

Projet Radius

Serveur RADIUS

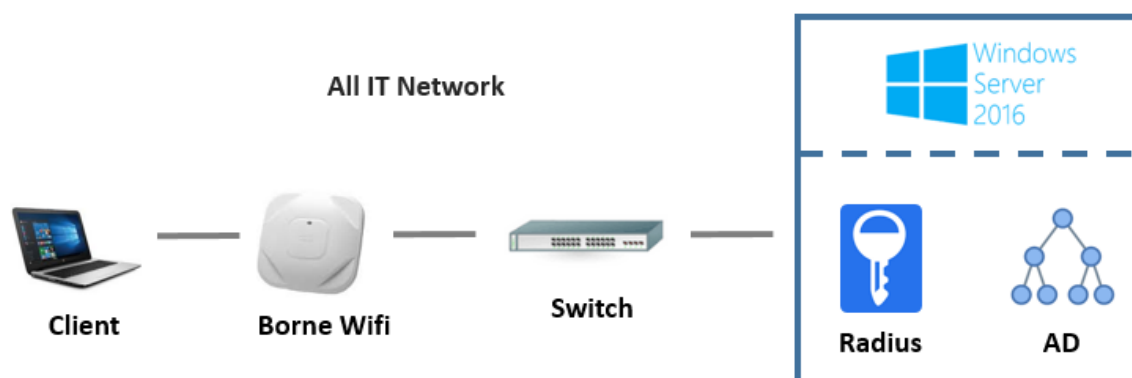
RADIUS (*Remote Authentication Dial-In User Service*) est un protocole client-serveur permettant de centraliser des données d'authentification. Le fonctionnement du service **RADIUS** est basé sur un système client/serveur qui va avoir pour rôle de définir les accès d'utilisateurs distants à un réseau.

Dans ce tutoriel, nous allons mettre en place un serveur **RADIUS** pour l'utiliser dans l'authentification WiFi, afin de sécuriser au maximum l'accès au réseau sans fil. A la place d'utiliser une clé pour se connecter au réseau, nous allons utiliser les informations d'authentification d'un Active Directory. Si vous n'avez pas d'Active Directory vous pouvez [consulter cet article](#) qui va vous expliquer comment mettre en place celui-ci. Je vous conseille également d'avoir [un serveur DHCP sur votre réseau](#), sinon vous devrez effectuer la configuration réseau de vos équipements manuellement. Ce tutoriel va être réalisé sur Windows Server 2016.

Mise en place serveur

Schéma de l'infrastructure

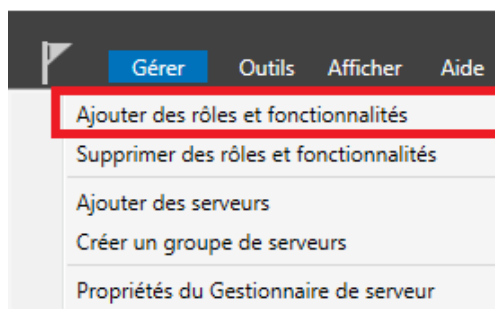
Voici l'infrastructure que nous allons mettre en place :



Lorsqu'un client va se connecter au réseau (SSID) présent sur la borne Wifi. Celle-ci va transmettre la requête au serveur **RADIUS**. Le serveur va ensuite vérifier si les identifiants de sessions de la personne sont bien présents sur l'Active Directory, si c'est le cas l'accès est autorisé sinon l'accès est refusé. Dans ce tutoriel l'Active Directory et le **RADIUS** sont sur le même serveur mais vous pouvez les installer sur deux serveurs différents.

