JANVIER 2025

Mise en place d'une solution WIFI sécurisée

Auteurs : COMBETTES Elise, Gana Stéphane

Validateurs : DEGEN Loïc, SAMMARTANO Joseph

ASSURMER

SOMMAIRE

Récapitulatif de la demande / Organisation de travail

Dans le cadre de la création du serveur pour Assurmer, il est important de permettre aux utilisateurs d'accéder facilement et de manière sécurisée à un réseau sans fil.

Étapes principales

- **Planification** :Définir les besoins de l'entreprise en terme de connectivité.
- **Installation et configuration** : Nous installerons la borne et allons la paramétrer en accord avec les besoins de l'entreprise.
- **Sécurisation et tests** : La sécurité est essentielle. Nous mettrons en place des mots de passes robustes pour l'administration et la connexion en utilisant les protocoles adéquats.
- **Ajout d'un Radius** : nous créerons un serveur Radius afin de mieux gérer les accès à ce réseau sans fil avec une authentification centralisée.

Organisation et gestion

Pour garantir la réussite du projet, les tâches seront structurées et documentées étape par étape. Nous avons travaillé en binôme afin de pouvoir se répartir les tâches au mieux.

Présentation de la norme IEE802.11

Les réseaux Wi-Fi sont régis par des normes qui définissent les caractéristiques de communication sans fil. Ces normes évoluent pour répondre aux besoins croissants en matière de débit, de portée et de sécurité. Parmi les plus courantes, on trouve les normes **802.11a**, **802.11n** et **802.11ac**.

Normes Wi-Fi : 802.11a, 802.11n et 802.11ac

Norme	Bande de fréquence	Débit maximal	Portée	Avantages	Inconvénients
802.11a	5 GHz	54 Mbps	Faible	Moins d'interférences	Portée limitée, débit faible
802.11n	2,4 GHz et 5 GHz	600 Mbps	Bonne	Dual-band, MIMO pour meilleure portée	Interférences en 2,4 GHz
802.11ac	5 GHz	1,3 Gbps	Moyenne	Débit élevé, MU-MIMO, beamforming	Portée réduite en 5 GHz

802.11a : Fonctionne sur la bande 5 GHz, avec un débit de 54 Mbps, mais sa portée est limitée.

802.11n : Utilise les bandes 2,4 GHz et 5 GHz, avec un débit théorique de 600 Mbps. La portée et la capacité sont améliorées grâce à la technologie MIMO.

802.11ac : Fonctionne uniquement en 5 GHz, avec un débit pouvant atteindre 1,3 Gbps. Il utilise des canaux plus larges et des technologies comme MU-MIMO et beamforming pour améliorer la performance, mais la portée est plus faible.

Comparatif des protocoles de sécurité Wi-Fi

Les protocoles de sécurité sont essentiels pour protéger les données sur les réseaux Wi-Fi. Voici un comparatif des principaux protocoles utilisés.

Protocole	Chiffrement	Sécurité	Avantages	Inconvénients
WEP	RC4	Faible	Facile à configurer	Très vulnérable aux attaques
WPA	TKIP	Moyenne	Meilleure sécurité que WEP	Vulnérable aux attaques par injection
WPA2	AES	Élevée	Très sécurisé, largement utilisé	Pas de protection contre les attaques par force brute
WPA3	AES + SAE	Très élevée	Protection renforcée contre les attaques par force brute, configuration simplifiée	Nécessite des équipements compatibles WPA3

-WEP : Le plus ancien, il utilise le chiffrement RC4, mais est aujourd'hui obsolète en raison de ses nombreuses vulnérabilités.

-WPA : Introduit le chiffrement TKIP, offrant une meilleure sécurité que WEP, mais reste vulnérable aux attaques par injection de paquets.

-WPA2 : Utilise AES, un chiffrement beaucoup plus robuste. C'est le protocole recommandé pour la plupart des réseaux modernes.

-WPA3 : Introduit un chiffrement renforcé avec AES et une meilleure protection contre les attaques par force brute grâce à SAE (Simultaneous Authentication of Equals).

-Pour résumer

Le choix de la norme Wi-Fi dépend des besoins en débit et en couverture. **802.11n** et **802.11ac** sont les plus adaptées pour des environnements modernes, offrant un bon compromis entre performance et portée. En matière de sécurité, **WPA2** reste le plus utilisé, mais **WPA3** apporte des améliorations significatives, notamment pour protéger contre les attaques par force brute et simplifier la configuration. Il est recommandé d'utiliser WPA2 ou WPA3 pour garantir la sécurité des réseaux.

Procédure d'installation
1 - Initialisation

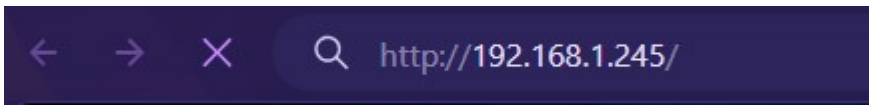
Dans notre cas nous allons utiliser une borne Cisco modèle WAP371.

