Mathieu URGIN
Clément MONTMAYEUR

Installation et configuration du protocole Radius sur Windows Server 2022

AssurMer
13.11.2024
Validé par DSI AssurMer v1.1

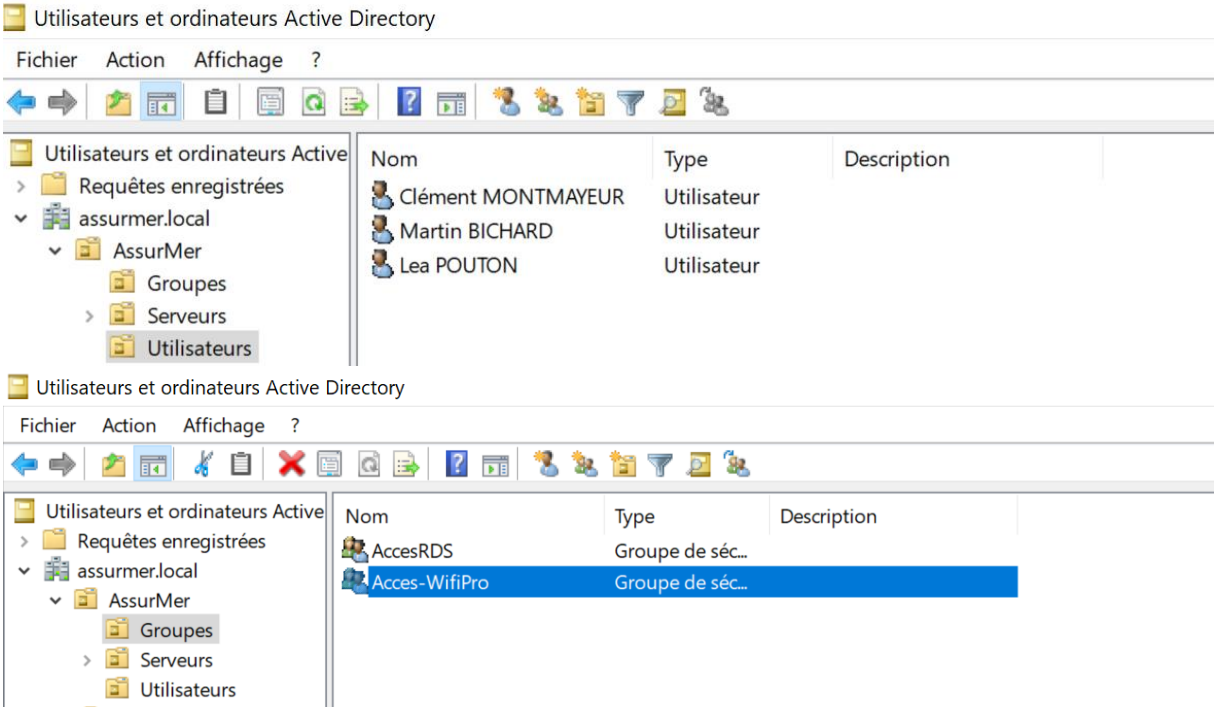
Sommaire :

- P0 – Introduction et prérequis
- P1 – Installation et configuration du service de certificat
- P2 – Installation et configuration du service NAP
- P3 – Configuration de la borne WiFi
- P4 – Dépannage

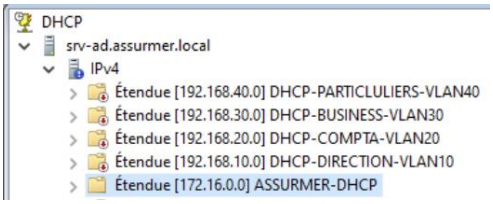
P0 – Introduction et prérequis

La mise en place du protocole radius sur l'infrastructure d'AssurMer permettra entre autres d'authentifier les utilisateurs sur la/les borne(s) Wifi du réseau via leurs sessions utilisateur, ce qui permettra de gérer les accès de chaque utilisateur.

Pour cela, nous avons mis en place un serveur Active Directory sous Windows Serveur 2022 dans le domaine assurmer.local, dans lequel nous avons créé des utilisateurs, ainsi qu'un groupe de sécurité, accordé pour l'accès au réseau Wifi,



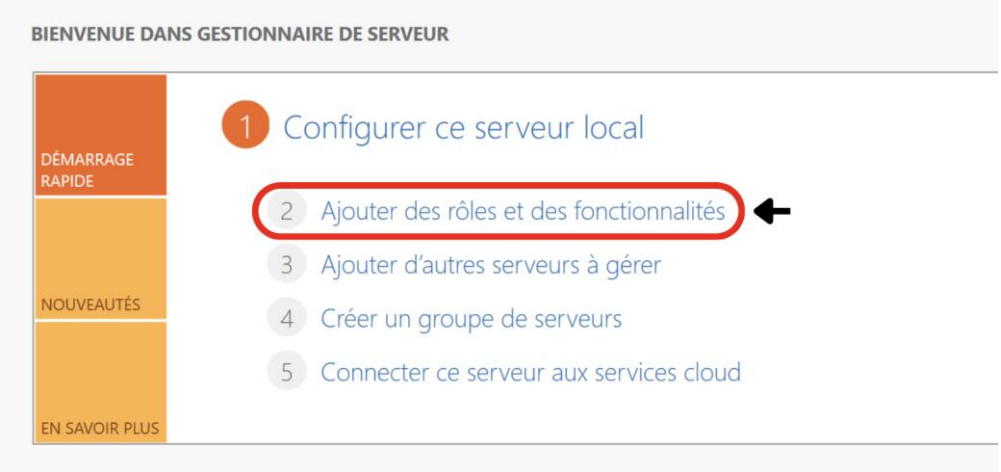
Information AD :
Nom Serveur : WSRV2K22-AD1
Adresse IP : 172.16.0.1 (Static)
OS : Windows Server 2022 Standard
5 Etendu DHCP activé (1 par VLAN)