Installation Rôle

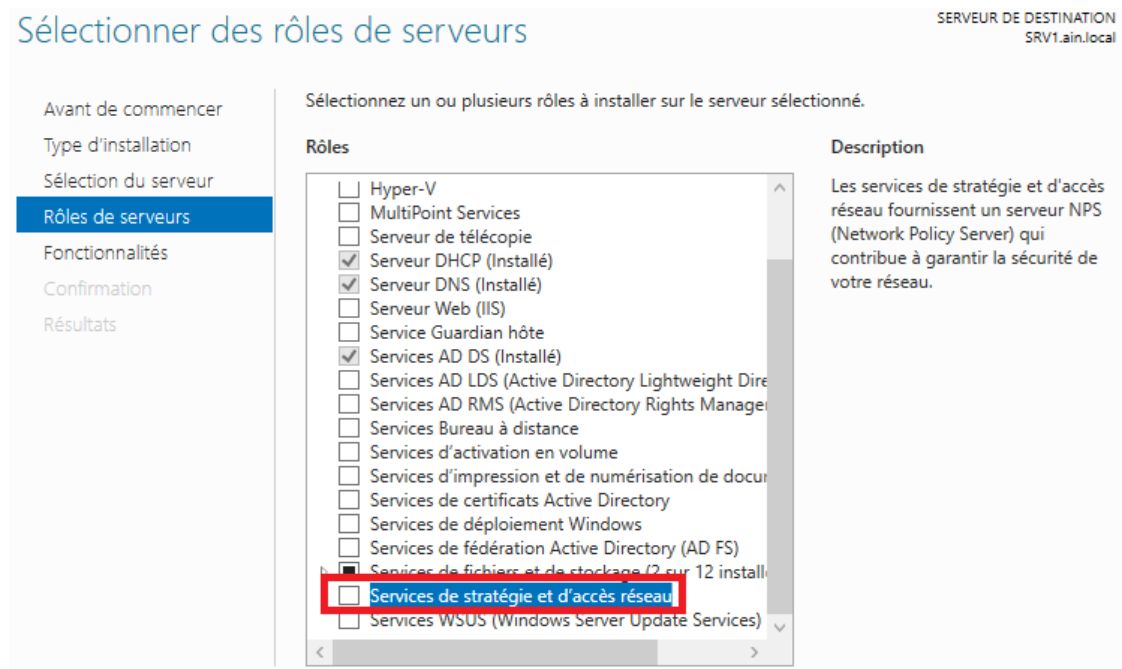
Pour commencer, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».



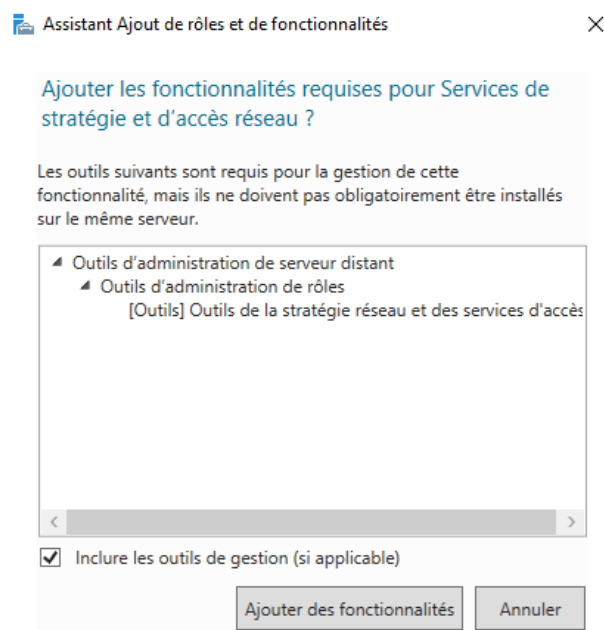
Sur la première fenêtre laissez coché « Installation basée sur un rôle ou une fonctionnalité ».



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 ».

