BTS SIO SISR A2

DELOUIS kylian

BAY Enzo

SICOT-DURIVEAU Alexia

Infrastructure Assurmer

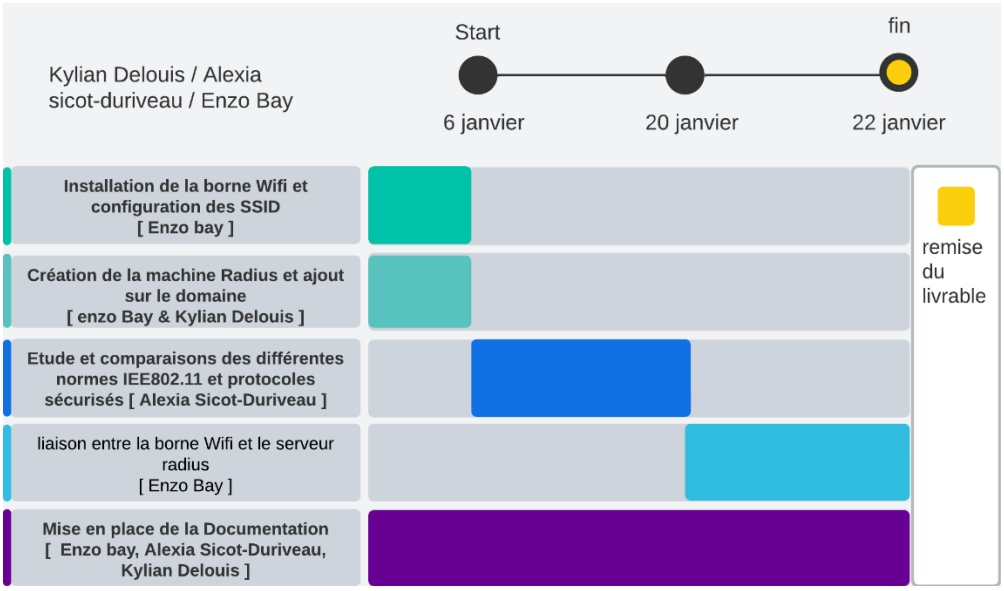
Un nouvel équipement Nomade et Sécurisé
ASSURMER

ASSURMER

Sommaire

Planning de travail et répartition des tâches

Un diagramme de Gantt est un outil essentiel pour la gestion de projet, en particulier lorsqu'il s'agit de répartir efficacement les tâches au sein d'une équipe. Dans notre cas, l'utilisation d'un diagramme de Gantt nous a permis de structurer notre travail de manière claire et organisée.



- **Enzo Bay**
    - Installation de la borne WiFi et configuration des SSID
    - Création de la machine Radius et ajout sur le domaine (avec Kylian Delouis)
    - Liaison entre la borne WiFi et le serveur Radius
    - Mise en place de la documentation (avec Alexia Sicot-Duriveau et Kylian Delouis)
- **Kylian Delouis**
    - Création de la machine Radius et ajout sur le domaine (avec Enzo Bay)
    - Mise en place de la documentation (avec Enzo Bay et Alexia Sicot-Duriveau)
- **Alexia Sicot-Duriveau**
    - Étude et comparaisons des différentes normes IEEE 802.11 et protocoles sécurisés + comparaison
    - Mise en place de la documentation (avec Enzo Bay et Kylian Delouis)

Chaque membre de l'équipe à ainsi contribué à différentes phases du projet, certaines tâches étant réalisées en collaboration afin d'assurer une meilleure répartition du travail et une complémentarité des compétences.

Présentation de la norme IEE802.11

Le standard IEEE802.11 a été créé par le groupe de travail 11 du comité de normalisation LAN/MAN de l'Institute of Eletrical and Electronics Engineers (IEEE).Ce groupe de travail a publié la première version de la norme en 1997, établissant les bases des réseaux WIFI. La norme IEEE 802.11 a été créée pour répondre à la demande croissante de connectivité sans fil et pour établir un standard commun permettant l'interopérabilité entre différents appareils et fabricants.Cette norme se réfère à la couche 1 et à la couche 2 du modèle OSI :

-Elle utilise la couche physique (1) pour la transmission des données sur les différents supports physiques. Les ondes radios en sont une.
-Elle utilise aussi la sous-couche MAC (2) pour la liaison de données. Elle gère l'accès au canal de communication et assure la transmission des données entre les appareils.

Différents types de Normes :

Il existe 3 variantes de la norme IEEE 802.11

-**IEEE 802.11 FHSS** (Frequency Hopping Spread Spectrum) utilise la technique de l'étalement de spectre par saut de fréquence.
-**IEEE 802.11 DSSS** (Direct Sequence Spread Spectrum) utilise la technique de l'étalement de spectre par fréquence directe.
-**IEEE 802.11 IR** utilise la lumière infrarouge pour la transmission des données.

Ses trois types de produits ne sont d'ailleurs pas compatibles entre eux au niveau physique.

Le standard IEEE 802.11 a évolué avec l'ajout de nouvelles couches physiques :

- **IEEE 802.11b** : Utilise la bande ISM avec des débits jusqu'à 11 Mbit/s, compatible avec IEEE 802.11 DSSS.
- **IEEE 802.11a** : Utilise la bande U-NII autour de 5 GHz avec des débits jusqu'à 54 Mbit/s, mais n'est pas compatible avec les précédents standards.
- **IEEE 802.11g** : Utilise la bande ISM avec des débits jusqu'à 20 Mbit/s, compatible avec IEEE 802.11 DSSS et IEEE 802.11b.
- **IEEE 802.11n** : Évolution de 802.11g intégrant la technologie MIMO.

La norme IEEE 802.11 définit les deux premières couches du modèle OSI : la couche physique et la couche liaison de données, cette dernière étant subdivisée en sous-couches LLC et MAC. La couche physique est divisée en sous-couches PMD et PLCP.

Différentes Couches Radio :

Les couches radio du standard IEEE 802.11/a/b/g utilisent des bandes sans licence :

- **Bande ISM** : Utilisée par 802.11/b/g autour de 2,4 GHz.
- **Bande U-NII** : Utilisée par 802.11a autour de 5 GHz, divisée en trois sous-bandes distinctes.

