Authentification AD sur pfsense

Prérequis

- Avoir Pfsense installé
- Avoir un Active Directory fonctionnel
- Avoir mis en tant que DNS principal sur Pfsense votre Active Directory

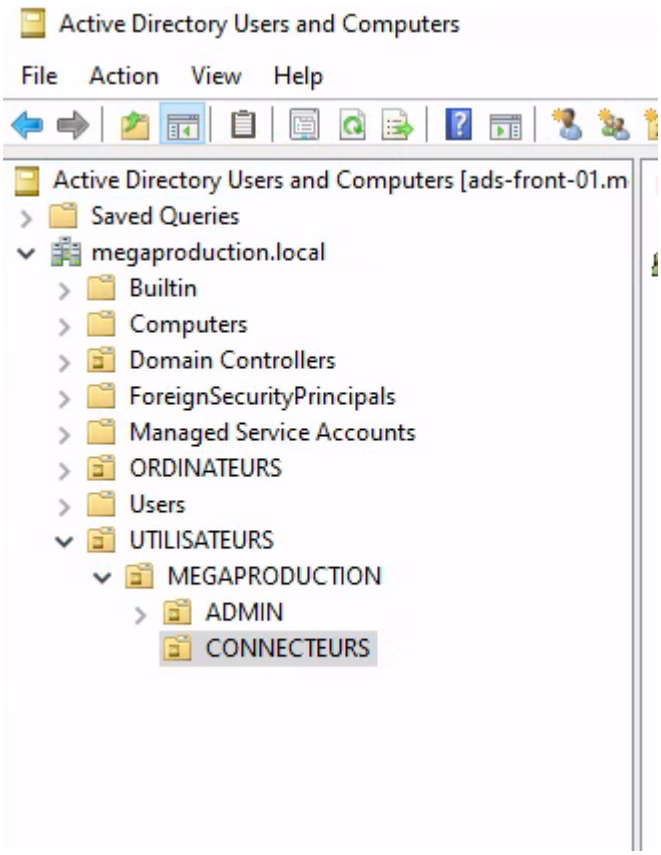
Préparation

Il vous faudra ici créer une OU, un groupe et un utilisateur spécifique afin de lié Pfsense à l'AD. Je m'explique, l'utilisateur créé nous permettra de lister les utilisateurs d'un ou plusieurs groupe AD.

Mise en place

Préparation des groupe active directory

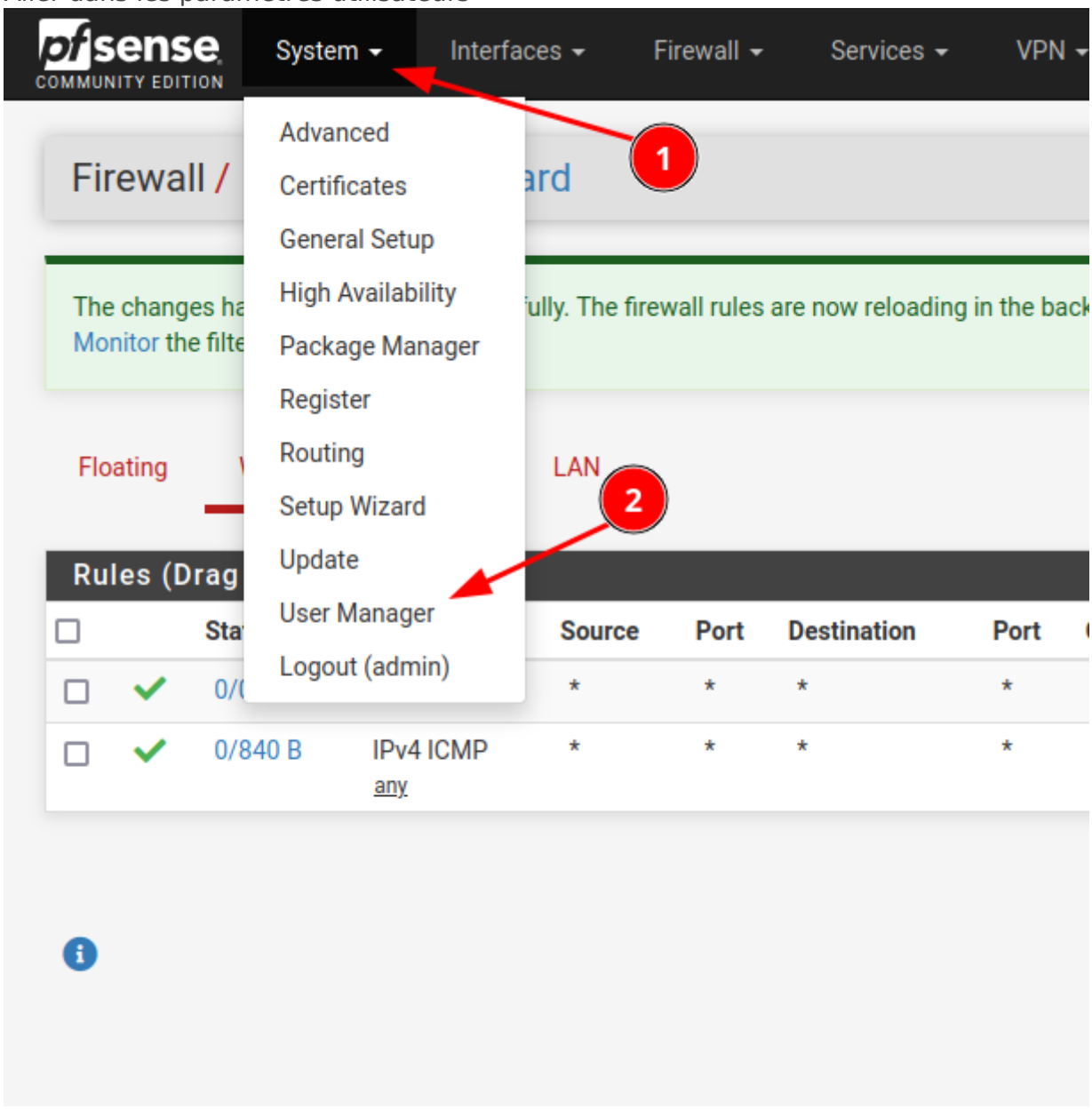
Voici l’arborescence de mon Active Directory