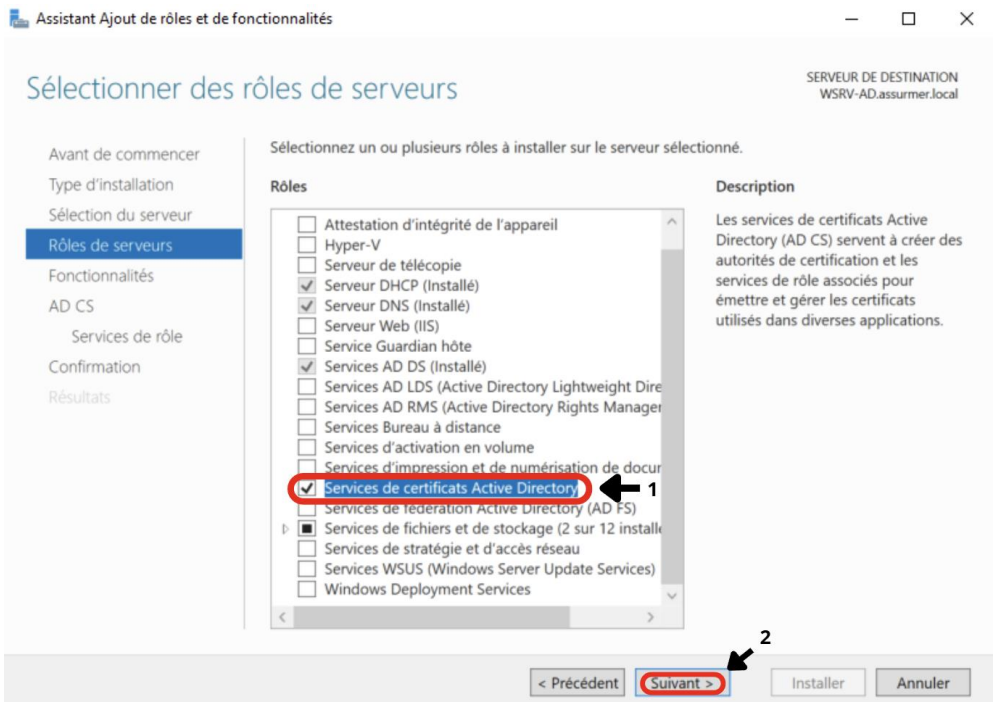
Information Borne Wifi :
Modelé : Cisco WAP371
IP : 172.16.0.10 (Static)
Sécurité WAP2 - Entreprise

P1 – Installation et configuration du service de certificat

Sur le serveur Active Directory, dans le gestionnaire de serveur,
Cliquez sur « Ajoutez des rôles et fonctionnalités »

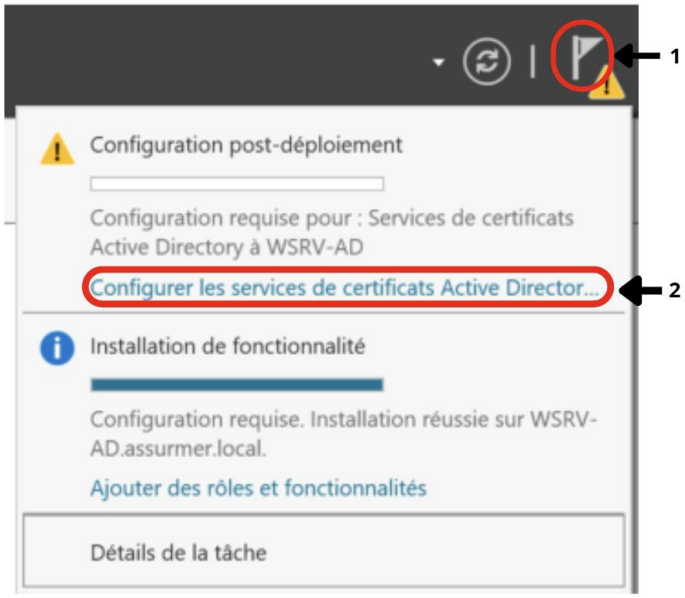


Cliquez sur suivant et sélectionnez le service de certificat active directory,

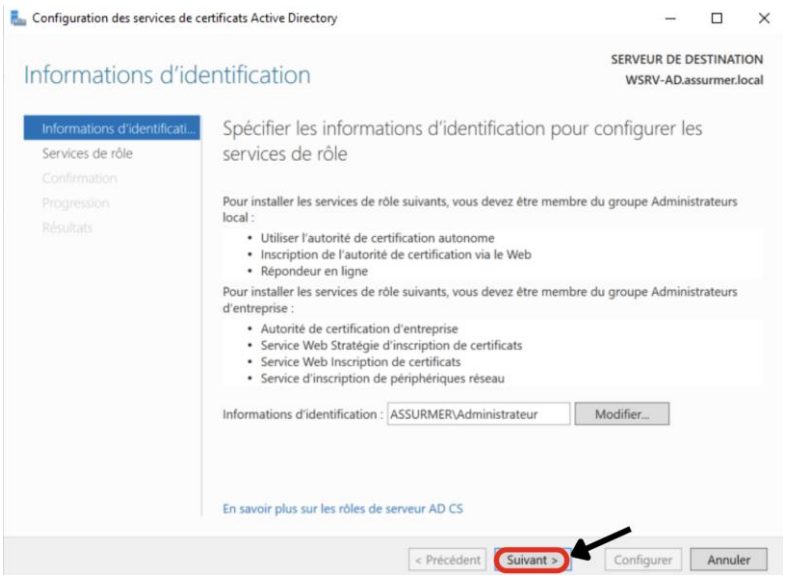


Puis cliquez sur « Suivant » puis « Installer

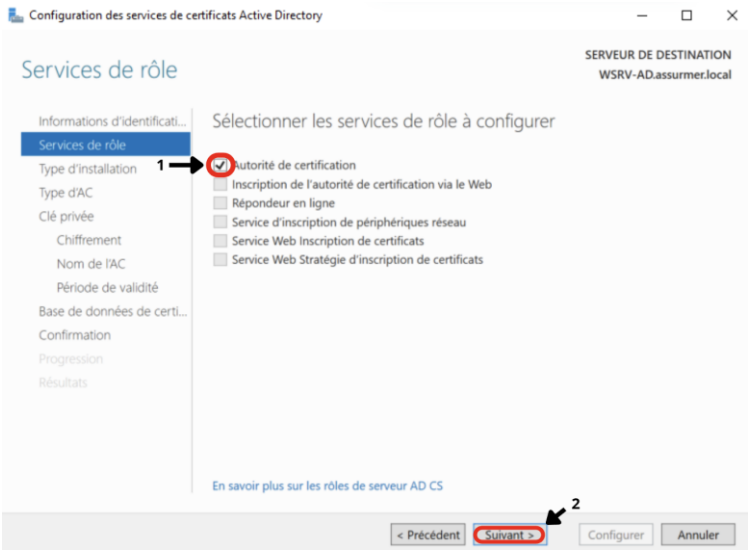
Dans le gestionnaire de serveur, dans la partie notification, cliquez sur « Configurez les services de certificats Active Directory,



