📑 **Documentation Technique : Infrastructure Réseau HA & Authentification Centralisée (AD/LDAP)**

Client : Lab SIO113

Environnement : pfSense CE (Master & Slave) + Windows Server 2022 (AD DS)

Objectif : Mise en place d'une Haute Disponibilité (HA) avec authentification des administrateurs via l'Active Directory.

---

1. Préparation de l'Active Directory (Windows Server)

L'Active Directory sert de source de vérité pour tous les comptes utilisateurs.

A. Création de la structure

1. **Utilisateur de liaison (Bind User) :** Création d'un compte standard nommé pfsense-auth dans l'OU Users. Ce compte permet au pare-feu de lire l'annuaire.
2. **Groupe d'administration :** Création d'un groupe de sécurité global nommé **Admins_AD**.
3. **Affectation :** Ajout de l'utilisateur administrateur (et tout autre admin futur) comme membre du groupe Admins_AD.

B. Paramètres réseau

- **IP du Contrôleur de Domaine :** 192.168.10.15
- **Domaine (Realm) :** SI0113.local
- **Base DN :** DC=SI0113,DC=local

---

2. Configuration du Serveur d'Authentification (pfSense Master)

Chemin : System > User Management > Authentication Servers

Paramètre	**Valeur**
Descriptive Name	mon_AD
Type	LDAP
Hostname or IP	192.168.10.15
Port / Transport	389 / TCP - Standard
Search Scope	**Entire Subtree** (Essentiel pour trouver les groupes)

Paramètre	Valeur
Base DN	DC=SI0113,DC=local
Authentication Containers	CN=Users,DC=SI0113,DC=local
Bind credentials	CN=administrateur,CN=Users,DC=SI0113,DC=local
User naming attribute	samAccountName
Group naming attribute	cn
Group member attribute	memberOf
Group Object Class	group

---

3. Gestion des Droits et Privilèges

Pour que les utilisateurs de l'AD puissent gérer le pfSense, on crée un miroir local du groupe distant.

A. Création du groupe local

Chemin : System > User Management > Groups

1. **Group Name :** Admins_AD (Doit être identique au nom dans l'AD).
2. **Scope :** Remote.
3. **Privilèges :** Ajouter le privilège **WebCfg - All pages**.

B. Activation de la méthode d'authentification

Chemin : System > User Management > Settings

- **Authentication Server :** Sélectionner mon_AD.
- **Enregistrer.**

---

4. Haute Disponibilité et Synchronisation (HA / XMLRPC)

Configuration du basculement et de la réplication entre le Master et le Slave.

A. Configuration sur le Master (.20)

Chemin : System > High Avail. Sync

1. **Synchronize Config to IP :** 192.168.10.30 (IP du Slave).
2. **Remote System Username :** admin.

3. **Remote System Password :** Mot de passe du compte admin du Slave.
4. **Options à synchroniser (cocher) :**
    - User manager users and groups
    - Authentication servers (e.g. LDAP, RADIUS)
    - Firewall rules / NAT / Virtual IPs (CARP).

B. Configuration sur le Slave (.30)

- **Action :** Laisser la page High Avail. Sync totalement **vide**. L'esclave reçoit les mises à jour de manière passive.

---

5. Procédures de Test et Validation

Test de communication LDAP

Utiliser l'outil **Diagnostics > Authentication** :

1. Sélectionner le serveur mon_AD.
2. Saisir les identifiants d'un compte membre de Admins_AD.
3. **Résultat attendu :** Une bannière verte confirmant l'authentification et affichant member of groups: Admins_AD.

Test de connexion à l'interface

1. Ouvrir une navigation privée.
2. Se connecter avec le login Windows (ex: administrateur).
3. Vérifier l'accès complet aux menus du pare-feu.