous cliquez sur suivant jusqu'au NOM de l'AC vous mettez ce que vous voulez soit pour nous :



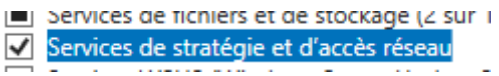
Puis vous cliquez sur suivant et vous allez appuyer sur configurer ici :



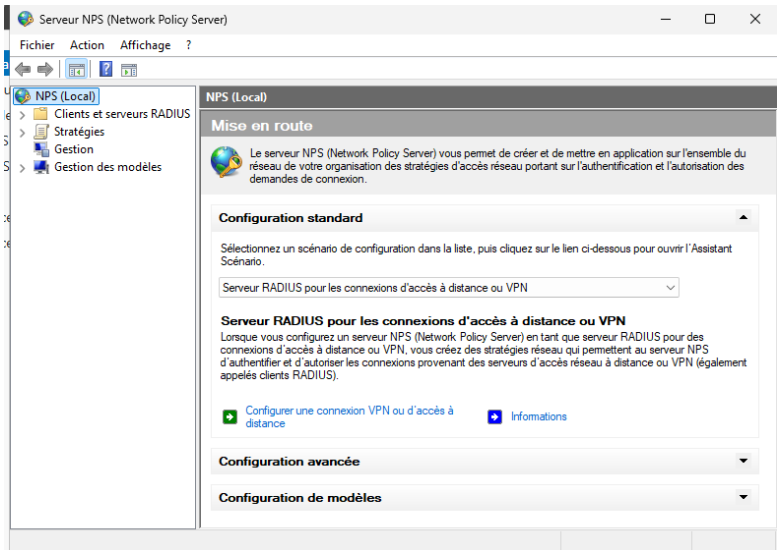
Et après configuration vous allez obtenir ceci :



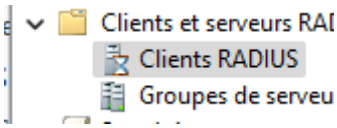
Et bien joué vous avez fini de configurer votre certification, ensuite nous allons installer le service NPS , soit même processus qu'avant sauf que vous allez ajouter un service.



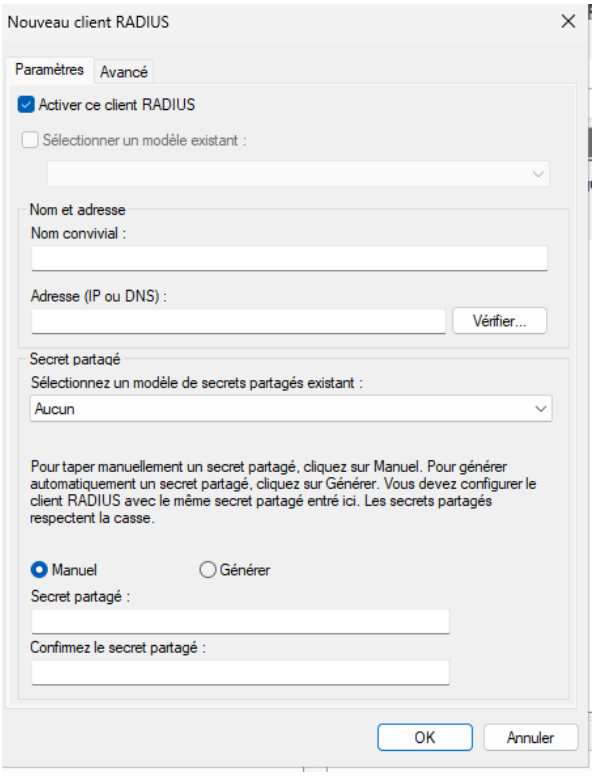
Ensuite nous allons le configurer soit nous allons taper npcs.msc et nous tombons sur ça :