Tout d'abord, alimentez la borne en la branchant électriquement.
Ensuite, reliez-la sur un port disponible de votre commutateur.

- A noter : si vous utilisez un port POE (Power Over Ethernet), il n'est pas nécessaire de l'alimenter autrement que via le câble Ethernet.

Après avoir alimenté la borne, attendez qu'elle termine son processus de démarrage. Les voyants lumineux indiqueront son état, généralement en passant par différentes couleurs/clignotements avant de se stabiliser.

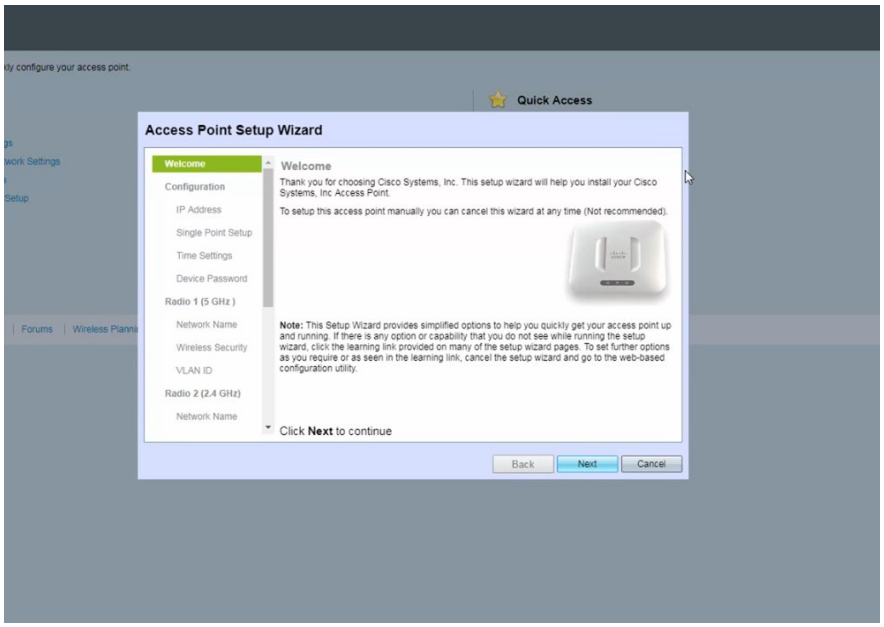
À ce stade, accédez à l'interface de gestion de la borne pour configurer ses paramètres. Pour cela, connectez un ordinateur au même réseau que la borne et ouvrez un navigateur web. Entrez l'adresse IP de la borne, qui, par défaut est : 192.168.1.245.



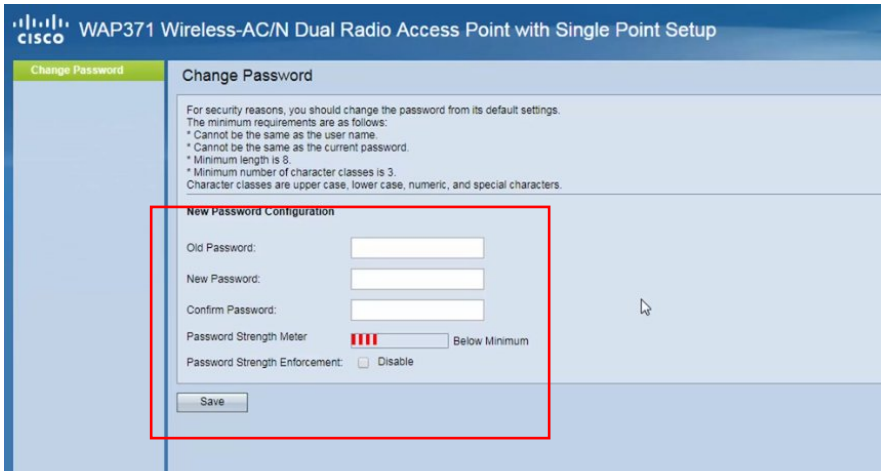
Une fois l'adresse IP saisie dans le navigateur, vous accéderez à l'interface de connexion de la borne. Connectez-vous avec les identifiants par défaut, dans notre cas ce sera CISCO / CISCO

2-Changement de mot de passe

Nous arrivons sur la page d'accueil de configuration, et notre première étape sera de changer ces identifiants immédiatement après la première connexion pour des raisons de sécurité.

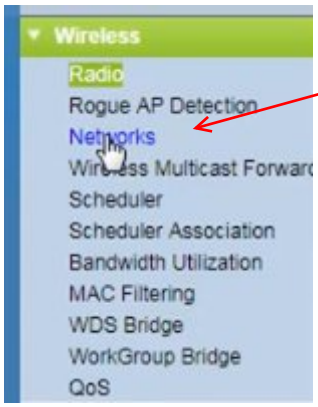


En poursuivant le « Setup Wizard », nous aurons l'occasion de changer le mot de passe puis se reconnecter avec les nouveaux identifiants.