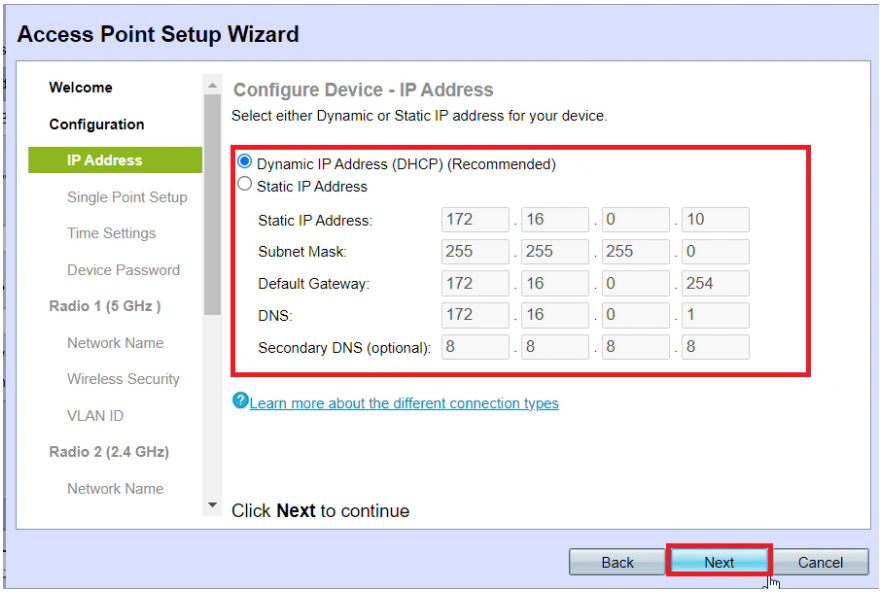
Les bandes de fréquences varient selon les pays et sont régulées par des organismes comme la FCC aux États-Unis, l'ETSI en Europe, et le MKK au Japon.

Etude comparative des protocoles de sécurité wifi

Protocole	Année d'introduction	Cryptage	Clé	Avantages	Inconvénients
WEP	1997	RC4	40/104 bits	Facile à configurer	Très vulnérable
WPA	2003	TKIP	128 bits	Amélioration par rapport à WEP	Vulnérable aux attaques par dictionnaire
WPA2	2004	AES	256 bits	Sécurité renforcée	Nécessite plus de puissance de traitement
WPA3	2018	SAE	128/192 bits	Protection contre les attaques par force brute	Adoption en cours

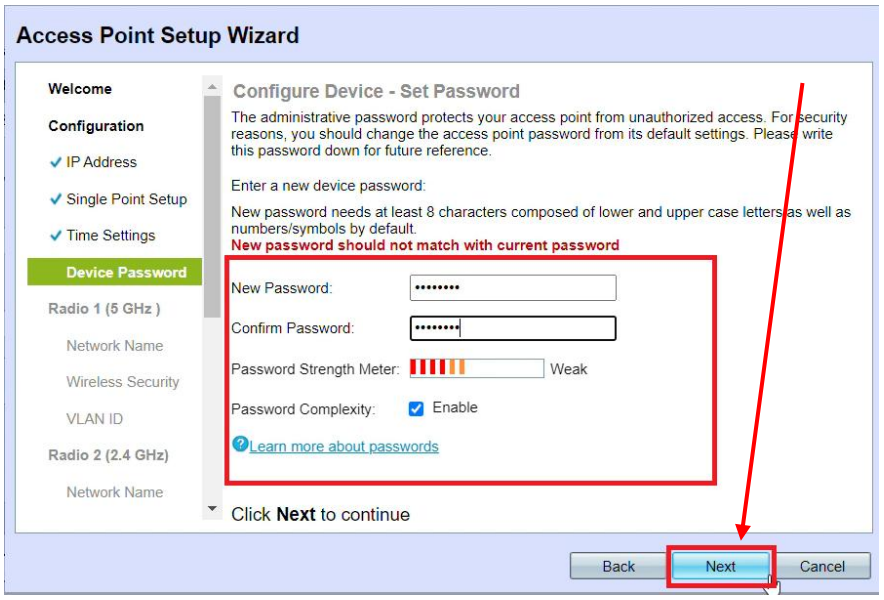
- **WEP (1997)** : Protocole obsolète avec chiffrement RC4 (40/104 bits), facile à configurer mais très vulnérable.
- **WPA (2003)** : Amélioration de WEP avec TKIP (128 bits), mais vulnérable aux attaques par dictionnaire.
- **WPA2 (2004)** : Sécurité renforcée avec AES (256 bits), nécessitant plus de puissance de traitement.
- **WPA3 (2018)** : Protection avancée contre les attaques avec SAE (128/192 bits), adoption en cours.

Configuration de l'adresse IP



Mise en place de l'adresse « 172.16.0.10 » comme adresse principale de la borne wifi, « 172.16.0.254 » comme adresse de la passerelle, « 172.16.0.1 » comme adresse DNS puis appuyez sur « Next »

Mise en place d'un mot de passe robuste

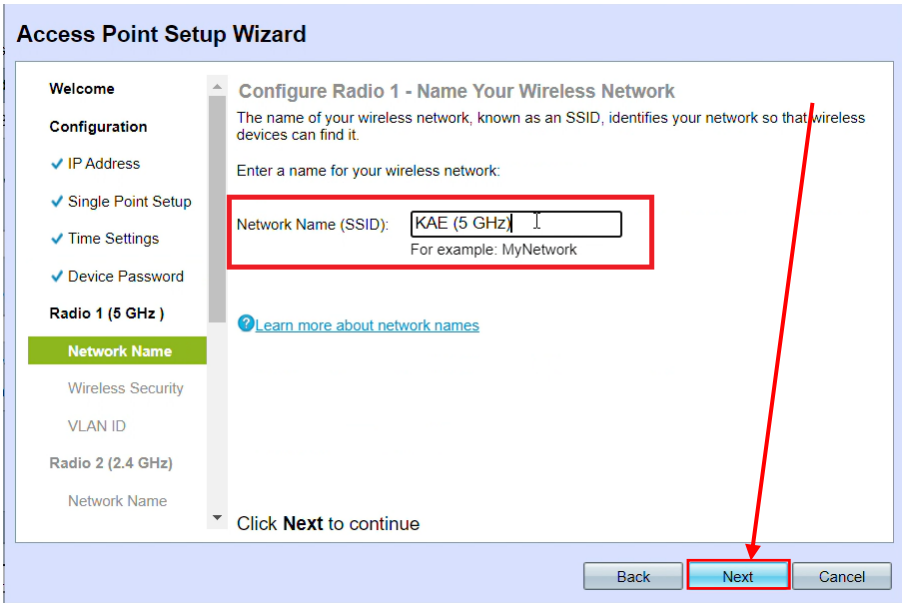


Mot de passe robuste ?