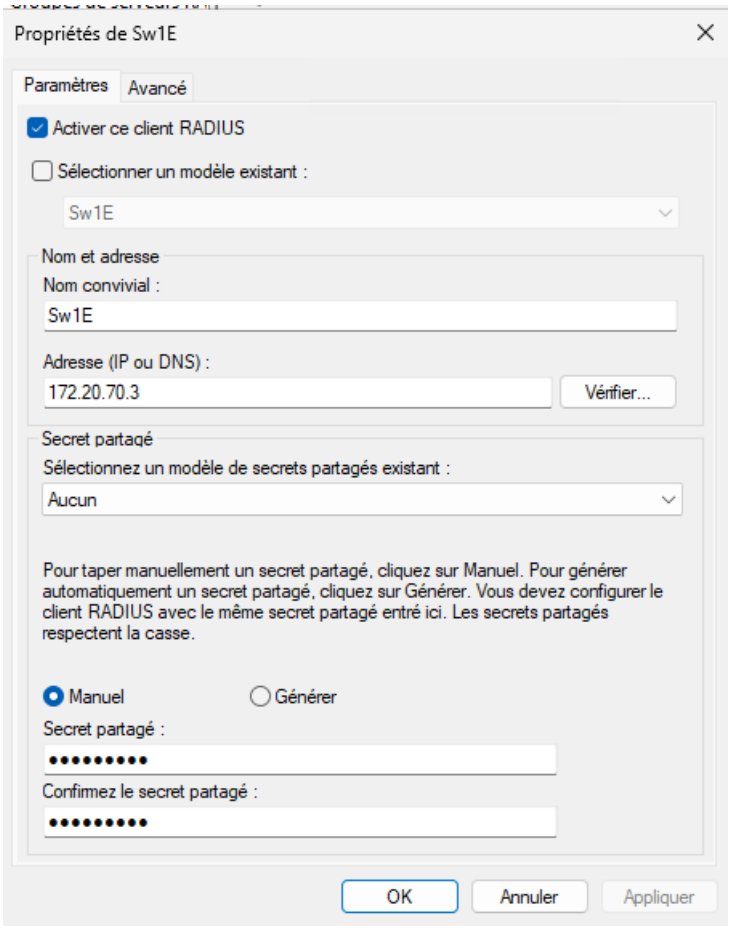
Ensuite vous allez dans Client et serveurs Radius vous déroulez et vous cliquez sur client radius :



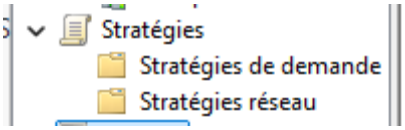
Puis click droit puis nouveau :



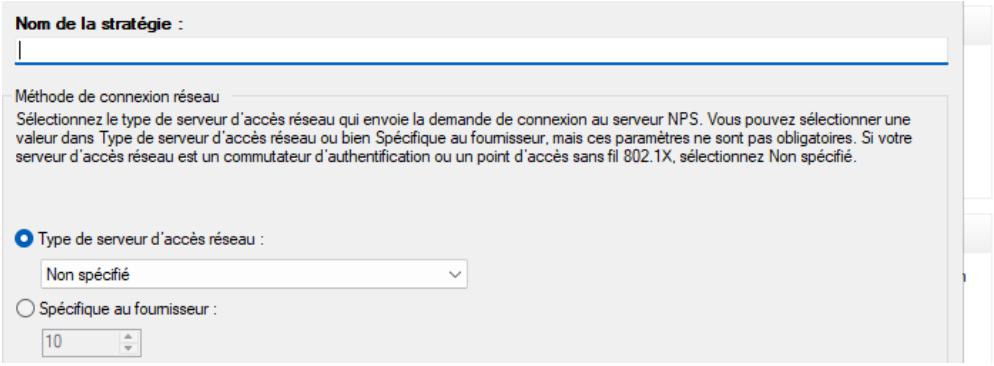
Maintenant nous allons mettre les infos de notre SWRC soit :



