

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

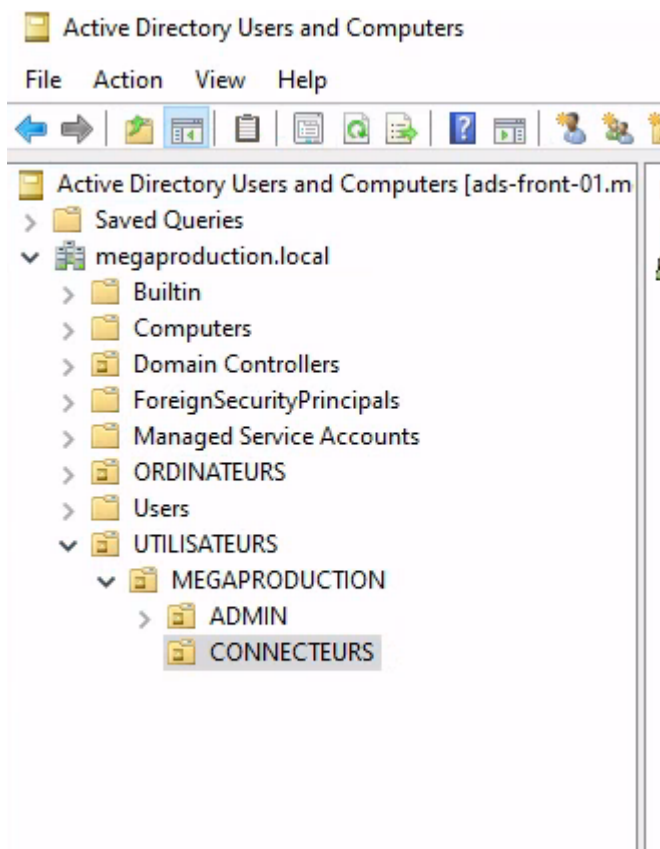
Préparation

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

Mise en place

Préparation des groupes Active Directory

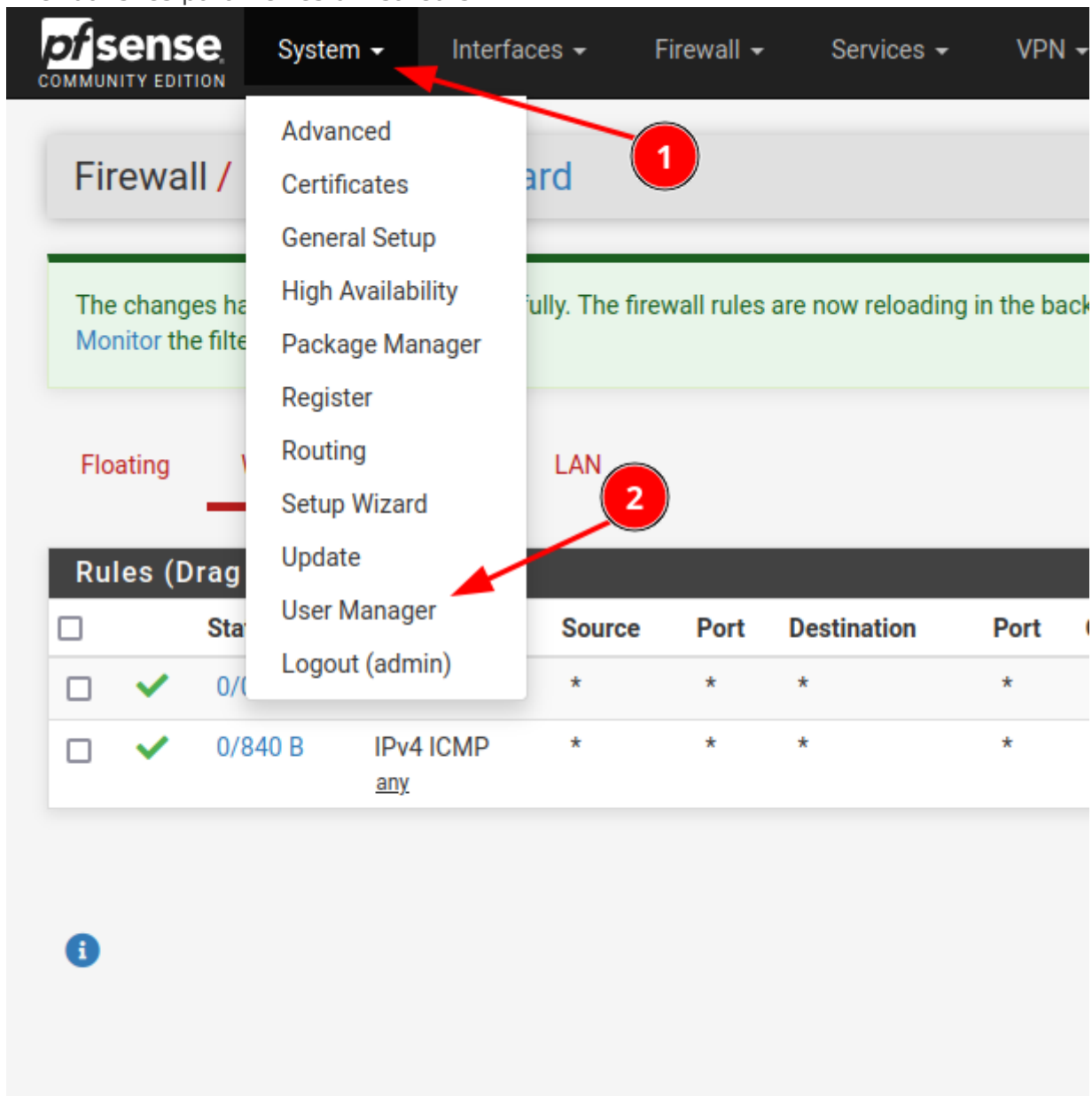
Voici l'arborescence de mon Active Directory