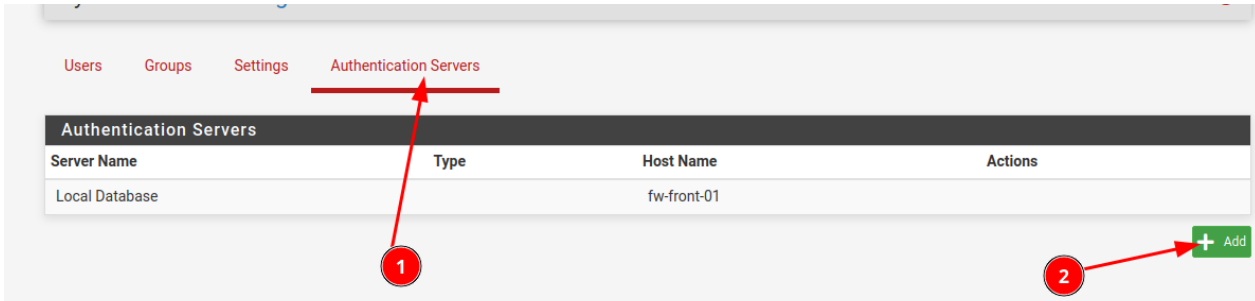
1. Créer un groupe GG_users_pfsense dans l'OU CONNECTEURS
2. Créer un utilisateur bind_pfsense et le mettre dans le groupe GG_users_pfsense

Préparation de Pfsense

1. Aller dans les paramètres utilisateurs



2. Ajouter un serveur d'authentification (Ne pas faire save à la fin)



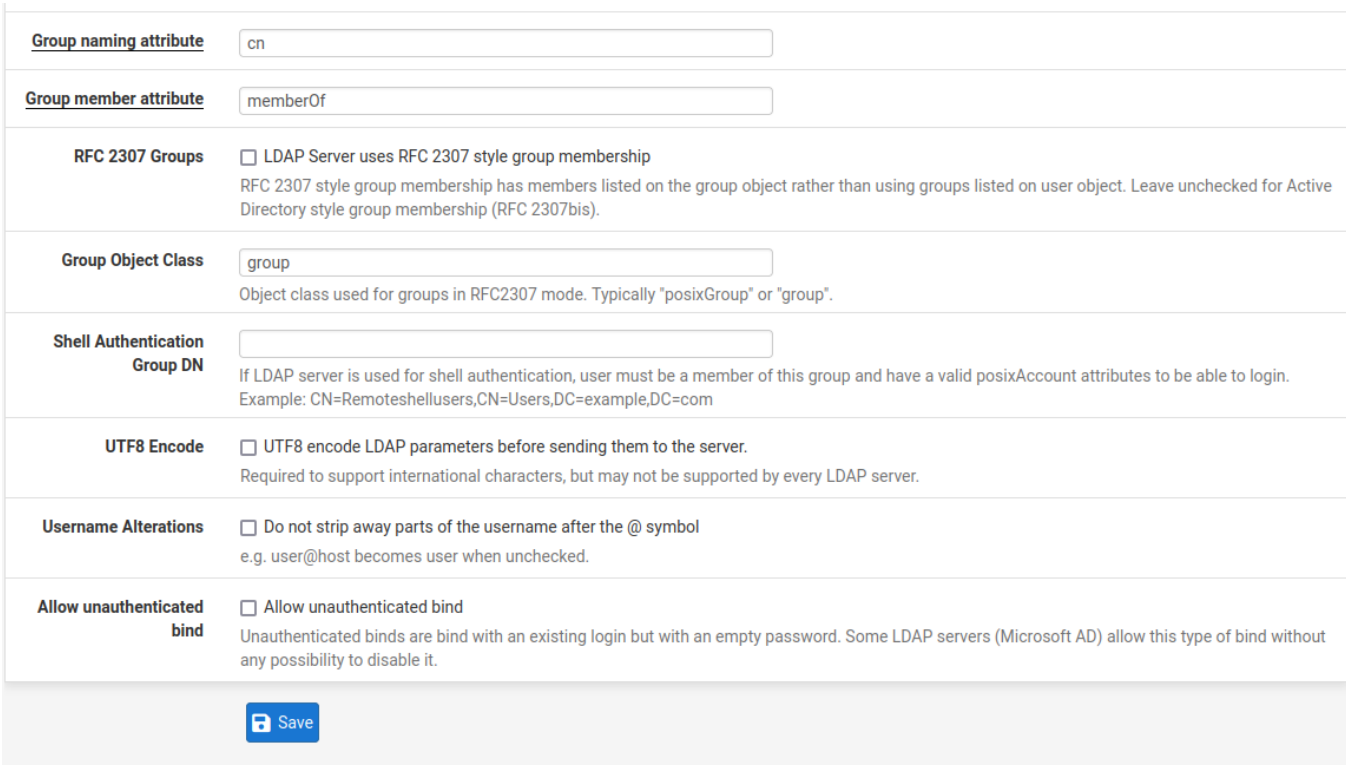
Users Groups Settings Authentication Servers