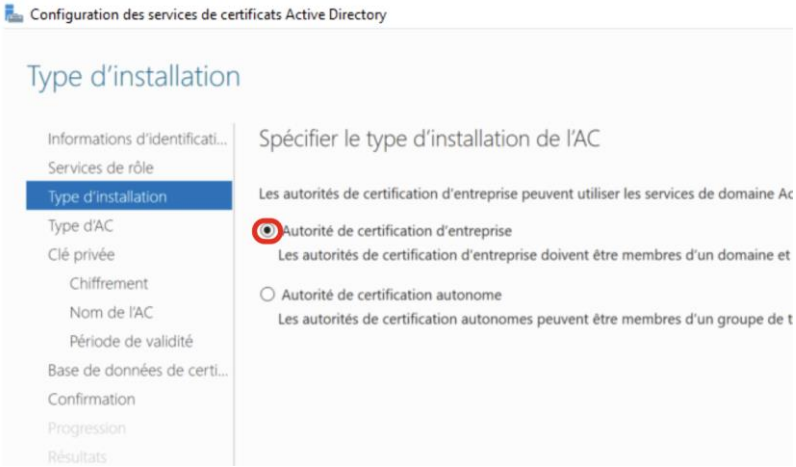
Ici, vous pouvez définir les identifiants utilisés pour la configuration du service, dans notre cas nous utiliserons l'identifiants par default du domaine, cliquez sur suivant,



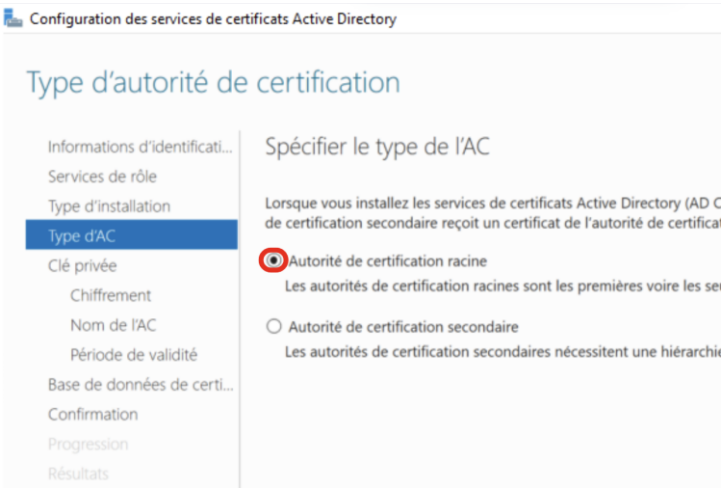
Ensuite, cochez « Autorité de certification », et faites suivant,



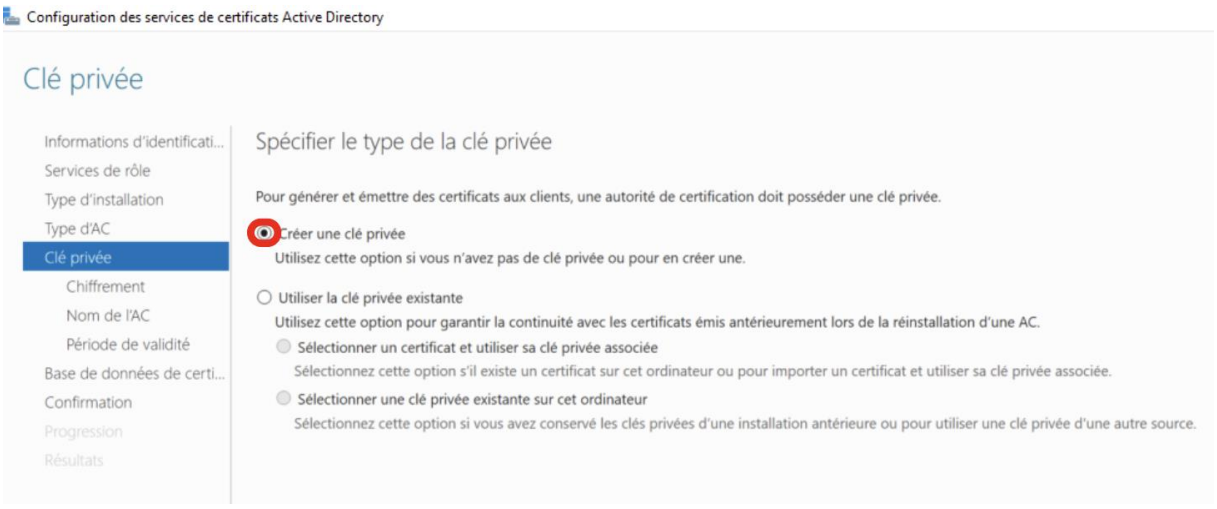
Laissez « Autorité de certification d'entreprise » coché, puis faites suivant,



Faites de même pour le type d'autorité de certification, cochez « Autorité de certification racine » puis, faites suivant,



Cliquez maintenant sur « Crée une clef privée » celle-ci servira au serveur radius pour l'authentification, puis cliquez sur suivant,



Ici, on définit le type de chiffrement utilisé pour l'authentification par certificat,

