MISE EN PLACE D'UN SERVEUR RADIUS POUR CONNEXION FILAIRE

StgInfo

RESE

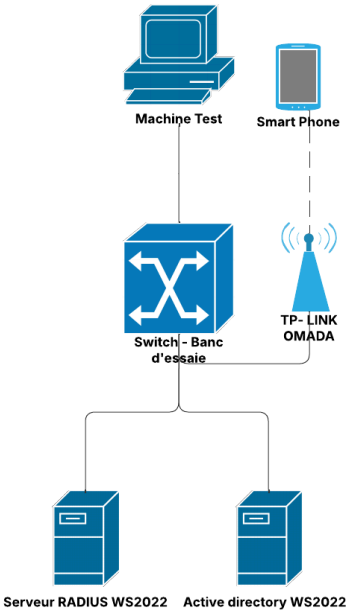
Table des matières :

1. Matériel requis

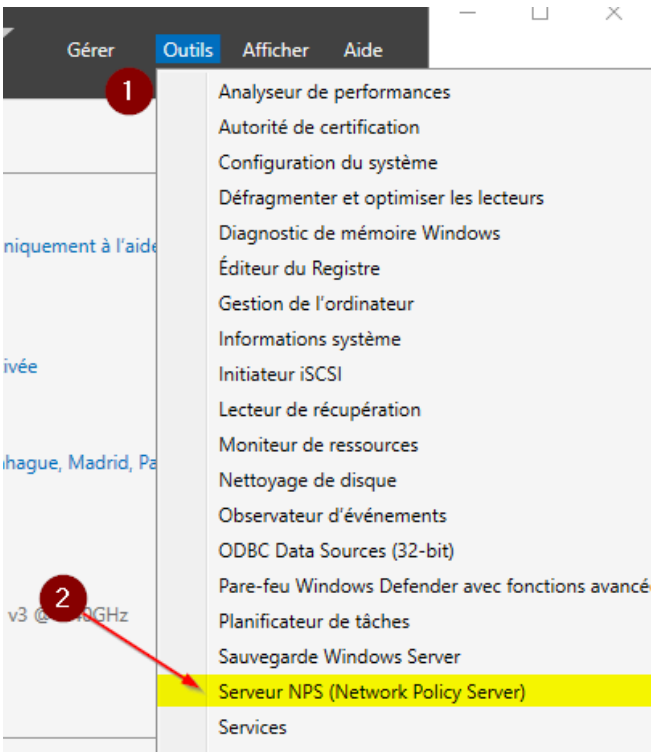
- **PC portable de test** (avec droits admin local)
- **Switch** (avec accès console/SSH)
- **Windows Server configuré en NPS**

Schéma réseau

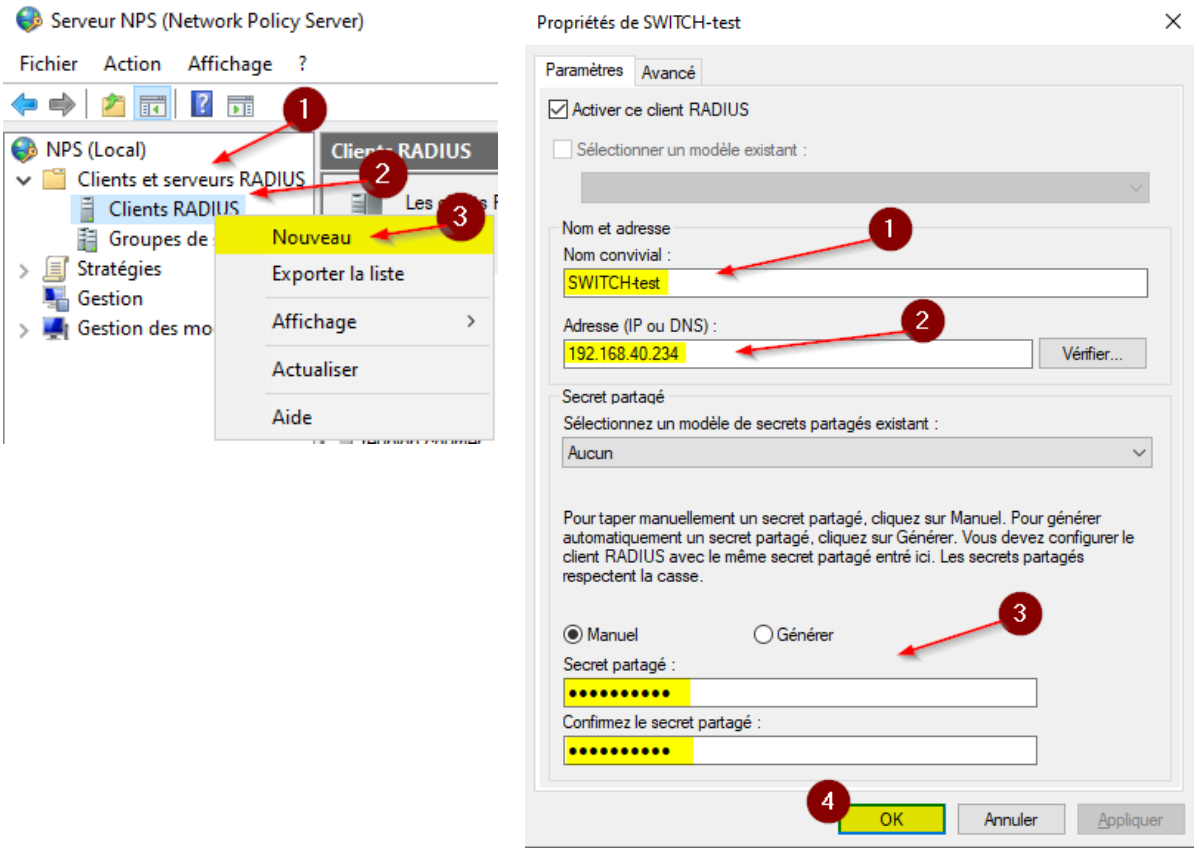
- **Port 48** : Connecté au serveur Windows 2022 / Réseau de la RESE
- **Port 5** : Connecté à la machine de test
- **Ports 5-10** : Authentification RADIUS EAP activée
- **Authentification 802.1X** : Mot de passe requis (peut être automatisé via GPO)



