Documentation Technique : Installation et Configuration de l'Architecture de Pare-feu pfSense

1. Introduction et Prérequis d'Infrastructure

La sécurisation d'un périmètre réseau informatique nécessite l'intégration d'une barrière de filtrage périmétrique robuste. Cette documentation traite du déploiement du pare-feu open-source **pfSense**. Elle formalise l'interconnexion entre la zone WAN (accès Internet extérieur) et les zones LAN protégées de l'organisation.

2. Actions Préalables (Avant l'accès à l'interface Web)

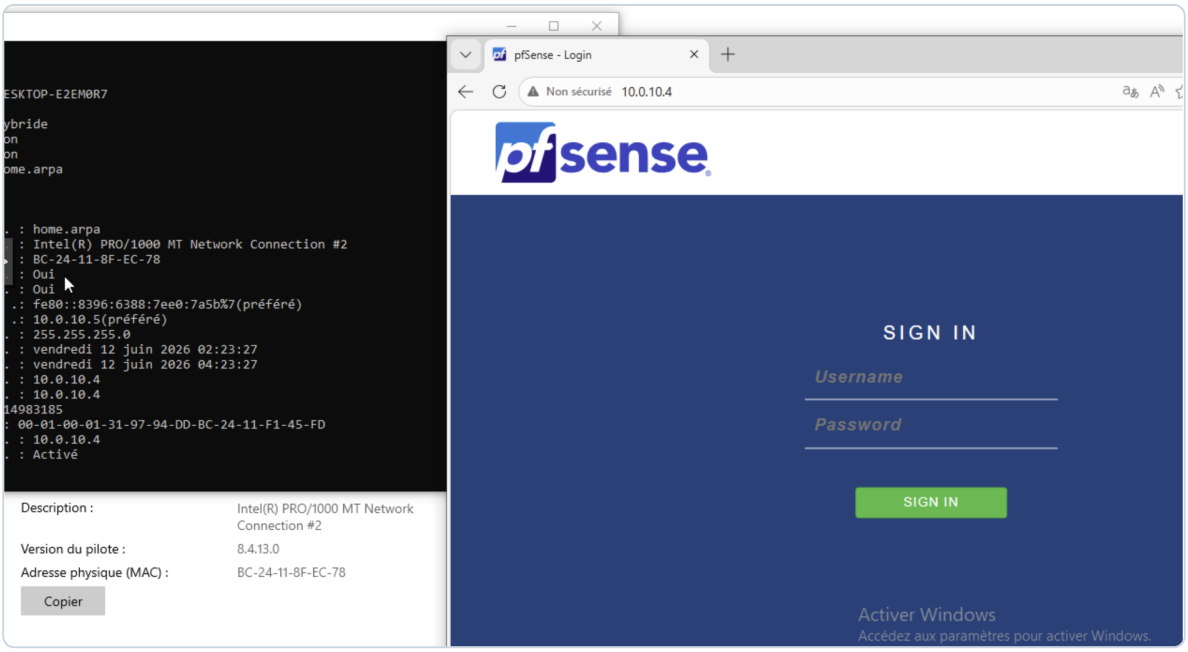
Afin de parvenir à l'assistant de configuration graphique accessible via le navigateur, les étapes système d'infrastructure suivantes ont été préalablement complétées en amont :

- **Création et provisionnement de la machine virtuelle :** Déploiement de l'instance sous l'hyperviseur avec allocation des ressources matérielles (processeur, mémoire vive) et affectation des interfaces de communication.
- **Configuration des cartes réseau (vSwitches / Bridges) :** Attribution d'une première interface physique ou virtuelle connectée au commutateur externe (WAN) et d'une seconde interface connectée au commutateur interne isolé (LAN).
- **Boot sur l'ISO et installation de l'OS :** Chargement de l'image d'installation de pfSense, acceptation des conditions d'utilisation, partitionnement standard du disque virtuel et finalisation de l'installation du noyau BSD.
- **Configuration initiale des interfaces (Console CLI) :** Au premier démarrage dans l'invite système textuelle, assignation manuelle de l'interface LAN avec une adresse IP fixe de gestion et activation du service DHCP temporaire permettant à un poste d'administration de se connecter au même sous-réseau.
- **Première connexion :** Ouverture d'un navigateur web depuis un poste client du LAN à l'adresse IP définie, puis authentification à l'aide des identifiants d'usine par défaut (`admin / pfsense`).