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)

Authentication Servers

Server Name	Type	Host Name	Actions
Local Database		fw-front-01	



+ Add

Server Settings

Descriptive name

Type

LDAP Server Settings

Hostname or IP address

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

Transport

Peer Certificate Authority

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

Server Timeout

Timeout for LDAP operations (seconds)

Search scope **Level**

Base DN

Authentication containers

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

Select a container

Extended query Enable extended query


Bind anonymous Use anonymous binds to resolve distinguished names

Bind credentials

Initial Template

User naming attribute

Group naming attribute	<input type="text" value="cn"/>
Group member attribute	<input type="text" value="memberOf"/>
RFC 2307 Groups	<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).
Group Object Class	<input type="text" value="group"/> Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".
Shell Authentication Group DN	<input type="text"/> If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login. Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com
UTF8 Encode	<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server. Required to support international characters, but may not be supported by every LDAP server.
Username Alterations	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol e.g. user@host becomes user when unchecked.
Allow unauthenticated bind	<input type="checkbox"/> Allow unauthenticated bind Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

 Save

3. Choisir le container d'authentification

The screenshot shows the Mikrotik WinBox interface for configuring LDAP authentication. A modal dialog titled "Select LDAP containers for authentication" is open, displaying a list of containers with checkboxes. A red circle with the number "2" points to the list, and a red circle with the number "3" points to the "Save" button. In the background, the "Authentication containers" field is visible with a search icon and the text "Select a container", with a red circle and the number "1" pointing to it.