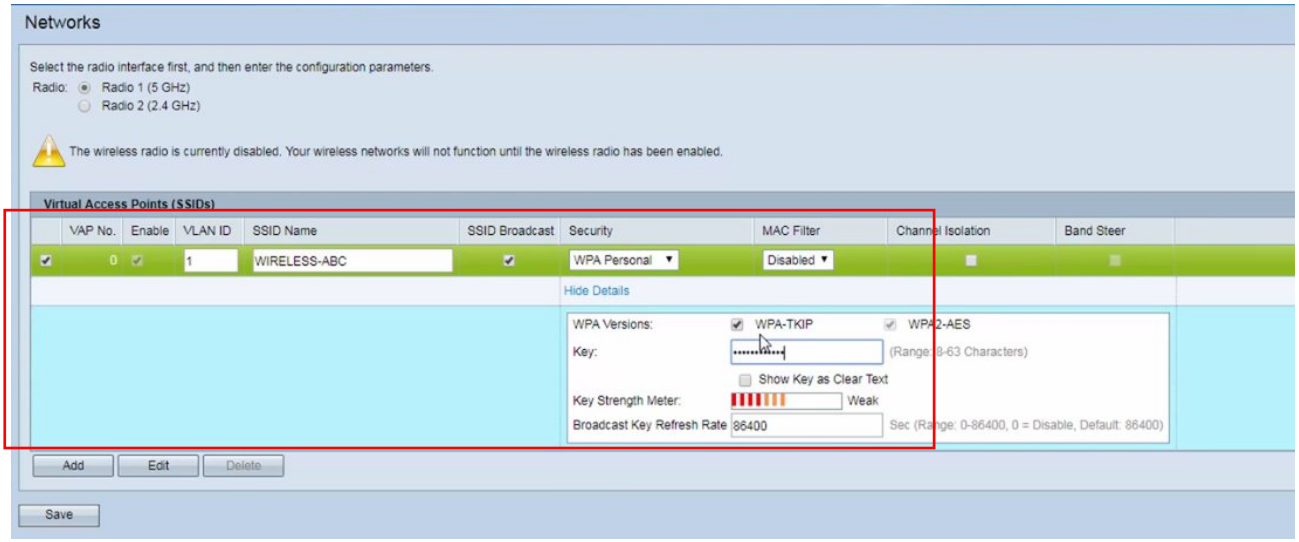


3-Paramétrage des réseaux sans-fil

Ensuite nous allons nous rendre dans la rubrique « Wireless », puis « Networks » afin d'activer une à une les bandes 2,4 et 5GHz.

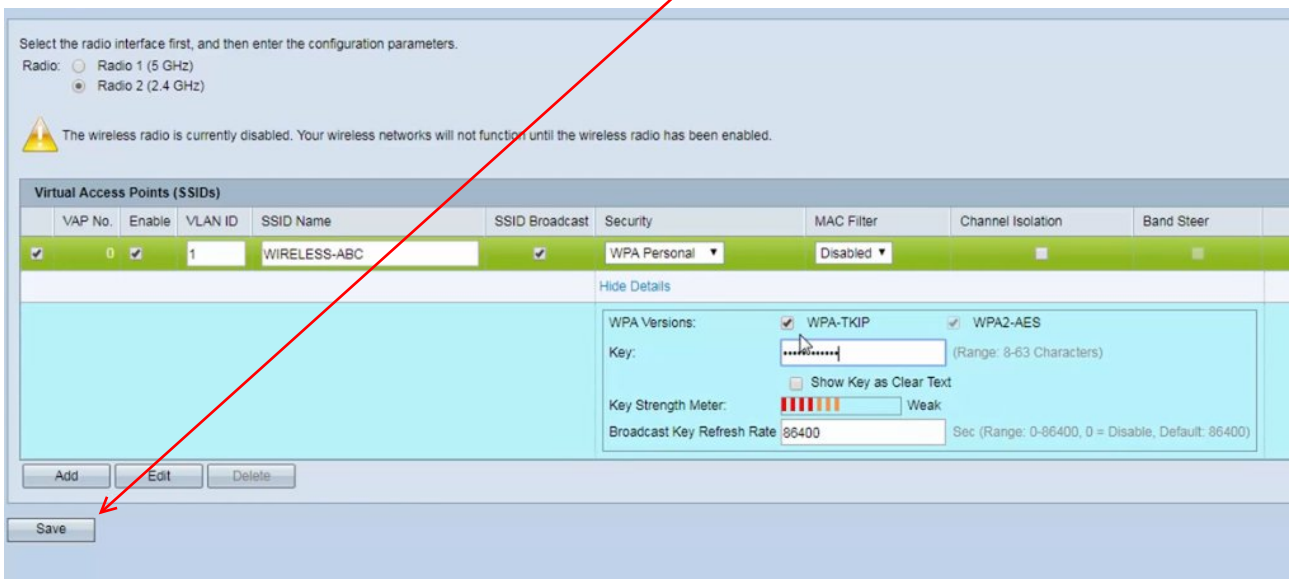


On attribue un nom par bande (SSID), un VLAN ID si nous voulons segmenter notre réseau. Également choisir le type de protection, ici nous n'avons pas d'autre choix que WPA-TKIP et WPA2. Une fois votre protocole choisi, créez un mot de passe dédié.