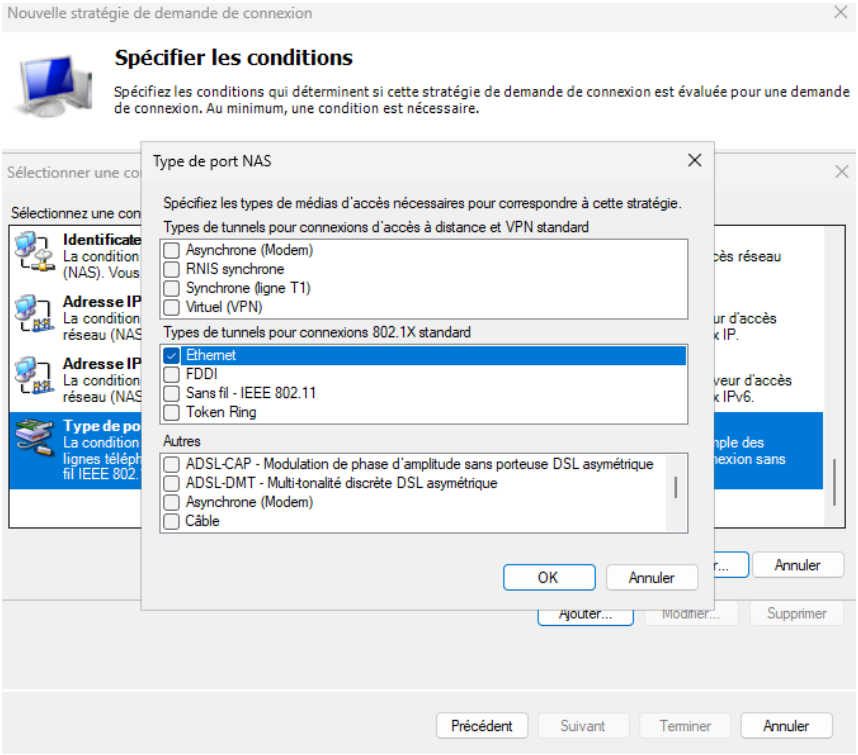
Ensuite nous allons faire deux stratégie, une d'accès réseau et une stratégie de connexion. Pour l'accès réseau vous allez ici :



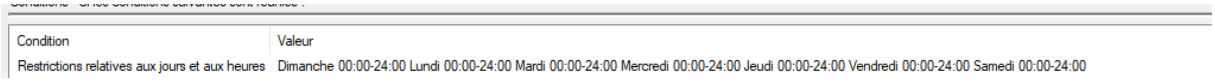
Click droit nouveau dans stratégie de demande vous tombez sur ça :



Vous allez mettez un nom comme vous voulez puis suivant puis dans conditions vous ajouter une conditions et vous allez tout en bas “type de port NAS “ et vous cochez Ethernet puis suivant puis terminer.