Select LDAP containers for authentication

Containers

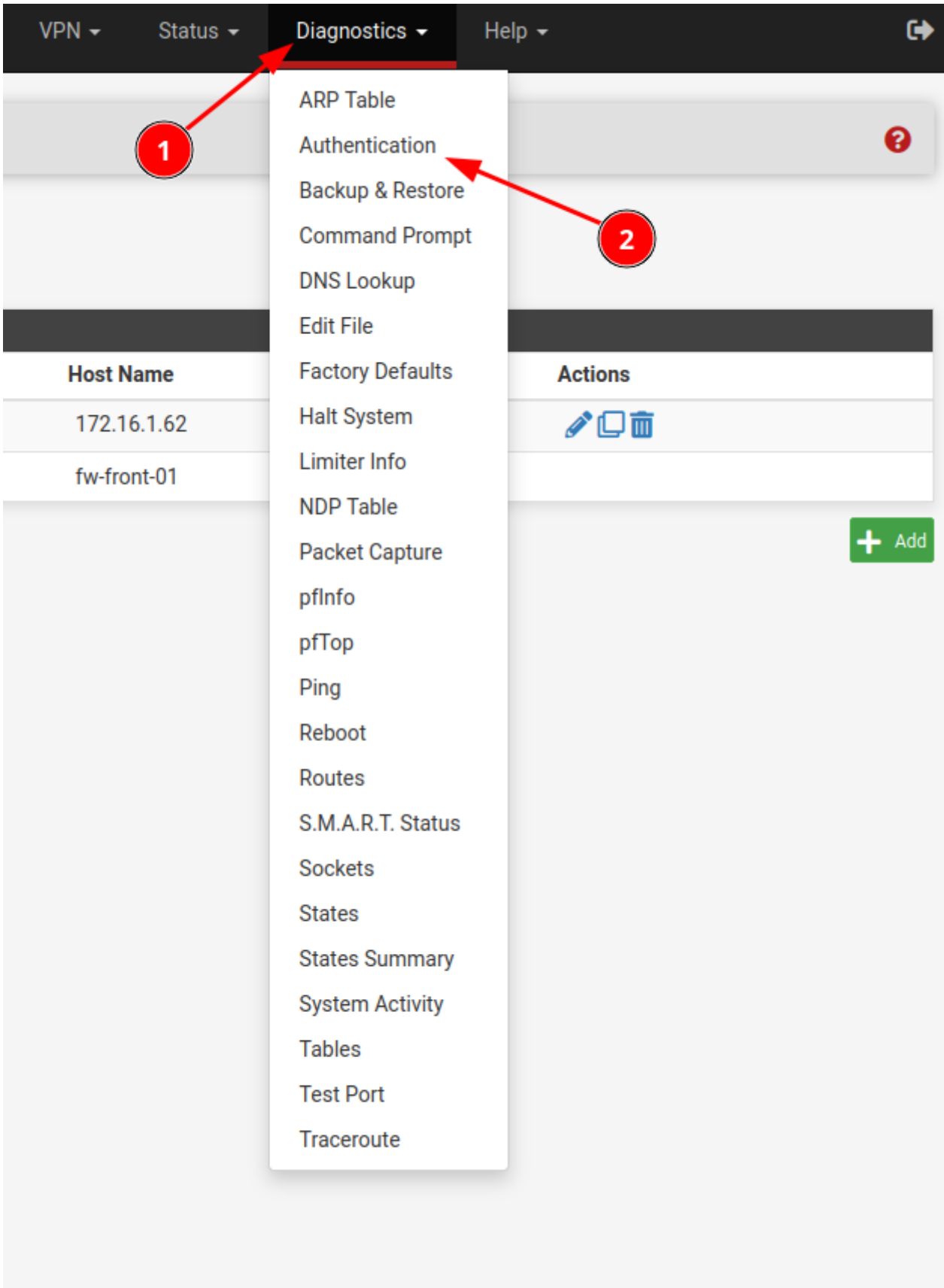
- OU=ADMIN,OU=MEGAPRODUCTION,OU=UTILISATEURS,DC=megaproduction,DC=local
- OU=CONNECTEURS,OU=MEGAPRODUCTION,OU=UTILISATEURS,DC=megaproduction,DC=local
- OU=Domain Controllers,DC=megaproduction,DC=local
- OU=MEGAPRODUCTION,OU=ORDINATEURS,DC=megaproduction,DC=local
- OU=MEGAPRODUCTION,OU=UTILISATEURS,DC=megaproduction,DC=local
- OU=ORDINATEURS,DC=megaproduction,DC=local
- OU=UTILISATEURS,DC=megaproduction,DC=local
- CN=Users,DC=megaproduction,DC=local
- CN=Users,CN=Builtin,DC=megaproduction,DC=local

