

Documentation : Intégration de RADIUS avec pfSense et Création des Groupes AD

1. Introduction

Dans cette documentation, nous allons mettre en place **un serveur RADIUS basé sur Windows Server (NPS)** et l'intégrer à **pfSense**. L'objectif est de gérer **l'authentification centralisée** pour les accès à pfSense via **Active Directory (AD)**. Nous allons également créer des groupes "Admin" et "Invité" dans une OU spécifique afin de gérer les niveaux d'accès.

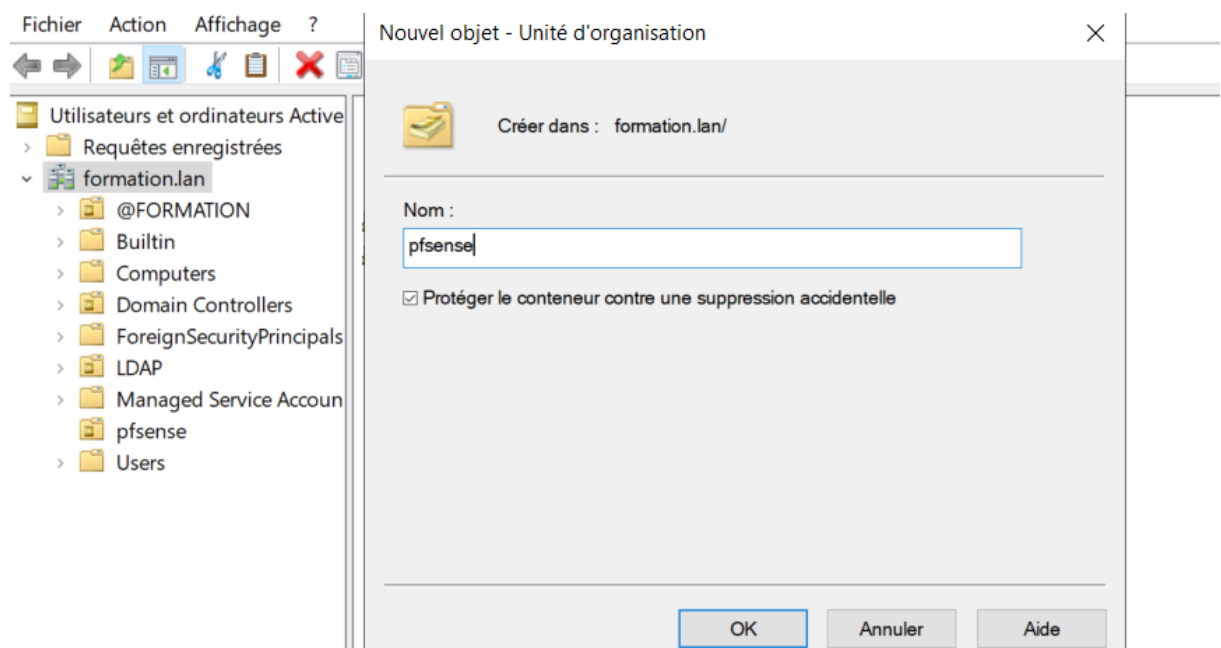
2. Prérequis

- Windows Server avec Active Directory fonctionnel.
- pfSense installé et configuré sur le réseau
- Network Policy Server (NPS) installé sur Windows Server.
- Communication réseau entre pfSense et Windows Server (ports RADIUS 1812 et 1813 ouverts).

3. Création de l'OU et des Groupes dans Active Directory

3.1 Création de l'Unité d'Organisation (OU) "pfSense"

1. Ouvrir "Active Directory Users and Computers > Clic droit sur ton domaine > Nouveau > Unité d'organisation.



3.2 Création des Groupes d'Accès

- 4 Dans l'OU pfSense, faire un **clic droit** > **Nouveau** > **Groupe** > **Créer le groupe "Admin"** :

Nom : pfSense-Admins.