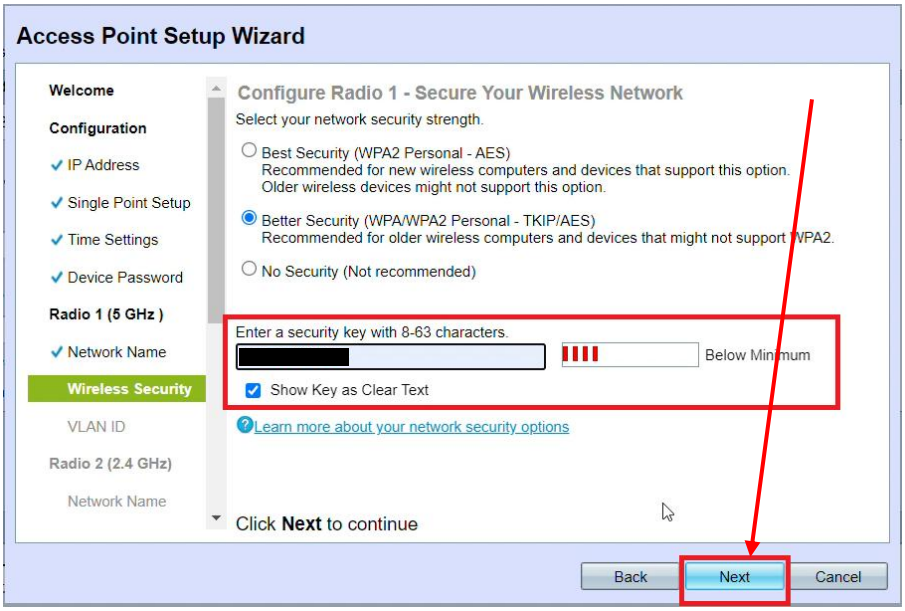
Un mot de passe robuste est un mot de passe difficile à deviner ou à casser, même à l'aide d'attaques automatisées. Il doit être suffisamment long (au moins 12 à 16 caractères) et inclure une combinaison de majuscules, de minuscules, de chiffres et de caractères spéciaux.

Mise en place du mot de passe robuste de votre choix qui permettra de se connecter au la borne wifi puis appuyez sur « Next »

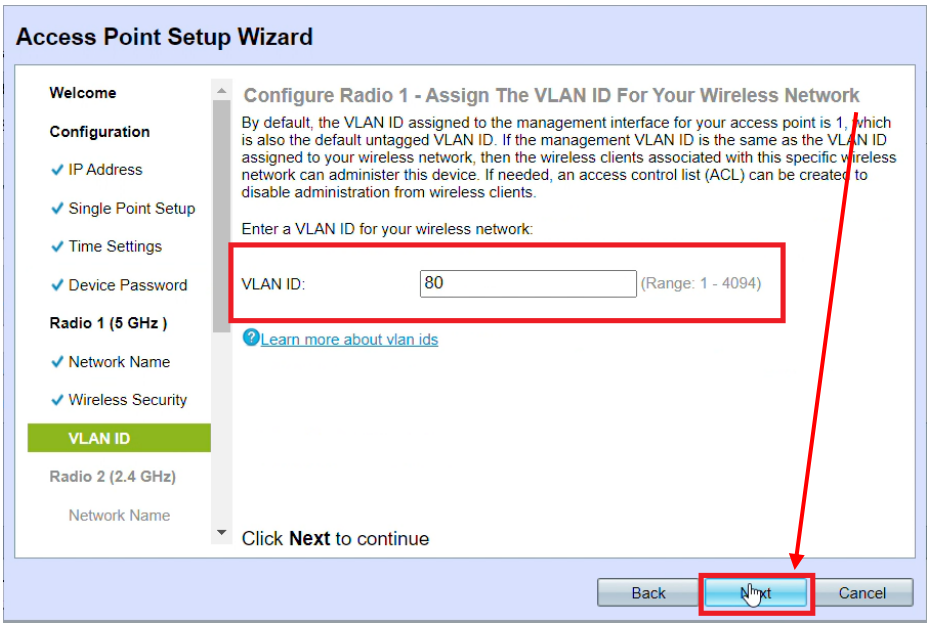
Création d’une cellule wifi en 5Ghz



Création d’une cellule wifi en radio 5 GHz qui permettra de diffuser un réseau wifi, ici appeler « KAE (5 GHz) » puis appuyez sur « Next »



Mise en place d’un mot de passe robuste nous permettant de nous connecter à notre réseau wifi puis appuyez sur « next »

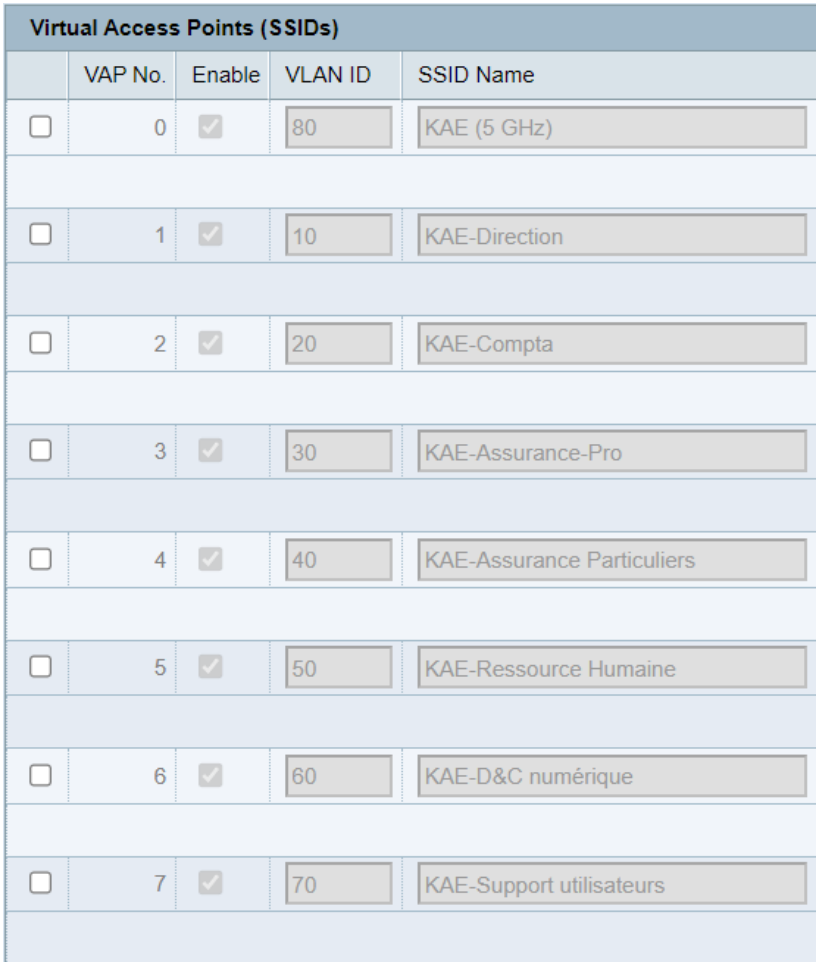


Attribution du vlan correspondant au réseau wifi, ici le vlan est « 80 » puis appuyez sur « Next ».

