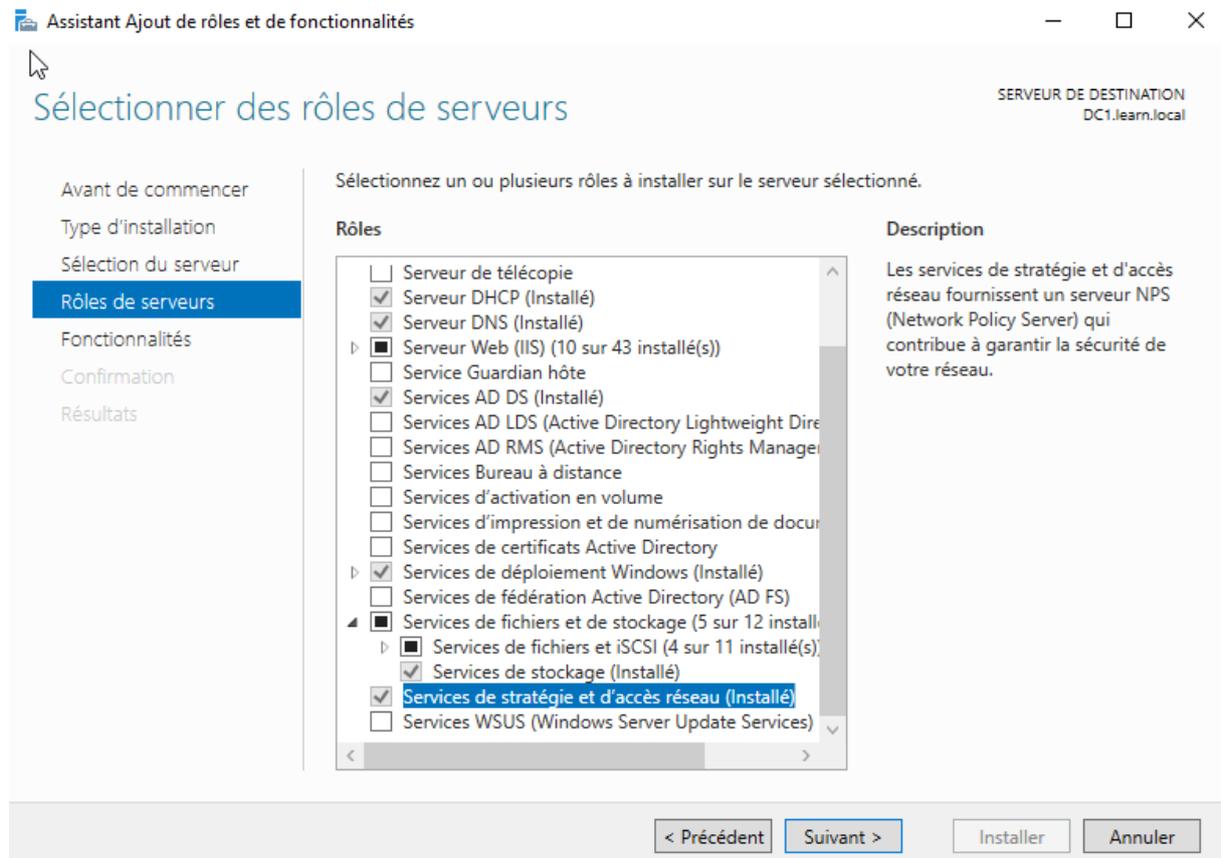
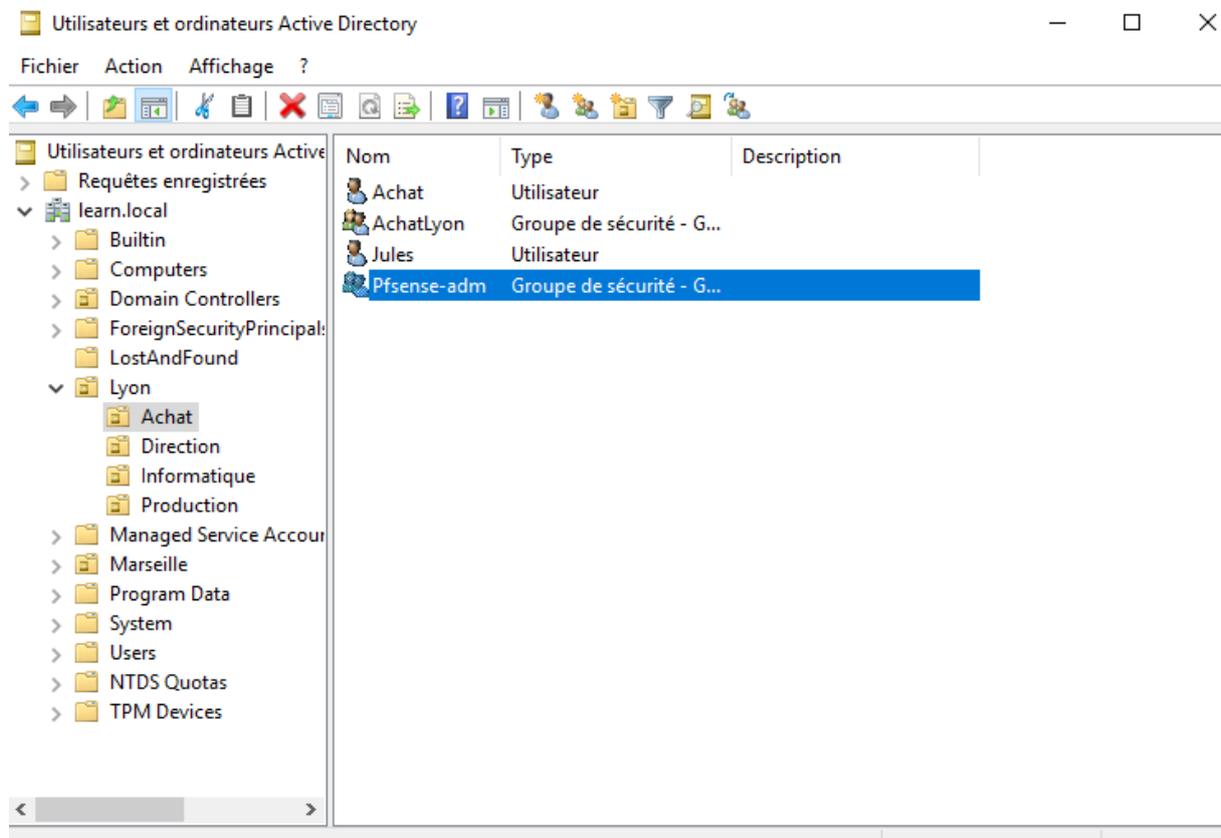