Confirmer les sélections d'installation

SERVEUR DE DESTINATION
SRV1.ain.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'accès
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

☒ Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès
Services de stratégie et d'accès réseau

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

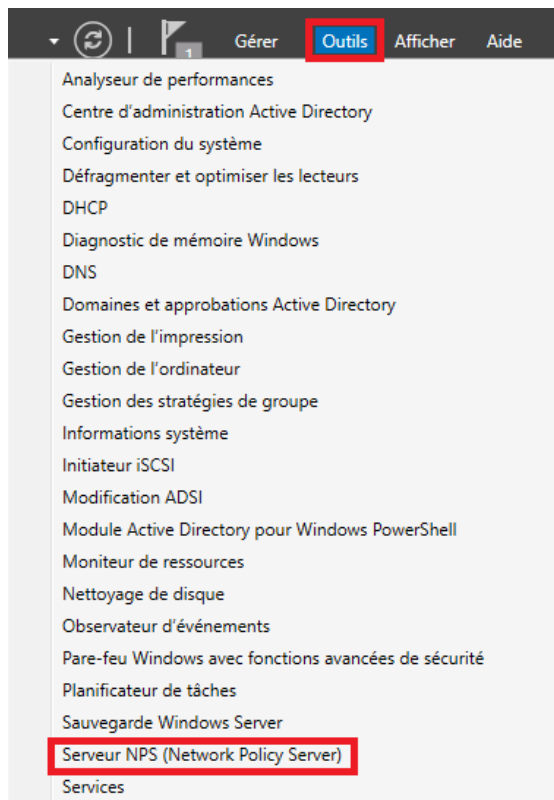
< Précédent Suivant > Installer Annuler

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

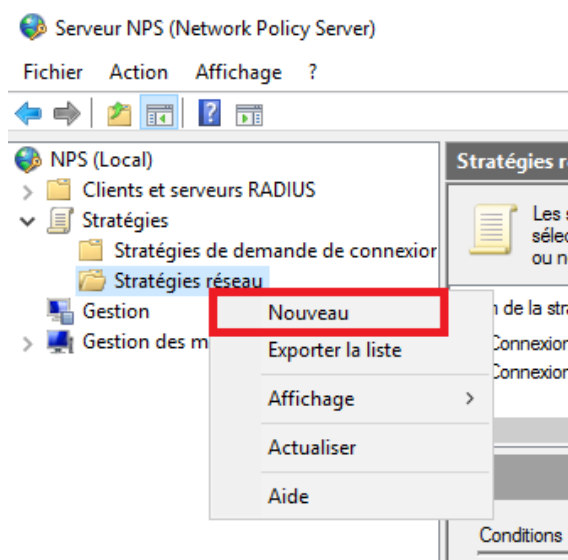
Configuration rôle

Définition du profil

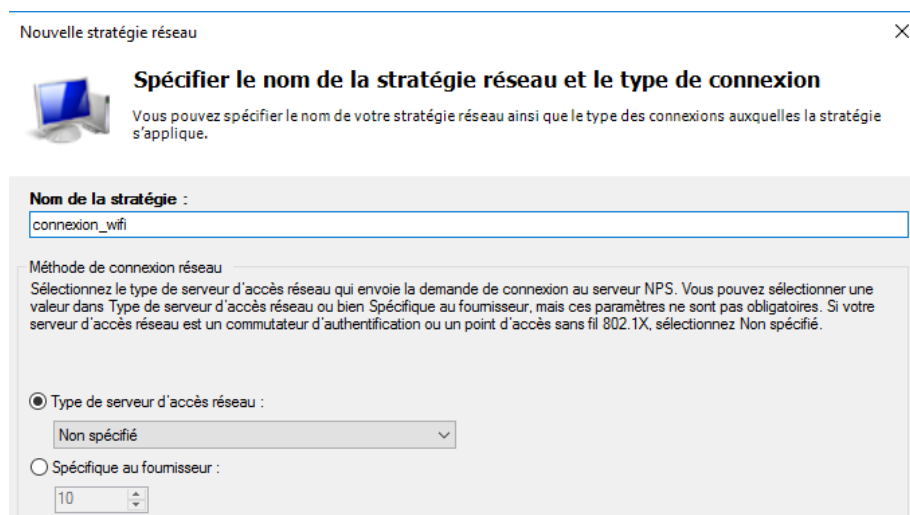
Maintenant que le rôle est installé nous allons devoir le configurer. Pour cela dans le gestionnaire de serveur cliquez sur « Outils » puis sur « Serveur NPS (Network Policy Server) ».



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 ».



Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

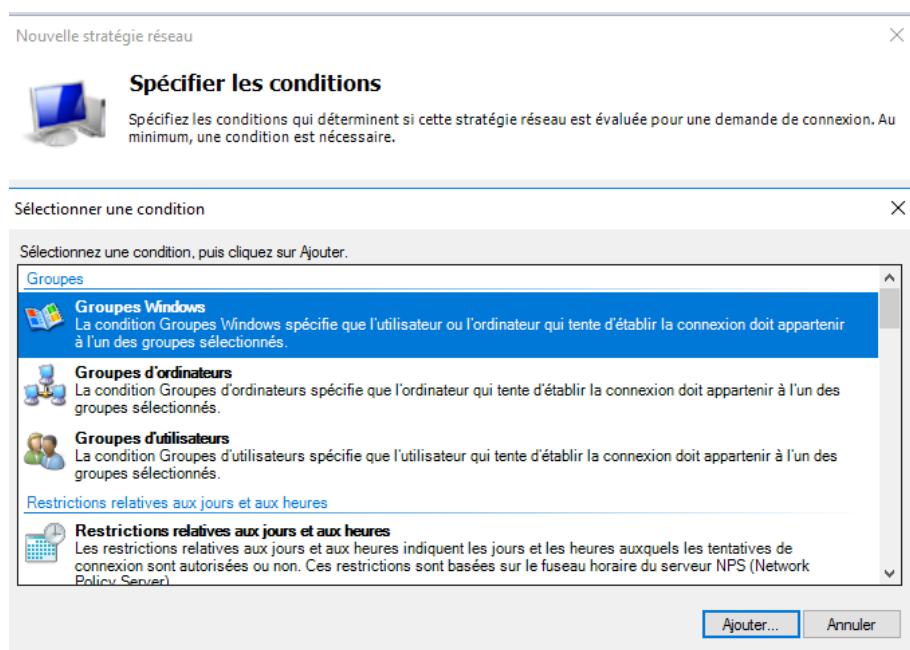
Nom de la stratégie :
connexion_wifi

Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :
Non spécifié

☐ Spécifique au fournisseur :
10

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



Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

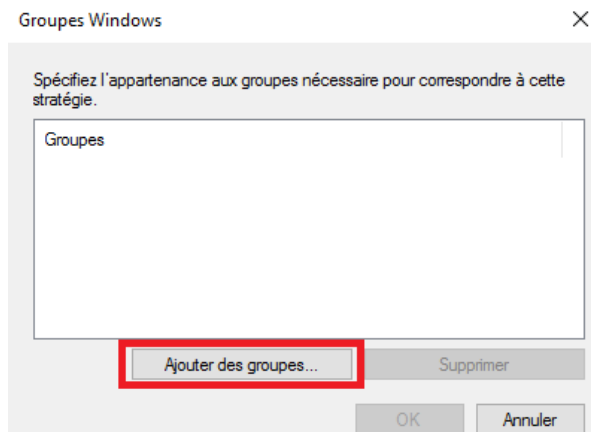
- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

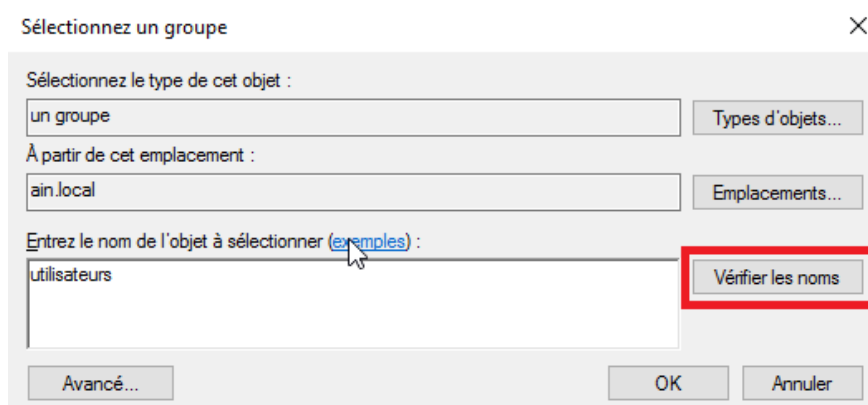
Ajouter... Annuler

Cliquez sur « Ajouter des groupes ».