- A noter : WPA avec TKIP (Temporal Key Integrity Protocol) est une norme plus ancienne et moins sécurisée, vulnérable à certaines attaques. WPA2, utilisant AES (Advanced Encryption Standard), offre une sécurité beaucoup plus robuste et est recommandé pour protéger les réseaux modernes.

Enfin, faîtes de même avec la bande 2.4GHz, puis « Save ».

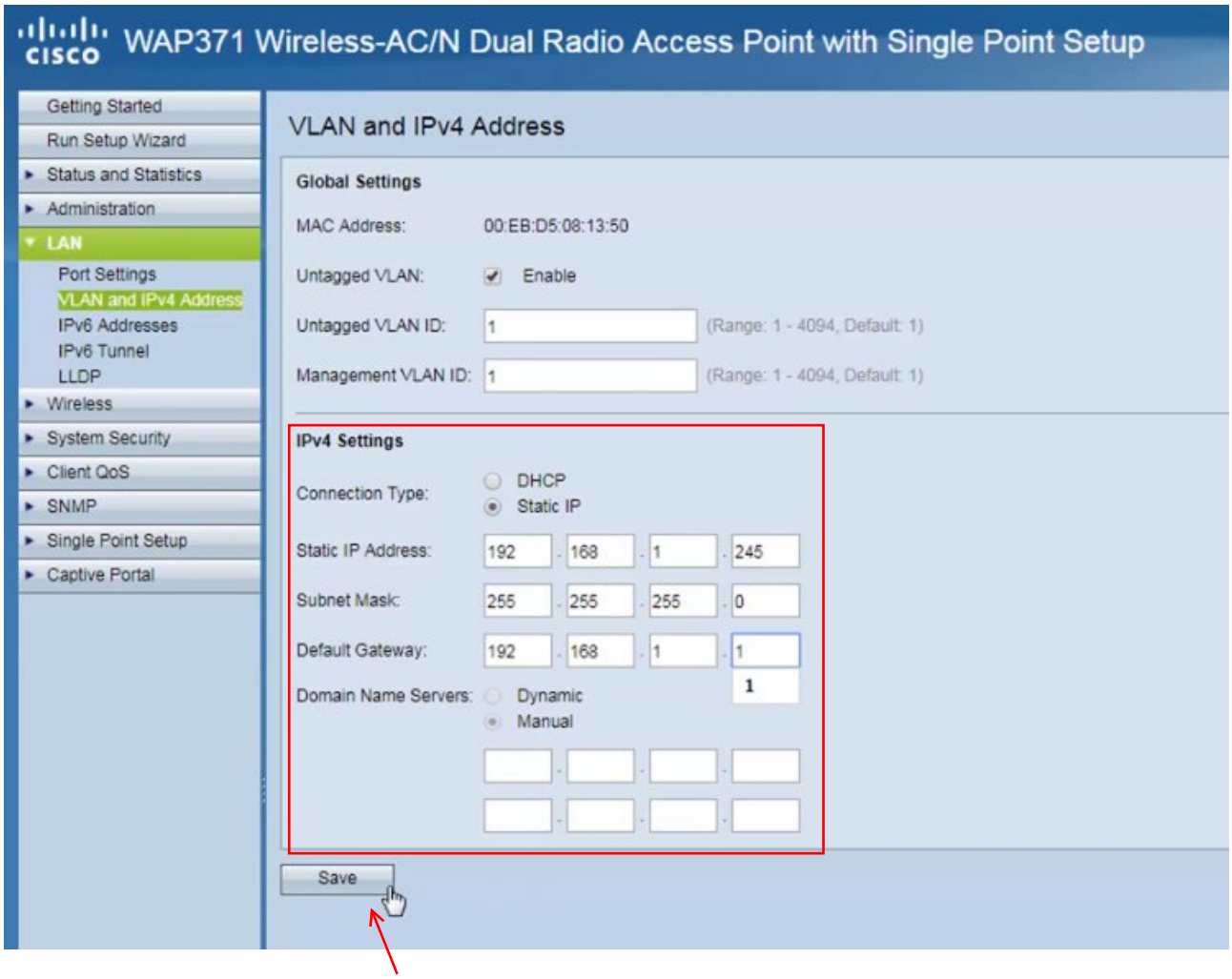


La prochaine étape consiste à activer l'antenne, sans quoi nous ne pourrons pas détecter le ou les réseaux Wifi.
Il faudra donc se rendre toujours dans « Wireless » puis « Radio », puis sous « Basic Settings », sélectionner « Enable » pour l'option 2,4 et 5GHz. Sauvegardez avec le bouton « Save » tout en bas de la page.