The screenshot shows the 'Général' tab of the Group Creation Wizard. The group name is 'pfSense-Admins'. The 'Nom de groupe (antérieur à Windows 2000)' field contains 'pfSense-Admins'. The 'Description' and 'Adresse de messagerie' fields are empty. Under 'Étendue du groupe', 'Globale' is selected. Under 'Type de groupe', 'Sécurité' is selected.

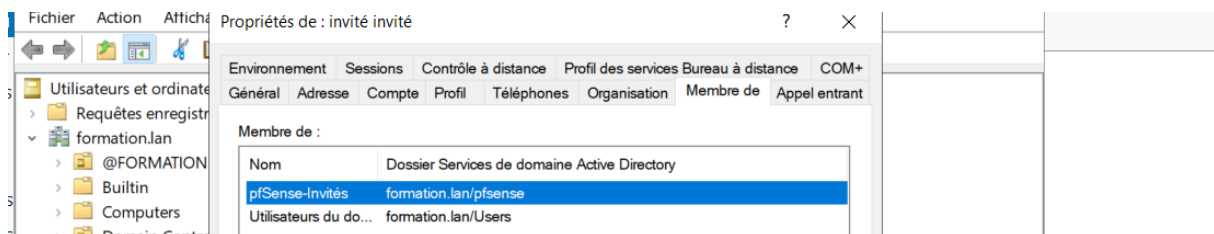
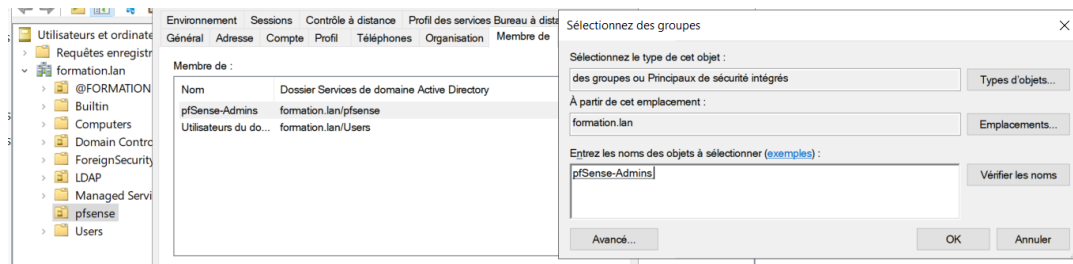
Nom : pfSense-Invités

The screenshot shows the 'Général' tab of the Group Creation Wizard. The group name is 'pfSense-Invités'. The 'Nom de groupe (antérieur à Windows 2000)' field contains 'pfSense-Invités'. The 'Description' and 'Adresse de messagerie' fields are empty. Under 'Étendue du groupe', 'Globale' is selected. Under 'Type de groupe', 'Sécurité' is selected. A 'Remarques' field is visible at the bottom.

3.3 Ajout des Utilisateurs aux Groupes

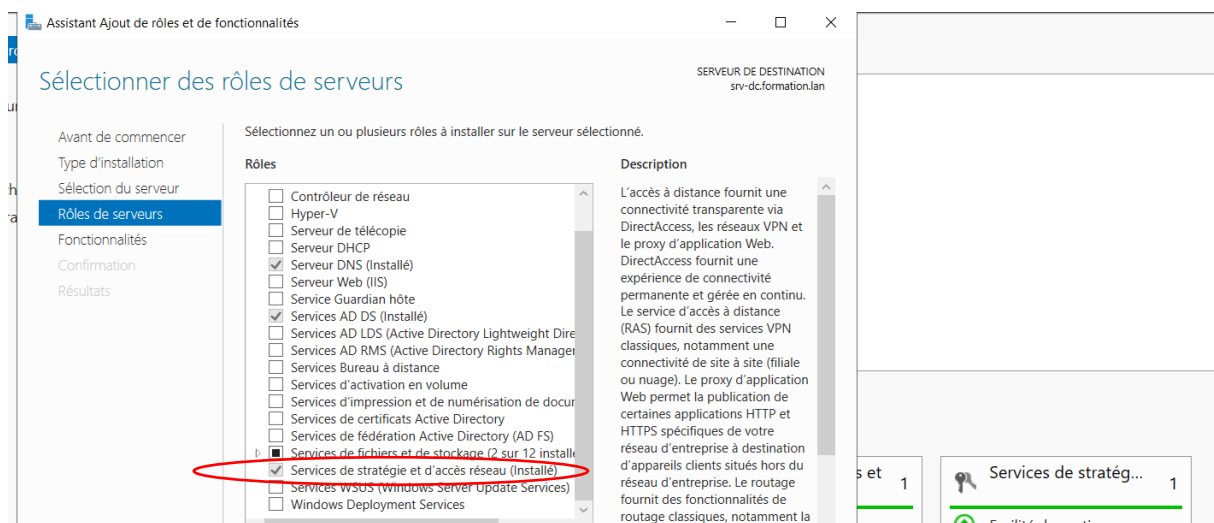
1. Dans l'OU pfSense, faire un **clic droit sur un utilisateur** > **Propriétés** > **"Membre de"**, puis **Ajouter** :