3. Assistant de Configuration et Déploiement Réseau

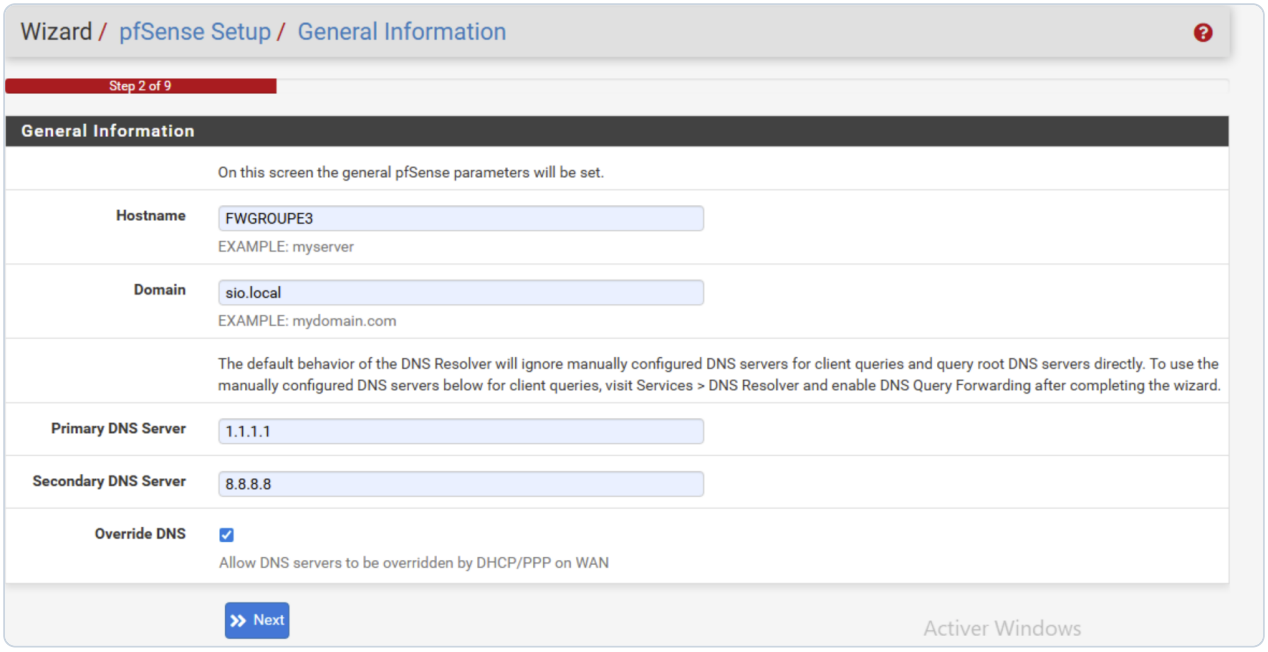
Étape 3.1 : Initialisation de l'assistant général

Une fois authentifié, l'assistant guidé pas à pas s'initialise. Il permet de passer en revue les paramètres globaux de la plateforme, de configurer les serveurs de noms, le fuseau horaire ainsi que les règles de routage par défaut des interfaces d'entrée et de sortie.



