

Ficher de procédure : Configuration serveur d'authentification Pfsense

Table des matières

Accéder au PfSense de Bordeaux (R3).....	2
Déclarer l'annuaire Active Directory sur Pfsense	2

Accéder au PfSense de Bordeaux (R3)

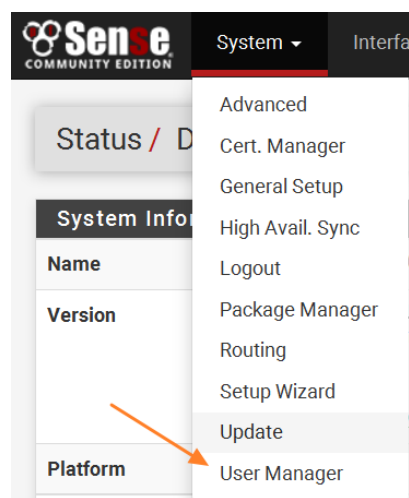
IP : 192.168.14.102

Login : admin

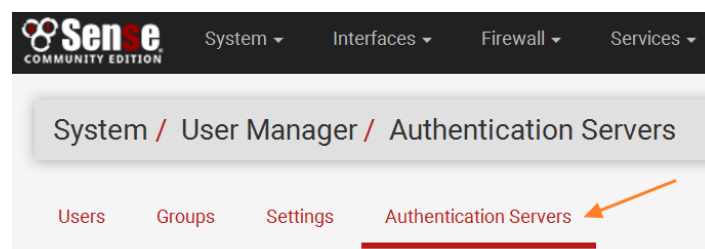
Mot de passe : R3holo3d

Déclarer l'annuaire Active Directory sur Pfsense

Cliquez sur le bouton "System" puis "User Manager" qui permet de gérer les utilisateurs et les groupes pfSense, ainsi que de configurer un serveur d'authentification.



Cliquez ensuite sur "Authentication Servers".



Renseignez les champs suivants :

Paramètres du serveur	
Nom descriptif	Portail captif
Type	LDAP
Paramètres serveur LDAP	
Nom d'hôte ou adresse IP	172.29.96.230 <small>NOTE : Lors de l'utilisation de SSL ou STARTTLS, ce nom d'hôte DOIT correspondre au Common Name (CN) du certificat SSL du serveur LDAP.</small>
Valeur du port	389
Transport	TCP - Standard
Autorité de certification du pair	Global Root CA List <small>cette option est utilisée si les options 'Chiffrement SSL' ou 'TCP - STARTTLS' sont choisies. Elle doit correspondre à la CA présente dans l'AD ou des problèmes vont survenir.</small>
Version du protocole	3
Délai de connexion au serveur	25 <small>Délai des opérations LDAP (secondes)</small>

- Nom : nom du serveur + domaine
- Type : LDAP
- Nom Hôte / IP : nom (si DNS) ou IP

Les autres paramètres sont à laisser par défaut.

La suite du paramétrage est :

Champ de recherche	Level Sous-arbre entier
	Base DN DC=h3d,DC=lan
Conteneurs d'authentification	CN=Users,DC=h3d,DC=lan <small>Remarque: Semi-Colon séparé. Cela sera remplacé par la base de recherche dn ci-dessus ou le chemin de conteneur complet peut être spécifié contenant un composant dc =. Exemple: CN=Utilisateurs; DC=exemple, DC=com ou OU=Personal; OU = Freelancers</small>
Requêtes étendues	<input type="checkbox"/> Activer les requêtes étendues
Lier anonyme	<input type="checkbox"/> Utilisez des liens anonymes pour résoudre des noms distincts
Lier les informations d'identification	CN=ahaugel,CN=Users,DC=h3d,DC=lan

*Attribut de nommage utilisateur	<input type="text" value="cn"/>
---	---------------------------------

<u>Attribut de nommage de groupe</u>	<input type="text" value="cn"/>
---	---------------------------------

<u>Attribut de membre du groupe</u>	<input type="text" value="member"/>
--	-------------------------------------

Groupes RFC 2307 Le serveur LDAP utilise des appartenances aux groupes de type RFC 2307
L'appartenance à un groupe de style RFC 2307 comporte des membres listés sur l'objet de groupe plutôt que d'utiliser des groupes répertoriés sur un objet utilisateur. Laissez désactiver pour l'appartenance au groupe de style Active Directory (RFC 2307bis).

Classe d'objet de groupe	<input type="text" value="group"/>
---------------------------------	------------------------------------

Classe d'objet utilisée pour les groupes en mode RFC2307. Généralement, "posixGroup" ou "groupe".

Encodage UTF8	<input type="checkbox"/> UTF8 encode les paramètres LDAP avant de les envoyer au serveur. Nécessaire pour prendre en charge les caractères internationaux, mais peut ne pas être pris en charge par chaque serveur LDAP.
----------------------	---

Altérations de nom d'utilisateur	<input type="checkbox"/> Ne pas oublier la partie du nom d'utilisateur après le symbole @ p. ex. utilisateur@hôte devient utilisateur lorsque décoché.
---	---

Appuyer sur sauvegarder pour enregistrer les modifications.