Server Settings

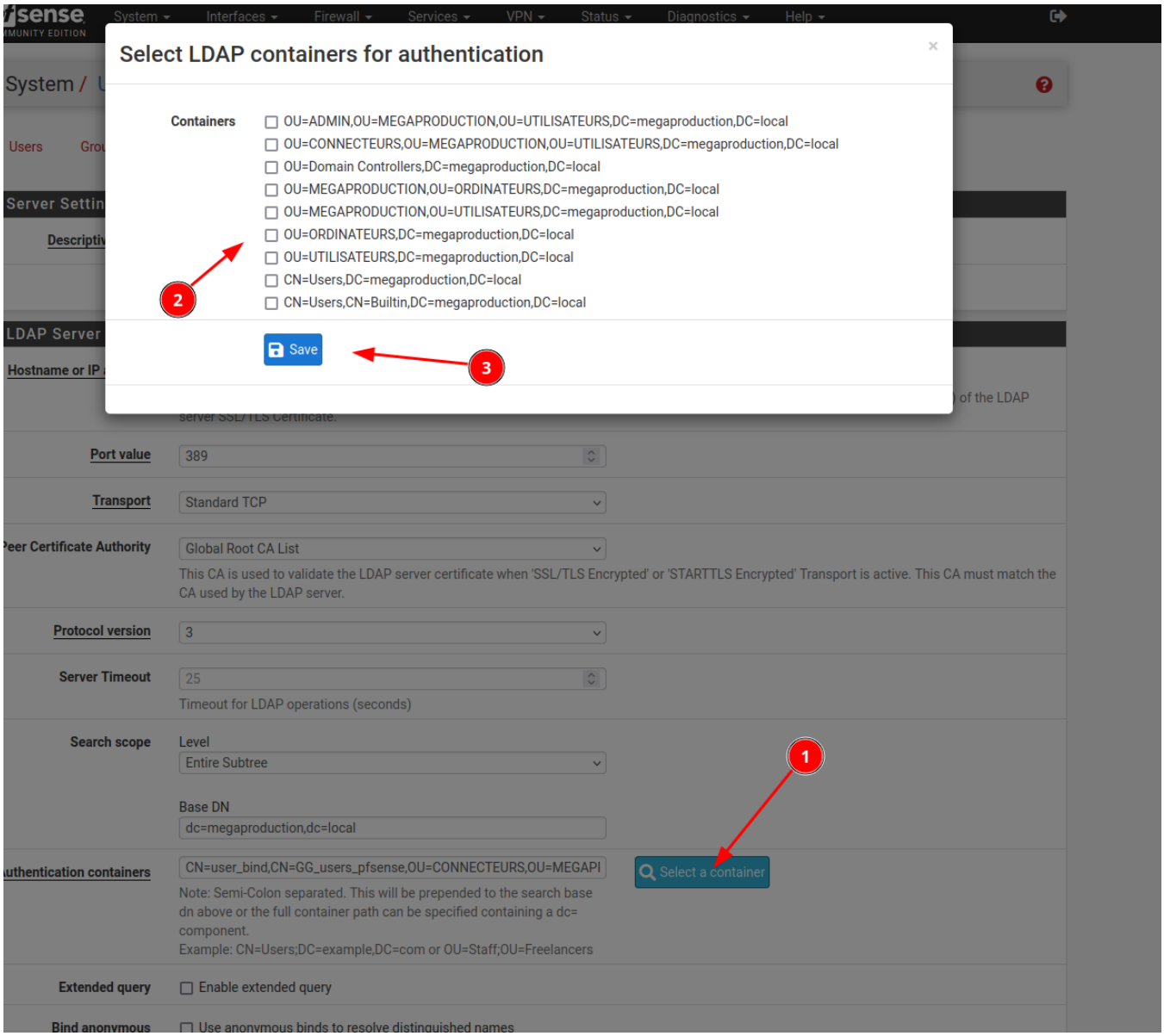
Descriptive name	ads-front-01
Type	LDAP

LDAP Server Settings

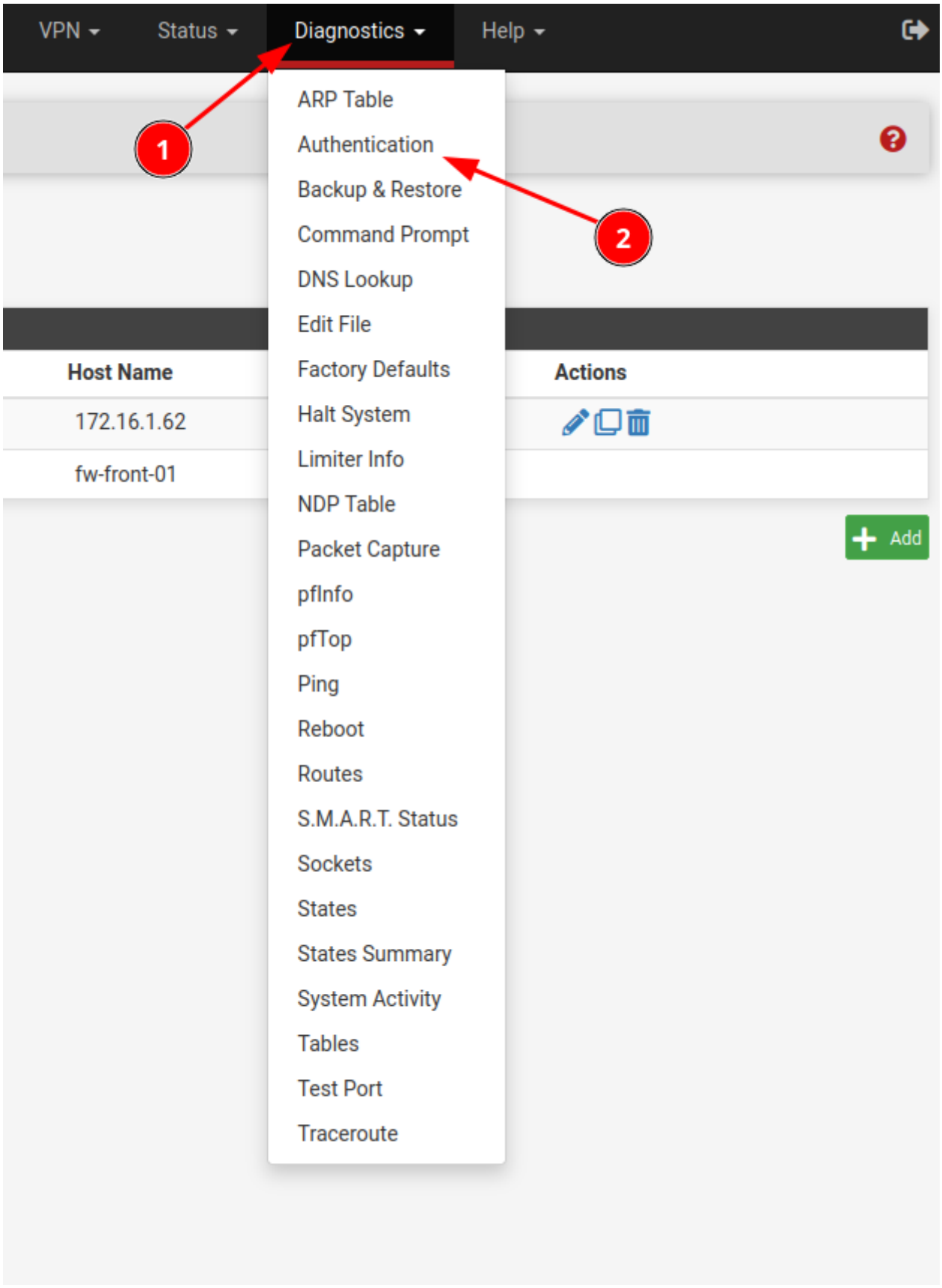
Hostname or IP address	172.16.1.62 NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.
Port value	389
Transport	Standard TCP
Peer Certificate Authority	Global Root CA List This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.
Protocol version	3
Server Timeout	25 Timeout for LDAP operations (seconds)
Search scope	Level Entire Subtree Base DN dc=megaproduction,dc=local
Authentication containers	CN=user_bind,CN=GG_users_pfsense,OU=CONNECTEURS,OU=MEGAPI Select a container Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers
Extended query	☐ Enable extended query
Bind anonymous	☐ Use anonymous binds to resolve distinguished names
Bind credentials	bind_pfsense •••••••
Initial Template	Microsoft AD
User naming attribute	samAccountName