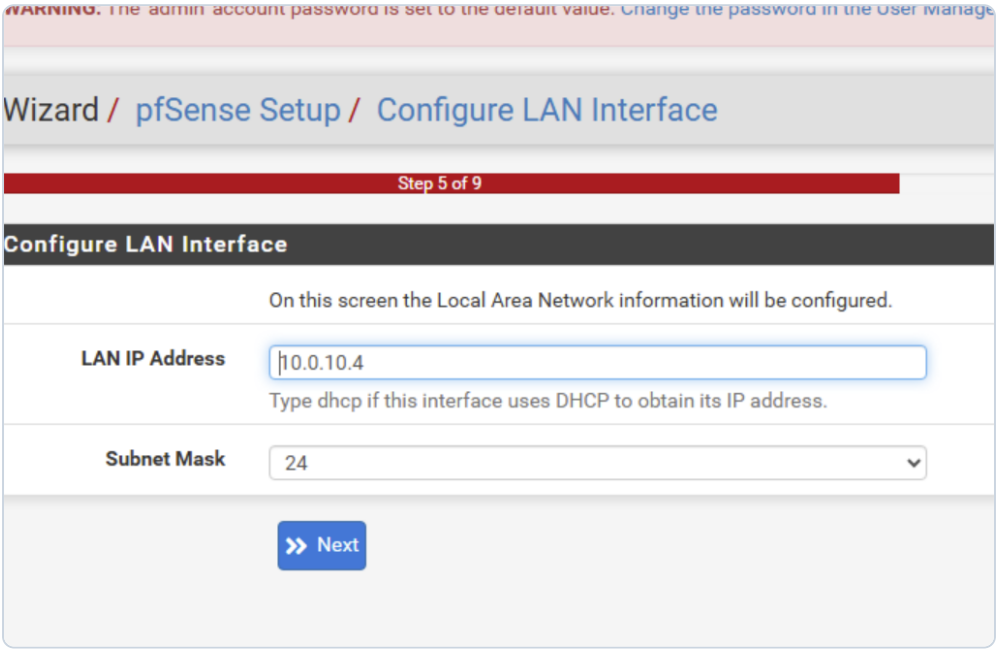
Étape 3.2 : Définition de l'identité et du domaine réseau

Cette étape permet de spécifier le nom d'hôte unique de l'équipement de sécurité ainsi que le suffixe DNS du domaine de l'organisation pour la centralisation et la traçabilité des logs.



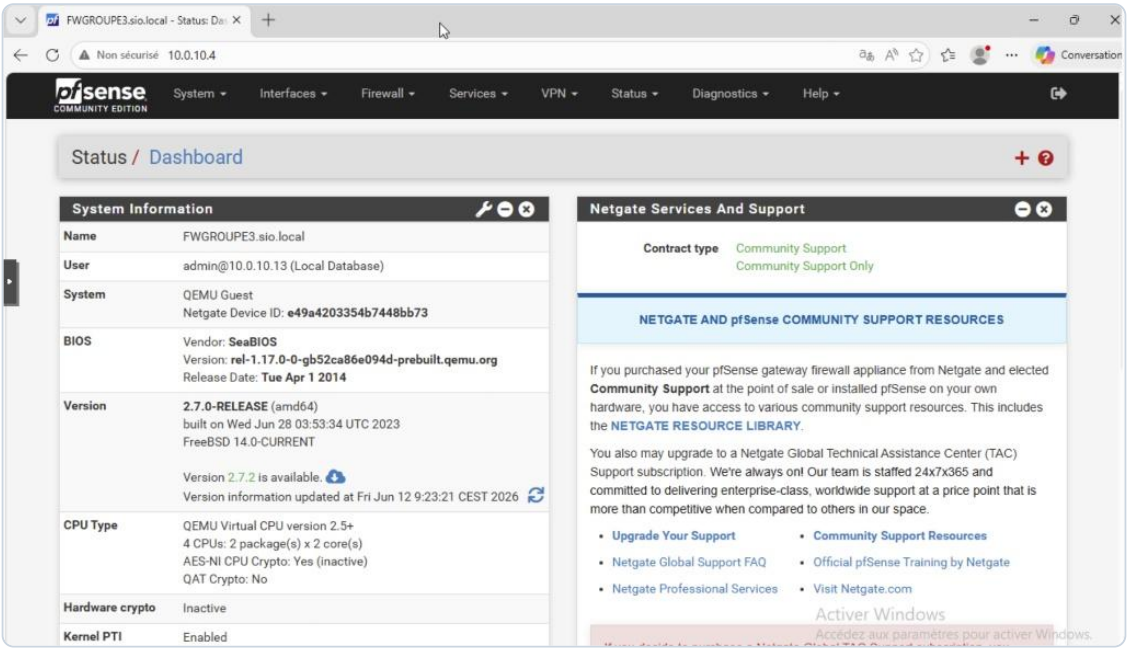
Étape 3.3 : Configuration de l'interface LAN

Paramétrage de l'interface réseau locale (Local Area Network). Cette étape fixe l'adresse IP statique privée du pare-feu qui servira de passerelle par défaut pour l'ensemble des équipements du réseau interne.