Il nous suffit donc de prévoir différents types de réseaux selon le service de l'utilisateur

Ainsi, 7 réseaux serons donc opérationnel tel que :

- Direction
- Compta
- Assurance Pro
- Assurance Particuliers
- Ressource Humaine
- D&C Numérique
- Support Utilisateur



Définition d'un serveur Radius et Certificat :

Une solution RADIUS (Remote Authentication Dial-In User Service) est un protocole permettant l'authentification, l'autorisation des utilisateurs souhaitant accéder à un réseau, notamment en WiFi ou via VPN. Son fonctionnement repose sur un modèle client-serveur où les équipements réseau (comme les points d'accès WiFi ou les pare-feux) agissent en tant que clients RADIUS, et le serveur RADIUS gère les requêtes d'authentification en se basant sur une base de données d'identifiants.

Connexion de l'utilisateur :

- Lorsqu'un utilisateur essaie de se connecter au réseau, son appareil **envoie une demande** d'accès au serveur RADIUS via un point d'accès WiFi ou un autre équipement réseau.
- Au lieu d'utiliser un mot de passe, la connexion peut se faire avec un **certificat numérique**, un fichier sécurisé qui prouve l'identité de l'utilisateur.

Vérification du certificat :

- Le serveur RADIUS vérifie si le certificat est valide et s'il a été délivré par une autorité de confiance.
- Si tout est correct, l'accès est accordé, sinon il est refusé.

Attribution des droits :

- Une fois connecté, l'utilisateur est placé dans un groupe spécifique selon son profil (par exemple, accès limité pour les invités, accès total pour les employés).

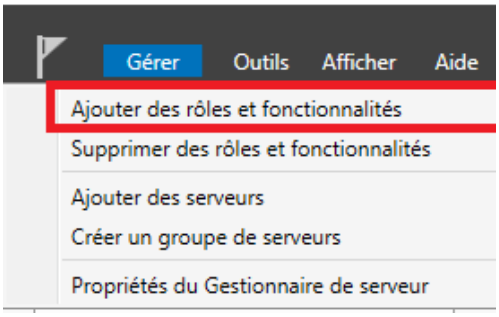
Suivi des connexions :

- Le serveur RADIUS enregistre les connexions pour savoir qui s'est connecté, quand et pendant combien de temps, ce qui est utile pour la sécurité du réseau.

En résumé, une solution RADIUS avec certificats permet de sécuriser les connexions réseau de manière efficace et automatique, en garantissant que seules les personnes autorisées peuvent se connecter.

Création du serveur Radius

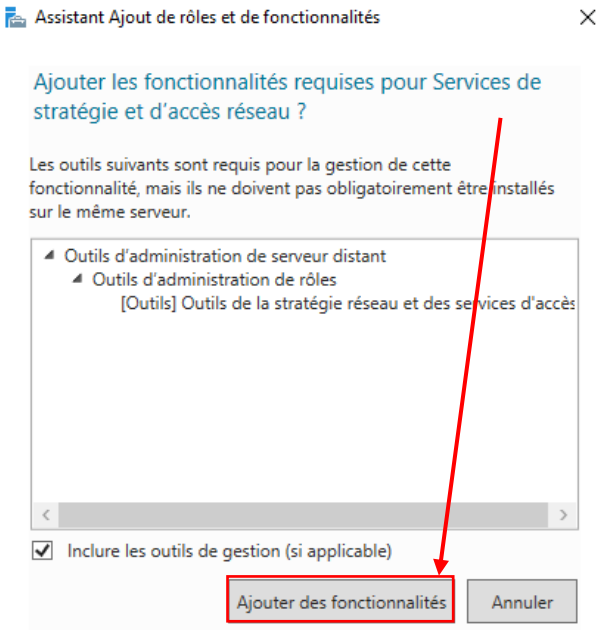
Pour commencer, allez dans le **gestionnaire de serveur**, cliquez sur « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** ».



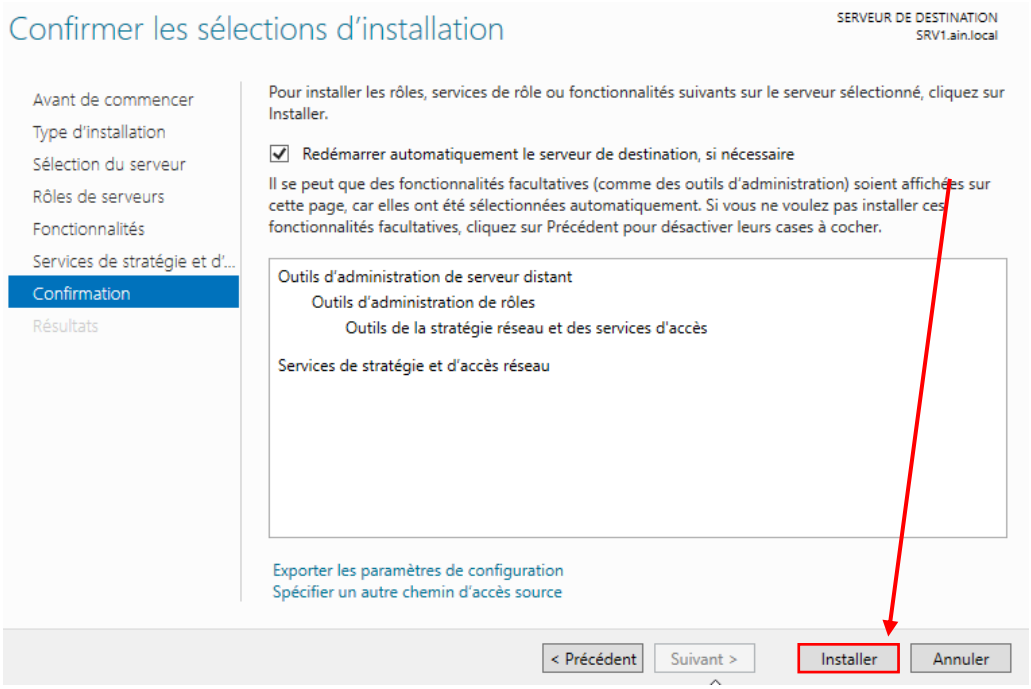
Sur la première fenêtre laissez cocher « **Installation basée sur un rôle ou une fonctionnalité** ».