RADIUS & PFSENSE



4. Installation et Configuration du Serveur RADIUS (NPS) sur Windows Server

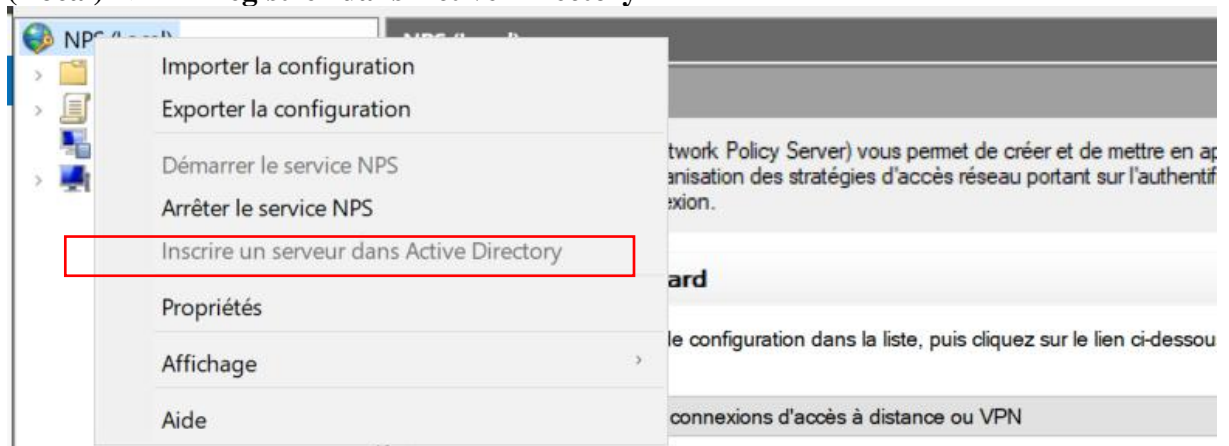
4.1 Installation du Rôle NPS



4.2 Enregistrer NPS dans Active Directory

RADIUS & PFSense

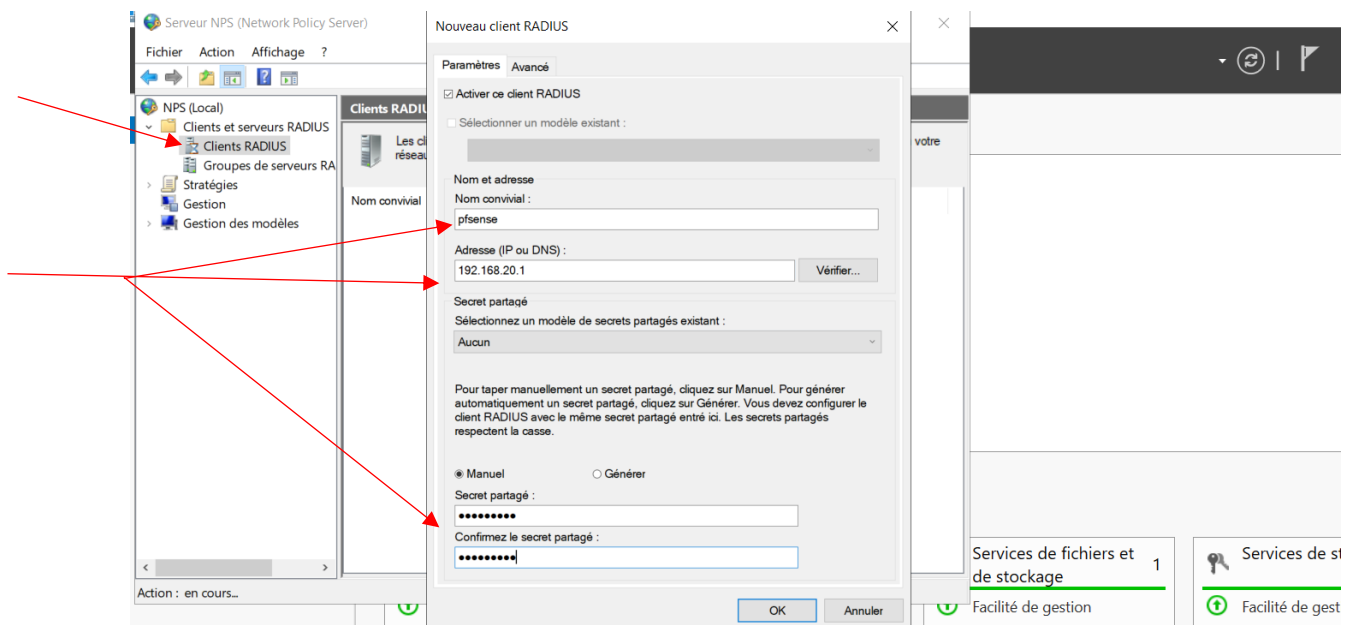
1. **Ouvrir NPS via Outils > Network Policy Server >> Faire un clic droit sur "NPS (Local)" > "Enregistrer dans Active Directory"**



4.3 Ajouter pfSense comme Client RADIUS

- 5 Dans NPS, aller dans "RADIUS Clients et Serveurs" > "Clients RADIUS" > Clic droit > Nouveau.

Remplir les champs :



4.4 Création des Politiques d'Accès

1. Aller dans "Stratégies" > "Stratégies de réseau" > Créer une nouvelle stratégie pour les Admins :
 - o Nom : Accès_Admin_pfSense.

RADIUS & PFSENSE

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 :

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 :

☐ Spécifique au fournisseur :

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.

Condition	Valeur
Sélectionner 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 appartient à l'un des groupes sélectionnés.
	Groupes d'ordinateurs La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion appartient à l'un des groupes sélectionnés.
	Groupes d'utilisateurs La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion appartient à l'un des groupes sélectionnés.
Restrictions relatives aux jours et aux heures Les restrictions relatives aux jours et aux heures indiquent les jours et les heures de la semaine pour lesquels la connexion est autorisée ou non. Ces restrictions sont basées sur le fuseau horaire du serveur.	

Description de la condition :

Sélectionner un groupe

Sélectionnez le type de cet objet :

À partir de cet emplacement :

Entrez le nom de l'objet à sélectionner (exemples) :

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.

RADIUS & PFSENSE

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 :

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

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.

