

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)

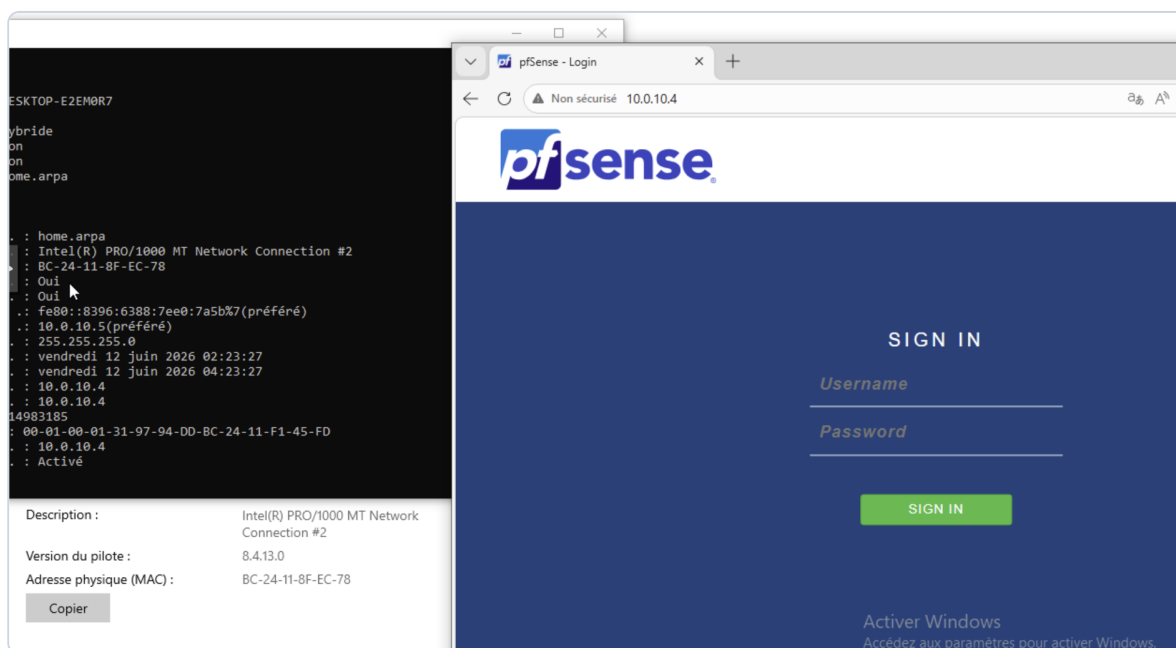
Afin de parvenir à l'assistant de configuration graphique accessible via le navigateur, les étapes système d'infrastructure suivantes ont été préalablement complétées en amont :

- **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.

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname	FWGROUPE3 EXAMPLE: myserver
Domain	sio.local EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	1.1.1.1
Secondary DNS Server	8.8.8.8
Override DNS	☒ Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#) Activier Windows

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.

WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

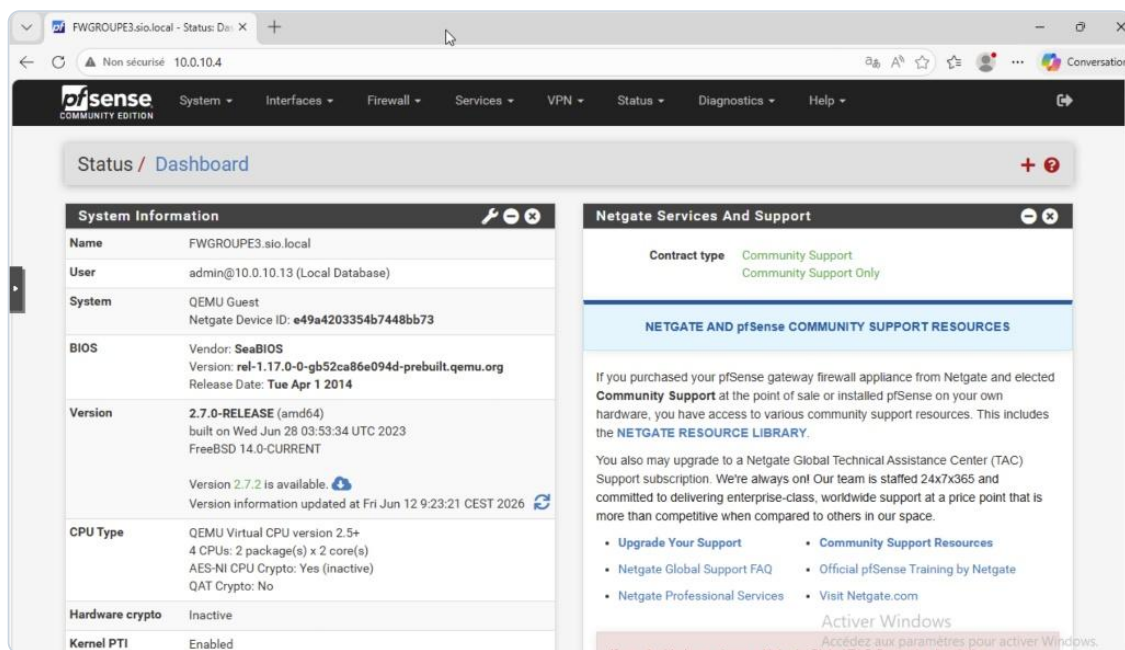
On this screen the Local Area Network information will be configured.

LAN IP Address	10.0.10.4 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24

[Next](#)

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.

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
vtnet1 (lan)	15		MZ	 
vtnet1 (lan)	25		DMZ	 
vtnet1 (lan)	35		PRIVATE	 
vtnet1 (lan)	45		GUEST	 
vtnet1 (lan)	50		SERVEUR	 
vtnet1 (lan)	99		MANAGEMENT	 

Étape 3.6 : Assignment 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.

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	vtnet0 (bc:24:11:d9:fb:03)	
LAN	vtnet1 (bc:24:11:a7:33:12)	Delete
OPT1	VLAN 15 on vtnet1 - lan (MZ)	Delete
OPT2	VLAN 25 on vtnet1 - lan (DMZ)	Delete
OPT3	VLAN 35 on vtnet1 - lan (PRIVATE)	Delete
OPT4	VLAN 45 on vtnet1 - lan (GUEST)	Delete
OPT5	VLAN 50 on vtnet1 - lan (SERVEUR)	Delete
OPT6	VLAN 99 on vtnet1 - lan (MANAGEMENT)	Delete

Save

Activer Windows
Accédez aux paramètres pour activer Windows

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.

General Configuration

Enable ☒ Enable interface

Description MZ
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxx
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 10.15.0.1

IPv4 Upstream gateway None + Add a new gateway

Activer Windows
Accédez aux paramètres pour activer Windows

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.