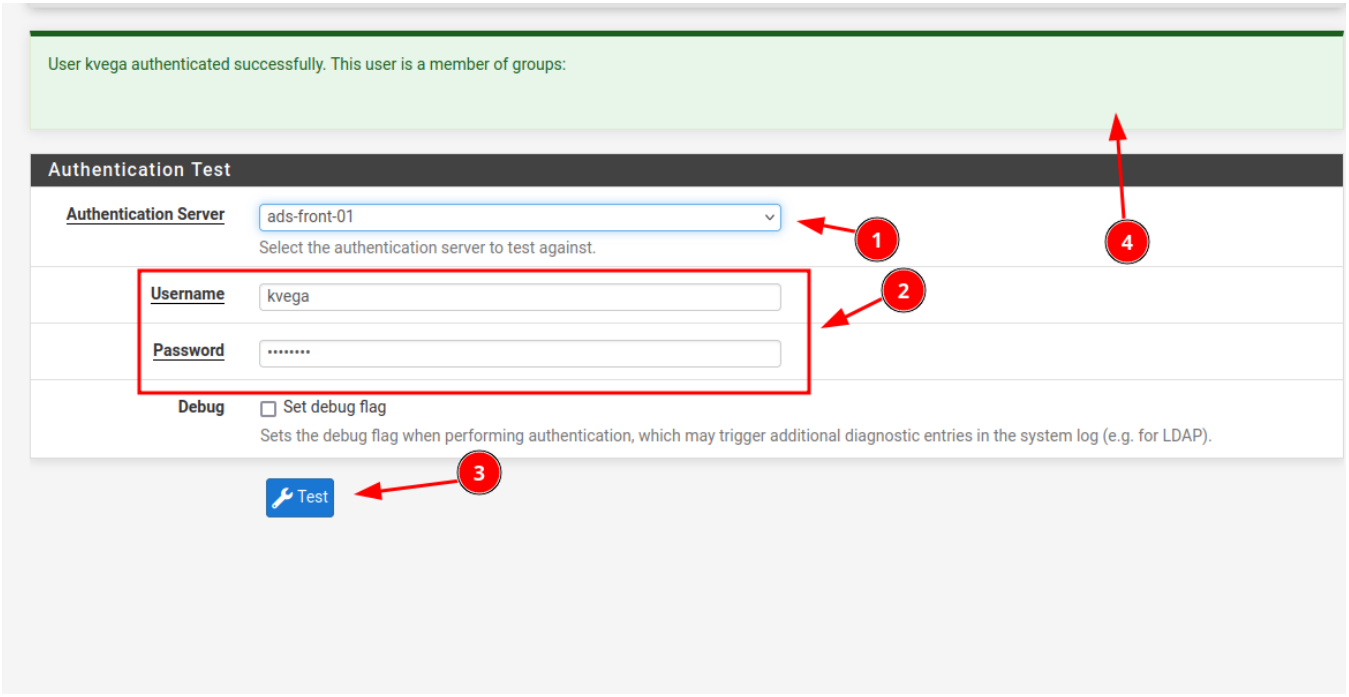


3. Choisir le container d'authentification



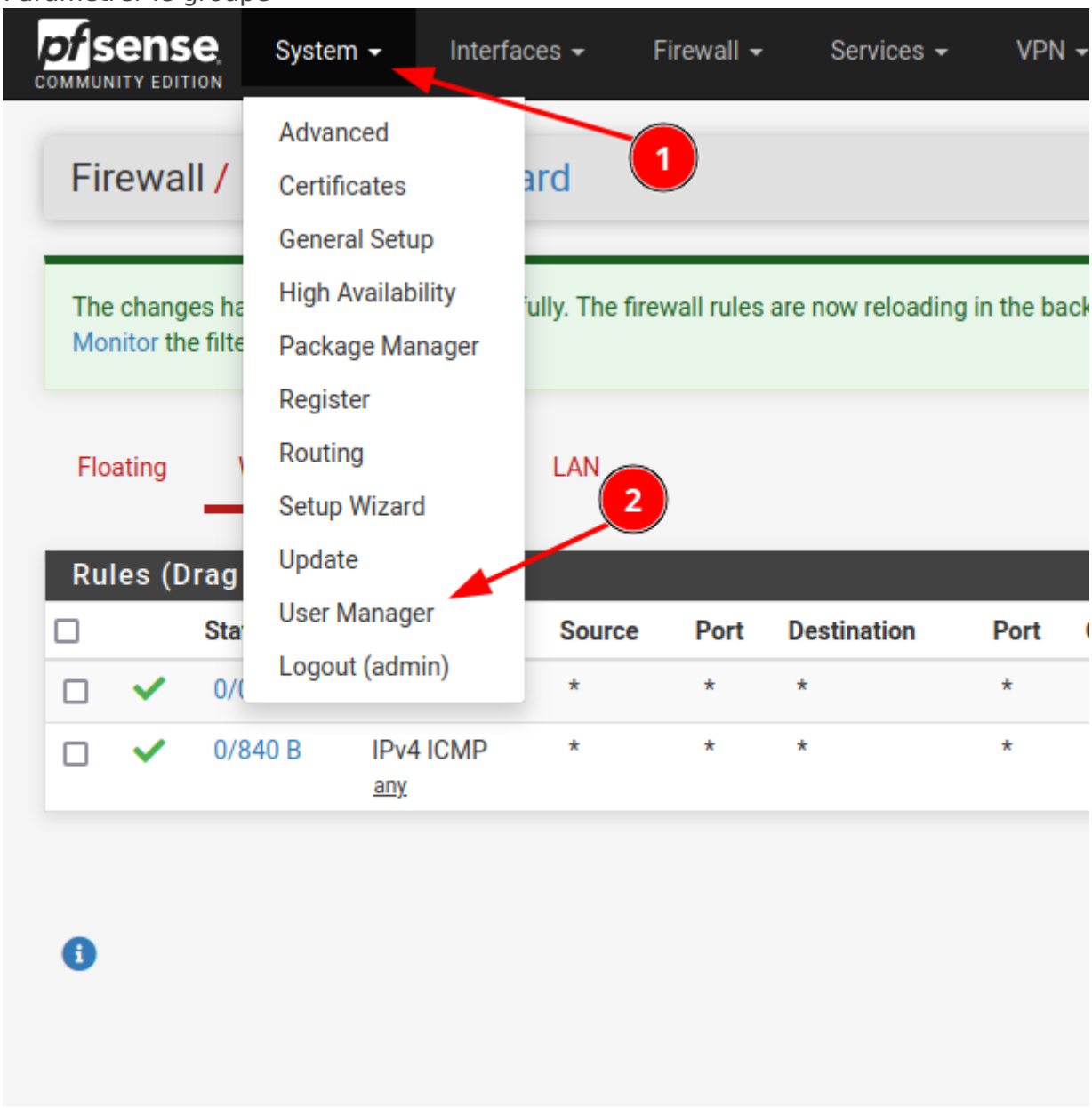
4. Sauvegarder la configuration.
5. Tester l'authentification