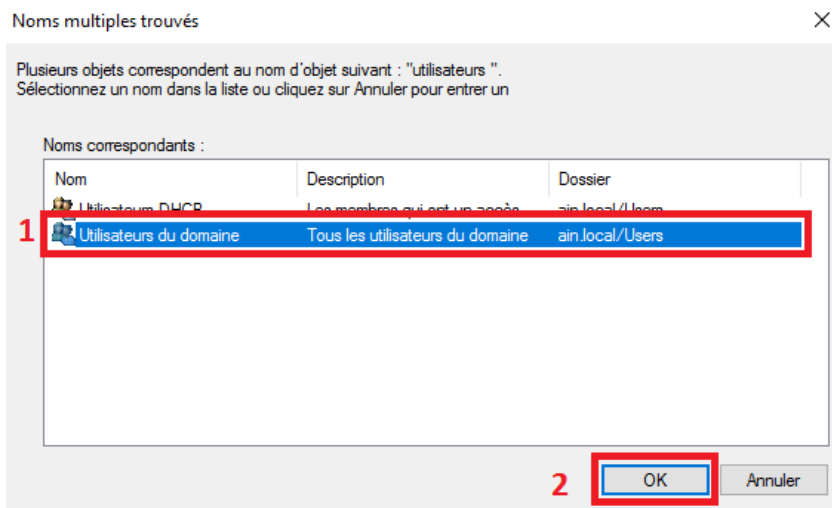


Vous allez ensuite devoir sélectionner le groupe. Sachez que je vais prendre un groupe qui contient tous les utilisateurs du domaine. Vous pouvez restreindre l'accès en créant un groupe sur l'Active Directory et en intégrant à ce groupe les utilisateurs pouvant se connecter au réseau WiFi en question.

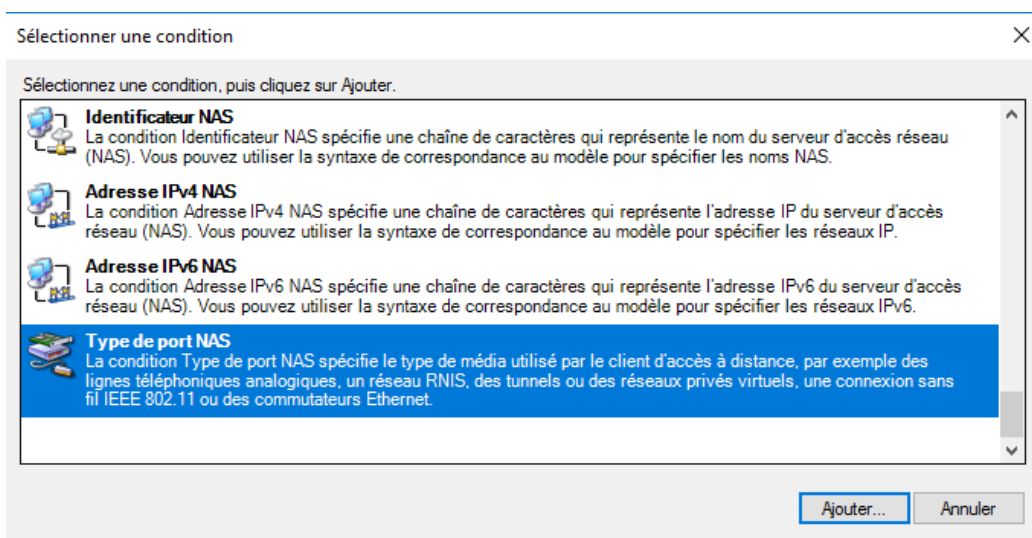
Écrivez utilisateurs et cliquez sur « Vérifier les noms »



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.

Spécifiez les types de médias d'accès nécessaires pour correspondre à cette stratégie.