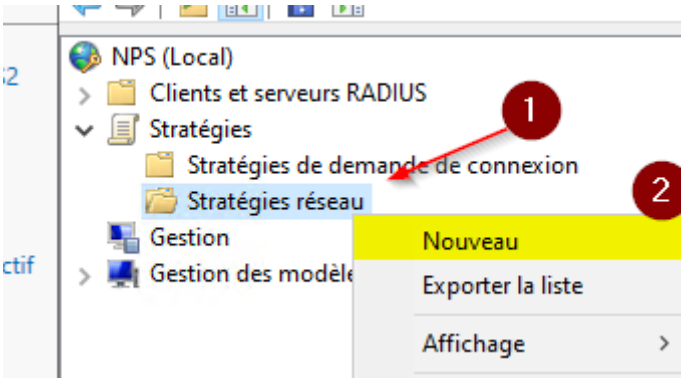
2. Configuration du serveur Radius & NPS

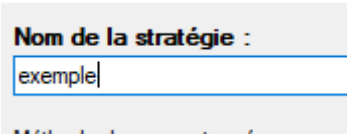


Le switch doit être ajouté en tant que client RADIUS sur le serveur NPS. Cela implique de spécifier son adresse IP et un mot de passe partagé, qui sera utilisé lors de la configuration du switch.

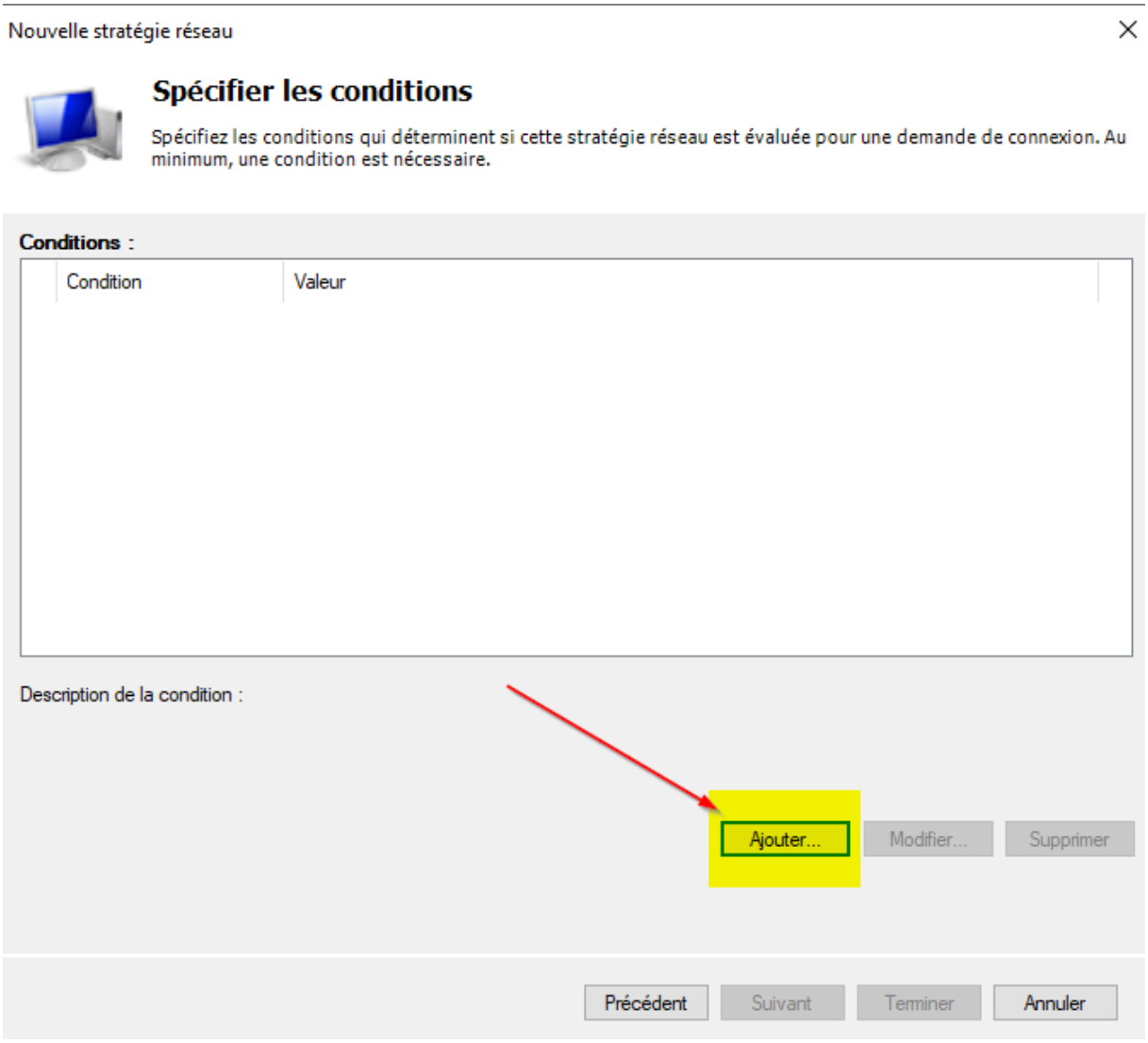


Ensuite, une règle de stratégie réseau est définie pour autoriser les connexions du groupe cible, en utilisant PEAP et un mot de passe pour l'authentification.