Le chiffrement SHA256 étant déjà très sécurisé, avec une longueur de clé de 2048, c'est le moyen le plus adapté dans notre situation, cliquez ensuite sur suivant,

Dans cette partie, laissons les valeurs par default, cliquez sur suivant,

Ici on peut définir la période de validité du certificat avant d'être renouvelé, 2 ans est un bon compromis sécurité/praticité,

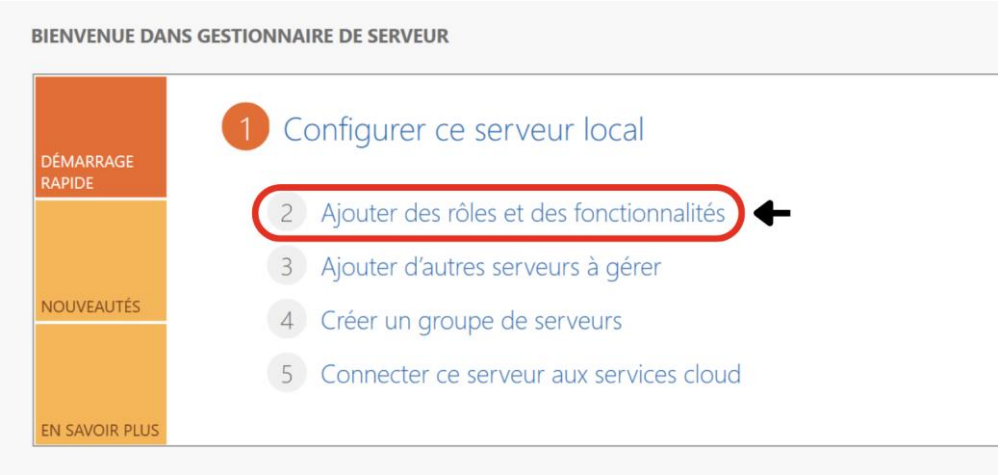
Cliquez sur suivant, puis « Configurer » et enfin « Close »

La configuration du service de certificat Active Directory est maintenant terminé.

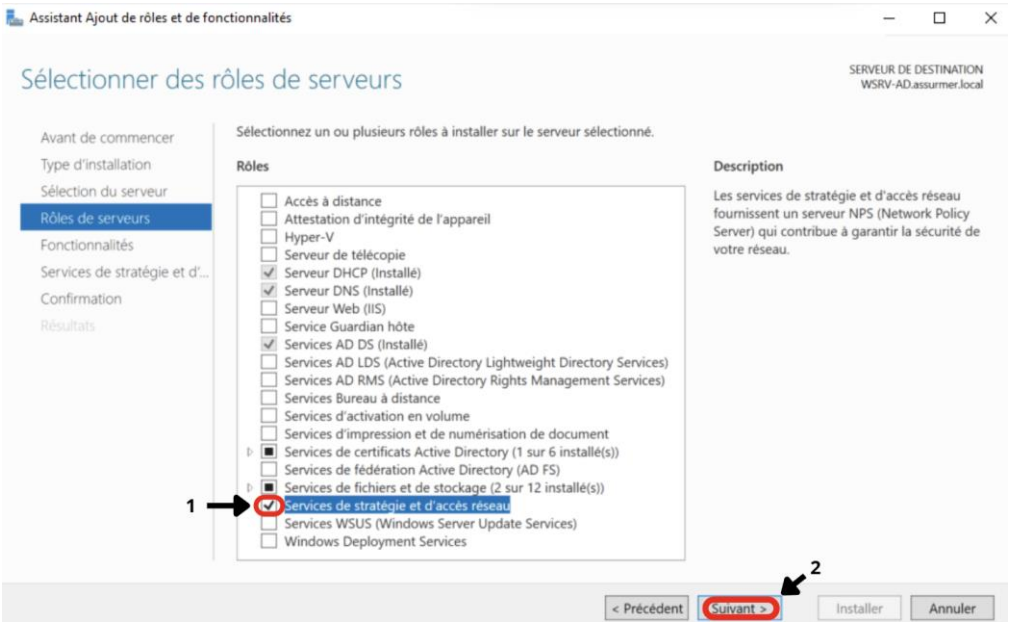
P2 – Installation et configuration du service NAP

Dans cette seconde partie, nous installons le service permettant de gérer les politiques d'accès réseau (NAP).
Cela inclut la configuration des règles pour authentifier et autoriser les utilisateurs ou appareils.

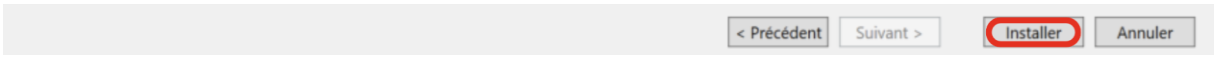
Retournez dans le gestionnaire de serveur et une ajoutez une nouvelle fonctionnalité,



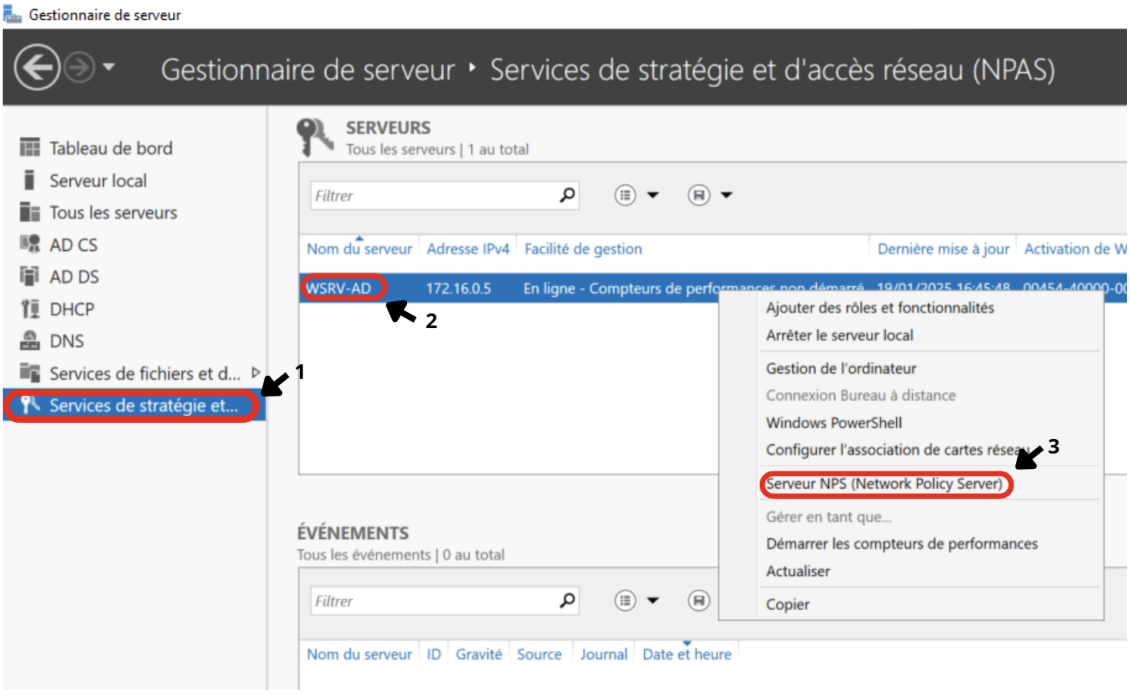
Sélectionnez « Service de stratégie et d'accès réseau, puis faites « Suivant »