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

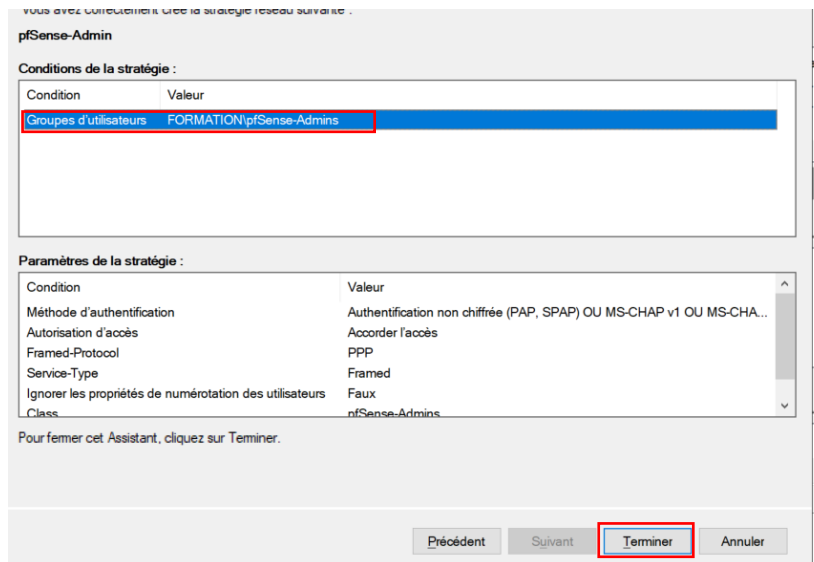
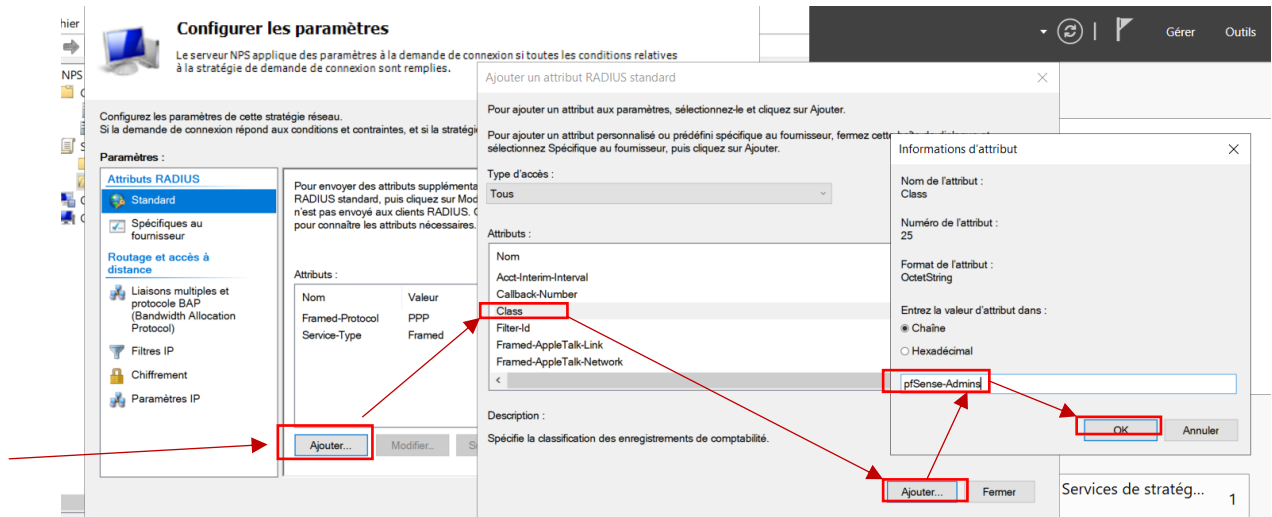
Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

☐ Déconnecter au-delà de la durée d'inactivité maximale

1

Précédent **Suivant** Terminer Annuler

RADIUS & PFSense



2. Créer une politique pour les invités : même étape pour pfsense-Invités



Appliquer et redémarrer NPS.