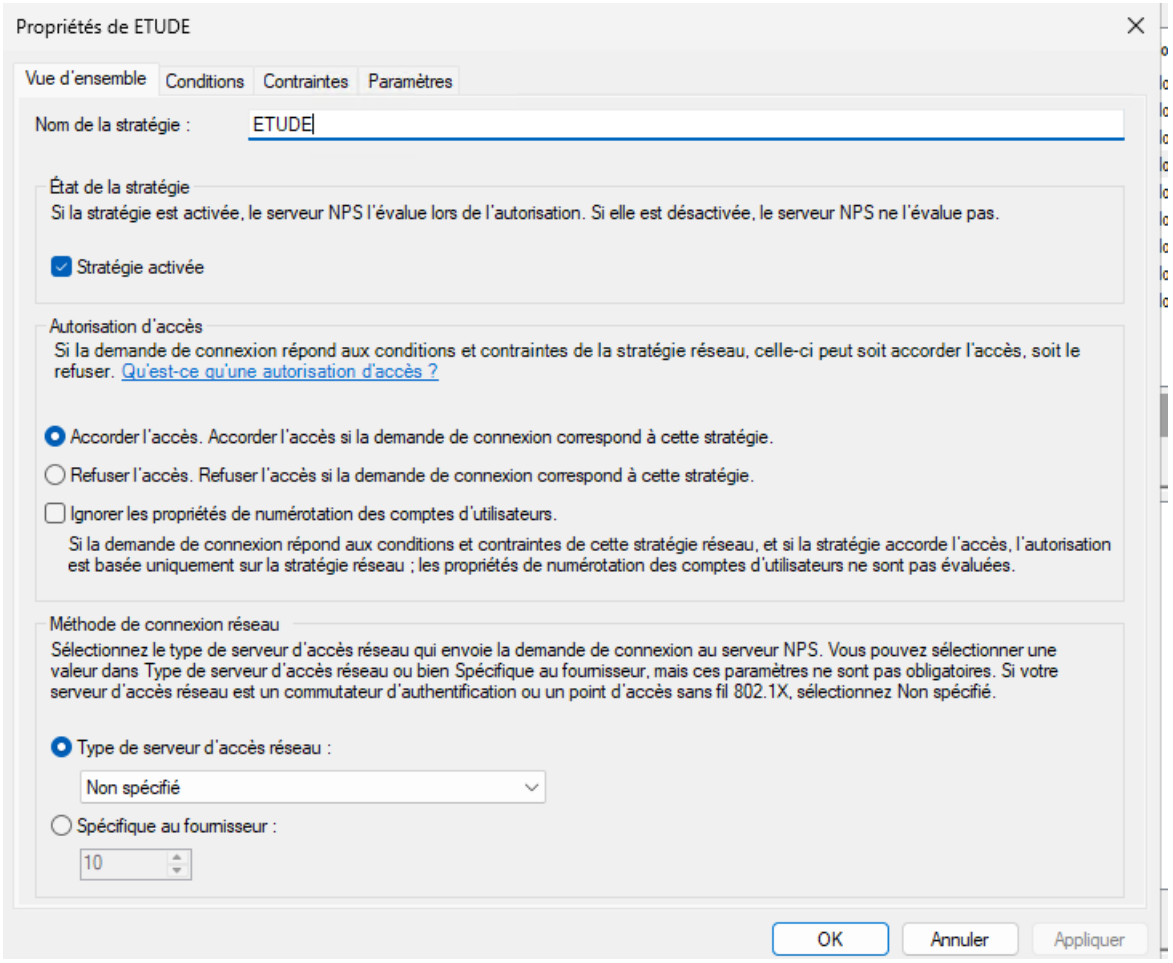


Et vous aller aussi ajouter une condition « Restriction relatives aux jours et aux heures » et vous allez mettre ceci :

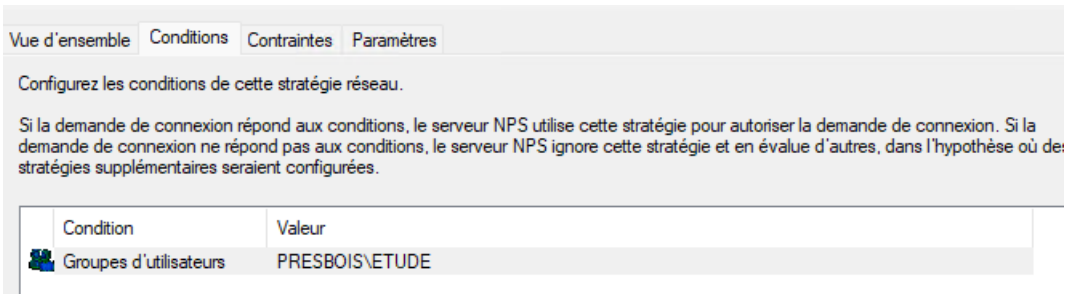


Vous avez fini la stratégie de demande.

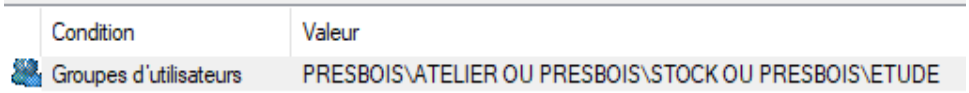
Ensuite vous allez faire un clic droit Stratégie de réseau puis faut mettre un nom et mettre ces configurations pour la première page :



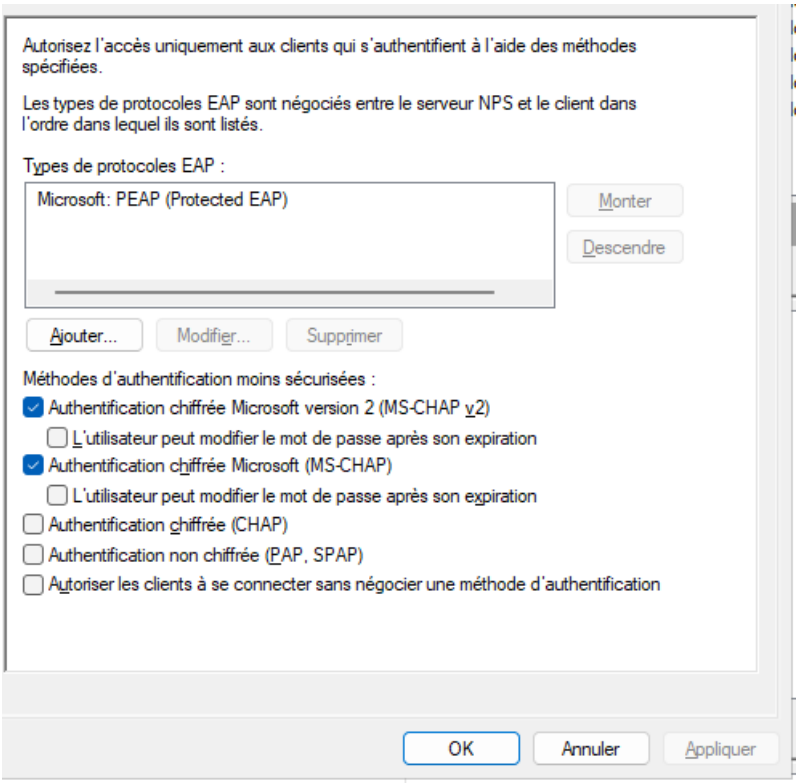
Puis pour l'onglet connexion vous allez mettre ceci pour ETUDE par exemple :