Sur la fenêtre suivante « **Sélection du serveur** » laissez par défaut et cliquez à nouveau sur « **Suivant** ». Vous arriverez sur la fenêtre de sélection des rôles, cochez « **Services de stratégie et d'accès réseau** ».

Cliquez sur « **Ajouter des fonctionnalités** » et cliquez sur « **Suivant** ».

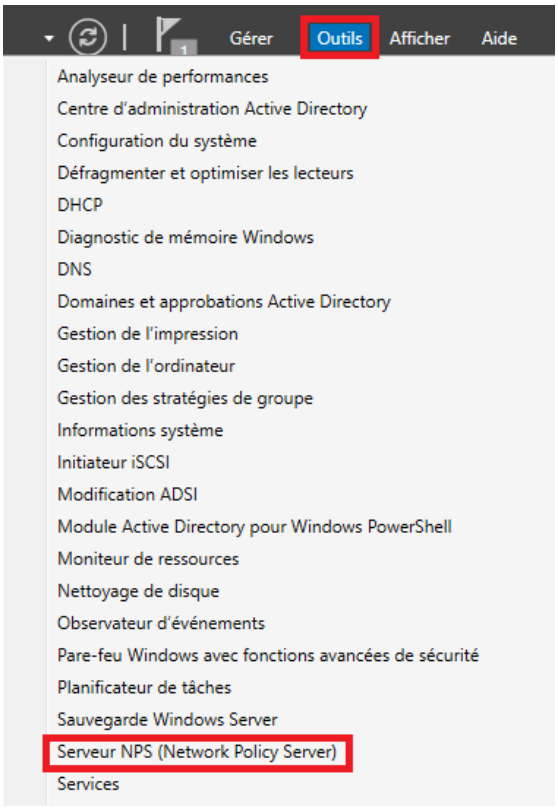


Cliquez sur « **Suivant** » jusqu'à arriver sur la fenêtre de confirmation d'installation du rôle et cliquez sur « **Installer** ».

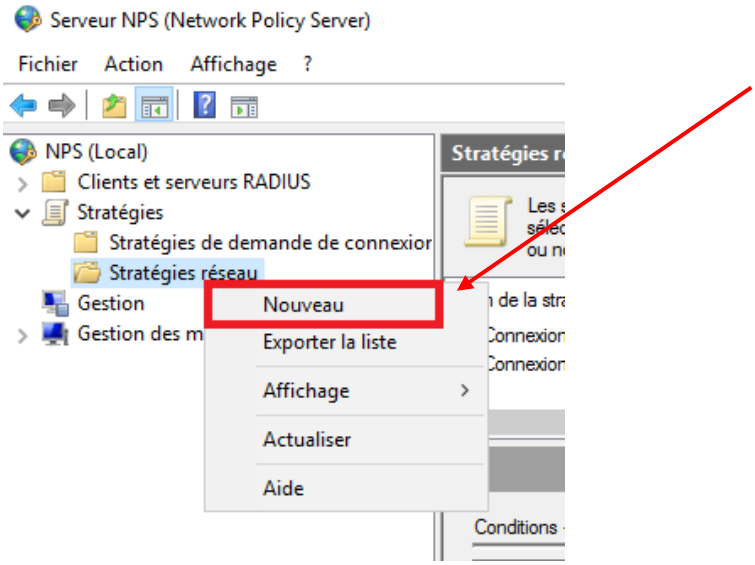


Patientez quelques minutes jusqu'à l'installation du rôle.

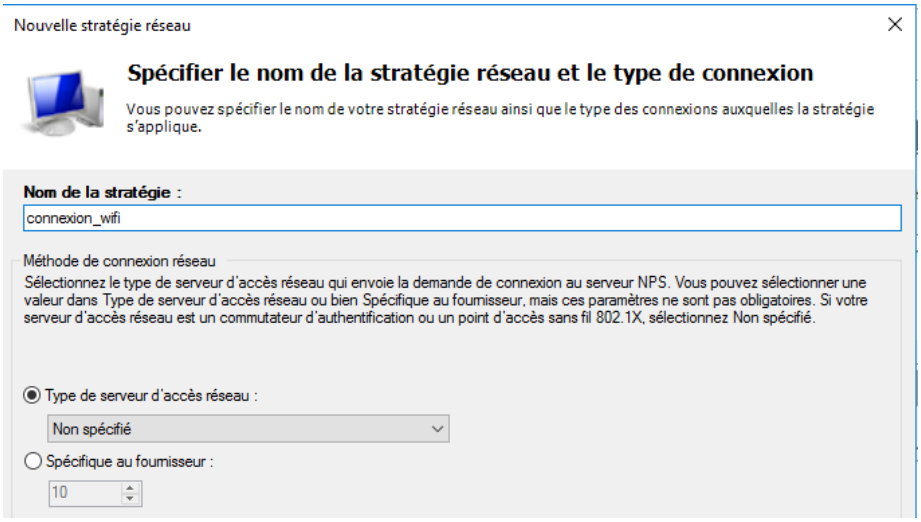
Maintenant que le rôle est installé nous allons devoir le configurer. Pour cela dans le gestionnaire de serveur cliquez sur « **Outils** » puis sur « **Serveur NPS (Network Policy Server)** ».