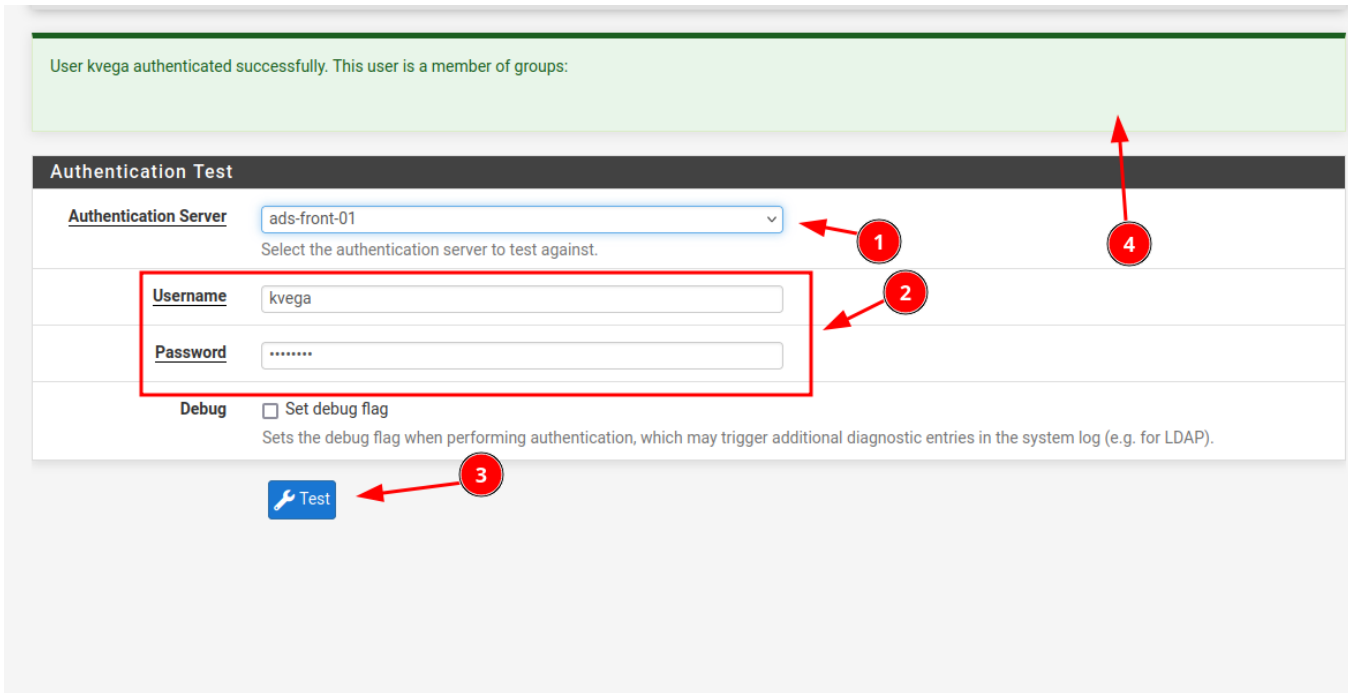
Save

Authentication containers: CN=user_bind,CN=GG_users_pfsense,OU=CONNECTEURS,OU=MEGAPI