4-Ajout d'une adresse IP fixe pour la borne

Pour finir, nous allons lui attribuer une adresse IP fixe afin de pouvoir accéder au management de la borne à l'avenir.

Allez dans la rubrique « LAN » puis « VLAN and IPV4 Address ».
Sous « Connection Type », sélectionnez « Static IP » et remplissez les champs avec les valeurs adaptées à votre réseau.
Une adresse IP libre, le bon masque de sous réseau, la passerelle par défaut ainsi que la ou les adresses DNS.



Sauvegardez avec le bouton « Save » et redémarrez la borne.

Votre réseau wifi est opérationnel.

Présentation du fonctionnement de Radius et des certificats

Le protocole RADIUS (Remote Authentication Dial-In User Service) est une solution client/serveur permettant de centraliser l'authentification et l'autorisation des utilisateurs qui souhaitent accéder à un réseau, comme les réseaux sans fil, VPN ou services d'accès à distance.

Fonctionnement de RADIUS :
Le client RADIUS, souvent un point d'accès Wi-Fi, un commutateur ou un routeur, sert de point d'entrée au réseau. Il recueille les informations d'identification de l'utilisateur et les envoie au serveur RADIUS pour vérification. Ce dernier compare les informations avec une base de données d'utilisateurs (par exemple, un annuaire LDAP ou Active Directory) et renvoie une réponse pour accepter, rejeter ou défier l'accès.

Processus d'authentification :

1. L'utilisateur tente de se connecter via le client RADIUS.
2. Le client demande les informations d'identification de l'utilisateur.
3. Ces informations sont envoyées au serveur RADIUS.
4. Le serveur RADIUS authentifie l'utilisateur.
5. Le serveur renvoie une réponse pour accepter ou rejeter l'accès.
6. Si l'accès est accordé, le client fournit les services réseau appropriés.

Intégration des certificats dans RADIUS :

Pour renforcer la sécurité, RADIUS peut utiliser des certificats numériques avec le protocole EAP-TLS, qui repose sur des certificats pour authentifier mutuellement le client et le serveur. Une Autorité de Certification (CA) génère et signe les certificats pour le serveur et les clients. Lors de l'authentification, le serveur vérifie le certificat du client et vice versa.

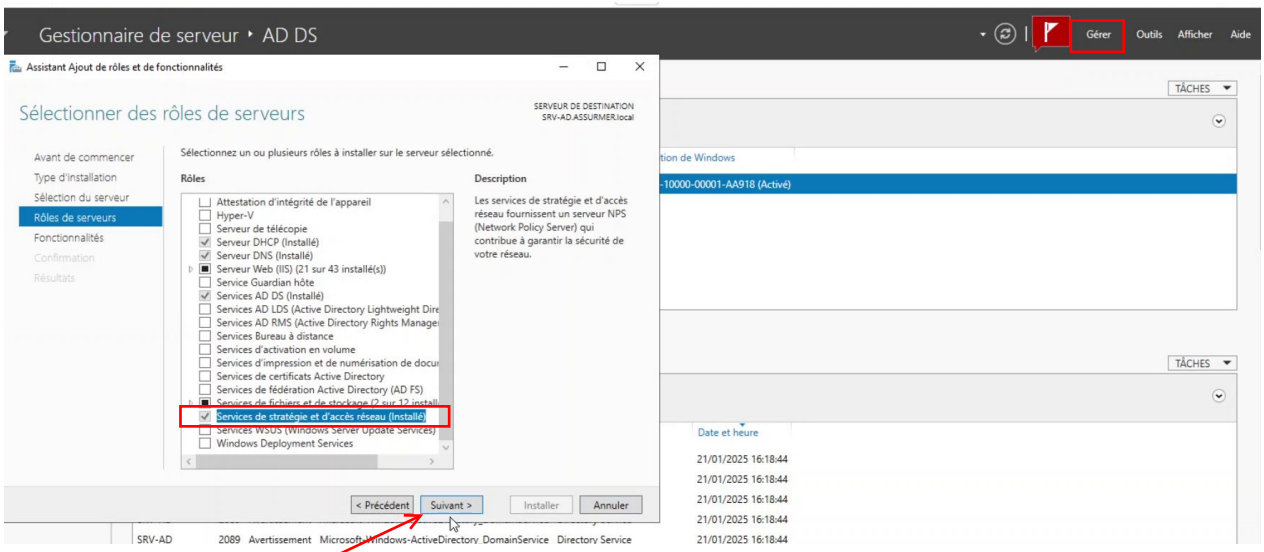
Processus d'authentification avec EAP-TLS :

1. Le client initie la connexion via le client RADIUS.
2. Le client transmet la demande au serveur RADIUS en utilisant EAP-TLS.
3. Le serveur RADIUS présente son certificat au client.
4. Le client vérifie le certificat du serveur.
5. Le client envoie son certificat au serveur RADIUS.
6. Le serveur RADIUS vérifie le certificat du client.
7. Si les certificats sont validés, une session chiffrée est établie et l'accès est accordé.