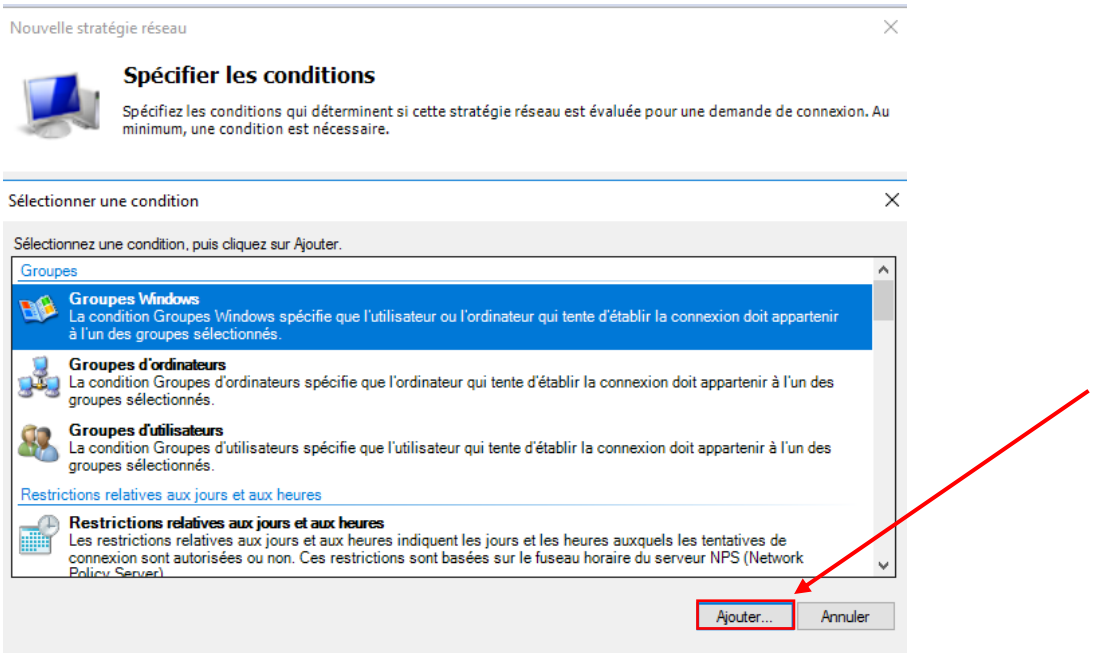
Vous arriverez sur la fenêtre d'administration de ***RADIUS***. Nous allons commencer par configurer la stratégie de connexion à notre réseau Wifi. Dépliez le menu « **Stratégie** », faites un clic droit sur « **Stratégies réseau** » et sélectionnez « **Nouveau** ».



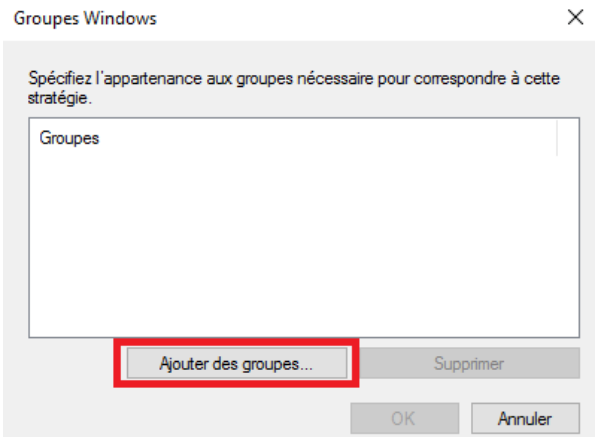
Vous allez arriver sur la fenêtre ci-dessous. Entrez le nom de votre stratégie et cliquez sur « **Suivant** ».



Pour la condition cliquez sur « **Ajouter** » et sélectionnez « **Groupes Windows** » et cliquez à nouveau sur « **Ajouter** »

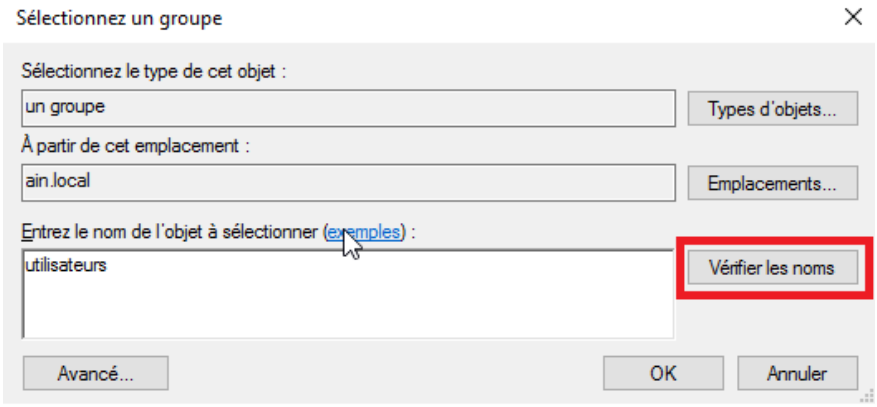


Cliquez sur « **Ajouter des groupes** ».

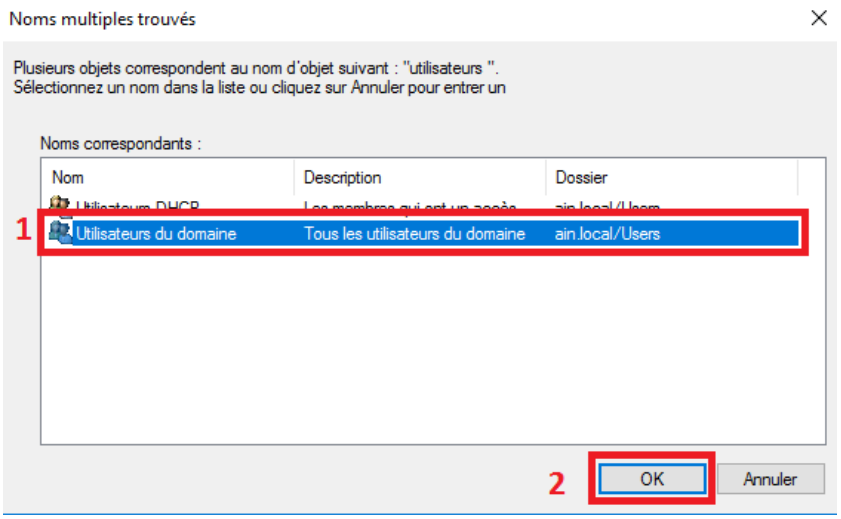


Vous allez ensuite devoir sélectionnez le groupe des utilisateurs pouvant se connecter au réseau WiFi en question.