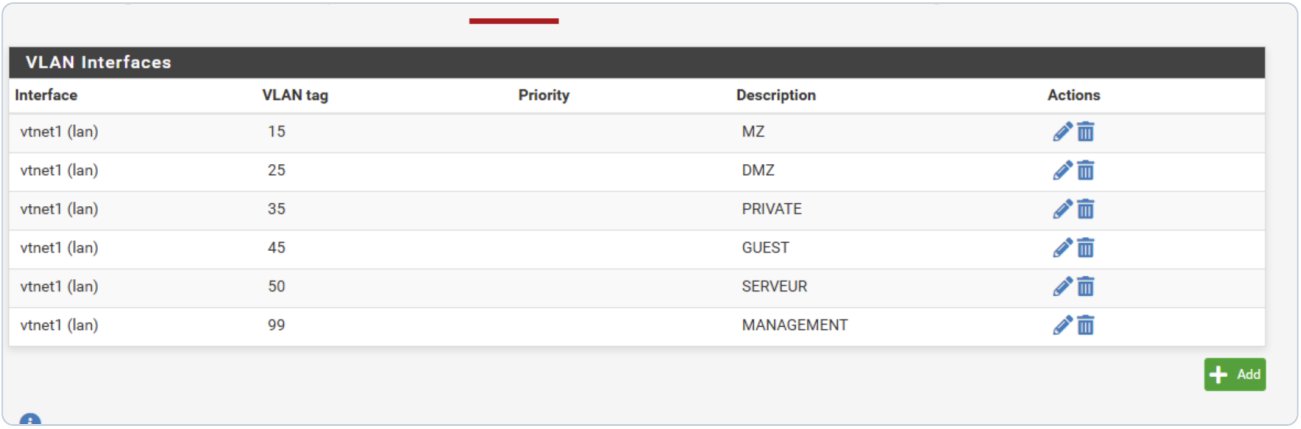
Étape 3.4 : Vue sur le dashboard de pfSense

Accès et contrôle visuel depuis le tableau de bord principal de pfSense. Cette interface permet d'avoir une vue globale sur les ressources système consommées, l'état d'activité des liaisons ainsi que les services actifs sur la plateforme.



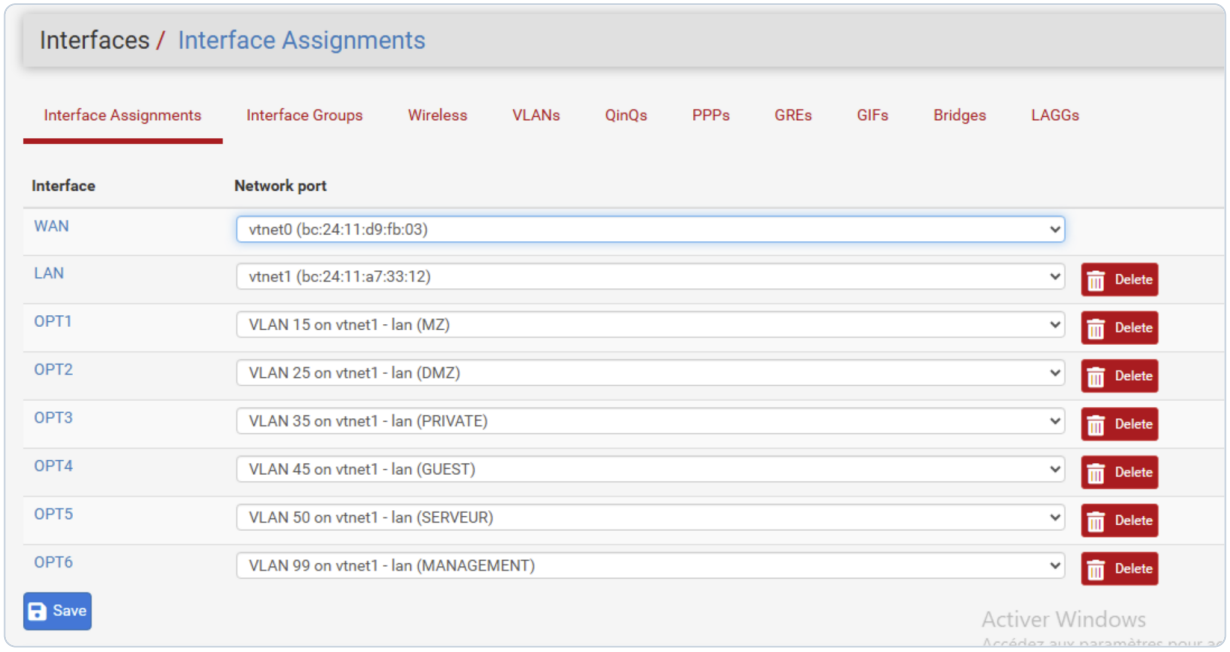
Étape 3.5 : Configuration de l'interface WAN