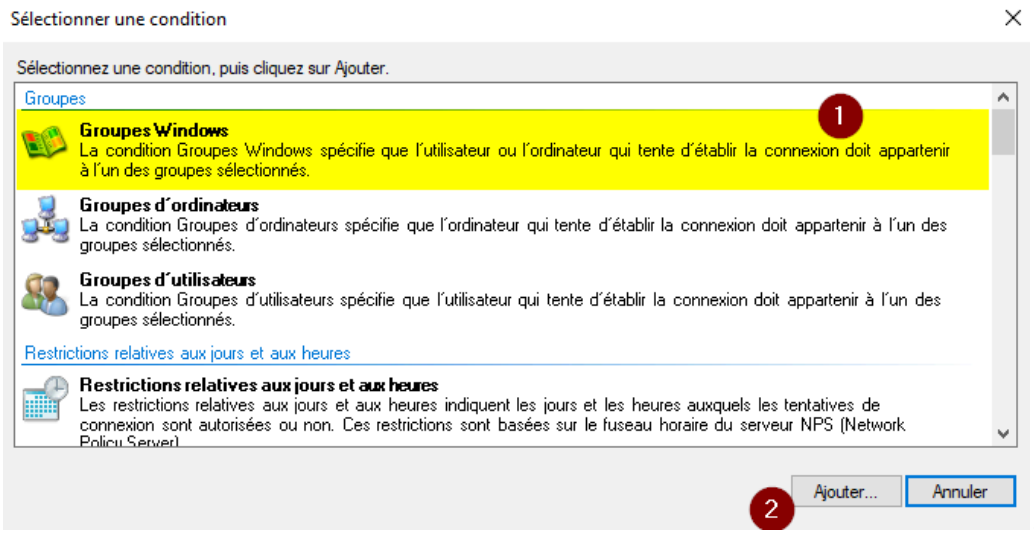




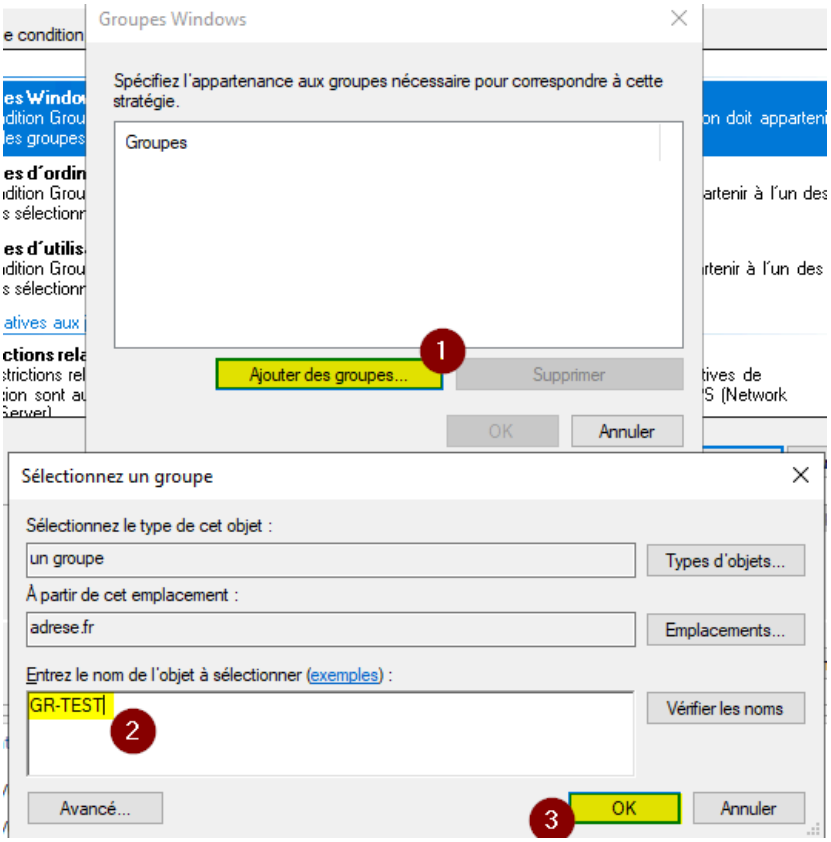
Donner un nom a la stratégie (sera visible dans les logs)



Ajoute une condition de connexion

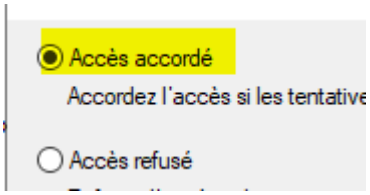


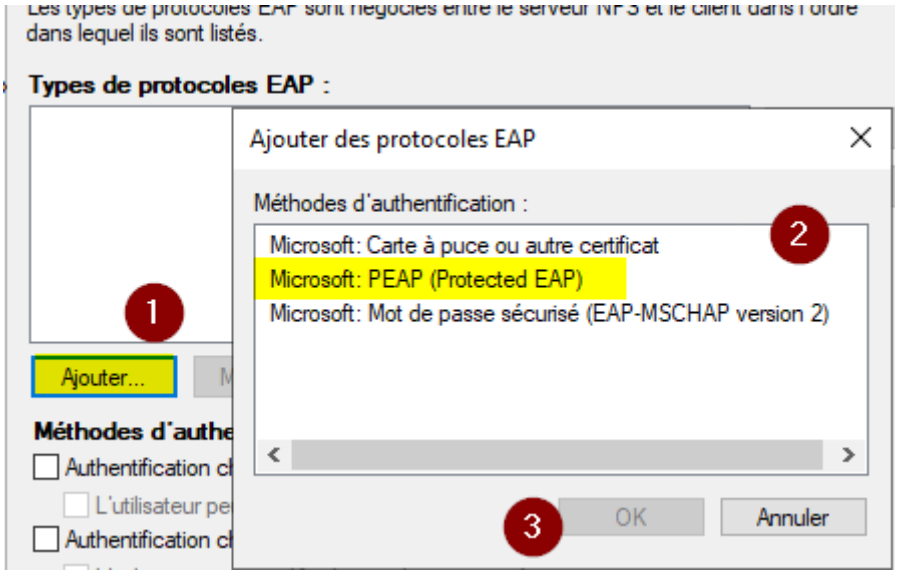
Sélectionner Groupe Windows afin que la stratégie fonctionne sur des utilisateurs et des ordinateurs. Pour que la stratégie ne soit effective uniquement sur des utilisateurs sélectionner groupe d'utilisateurs et ordinateurs pour que la stratégie soit effective sur des PC uniquement.