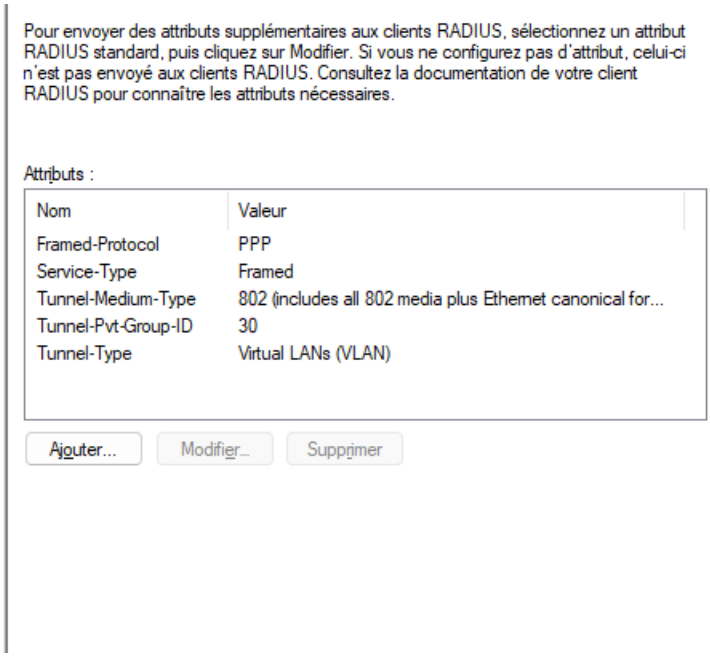
Puis dans les conditions vous faite ajouter, puis groupe utilisateur et vous mettez vos groupes et vous obtenez ceci :



Ensuite pour les contraintes :



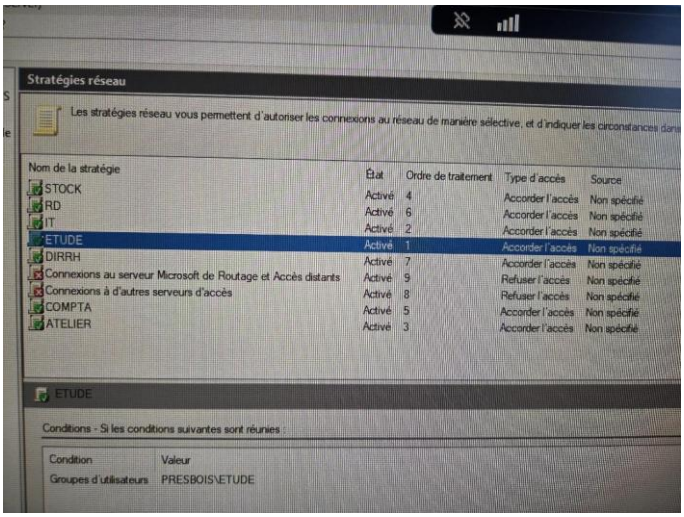
Et pour terminer les paramètres :



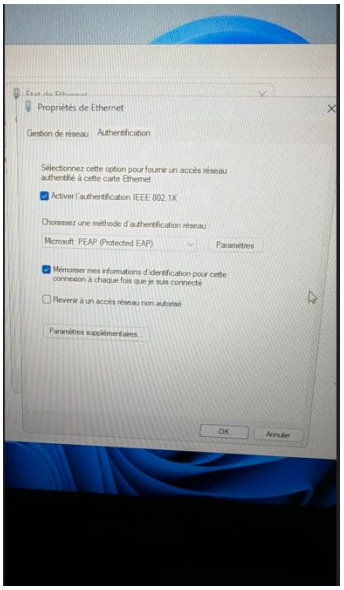
Et le Tunnel-Pvt-Group-ID 30 correspond au VLAN etc etc.