Select a container

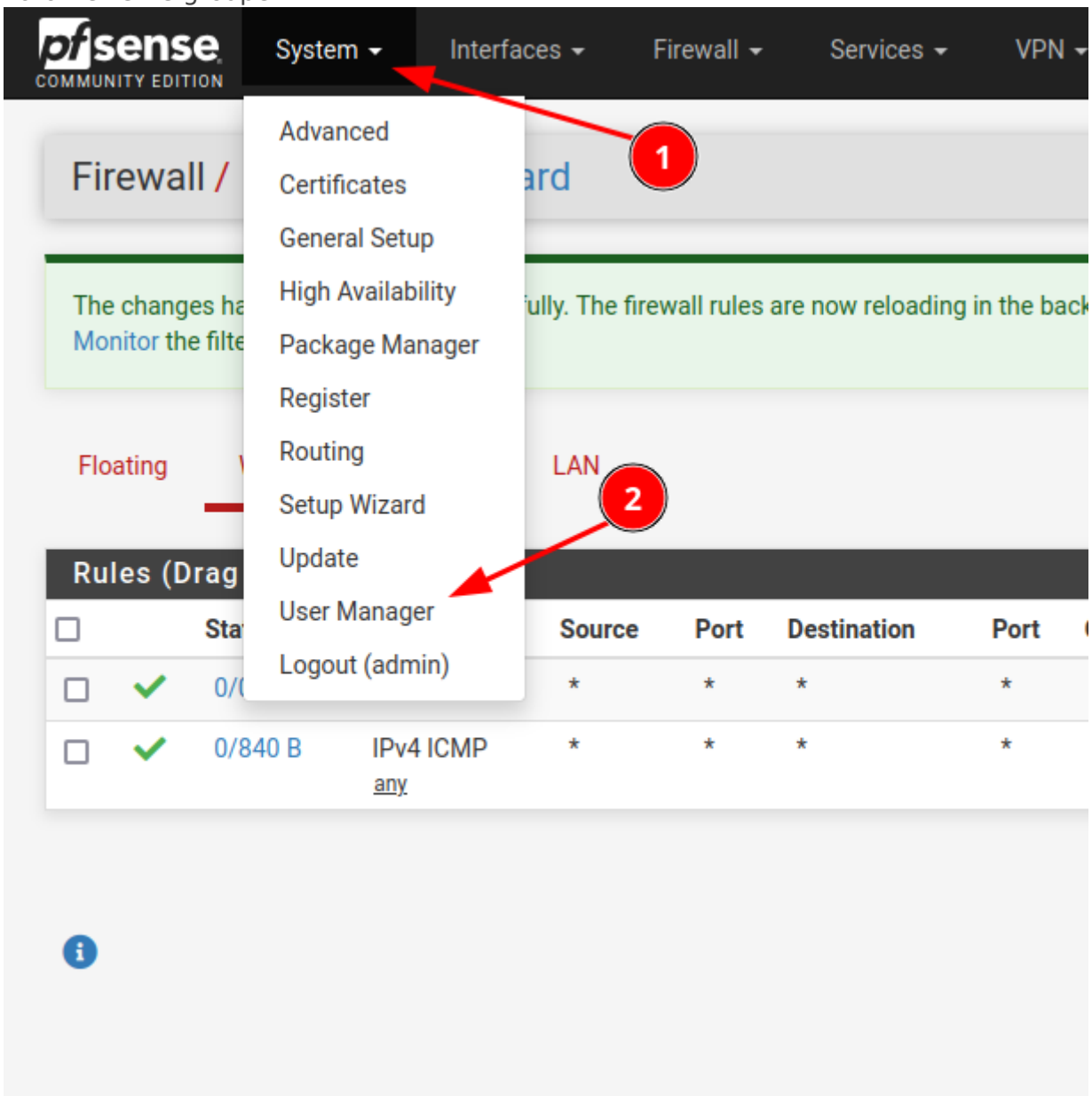
4. Sauvegarder la configuration.
5. Tester l'authentification





Mise en place de l'authentification





1. Paramétrer le groupe




Users Groups Settings Authentication Servers

1

Groups

Group name	Description	Member Count	Actions
all	All Users	1	 
admins	System Administrators	1	 



2

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

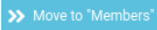

Group description, for administrative information only

Group membership


admin

Not members

Members








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




3

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

Groups

Group name	Description	Member Count	Actions
GG-ADMIN-DOMAIN		0	  
admins	System Administrators	1	 
all	All Users	1	 



Group Properties

Group name

Scope

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

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](#)

Group Privileges

Group GG-ADMIN-DOMAIN

Assigned privileges

- WebCfg - System: Static Routes: Edit route
- WebCfg - System: Update: Settings
- WebCfg - System: User Manager
- WebCfg - System: User Manager: Add Privileges
- WebCfg - System: User Manager: Settings
- WebCfg - System: User Password Manager
- WebCfg - System: User Settings
- WebCfg - VPN: IPsec
- WebCfg - VPN: IPsec: Edit Phase 1
- WebCfg - VPN: IPsec: Edit Phase 2
- WebCfg - VPN: IPsec: Edit Pre-Shared Keys
- WebCfg - VPN: IPsec: Mobile
- WebCfg - VPN: IPsec: Pre-Shared Keys List
- WebCfg - VPN: IPsec: Settings
- WebCfg - VPN: L2TP
- WebCfg - VPN: L2TP: Users
- WebCfg - VPN: L2TP: Users: Edit
- WebCfg - VPN: WireGuard
- WebCfg - XMLRPC Interface Stats
- WebCfg - XMLRPC Library

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

Filter

Show only the choices containing this term

Privilege information

The following privileges effectively give administrator-level access to users in the group because the user gain edit system files, modify users, change passwords or similar:

- User - System: Copy files (scp)
- User - System: Shell account access
- System - HA node sync
- WebCfg - All pages
- WebCfg - Diagnostics: Backup & Restore
- WebCfg - Diagnostics: Command
- WebCfg - Diagnostics: Configuration History
- WebCfg - Diagnostics: Edit File
- WebCfg - Diagnostics: Factory defaults
- WebCfg - OpenVPN: Servers Edit Advanced
- WebCfg - OpenVPN: Client Specific Override Edit Advanced
- WebCfg - OpenVPN: Clients Edit Advanced
- WebCfg - System: Authentication Servers
- WebCfg - System: Group Manager
- WebCfg - System: Group Manager: Add Privileges
- WebCfg - System: User Manager
- WebCfg - System: User Manager: Add Privileges
- WebCfg - System: User Manager: Settings

Please take care when granting these privileges.

Save Filter Clear

Tout selectionner pour un admin

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

Settings

Session timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server

Password Hash Algorithm

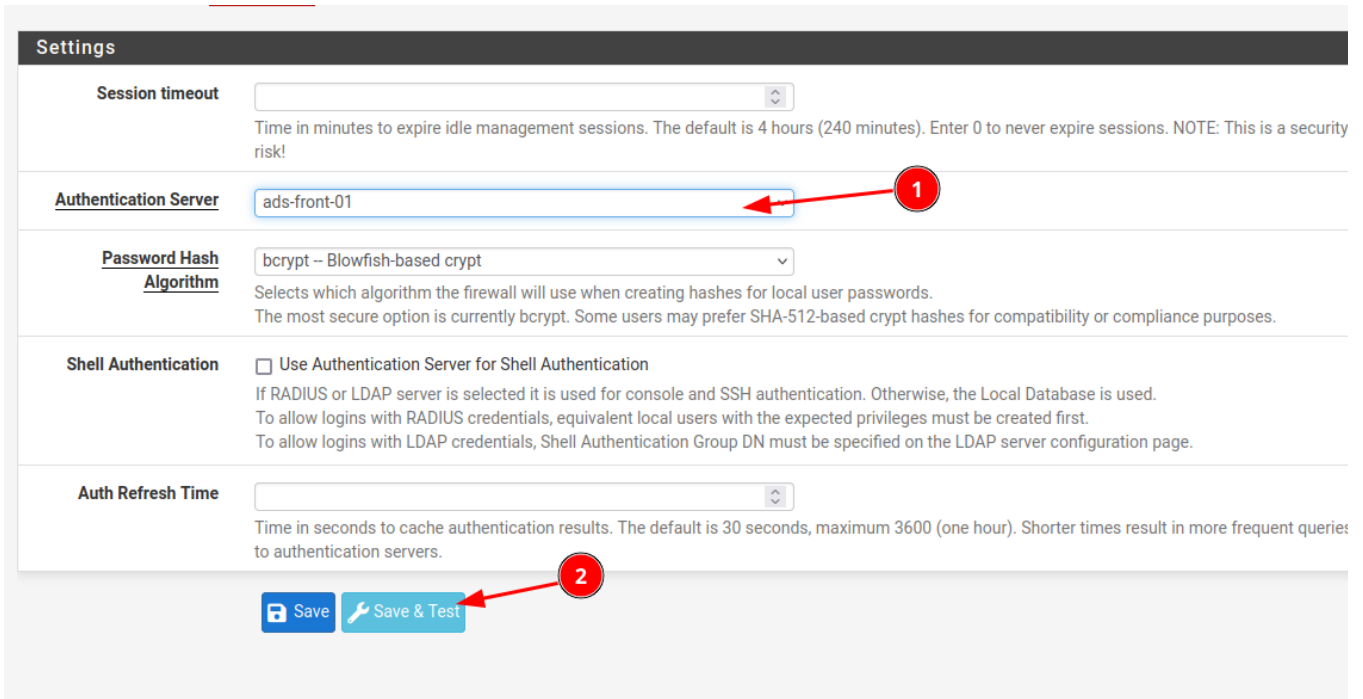
Selects which algorithm the firewall will use when creating hashes for local user passwords. The most secure option is currently bcrypt. Some users may prefer SHA-512-based crypt hashes for compatibility or compliance purposes.

Shell Authentication Use Authentication Server for Shell Authentication

If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

Auth Refresh Time

Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.



5. tester

Revision #3

Created 2024-10-14 15:06:49 UTC by kvega

Updated 2024-10-14 15:49:18 UTC by kvega