Puis « Installer »

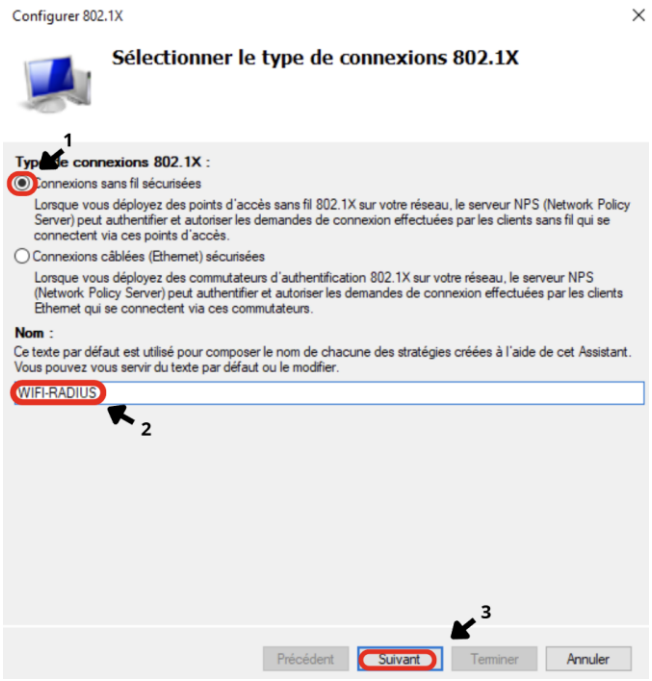


Passons ensuite à la configuration du NAP, dans le gestionnaire de service cliquez sur « Service de stratégie et d'accès réseau (NPAS) et faites un clic droit sur le nom de machine, puis Serveur NPS,

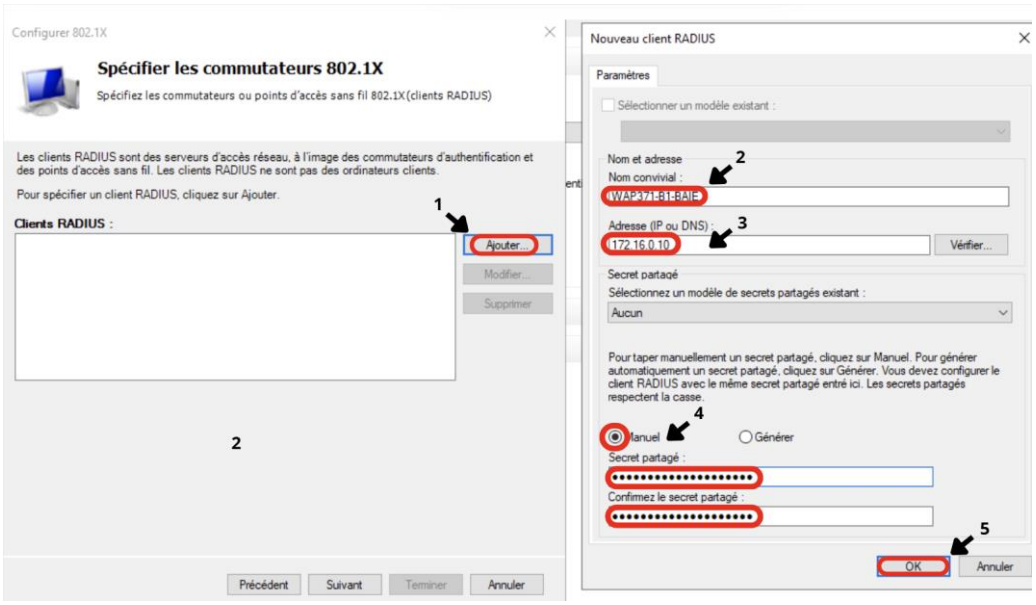


Choisissez « Serveur RADIUS pour les connexions câblées ou sans fil 802.1X, et cliquez sur Configurez 802.1X,

Sélectionnez « Connexions sans fils sécurisé, et donnez le nom que vous souhaitez, cliquez ensuite sur suivant,



Dans cette partie de la configuration nous ajoutons le client radius, et dans ce cas, la borne Wifi, Cliquez donc sur « Ajouter » et renseignez les informations de la bornes Wifi que vous possédez,