L'utilisation de certificats numériques avec RADIUS assure une authentification forte et protège contre les accès non autorisés, garantissant ainsi une sécurité accrue pour les réseaux sensibles.

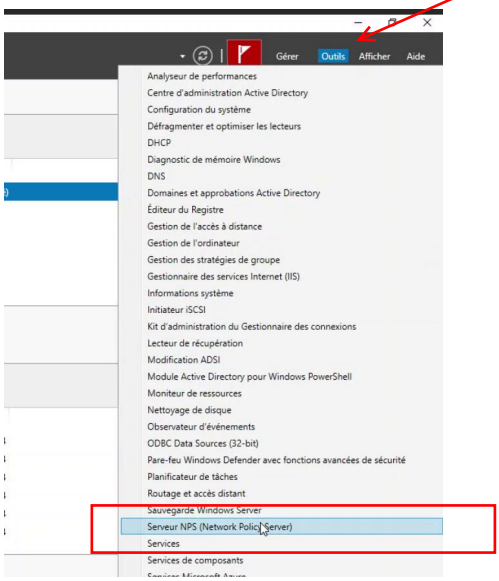
Procédure d'installation et de configuration d'un client Radius

Commencez par ouvrir le Gestionnaire de serveur. Cliquez sur Ajouter des rôles et des fonctionnalités dans le menu du gestionnaire de serveur.
Dans l'assistant, sélectionnez Suivant jusqu'à l'écran des rôles. Cochez Network Policy and Access Services, puis cliquez sur Suivant et sélectionnez Network Policy Server (NPS).

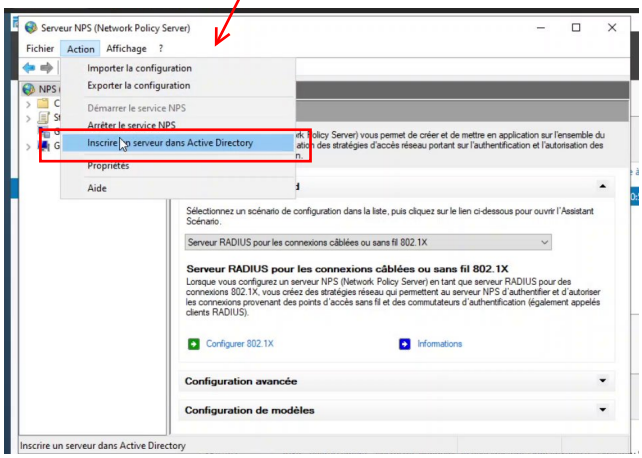


Cliquez sur Installer et attendez que l'installation se termine. Une fois l'installation terminée, cliquez sur Fermer.

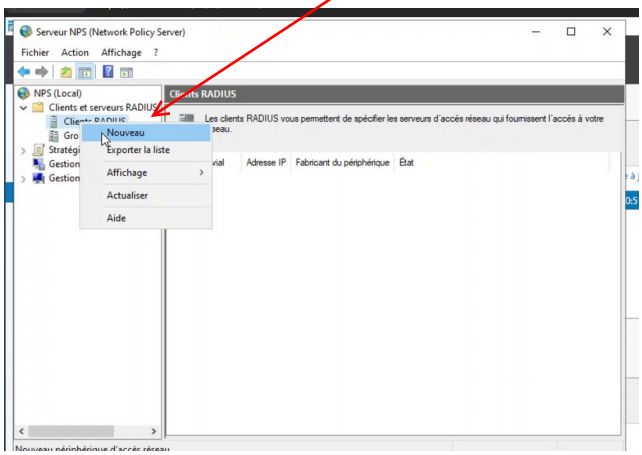
Accédez à Network Policy Server en allant dans Outils dans le gestionnaire de serveur, puis sélectionnez Network Policy Server.



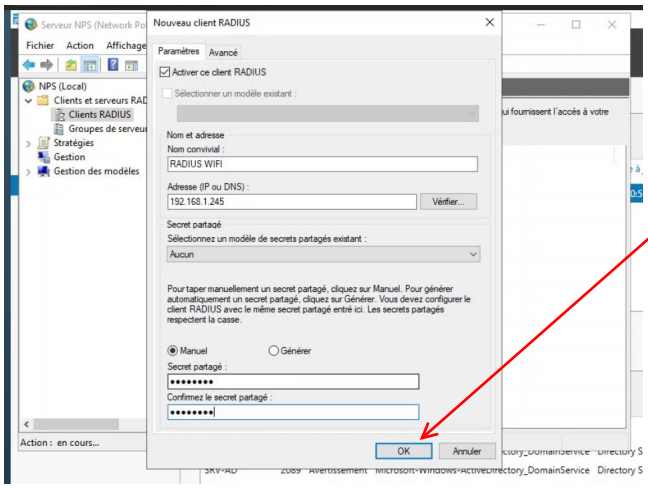
Dans la fenêtre NPS, faites un clic droit sur NPS (Local) dans le panneau de gauche et choisissez Enregistrer ce serveur dans Active Directory. Cela permettra au serveur RADIUS de s'intégrer à Active Directory.



