[**Objectif**](#_mrlh433jczr8) **2**

[Besoins](#_6f9qsgj57vpl) 2

[**Principe**](#_rvn1l9hzo3yc) **3**

[**Création du domaine**](#_ixbtjarzolyf) **4**

[**Création d’un Active Directory**](#_sod6g6xg9s7e) **5**

[AD par défaut](#_efcejky533jm) 5

[Création d’une unité d’organisation](#_eek7mpvh1qau) 6

[Création d’un utilisateur](#_dnk3swbnbu3m) 8

[**Installation des services de certificat Active Directory**](#_j1hhpxejp5op) **8**

[**Création du RADIUS**](#_afckyikv6rgp) **14**

[Installation](#_d2e8ge2y59vv) 14

[Configuration](#_p6tgt3u6wild) 15

[Créer une stratégie de demande de connexion](#_6ry3yf9da4a8) 17

[Créer une stratégie réseau](#_iob866xzvrye) 20

[Insertion NPS dans l’AD](#_lwq13e54s278) 25

[**Résultat**](#_jm5i9q61on57) **26**

[**Mise en place de GPO**](#_t0gmzll4kdpa) **28**

[**Mise en place de la borne Wi-Fi**](#_1vvfvykax7ef) **28**

<https://docs.google.com/document/d/1s6KUh6BO9-jK0DKZXIVPBqHG18IeAAIeBY9gG6a2uAM/edit>

<https://docs.google.com/document/d/1OvyiHb32vCL2yc05MjIS1zAyQ57nk8SBPgD3NblmogE/edit>

# 

# Objectif

* Sécuriser l’accès au réseau sans fil via un serveur RADIUS
* Seuls les utilisateurs répertoriés dans l’Active Directory seront autorisés
* Aucune communication avec le LAN avant que l’utilisateur soit authentifié

## Besoins

* Un serveur Windows
* Un Active Directory avec des utilisateurs
* Un domaine fonctionnel
* Un certificat à partager avec les utilisateurs
* Le service NPS (Network Policy Server) installé
* Un point Wi-Fi compatible avec la norme WPA2 Enterprise

# 

# Principe

Dans ce type de structure, la station désirant accéder au réseau est appelée **supplicant**, le PA (client du serveur RADIUS) est appelé **Authenticator** et le serveur RADIUS **Authentication Server.**

La particularité de ce mécanisme est que le *Supplicant* ne communique pas en direct avec le serveur RADIUS pour son authentification (car il n’a pas encore accès à ce réseau). il le fera donc uniquement au travers de *l’Authenticator* (le PA dans notre cas)

La séquence d’authentification par serveur RADIUS s’effectue grâce aux protocoles **EAP** (entre le *supplicant* et *l’authenticator*) et **RADIUS** (entre *l’authenticator* et le serveur RADIUS). Les échanges de clés ou de couples *username/password* sont eux-mêmes cryptés.

|  |
| --- |

1. La station essaye d’effectuer une association classique avec le PA
2. Le PA demande à la station une identification EAP (username/password)
3. La station envoie les credentials au PA qui les transmet au serveur Radius
4. Un processus de “challenge text” se déroule entre le serveur RADIUS et la station via le PA
5. En cas de succès, l’association est faite et la station a accès au réseau “derrière” le PA

# Création du domaine

|  |
| --- |

Ajouter un catalogue global puis laisser par défaut les autres options.

# 

# Création d’un Active Directory

## AD par défaut

|  |
| --- |

## 

## Création d’une unité d’organisation

|  |
| --- |

Nommer l’OU

|  |
| --- |

résultat :

|  |
| --- |

## 

## Création d’un utilisateur

|  |
| --- |

Résultat :

|  |
| --- |

# Installation des services de certificat Active Directory

Pour configurer les certificats, il faut ajouter ce rôle :

|  |
| --- |

Choisir la première option :

|  |
| --- |

Sélectionner le mode entreprise :

|  |
| --- |

Choisir la certification racine :

|  |
| --- |

On va maintenant créer une clé privée :

|  |
| --- |

Cocher la case

|  |
| --- |

Ne rien toucher.

|  |
| --- |

Emplacement des BDD :

|  |
| --- |

Clic sur configurer et laisser Windows faire.

Ensuite, exporter le certificat pour pouvoir l’installer sur les téléphones.

# Création du RADIUS

## Installation

Installer le service “Services de stratégie et d’accès réseau”

|  |
| --- |

Message de confirmation

|  |
| --- |

## 

## Configuration

page d’accueil

|  |
| --- |

|  |
| --- |
| On va créer un client RADIUS (le point Wi-Fi) |

|  |
| --- |

## Créer une stratégie de demande de connexion

|  |
| --- |

Edition de la stratégie :

|  |
| --- |
| Laisser “non spécifié” car cela concerne les VPN et bureau à distance : |

Dans “Conditions”, ajouter un type de port NAS et cocher les connexions 802.11.

|  |
| --- |
|  |
|  |

Dans l’onglet “Paramètres”, on va choisir la méthode d’authentification.

|  |
| --- |
| Choisir “PEAP” et le modifier, vérifier qu’il utilise bien le certificat précédemment créé : |
| Il n’y a plus qu’à appliquer. |

## Créer une stratégie réseau

|  |
| --- |

|  |
| --- |

Ajouter le groupe Windows, prendre le groupe wifi créé dans l’AD précédemment

|  |
| --- |

| Accorder l’accès à l’utilisateur |
| --- |
|  |

| Choisir les méthodes d’authentification |
| --- |
|  |

La configuration est terminée, il faut ajouter le NPS dans l’AD.

Dans “stratégies réseau” :

|  |
| --- |
| Mettre “port NAS sans fil” |
| Dans contraintes, utiliser le PEAP, vérifier que le certificat précédemment créé est bien utilisé : |

## 

## Insertion NPS dans l’AD

|  |
| --- |

|  |
| --- |

Activer le WPA2 Enterprise avec le secret créé (groupe3) sur le routeur WIFI, laisser le port par défaut. Renseigner le secret dans la configuration de la borne Wi-Fi.

# 

# Résultat

Au préalable, installer le certificat ([ici](https://drive.google.com/open?id=1GFozRVvobLiZCFtcwqXrIVaoDqk9LWuo)) sur le téléphone.

On constate que la connexion est réussie

|  |
| --- |
| Vue du message 4400 : |
| Il s’agit de la connexion entre le serveur RADIUS et la borne Wi-Fi. |
| Message 6272 : |
| Le téléphone s’est connecté avec succès, on peut voir les informations suivantes : |
| Informations du serveur NAS (borne Wi-Fi) |
| Information sur la stratégie de sécurité utilisée : |

# Mise en place de GPO

[DOC GPO](https://docs.google.com/document/d/1Wo-AqbTGtlo27W0FAmPxOUWEJ5xRiFq9GQXhhkI6BJI/edit#)

# Mise en place de la borne Wi-Fi

[DOC Wi-Fi](https://docs.google.com/document/d/1swIOwSZXIpIXM8ZSa5H22WEP_vNVDnlhsH7HJKLMvFY/edit)