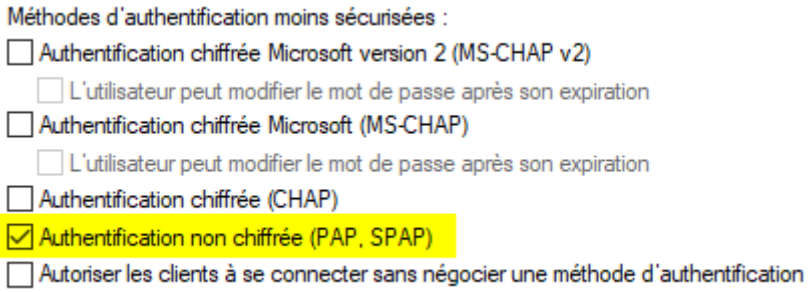
Sélectionner les groupes de personnes / ordinateurs pour qui la stratégie sera effective.

Ensuite, on **accord l'accès** :

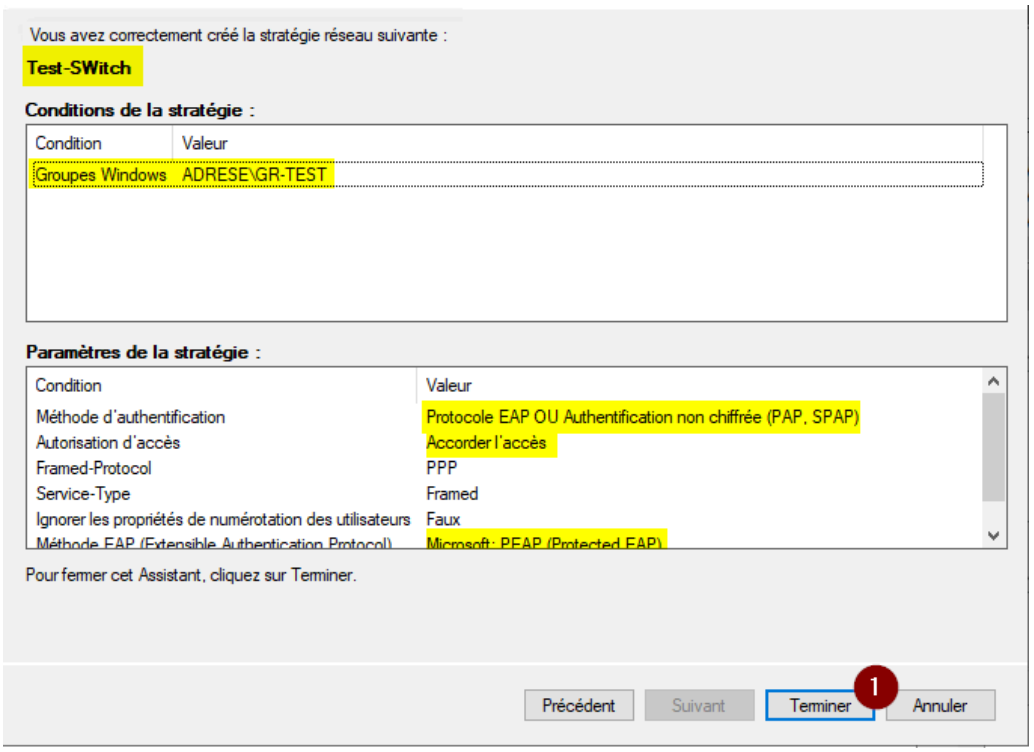




Puis, laissez coché seulement l'authentification non chiffré :



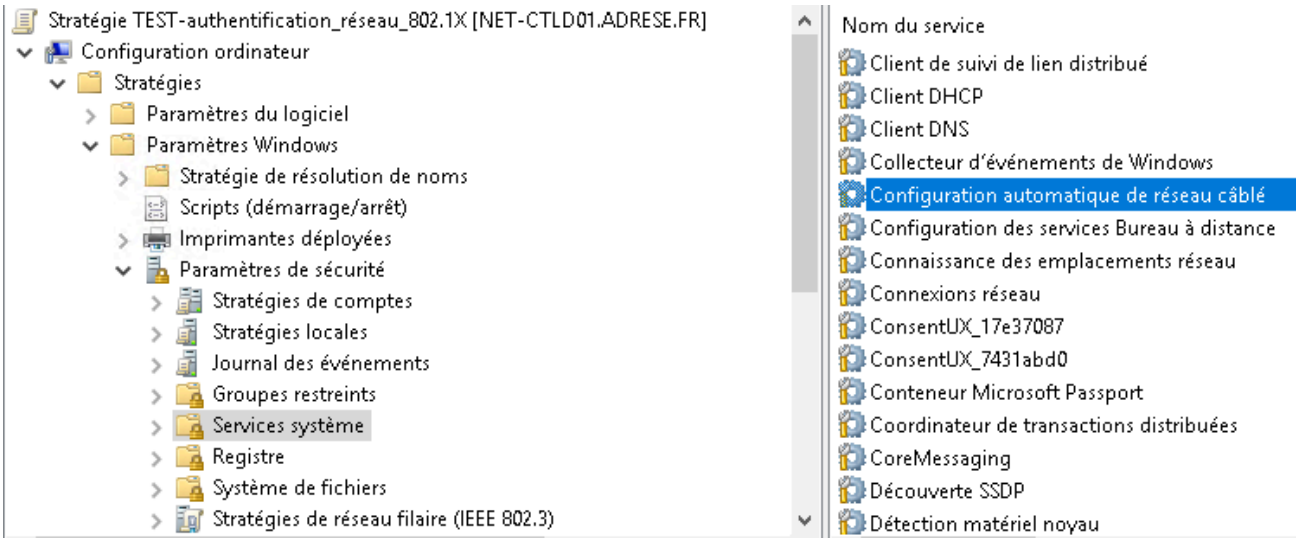
Une page apparait, cliquer sur non, puis cliquer sur suivant sur la page de récapitulatif final.