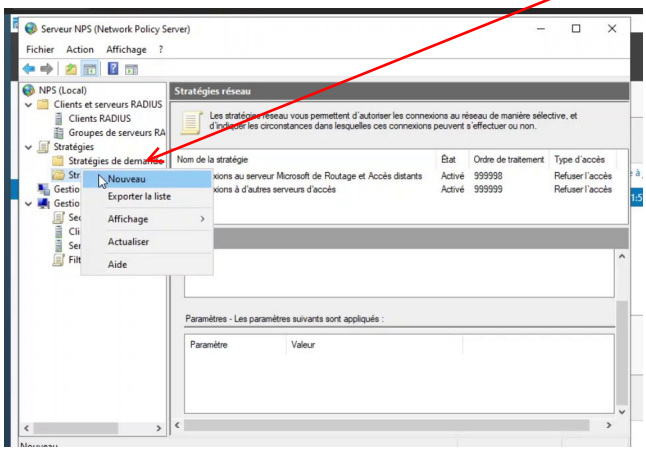
Ensuite, configurez les clients RADIUS. Dans la fenêtre NPS, sous Clients et serveurs RADIUS, faites un clic droit sur Clients RADIUS et sélectionnez Nouveau client RADIUS.



Donnez un nom au client (par exemple, un point d'accès Wi-Fi ou un commutateur). Entrez l'adresse IP ou le nom de domaine complet (FQDN) du client dans le champ approprié. Saisissez une clé partagée secrète que le client utilisera pour se connecter au serveur. Cliquez sur OK pour enregistrer les informations.

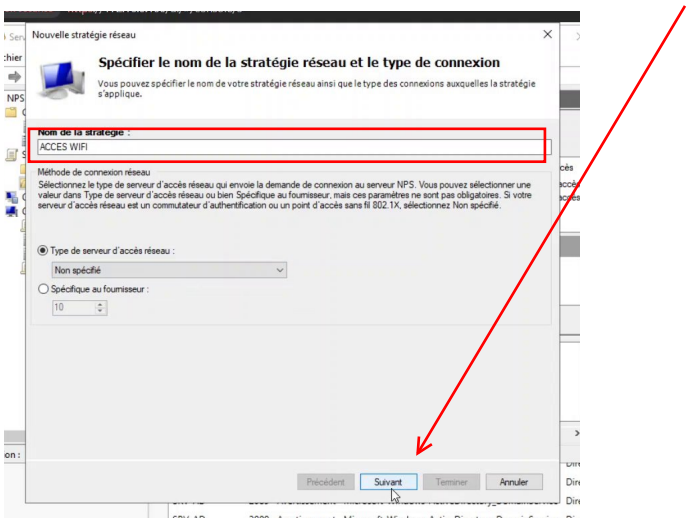


Vous devez maintenant créer une politique d'accès réseau. Sous Stratégies, cliquez sur Stratégies d'accès réseau, faites un clic droit et sélectionnez Nouveaux.

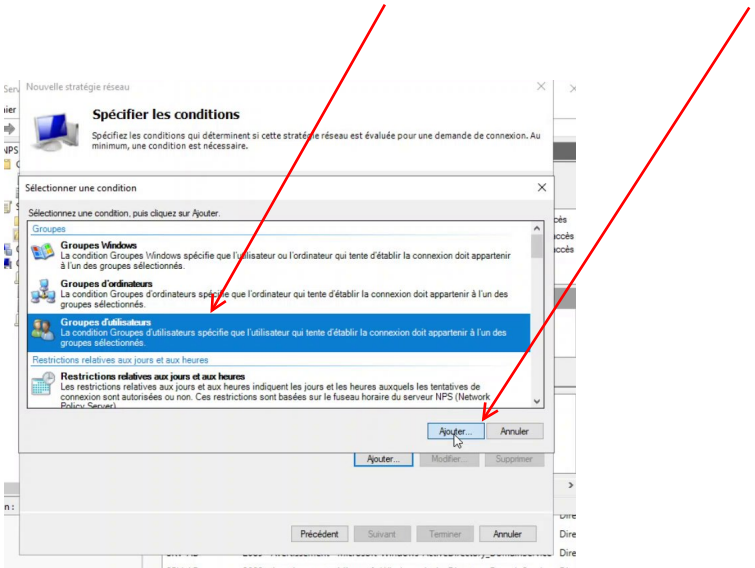


Suivez l'assistant pour configurer la politique d'accès en fonction de vos besoins (authentification par mot de passe, certificat, etc.). Vous pourrez définir des conditions, des contraintes et des paramètres de contrôle d'accès selon les exigences de votre réseau.