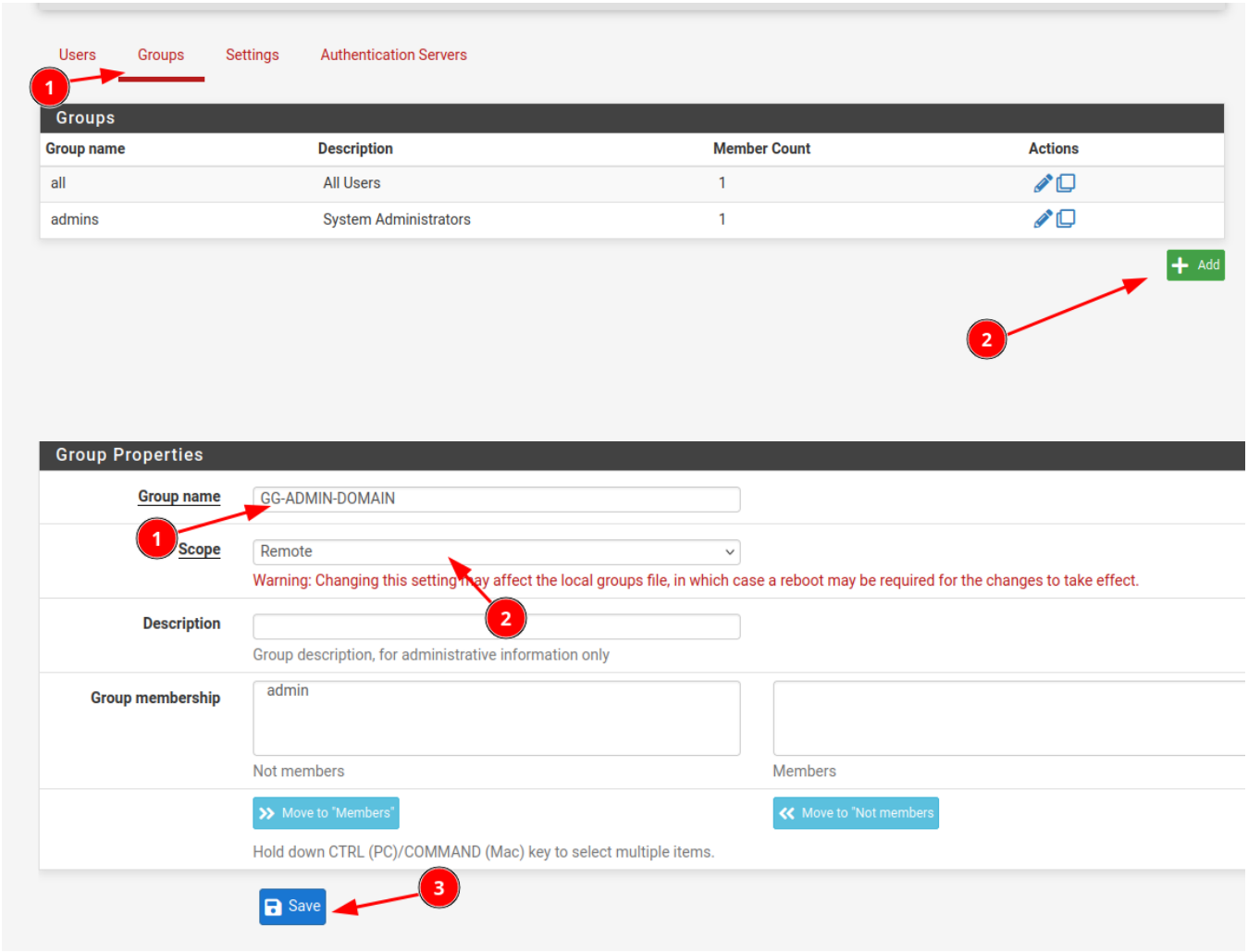

VPN
Status
Diagnostics
Help
ARP Table
Authentication
Backup & Restore
Command Prompt
DNS Lookup
Edit File
Factory Defaults
Halt System
Limiter Info
NDP Table
Packet Capture
pfInfo
pfTop
Ping
Reboot
Routes
S.M.A.R.T. Status
Sockets
States
States Summary
System Activity
Tables
Test Port
Traceroute
1
2
Host Name
Actions
172.16.1.62
fw-front-01
Add



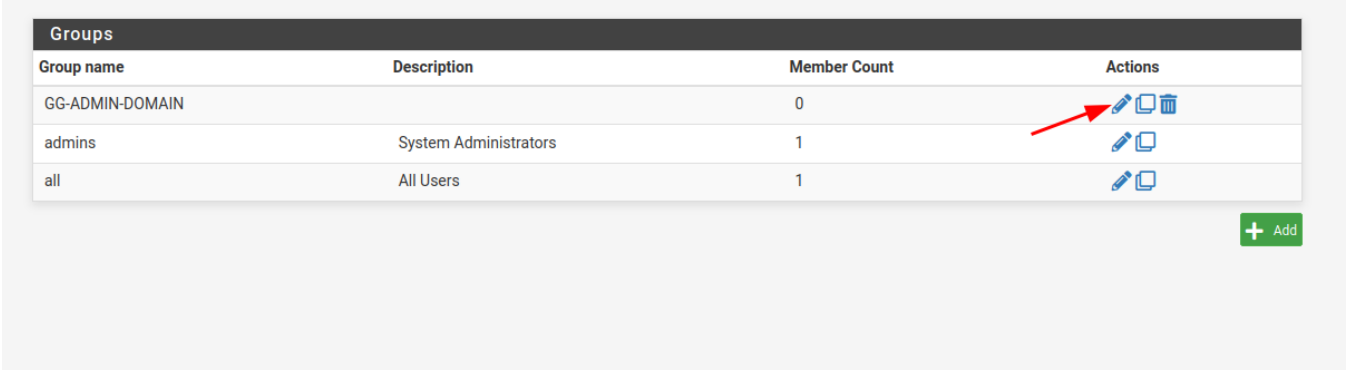
Mise en place de l'authentification