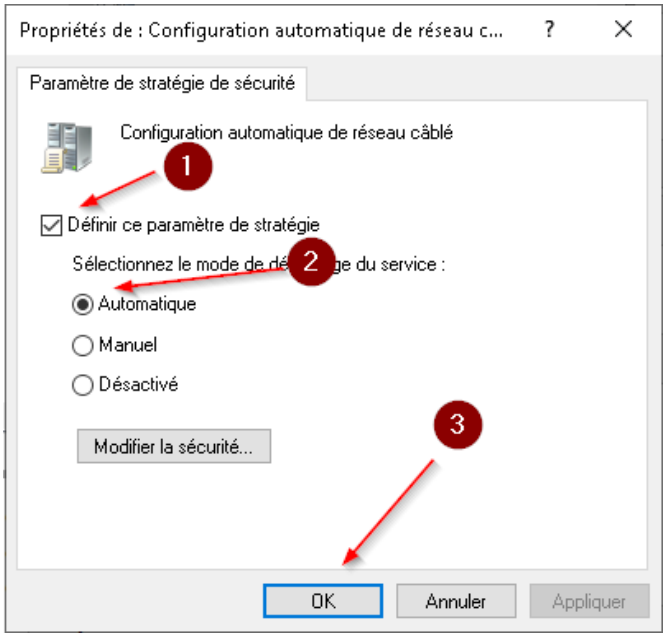
3. Configuration de l'authentification filaire 802.1X

L'authentification filaire repose sur la création d'une GPO dédiée.

Se rendre dans : **Configuration de l'ordinateur** > **stratégie** > **Paramètres Windows** > **Paramètres de sécurité** > **Services Systèmes** > **Configuration filaire automatique**

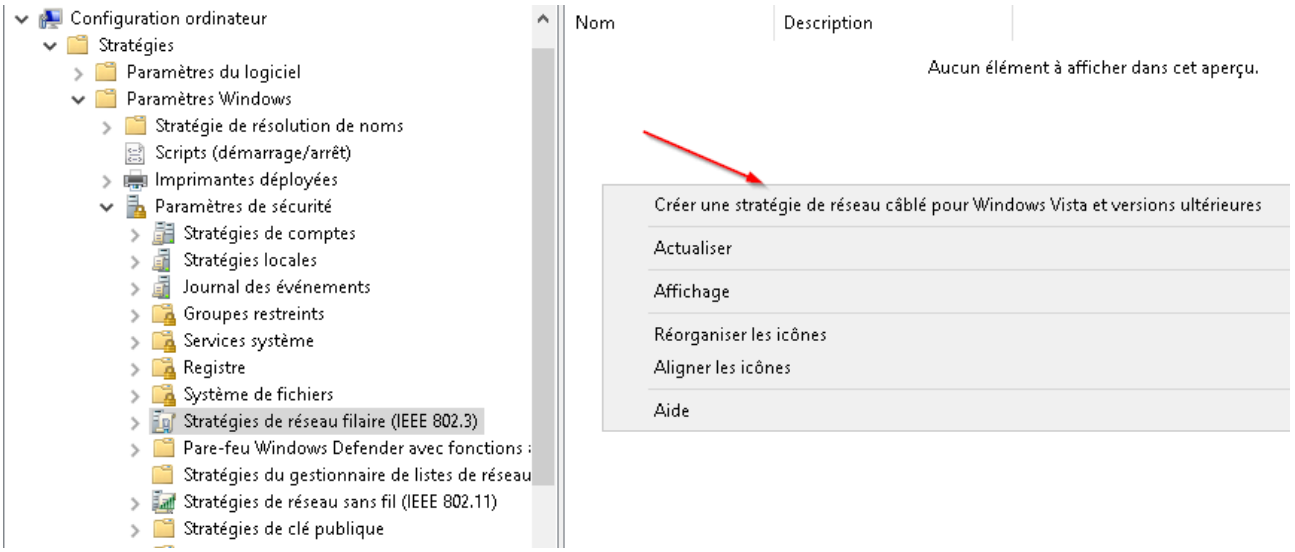


Puis, activer la configuration automatique :

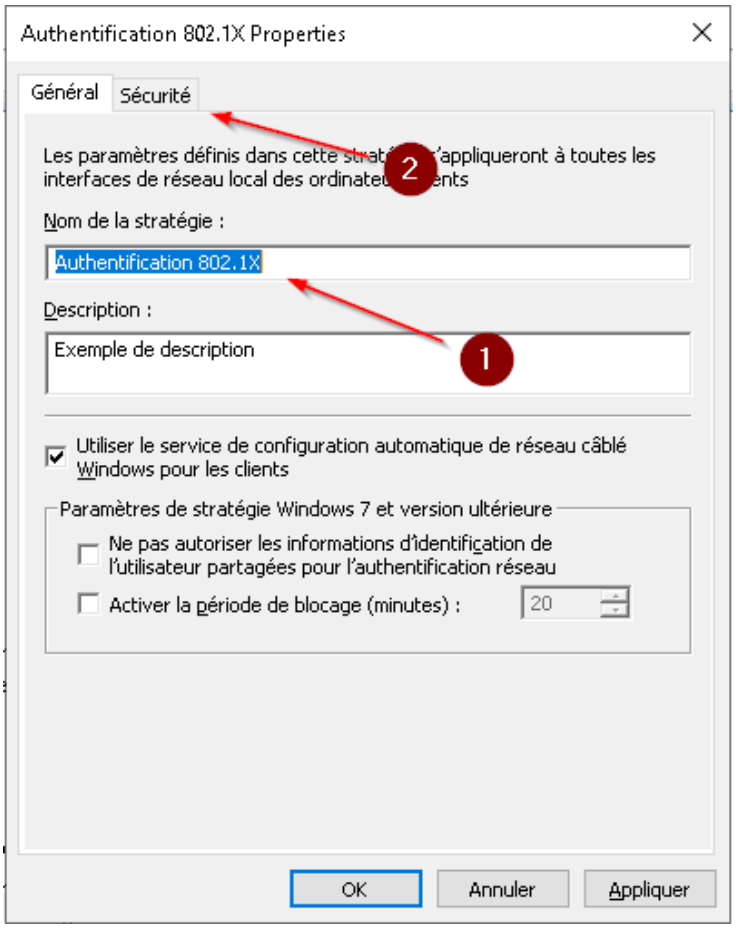


Ensuite dans : **Configuration de l'ordinateur** > **stratégie** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégie de Réseau Filaire (IEEE 802.3)**