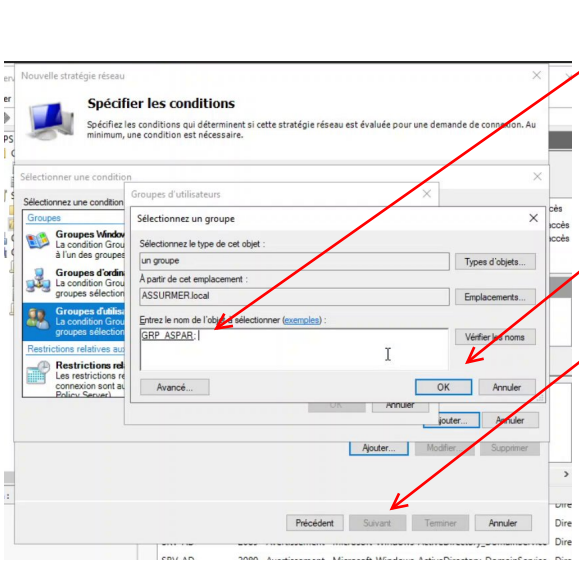
Ajoutez un nom à votre stratégie puis cliquez sur Suivant.



Dans notre cas, nous voulons autoriser des groupes d'utilisateurs, c'est à dire ceux référencés sur notre AD, choisissez donc Goupes d'utilisateurs, puis Ajouter.

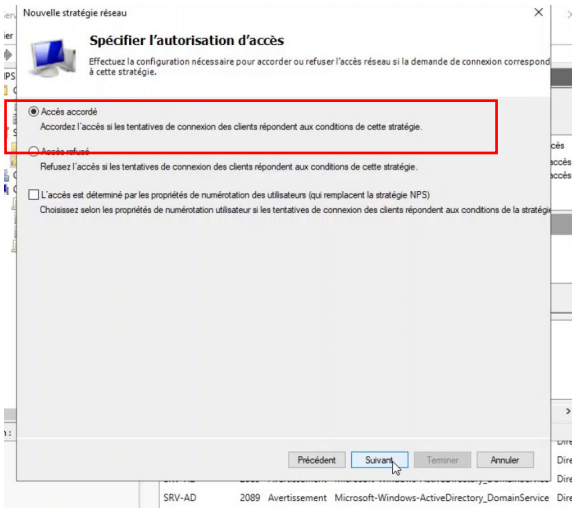


Dans les conditions, nous allons ajouter le groupe désiré. Cliquez sur OK puis Suivant.

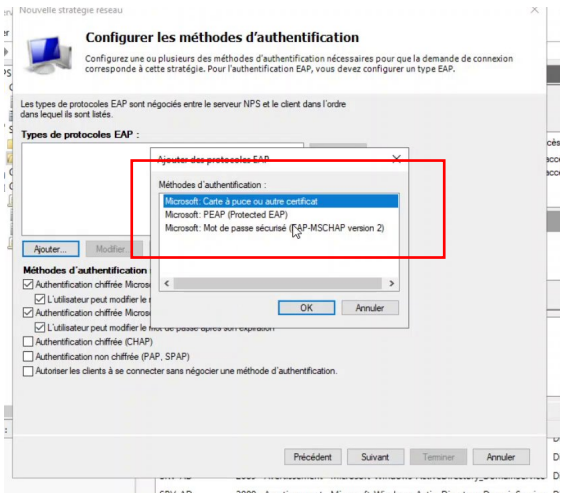


NB : il est possible d'ajouter des utilisateurs de divers groupes dans un groupe dédié au « Wifi », afin de faciliter l'accès à ce dernier.

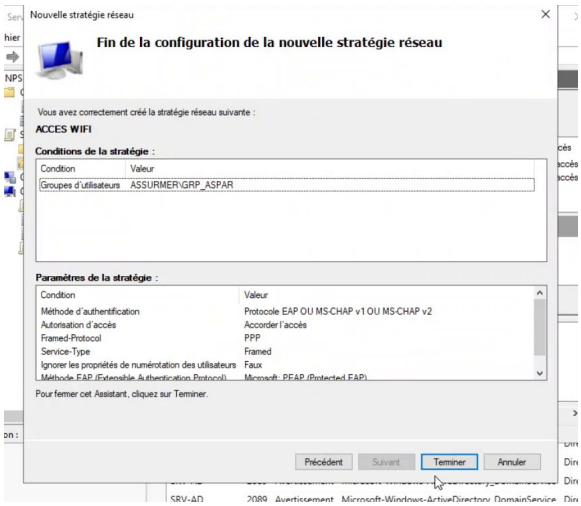
Ensuite, dans notre cas, l'objectif est d'autoriser ce groupe.
Si il est nécessaire de refuser l'accès à un groupe, alors c'est l'autre option qu'il faut choisir pour une nouvelle règle.
Cliquez sur Suivant.



Pour la méthode d’authentification, sélectionnez le protocole qui convient à vos besoins. Cliquez sur Suivant.



Vous avez donc créé une règle d’authentification Radius, il ne vous restes plus qu’à la tester en pratique.



Il est également recommandé d'activer les journaux d'audit pour suivre les événements d'authentification et d'autorisation. Sous Politiques, cliquez sur Journaux d'audit et sélectionnez Activer les journaux d'audit.