1. Paramétrer le groupe





2. Une fois le groupe créé lui donner les bon privilèges



Group Properties

Group name GG-ADMIN-DOMAIN

Scope Remote

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description

Group description, for administrative information only

Group membership

admin

Not members

Members

Move to "Members"

Move to "Not members"

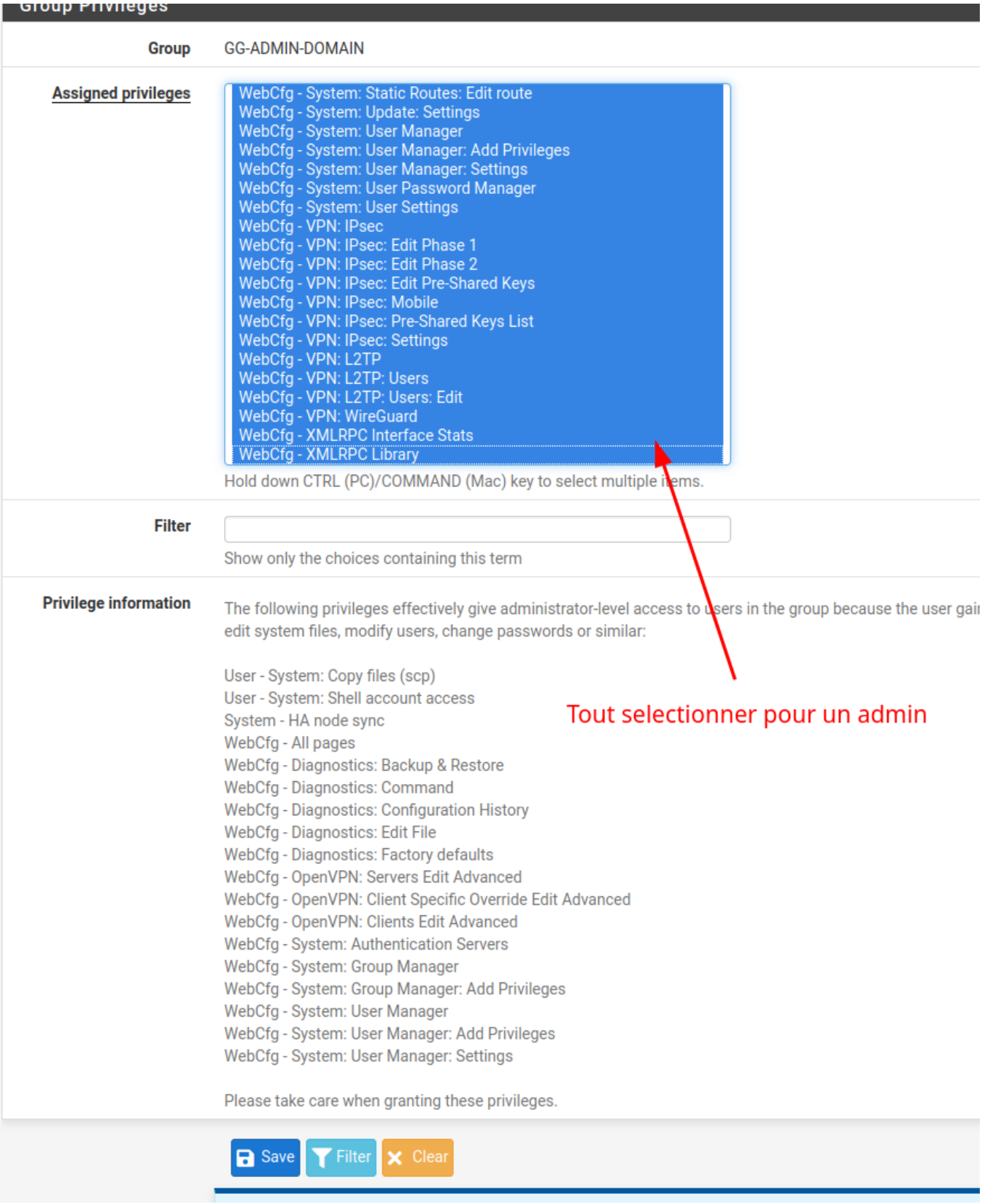
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