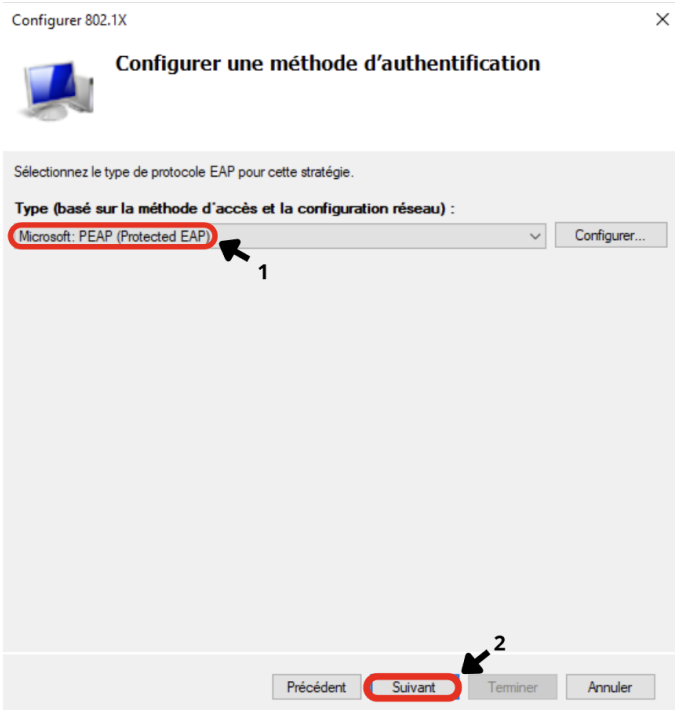


Définissez :

- Le nom de la borne
- Son adresse IP
- Le mot de passe qu'utilisera la borne pour se connecter au radius

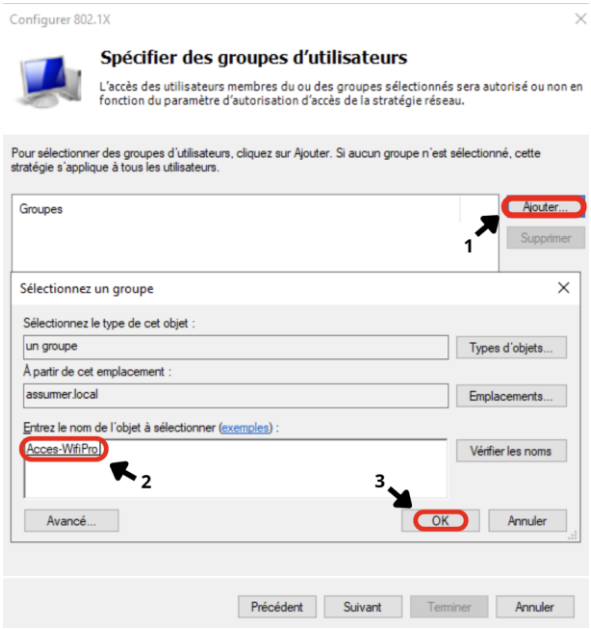
Cliquez ensuite sur OK, puis Suivant

Pour la méthode d'authentification, sélectionnez « Microsoft : PEAP » puis cliquez sur « Suivant »



Ici nous ajoutons le groupe utilisateur qui permettra l'accès pour les utilisateurs au Wifi de l'entreprise,

Cliquez sur « Ajouter », sélectionnez le groupe accès crée pour cela puis faites « OK » puis « Suivant »



Faites « Suivant » et Enfin « Terminer »

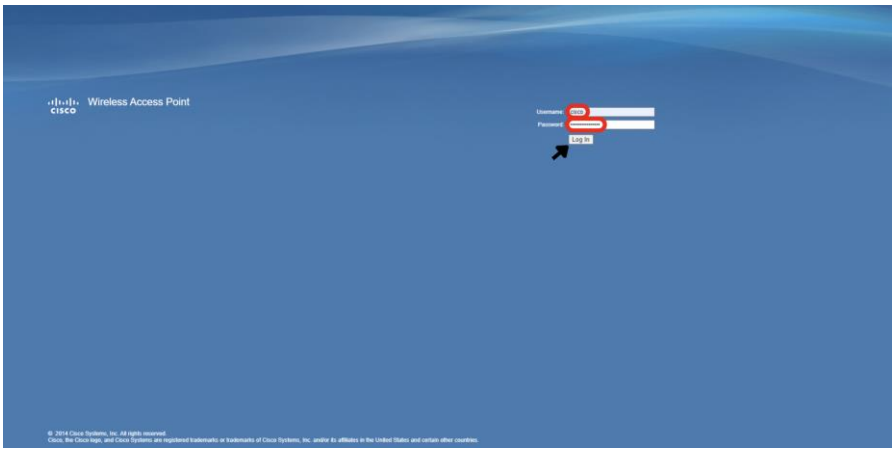
P3 – Configuration de la borne WiFi

Maintenant que le radius est correctement configuré pour accueillir la borne WiFi, ainsi que les utilisateurs, configurons la borne Wifi en elle-même,

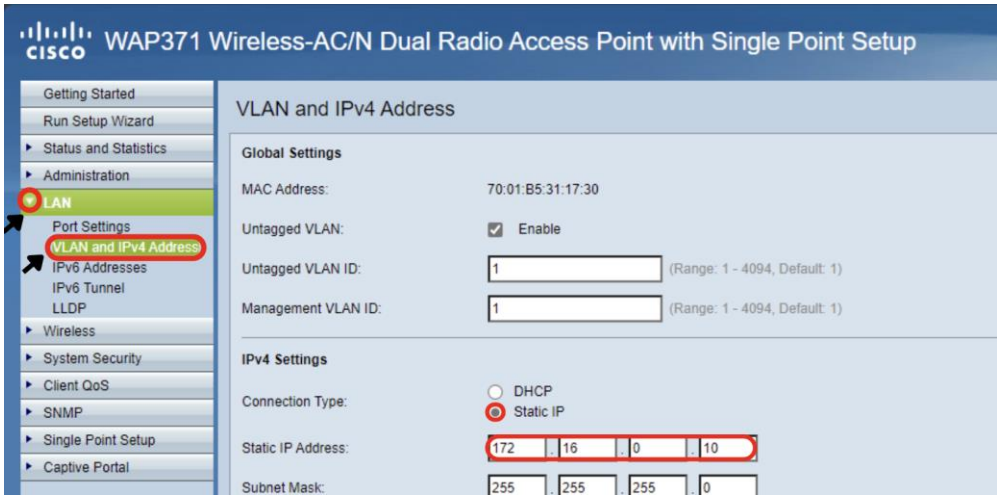
Branchez la borne Wifi sur votre infrastructure, dans le manuel d'utilisation, récupérez l'adresse IP par défaut de la borne, et connectée un poste configuré sur la même plage d'IP que la borne,