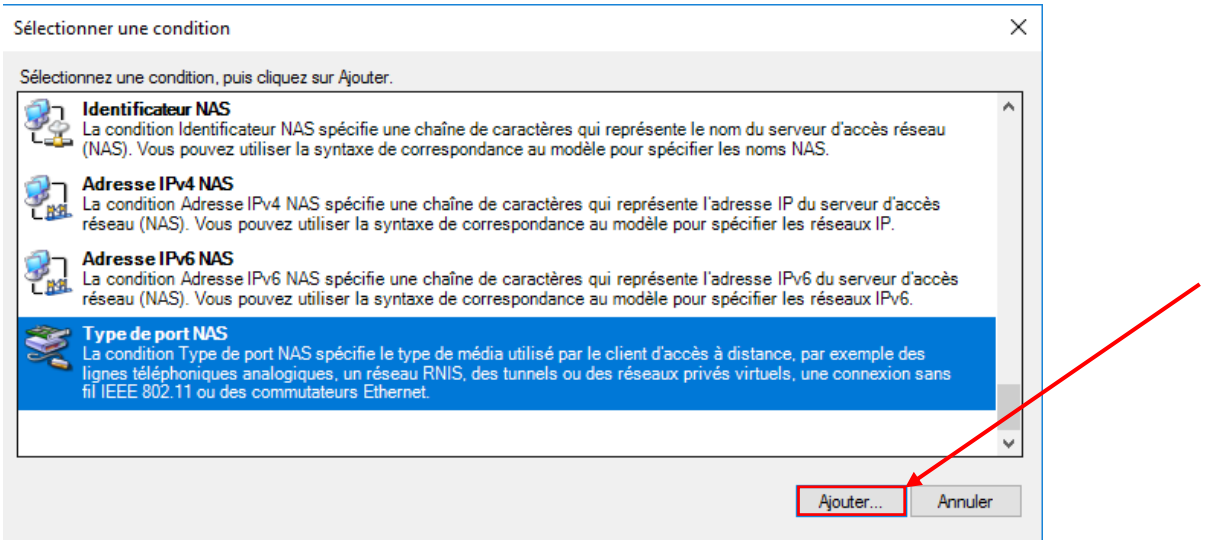
Écrivez utilisateurs et cliquez sur « **Vérifier les noms** »



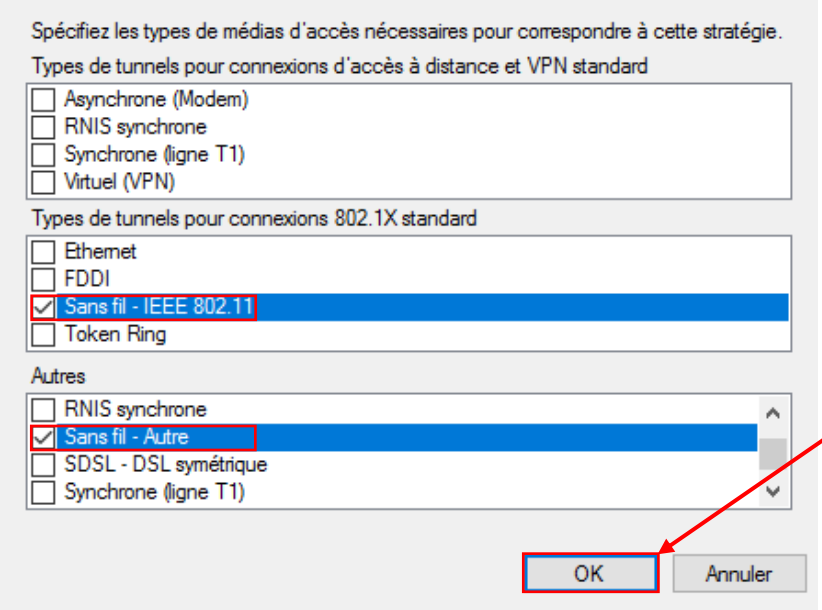
Sélectionnez « **Utilisateurs du domaine** » et cliquez sur « **OK** » jusqu'à revenir sur la fenêtre pour spécifier les conditions et cliquez de nouveau sur « **Ajouter** ».



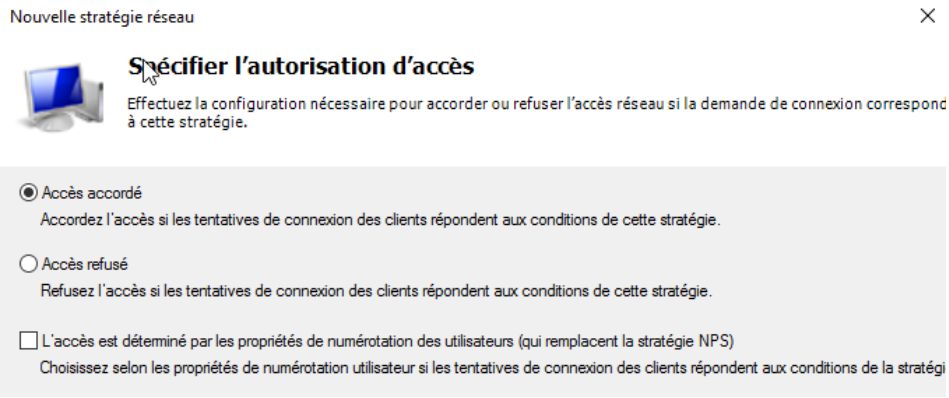
Cette fois ci sélectionnez « **Type de port NAS** » et cliquez sur « **Ajouter**».



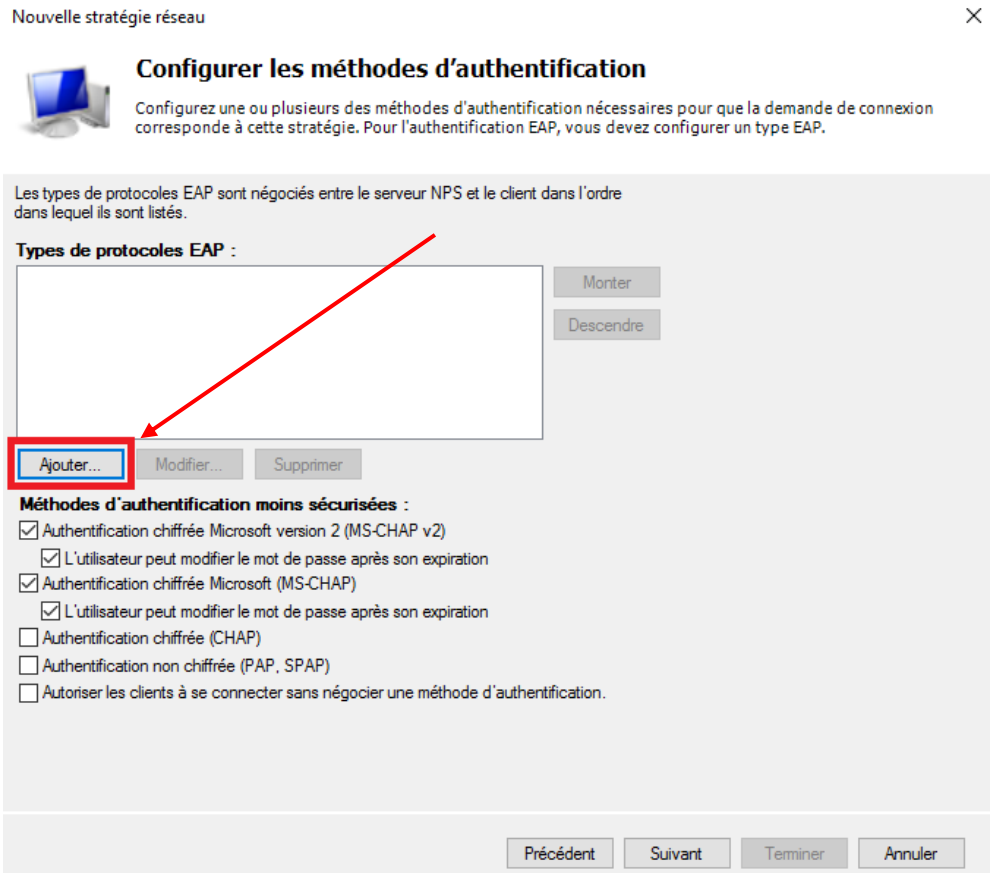
Sélectionnez les 2 options comme ci-dessous et cliquez sur « **OK** ». Cliquez sur « **Suivant** » sur la fenêtre des conditions.