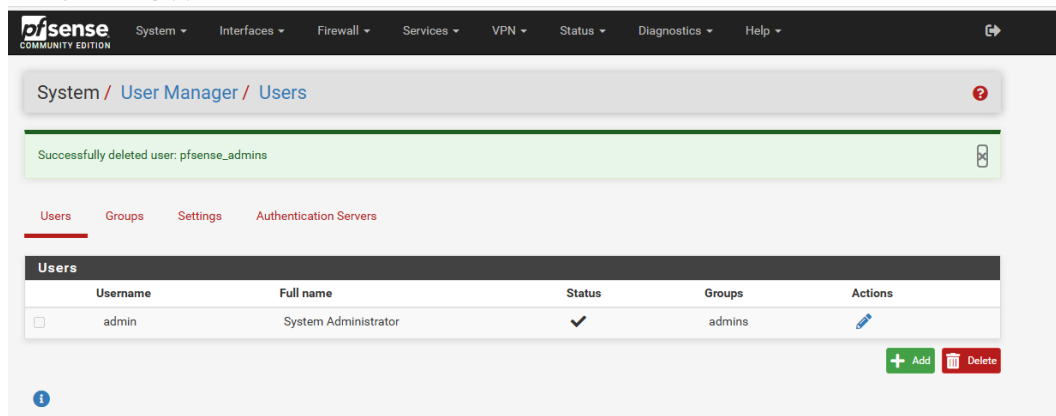
5. Configuration de pfSense pour Utiliser RADIUS

5.1 Ajout du Serveur RADIUS dans pfSense

RADIUS & PFSense

1. Se connecter à pfSense > Aller dans **"System"** > **"User Manager"** > **"Servers"** >>

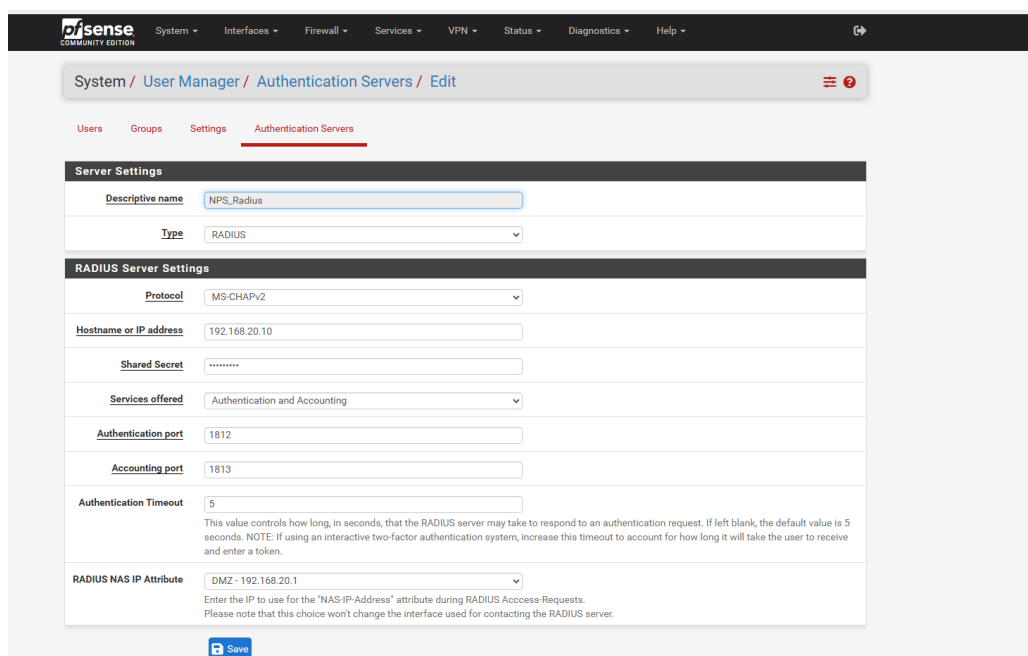
.168.10.1/system_usermanager.php



The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / User Manager / Users. A green message box states "Successfully deleted user: pfsense_admins". Below this, there are tabs for Users, Groups, Settings, and Authentication Servers. The Users tab is active, displaying a table with columns: Username, Full name, Status, Groups, and Actions. The table contains one entry: admin (System Administrator) with a status of checked and a group of admins. At the bottom right, there are buttons for Add and Delete.