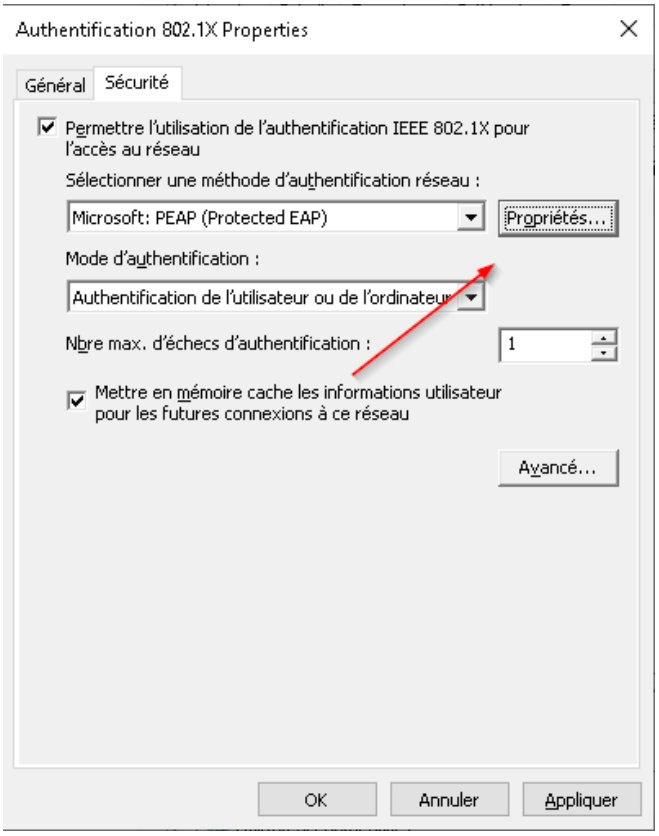
Clic droit pour créer une nouvelle stratégie :



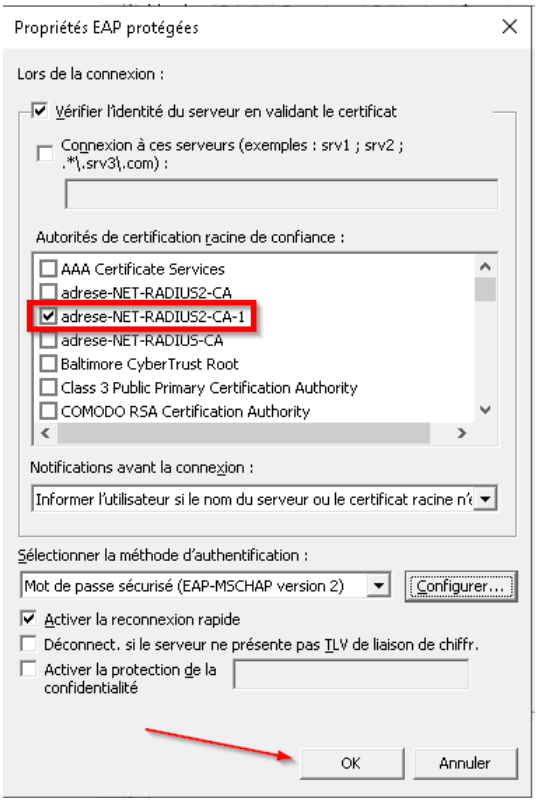
Lui donner un nom puis se rendre dans l'onglet sécurité :



Dans l'onglet sécurité, vérifier que la méthode d'authentification est bien PEAP Microsoft, puis se rendre dans les propriétés.



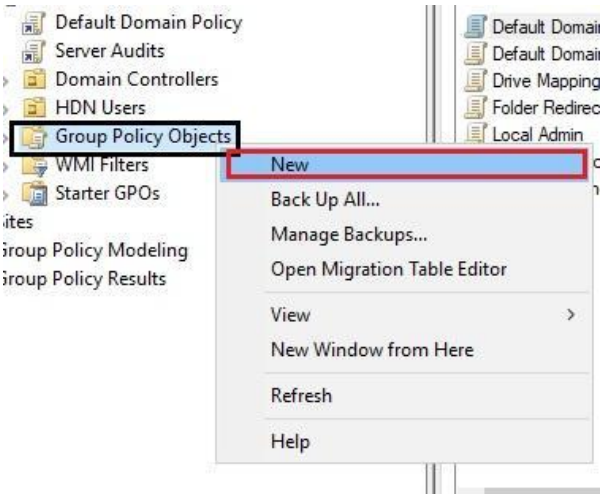
Enfin, sélectionner le certificat adrese-NET-RADIUS2-CA-1.



Valider et voilà.