Puis suivant puis terminer, bien joué vous avez toute cette partit radius et certification.

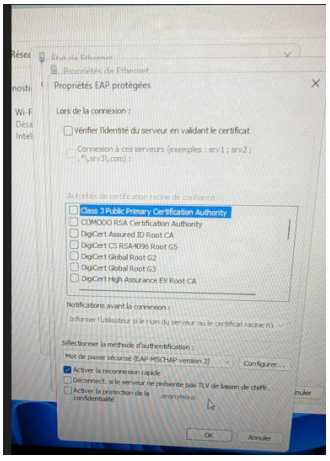
Il faut également mettre des ordres de priorité, mettre les stratégies liées au RADIUS en haut de « connexions… distants ». Comme sur l'image.



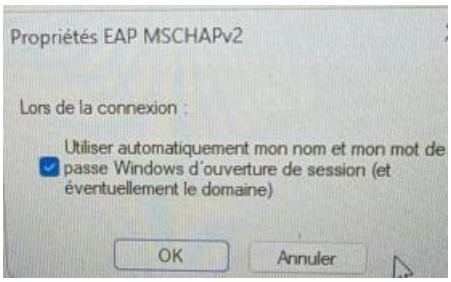
Ensuite pour la partit Poste client nous allons mettre ces paramètres dans la carte réseau ethernet propriété -> Authentication :



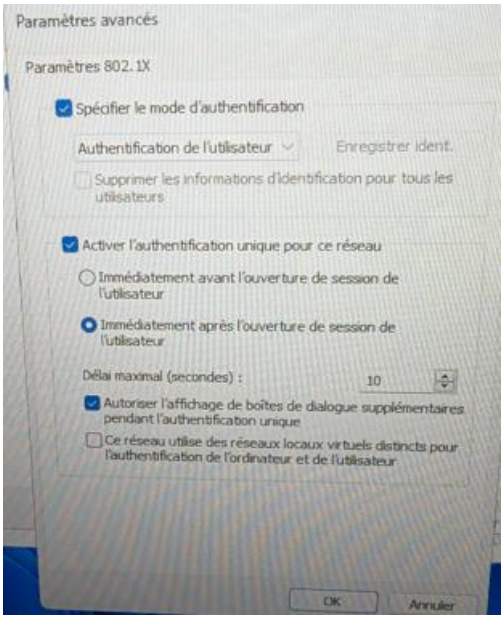
Puis dans paramètre :



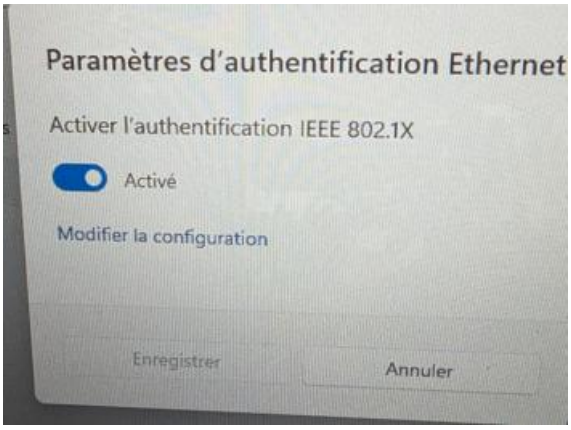
Puis dans Configurer :