Ajouter NPS au serveur principal



Puis créer un groupe de sécurité Pfsense-adm et y ajouter votre utilisateur



Ajouter le serveur Pfsense grâce a son adresse ip

Server NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS
 - Gro
 - Stratégi
 - Gestion
 - Gestion

Clients RADIUS

Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre seau.

Nom	Adresse IP	Fabricant du périphérique	État
	10.1.1.8	RADIUS Standard	Activé

Affiche l'aide pour l'élément sélectionné.

Ajouter une nouvelle stratégie réseau en cliquant droit sur stratégie réseau

Server NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RA
 - Stratégies
 - Stratégies de demande
 - Stratégies réseau
 - Gestion
 - Gestion des modèles

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 : pfsense adm strategie

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

Précédent **Suivant** Terminer Annuler

Ajouter le groupe Pfsense adm

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.

Conditions :

Condition	Valeur
 Groupes d'utilisateurs	LEARN\Pfsense-adm

Description de la condition :

La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Activer le PAP

Nouvelle stratégie réseau



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.

Stratégie de demande de connexion



Vous avez sélectionné une ou plusieurs méthodes d'authentification non sécurisées. Pour vous assurer que chaque protocole est correctement configuré pour l'accès à distance, la stratégie et les niveaux de domaine, suivez les procédures détaillées dans l'aide.

Voulez-vous afficher la rubrique d'aide correspondante ?

Oui

Non

Précédent

Suivant

Terminer

Annuler

Ensuite on ajoute un attribut class

Propriétés de Pfsense strat

Vue d'ensemble Conditions Contraintes Paramètres

Configurer la demande de connexion

Ajouter un attribut RADIUS standard

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :
Tous

Attributs :

- Nom
- Acct-Interim-Interval
- Callback-Number
- Class**
- Filter-Id
- Framed-AppleTalk-Link
- Framed-AppleTalk-Network

Description :
Spécifie la classification des enregistrements de comptabilité.

Ajouter... Fermer

OK Annuler Appliquer

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les paramètres de cette stratégie réseau.
Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

Standard

Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Class	pfSense adm

Paramétrer le serveur web pfSense comme ci-dessous

Server Settings

Descriptive name NPS radius victor

Type RADIUS

RADIUS Server Settings

Protocol PAP

Hostname or IP address 10.1.1.1

Shared Secret ●●●●●●

Services offered Authentication and Accounting

Authentication port 1812

Accounting port 1813

Authentication Timeout 5
This value controls how long, in seconds, that the RADIUS server may take to respond to an authen blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system to account for how long it will take the user to receive and enter a token.

RADIUS NAS IP WAN - 10.10.2.205

C'est bon tout fonctionne si on s'authentifie

Diagnosics / Authentication

User Victor authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server NPS radius victor

Select the authentication server to test against.

Username

Password

Debug Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in for LDAP).

Voulez-vous stocker le mot de passe pour 10.1.1.8? [Plus d'informations](#)