Types de tunnels pour connexions d'accès à distance et VPN standard

☐ Asynchrone (Modem)
☐ RNIS synchrone
☐ Synchrone (ligne T1)
☐ Virtuel (VPN)

Types de tunnels pour connexions 802.1X standard

☐ Ethernet
☐ FDDI
☒ Sans fil - IEEE 802.11
☐ Token Ring

Autres

☐ RNIS synchrone
☒ Sans fil - Autre
☐ SDSL - DSL symétrique
☐ Synchrone (ligne T1)

OK Annuler

Laissez coché « Accès accordé » et cliquez sur « Suivant ».

Nouvelle stratégie réseau

×



Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ Accès accordé

Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ Accès refusé

Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)

Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

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



Configurer les méthodes d'authentification

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter...

Modifier...

Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
 - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

Précédent

Suivant

Terminer

Annuler

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

Ajouter des protocoles EAP



Méthodes d'authentification :

Microsoft: Carte à puce ou autre certificat

Microsoft: PEAP (Protected EAP)

Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

<

>

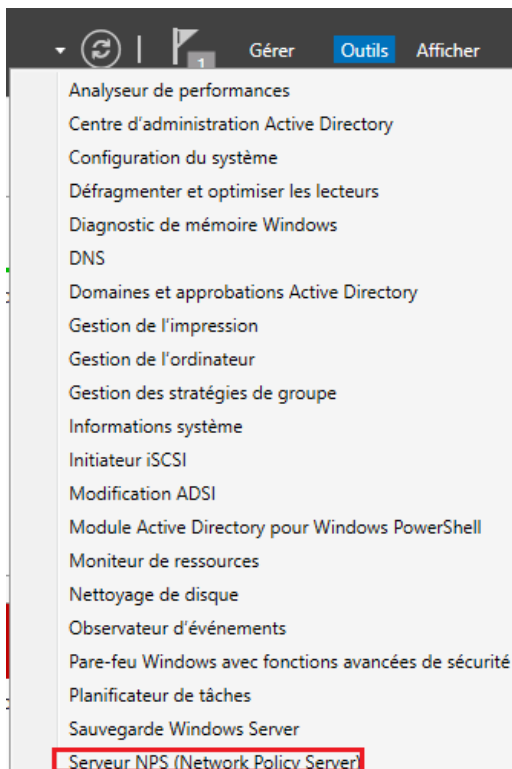
OK

Annuler

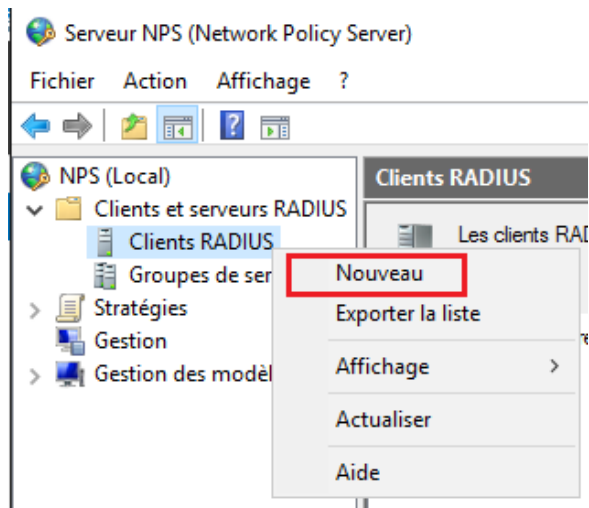
Sur la fenêtre suivante « Configurer des contraintes », laissez par défaut et cliquez sur « Suivant ». Faites de même pour la fenêtre « Configurer les paramètres ». Une fenêtre récapitulant la configuration va apparaître cliquez sur « Terminer ».

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 coché « 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 coché « Manuel » et renseignez la clé que vous saisirez aussi sur la borne WiFi.

Cliquez ensuite sur « OK ».

Nouveau client RADIUS



Paramètres

Avancé

☒ Activer ce client RADIUS☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel☐ Générer

Secret partagé :

Confirmez le secret partagé :