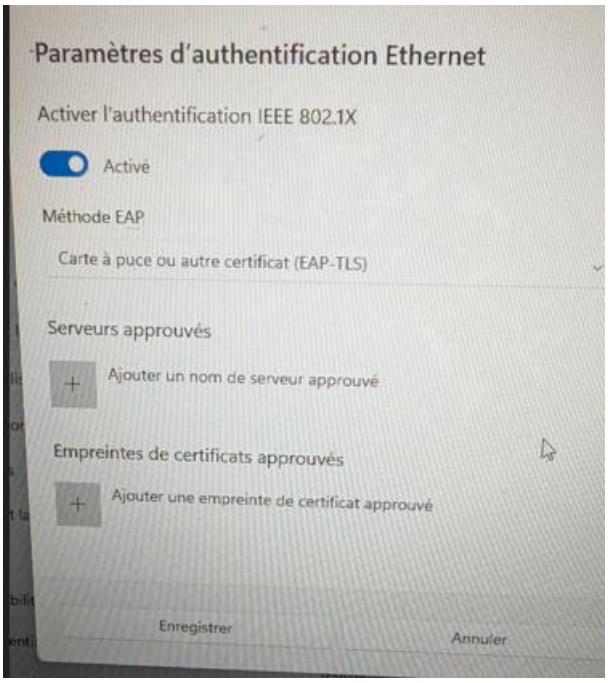
Puis on retourne avant et on fait paramètre supplémentaires et nous mettons cette configuration :



Puis nous allons aller dans les paramètres wifi et modifier ethernet et nous allons activer cette fonctionnalité :



Puis modifier la configuration et nous allons mettre ceci :



Et nous avons fini globalement la configuration de la confi de l'ad et du poste client manque plus que le Sw1E à configurer :

Premièrement sur chaque port du switch nous allons mettre ceci :

```
interface GigabitEthernet1/0/1
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast edge
!
interface GigabitEthernet1/0/2
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast edge
!
interface GigabitEthernet1/0/3
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast edge
!
```

switchport mode access : Le port est configuré en mode accès (destiné à brancher un terminal utilisateur final, comme un PC ou une IP phone, et non un autre switch).

authentication port-control auto : Active le contrôle d'accès sur le port. Le port est bloqué par défaut tant que l'utilisateur ou la machine ne s'est pas authentifié.

dot1x pae authenticator : Configure le port en tant qu'authentificateur selon la norme **IEEE 802.1X**. C'est lui qui va demander au client de s'identifier (via un serveur RADIUS par exemple).

spanning-tree portfast edge (anciennement *portfast*) : Désactive l'attente du protocole Spanning Tree (STP) sur ce port. Le port bascule immédiatement en état de transmission (forwarding) dès

Et ensuite nous allons mettre ces configurations globales dessus :