Configuration des règles et protocoles applicables à l'interface externe (Wide Area Network). C'est ici que l'on définit la méthode d'obtention de l'IP publique et l'activation des filtres de sécurité de premier niveau.



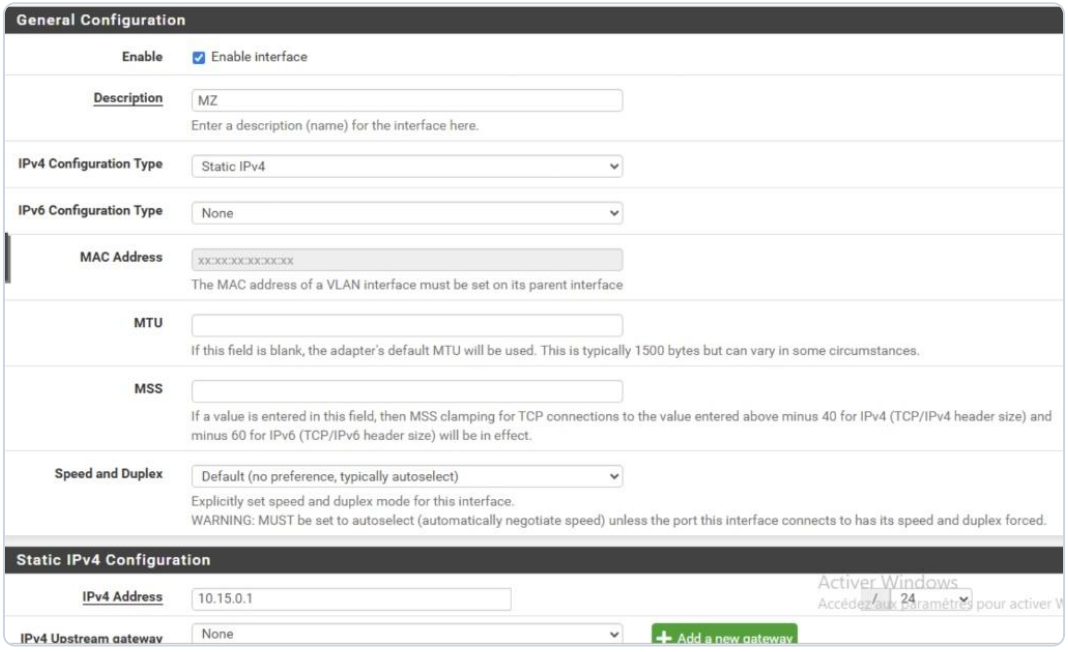
Étape 3.6 : Assignement des interfaces

Cette section détaille l'attribution des cartes réseau physiques ou virtuelles (ports correspondants du serveur) aux rôles logiques WAN, LAN ou aux différentes sous-interfaces créées.



Étape 3.7 : Exemple de configuration du VLAN MZ

Vue ciblée sur la page de configuration spécifique du VLAN MZ (Zone Militarisée / DMZ). Cette étape documente l'isolation réseau, l'adressage IP propre attribué à ce sous-réseau et les options d'encapsulation nécessaires.



4. Règles de Filtrage et Sécurité Périmétrique

Mise en place des politiques d'accès de sécurité au sein du pare-feu. Cette capture d'écran présente l'application d'une règle permissive générale (règle Any) sur le VLAN SERVEUR, autorisant l'intégralité

des flux initiés depuis cette zone vers les autres segments ou l'extérieur pour les besoins du déploiement.