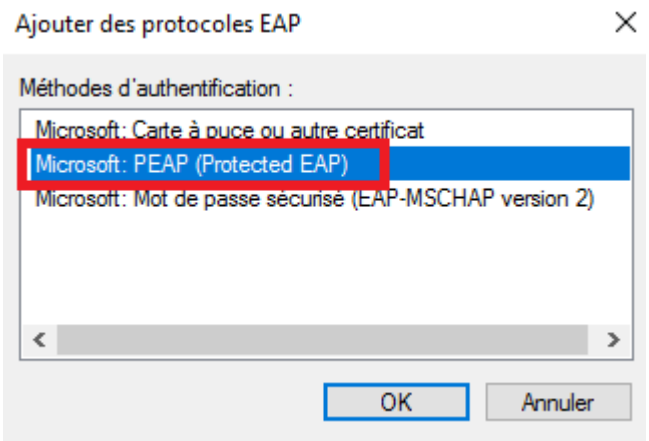
Laissez cocher « **Accès accordé** » et cliquez sur « **Suivant** ».



Pour les méthodes authentification, cliquez sur « **Ajouter…** ».



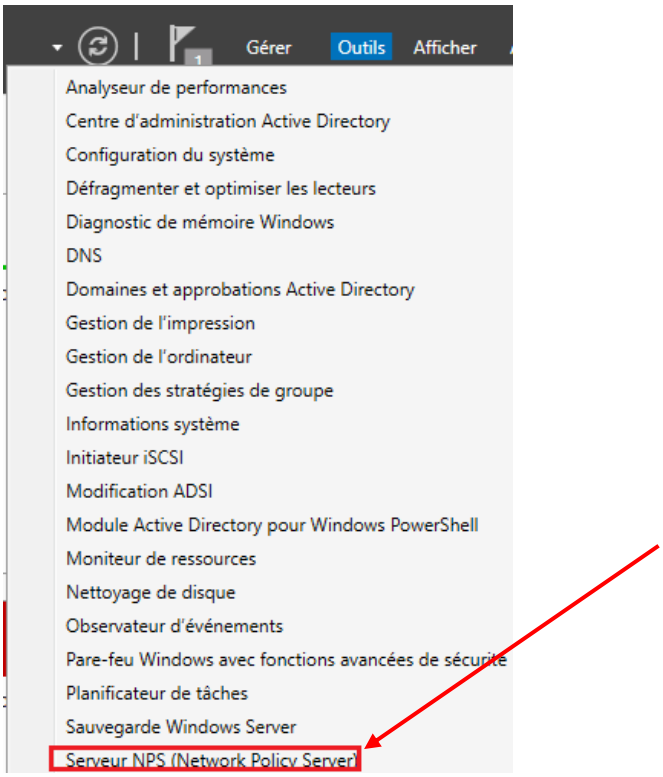
Sélectionnez « **Microsoft PEAP** » cliquez sur « **OK** » et cliquez sur « **Suivant** » sur l'autre fenêtre.



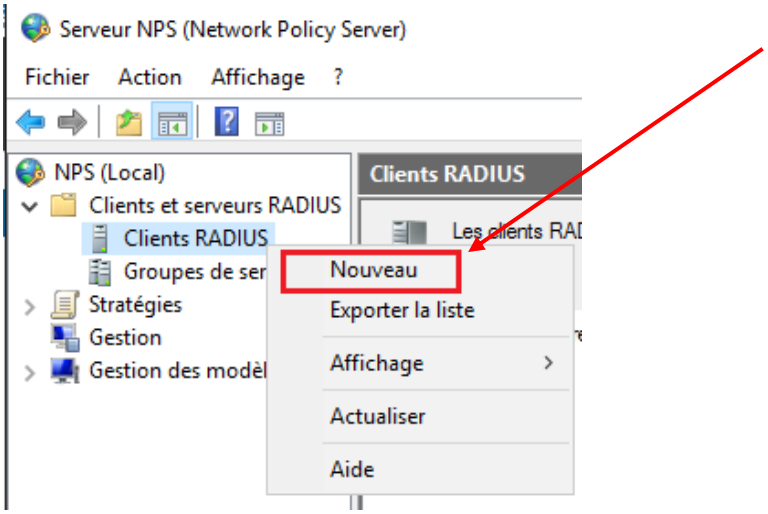
Sur la fenêtre suivante « **Configurer des contraintes** », laissez par défaut et cliquez sur « **Suivant** ». Faites de même pour la fenêtre « **Configurer les paramètres** ». Une fenêtre récapitulant la configuration va apparaître cliquez sur « **Terminer** ».

Ajout de la borne

Pour que l'accès fonctionne, nous allons devoir ajouter la borne WiFi sur le serveur ***RADIUS***. Elle va avoir le rôle de NAS (Network Access Server) qui est un équipement intermédiaire entre le serveur ***RADIUS*** et l'utilisateur. Allez dans le gestionnaire de serveur et cliquez sur « **Outils** » puis sur « **Serveur NPS (Network Policy Server)** »



Dans la fenêtre qui vient de s'ouvrir, déroulez le menu « **Client et serveurs RADIUS** », faites un clic droit sur « **Clients RADIUS** » et sélectionnez « **Nouveau** »



Nous allons renseigner les informations de la borne wifi sur le serveur.

- Laissez cocher « **Activer ce client RADIUS** ».
- Nom convivial : Entrez le nom d'hôte de la borne WiFi.
- Adresse IP : Renseignez l'adresse IP de la borne WiFi.
- Pour le secret laissez cocher « **Manuel** » et renseignez la clé que vous saisirez aussi sur la borne WiFi.

Cliquez ensuite sur « **OK** ».