Dans le cas de la borne Cisco WAP371, l'adresse IP par default est la 192.168.1.245,

Via un navigateur accéder à l'interface utilisateur, le mot de passe par default est « cisco »



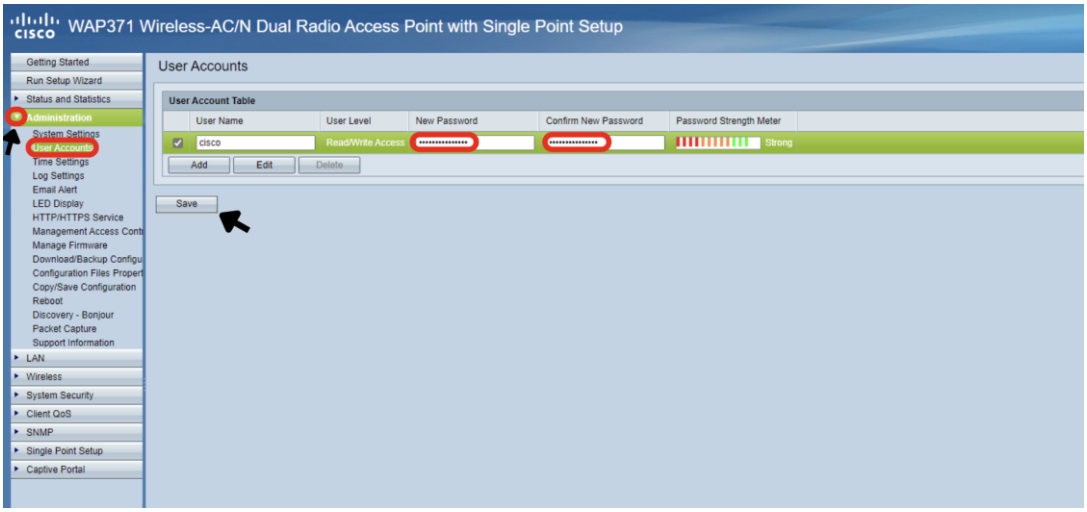
Ignorez l'utilitaire de configuration de base, et allez dans la partie « LAN » puis « VLAN and IPV4 Adress »



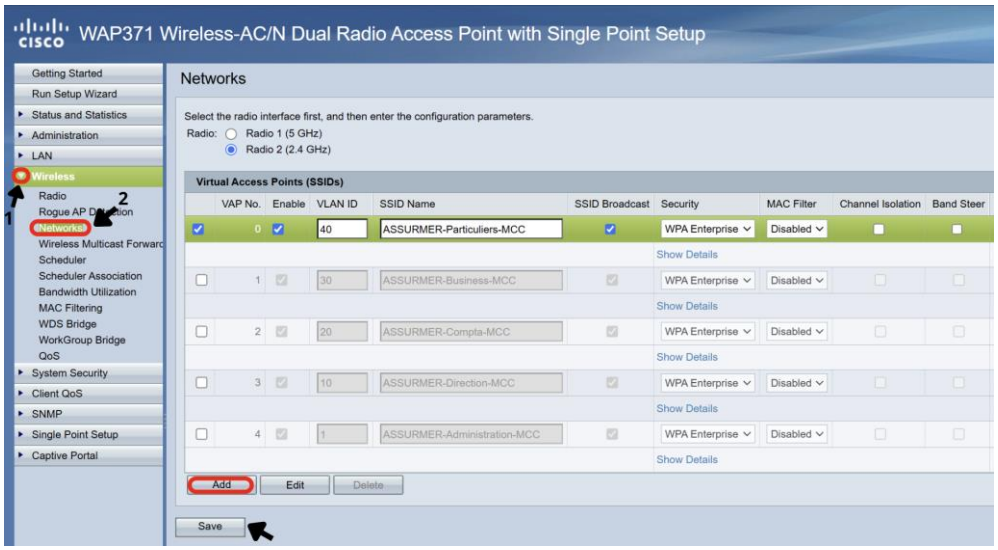
Ici, changez l'adresse IP de la borne par l'adresse souhaité, ici nous choisirons 172.16.0.10/24, puis appliquez la configuration,

Ensuite, reconnectez-vous à la borne sur sa nouvelle adresse IP, et dans la partie « Administration » puis « User Accounts » changez le mot de passe par defaut de la borne,

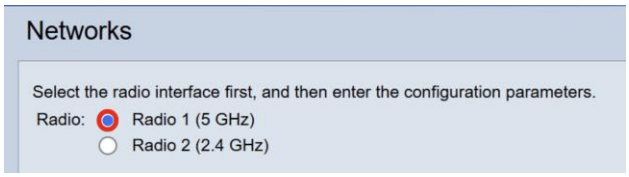
⚠ Etape Importante : L'utilisation de mot de passe faible constitue environ 30% des attaques cyber malveillante



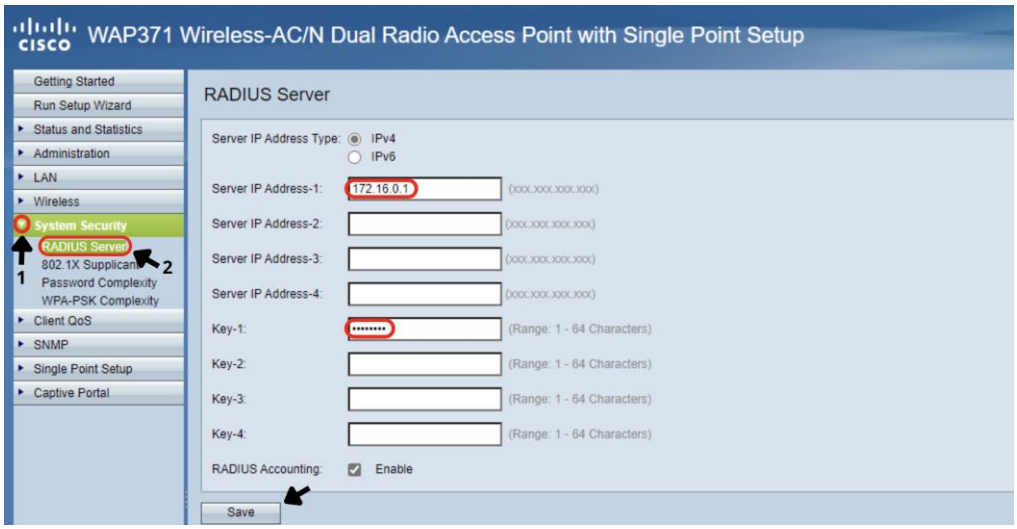
Après cela fait nous pouvons configurer le réseau étendu, allez dans « Wireless » puis « Networks », dans SSID Name, choisissez le nom de vos réseaux Wifi étendu, modifier le VLAN du réseau, et dans le type de sécurité, choisissez « WPA Entreprise » pour faire fonctionner l'authentification utilisateur,