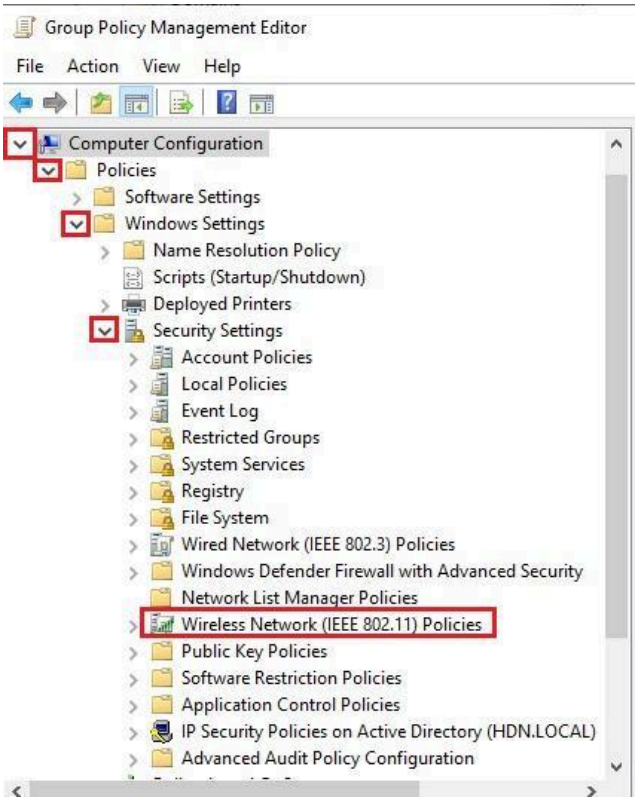
Déployer wifi par GPO

1. Créer une nouvelle GPO

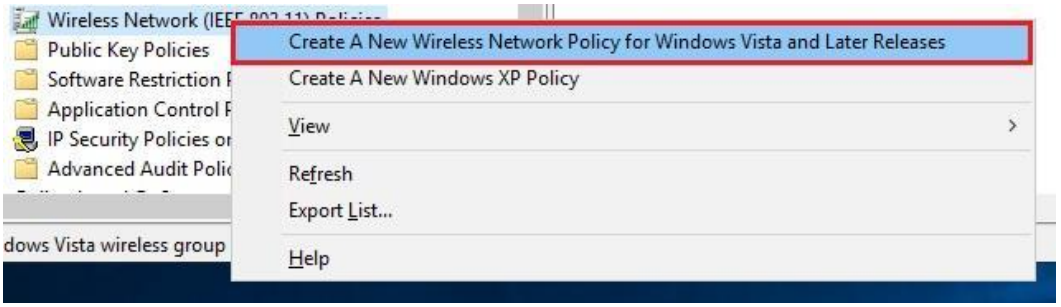


2. Lui donner un nom

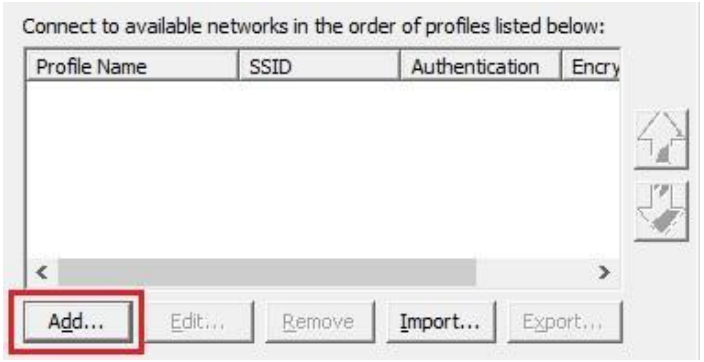
3.Dans Configuration de l'ordinateur > paramètres windows > paramètres de sécurité > stratégie de réseau sans fils (IEEE 802.11)



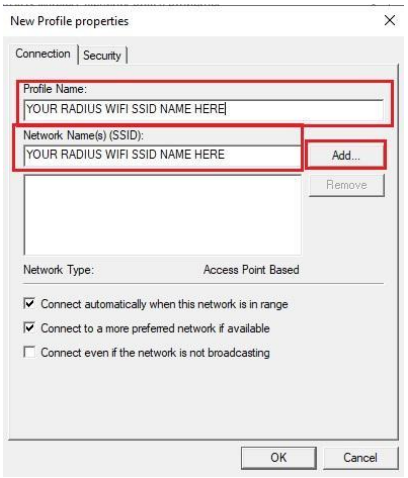
4. Clic droit sur **créer une nouvelle stratégie de réseau sans fils .**



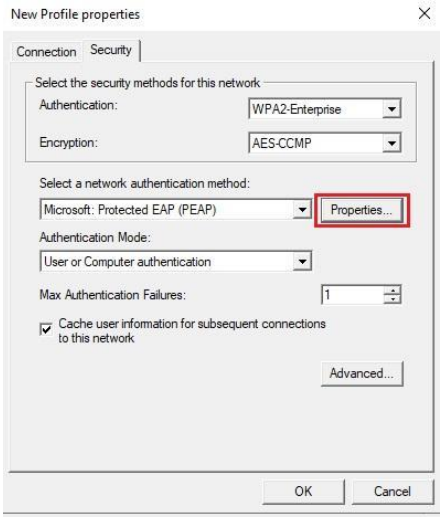
5.Cliquer sur ajouter puis infrastructure



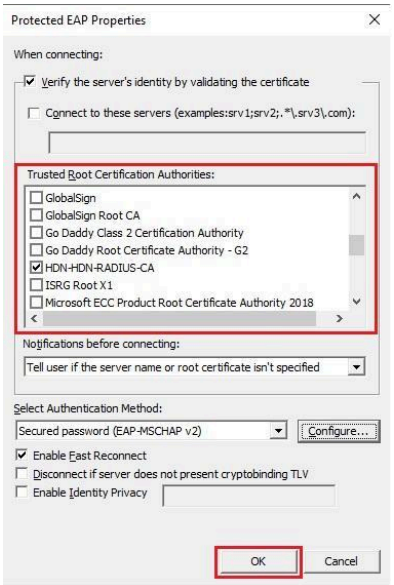
6. Donner un nom au WIFI (ce nom sera affiché dans la liste des wifi) puis le SSID