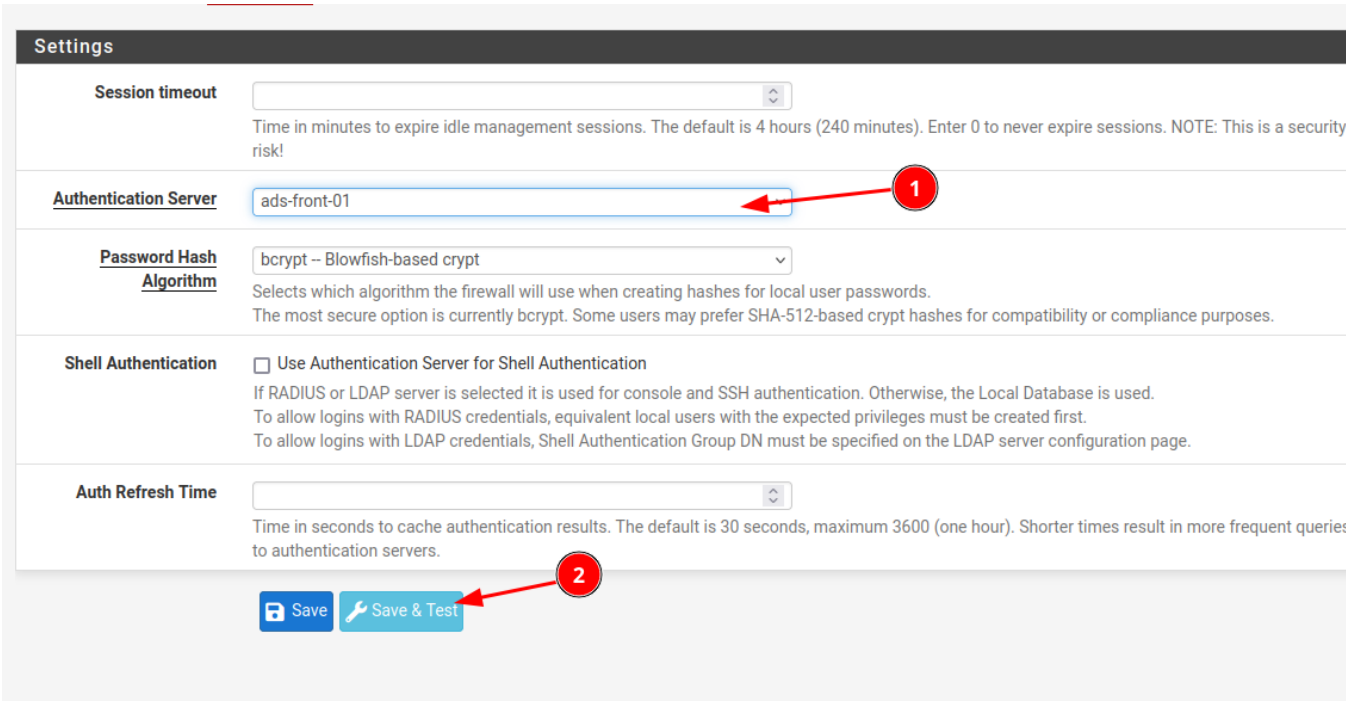
Name	Description	Action

Add

Save



3. Sauvegarder la configuration
4. Mettre en place l'authentification générale via l'Active Directory



5. tester

Revision #3
Created 2024-10-14 15:06:49 UTC by kvega
Updated 2024-10-14 15:49:18 UTC by kvega