Effectuez la même manipulation pour le réseau en 2,4Ghz,



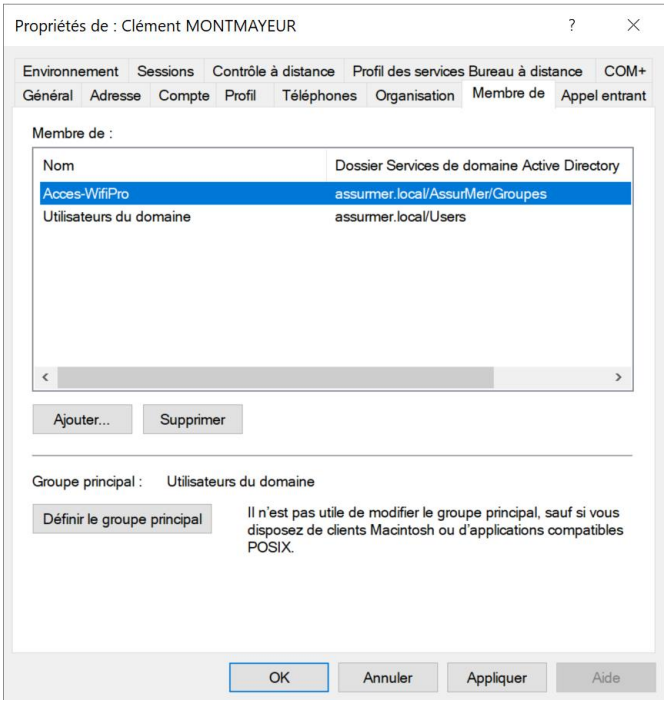
Dans la dernière étape, configurez l'authentification de la borne sur le radius, rendez-vous dans la partie « System Security » puis « Radius Server »



Renseigner l'adresse IPV4 du serveur Radius configuré précédemment, ainsi que le mot de passe que vous avez choisi (voir page 13) et faites « Save »

Désormais, le réseau configuré précédemment devrais apparaitre dans les réseau Wifi,

Pour donner l'accès à un utilisateur, attribuez lier le groupe « Acces-WifiPro »

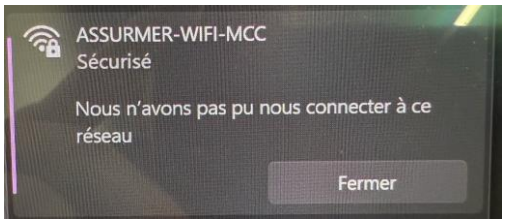


Désormais, vous pourrez vous connecter via les identifiants cette utilisateur sur ce réseau Wifi,

P3 – Dépannage

En cas de problème, voici un guide des problèmes les plus courant que vous pourrez rencontrer :

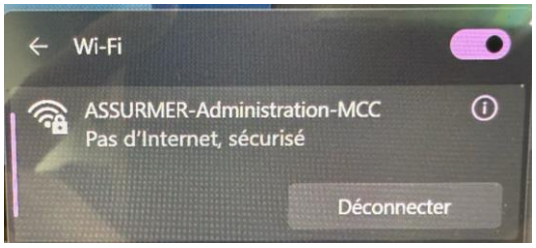
1 - « Nous n'avons pas pu nous connecter à ce réseau »



Solutions : Vérifier le paramétrage telle que :

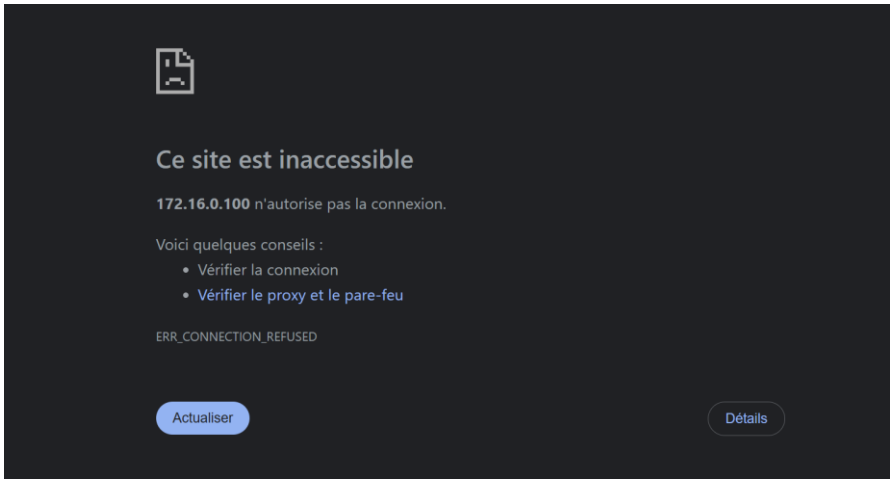
- Mot de passe d'authentification de la borne sur le radius
- Certificat utilisateur
- Mot de passe utilisateur

2 – « Connecté pas d'internet »



Vérifier que votre serveur DHCP est actif et qu'il est configuré sur le bon VLAN,

3 – Pas d'accès aux machines sur le réseau



Vérifier que votre réseau Wifi étendu est configuré sur le bon VLAN