7. Dans l'onglet sécurité, aller dans les propriétés

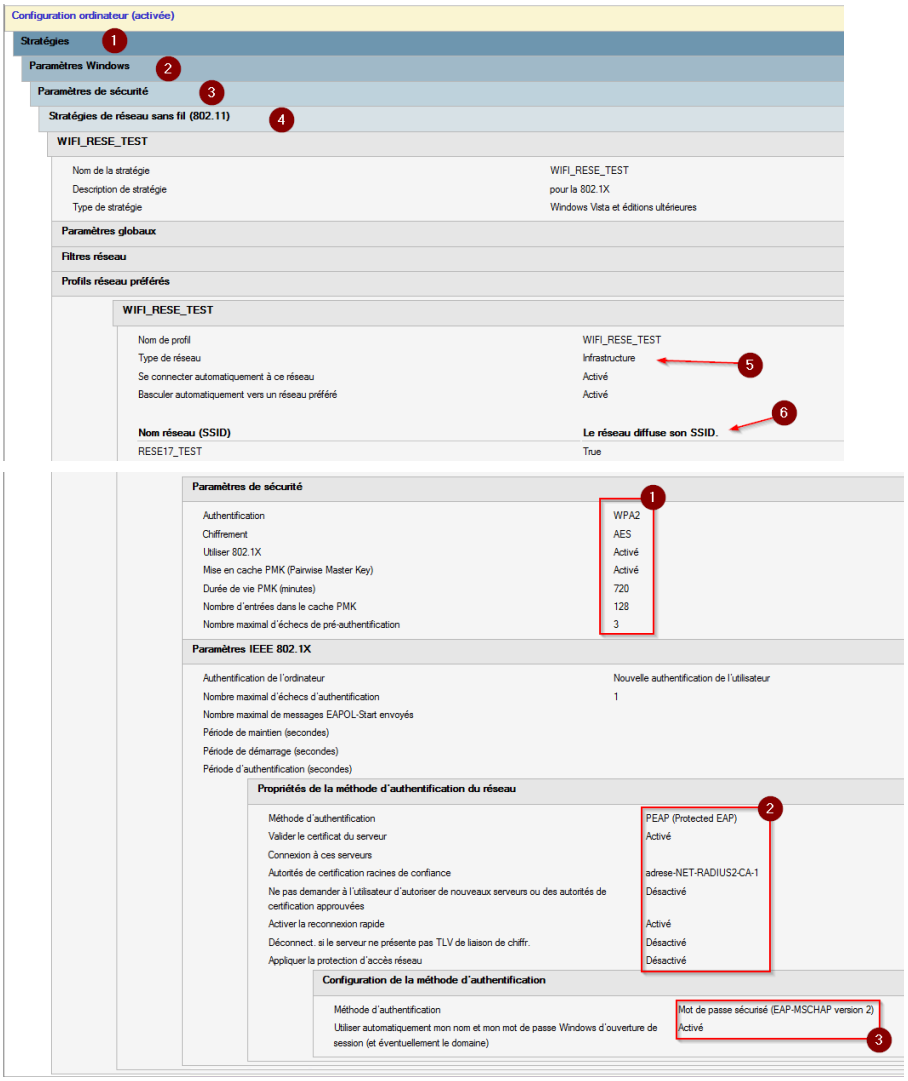


8. Sélectionner le bon certificat puis valider.



9. Valider pour terminer la configuration

A la fin de la configuration, le panneau de récapitulation doit ressembler à ça :



Un simple gpupdate /force est nécessaire pour appliquer la stratégie.

4. Configuration du switch

Switch utilisé : **HP procurve-48G-PoEP-2530**

Mise en place de l'authentification RADIUS sur le switch :

3. `radius-server host 192.168.40.111 key Password01`
    - Définit le serveur **RADIUS** avec l'adresse IP **192.168.40.111** et la clé partagée **Password01**
4. `aaa accounting network start-stop radius`

- Active la gestion des **logs de connexion** (accounting) pour le réseau, en envoyant un message **"start"** lors de l'authentification et un message **"stop"** à la déconnexion.

5. `aaa authentication port-access eap-radius`
   - Configure l'authentification des utilisateurs via le **protocole EAP** en utilisant le serveur **RADIUS**.
6. `aaa port-access authenticator 5-10`
   - Active la fonction **802.1X** sur les **ports 5 à 10** du switch, ce qui signifie que seuls les périphériques authentifiés via **RADIUS** pourront y accéder.
7. `aaa port-access authenticator active`
   - Active globalement la fonctionnalité **802.1X** sur le switch, appliquant ainsi les règles d'authentification configurées précédemment.

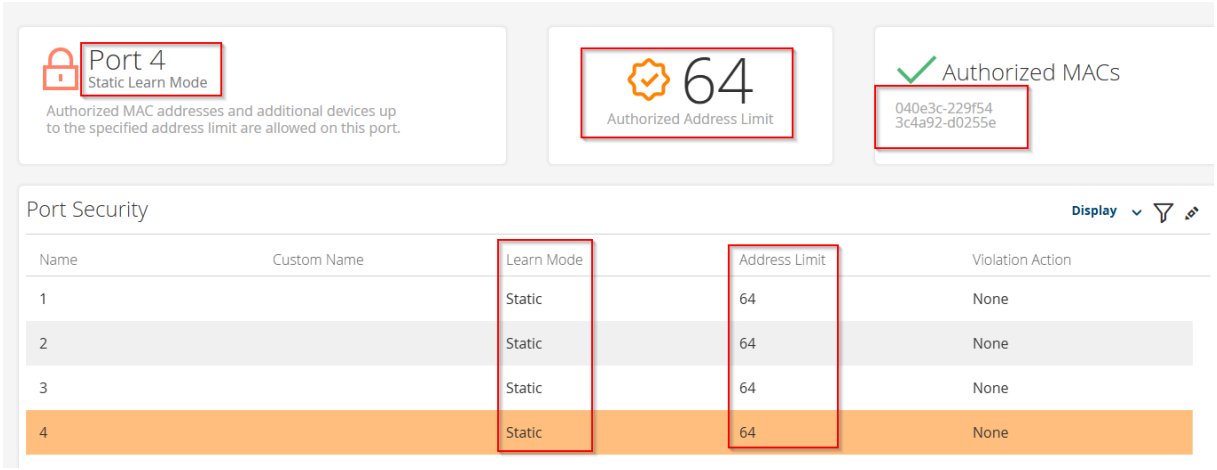
Mise en place de l'authentification par adresse MAC sur le switch :

1. Port-security <port(s)> learn-mode static
2. Port-security <port(s)> address-limit <nombre d'adresses MAC (max 64)>
3. Port-security <port(s)> mac-address <adresse MAC>

Exemple :

```
port-security 1-4 learn-mode static
port-security 1-4 address-limit 64
port-security 1-4 mac-address 040e3c-229f54
port-security 1-4 mac-address 3c4a92-d0255e
```

Résultat sur l'interface web :



5. Dépannage

Problèmes courants et solutions

Problème	Cause possible	Solution

Erreur d’authentification	Certificat invalide ou non installé	Vérifier le certificat et sa validité
Impossible de se connecter	Mauvais mot de passe partagé	Vérifier la configuration côté switch
GPO non appliquée	Problème de réplication AD	Forcer la mise à jour avec *gpupdate /force*

Restant à faire :

- Améliorer l’authentification avec des certificats client <-> serveur
- Configuration sur les clients légers Windows 10