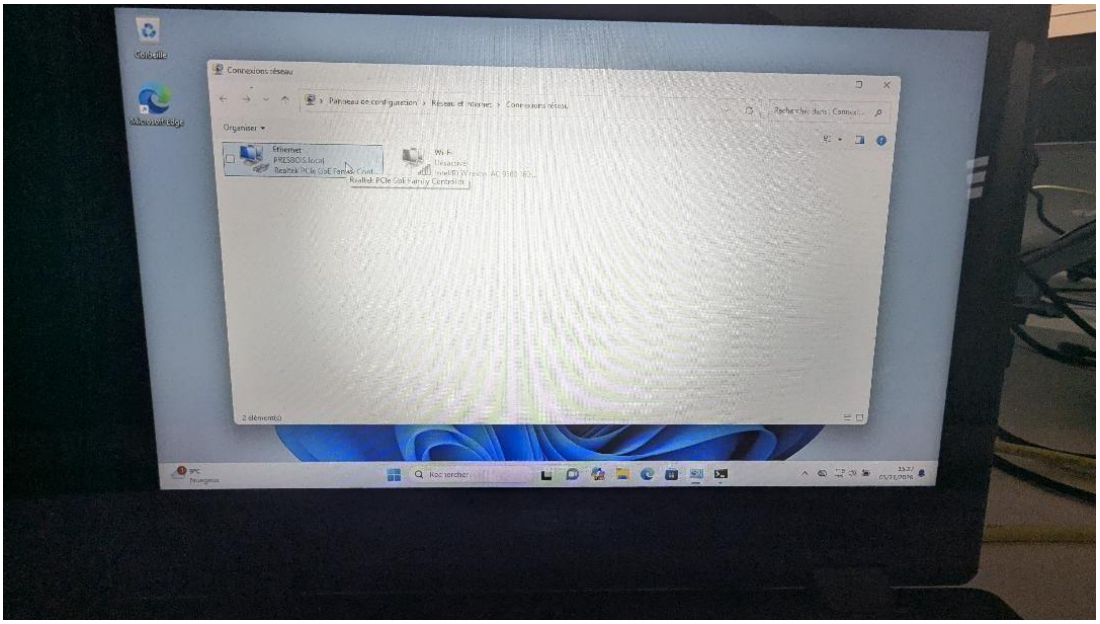
```
dot1x system-auth-control
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

dot1x system-auth-control : Active globalement le système d'authentification **IEEE 802.1X** sur l'équipement. C'est la commande maître indispensable pour que le switch autorise (ou refuse) l'authentification des machines sur ses ports d'accès.

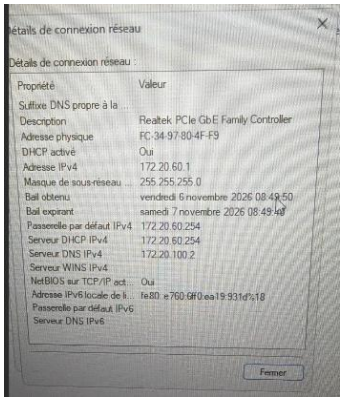
spanning-tree mode rapid-pvst : Configure le protocole Spanning Tree en mode **Rapid PVST+** (basé sur la norme 802.1w). Contrairement au STP classique qui met 30 à 50 secondes pour réagir en cas de changement de topologie, celui-ci converge en quelques secondes par VLAN pour éviter les boucles réseau tout en minimisant les coupures.

spanning-tree extend system-id : Active l'extension de l'ID système dans le Bridge ID du Spanning Tree. Cela permet d'inclure le numéro de VLAN directement dans les calculs de priorité des VLANs, ce qui est obligatoire pour faire fonctionner correctement le Rapid PVST+ sur tous les VLANs.

Après tout ça nous avons fini toutes les configurations du switch et AD / poste client donc quand nous nous connectons avec un utilisateurs de l'ad Soit Etude ou IT pour l'exemple nous tombons sur ça :

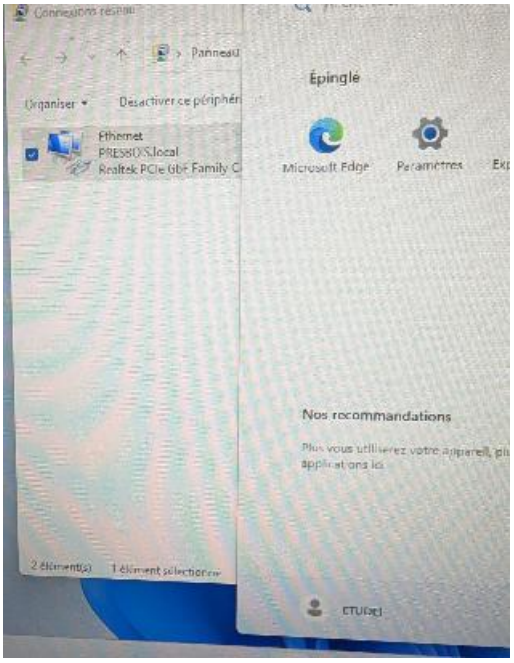


Pour IT nous voyons que nous sommes bien identifiées et quand nous regardons l'adresse IP :

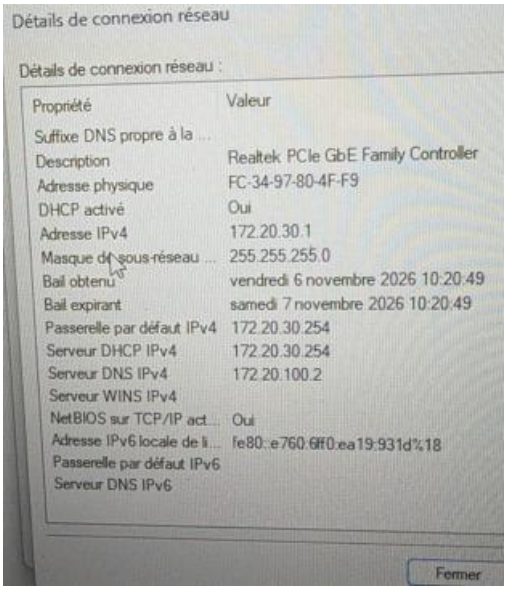


Et si nous changeons d'utilisateurs pour aller sur Etude par exemple :

Nous sommes bien identifié :



Et nous récupérons bien une adresse Ip en .30 soit :



Nous avons désormais Fini le Projet Radius.