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	Edit

2. Remplir les champs :



The screenshot shows the pfSense web interface for editing an authentication server. The breadcrumb trail is System / User Manager / Authentication Servers / Edit. The Authentication Servers tab is active. The form is divided into two sections: Server Settings and RADIUS Server Settings. The Server Settings section includes fields for Descriptive name (NPS_Radius) and Type (RADIUS). The RADIUS Server Settings section includes fields for Protocol (MS-CHAPv2), Hostname or IP address (192.168.20.10), Shared Secret (masked), Services offered (Authentication and Accounting), Authentication port (1812), Accounting port (1813), Authentication Timeout (5), and RADIUS NAS IP Attribute (DMZ - 192.168.20.1). A Save button is at the bottom.

Server Settings

Descriptive name: NPS_Radius

Type: RADIUS

RADIUS Server Settings

Protocol: MS-CHAPv2

Hostname or IP address: 192.168.20.10

Shared Secret: *****

Services offered: Authentication and Accounting

Authentication port: 1812

Accounting port: 1813

Authentication Timeout: 5

RADIUS NAS IP Attribute: DMZ - 192.168.20.1

Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

[Save](#)

3. Sauvegarder et appliquer les paramètres.

Système / Gestionnaire d'utilisateurs / Groupes / Modifier

Utilisateurs **Groupes** Paramètres Serveurs d'authentification

Propriétés du groupe

Nom de groupe pfsense-admin

Portée Distant
Avertissement : La modification de ce paramètre peut affecter le fichier des groupes locaux, auquel cas un redémarrage peut être nécessaire pour que les modifications prennent effet.

Description Groupe MS ADDS
Description du groupe, uniquement pour information administrative

Appartenance à un groupe

admin

Non membres Membres

>> Passer à "Membres" << Passer à "Non membres"

Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.

Enregistrer

6. Tests et Validation

6.1 Tester l'Authentification RADIUS sur pfSense

1. Aller dans **Diagnostics > Authentication >> NPS_Radius** comme serveur d'authentification.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Diagnostics / Authentication

User fofana@formation.lan authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server NPS_Radius
Select the authentication server to test against.

Username fofana@formation.lan

Password

Debug ☐ Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

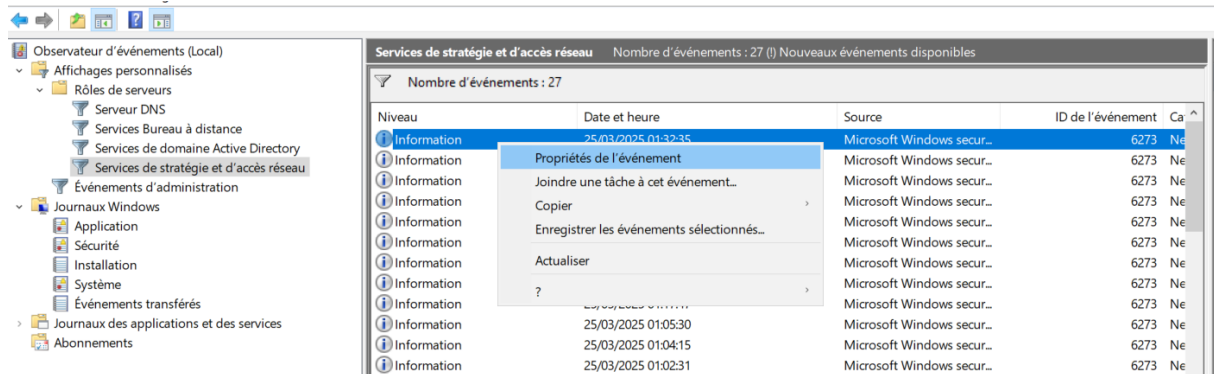
Test

NB : Si l'authentification ne passe pas

RADIUS & PFSENSE



Allez vérifier dans les évènements et vous aurez la cause du problème



Dans mon cas je dois donner l'autorisation d'appel entrant à mon utilisateur

