Mise en place d’un Pare-Feu pfSense

FOUR Lucas
Conseil départemental de la Drôme

Table des matières

Cahier des charges – Expression des besoins

| Descriptif de l'existant |

L'infrastructure de départ étant inexistante, je ne dispose d'aucun service réseau préconfiguré. Mon environnement se limite à un accès à Internet via le réseau local (LAN) du GRETA, qui me permet de télécharger les ressources nécessaires à la mise en place du projet.

| Besoin(s) |

Ce travail pratique a pour objectif de mettre en place une solution de pare-feu et de gestion réseau permettant la distribution automatique des paramètres réseau (adresses IP, passerelle, DNS) aux équipements du réseau. Le but est d'assurer la connectivité et le bon fonctionnement des machines clientes sans intervention manuelle sur chaque poste.

| Contrainte(s) |

La réalisation de ce travail pratique est soumise aux contraintes suivantes :

- **Contrainte de temps** : l'ensemble de la configuration doit être réalisé en quatre heures.
- **Contrainte logicielle** : la solution retenue est pfSense, déployée sur une machine virtuelle.
- **Contrainte fonctionnelle** : le service DHCP intégré à pfSense doit être activé et configuré pour assurer l'attribution automatique des paramètres réseau aux machines clientes.
- **Contrainte de configuration** : les paramètres réseau du pare-feu et ses services intégrés doivent être correctement définis.
- **Contrainte de validation** : le TP sera validé sur l'attribution correcte des adresses IP aux postes clients ainsi que sur la bonne communication entre pfSense et les machines du réseau.

Ressources

| Ressources mises à disposition |

Pour la réalisation de ce travail pratique, je dispose d'une machine hôte équipée de l'hyperviseur Hyper-V, utilisé comme solution de virtualisation pour le déploiement de pfSense sous forme de machine virtuelle. Cette machine hôte est connectée au réseau local (LAN) du GRETA, ce qui permet à pfSense de bénéficier d'un accès à Internet, nécessaire au téléchargement des mises à jour et à la configuration des services réseau.

| Ressources nécessaires à la mise en place |

Pour la mise en œuvre de ce travail pratique, plusieurs éléments matériels et logiciels sont nécessaires :

- Une machine hôte équipée d'un logiciel de virtualisation, en l'occurrence Hyper-V, afin de créer et gérer la machine virtuelle hébergeant pfSense ;
- Un accès à Internet, indispensable pour le téléchargement de l'image ISO de pfSense, ainsi que pour les mises à jour et la configuration des services réseau ;
- L'image ISO de pfSense, utilisée pour l'installation et la configuration du pare-feu au sein de l'environnement virtualisé.

| Gestion des ressources |

Le temps imparti pour ce travail pratique étant d'environ une heure, et celui-ci incluant l'installation et la configuration initiale de pfSense, j'ai procédé au pré-téléchargement de l'image ISO correspondante. Cette préparation en amont permet de gagner du temps lors de la création de la machine virtuelle et d'optimiser le déroulement du TP, notamment pour l'installation de pfSense et la configuration de ses services réseau, en particulier le service DHCP.

Analyse

Solutions	pfSense	OPENsense
Coûts	Gratuit (open source)	Gratuit (open source)
OS d'installation	Basé sur FreeBSD	Basé sur FreeBSD
Points forts	Solution très stable, largement éprouvée, nombreuses fonctionnalités, forte communauté	Interface moderne, mises à jour fréquentes, bonne modularité
Interface / utilisation	Interface Web complète, claire et robuste, adapté aux débutants comme aux administrateurs	Interface Web plus moderne et ergonomique
Mise en place	Rapide via image ISO, installation et configuration simples	Rapide également via ISO, configuration intuitive
Communauté / Support	Très grand communauté, documentation abondante, nombreux forums et tutoriels	Communauté active, documentation claire mais moins fournie
Idéal pour	Labs, formations, PME, environnements de production, virtualisation	Labs, PME, utilisateur recherchant une interface moderne
Limites	Interface graphique plus classique, évolutions parfois conservatrices	Mises à jour fréquentes pouvant occasionner des instabilités

| Choix d'une solution – Argumentation |

J'ai choisi d'utiliser pfSense comme solution de pare-feu et de serveur DHCP, car il offre une solution fiable, centralisée et open source pour la gestion des configurations réseau. Grâce à ses services intégrés, pfSense permet l'attribution dynamique des adresses IP ainsi que des paramètres essentiels (DNS, passerelle, masque de sous-réseau), ce qui simplifie l'administration du réseau et limite les risques d'erreurs liés à une configuration manuelle. Cette approche est particulièrement adaptée à un contexte pédagogique et professionnel, où la stabilité, la rapidité de mise en œuvre et la maîtrise des flux réseau sont des éléments essentiels.

| Plan d'adressage réseau |

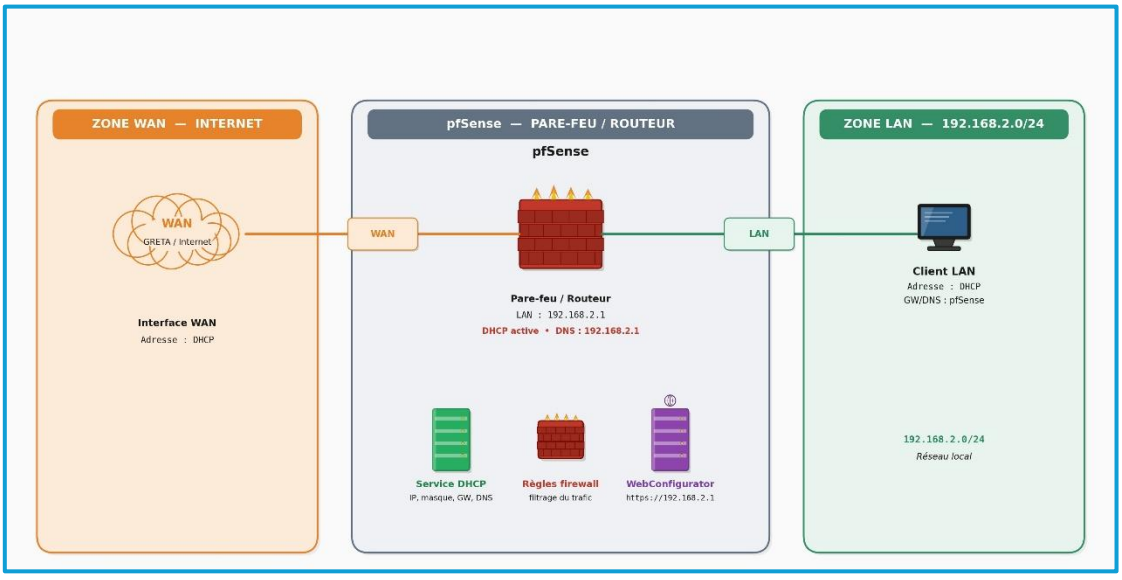
Tableau d'adressage :

Nom du réseau	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
LAN	192.168.2.0	255.255.555.0	192.168.2.1	192.168.2.254	192.168.2.255

Tableau des adresses IP :

Machines	Adresses IP	Masque de sous réseau	Passerelle par défaut	DNS
pfSense (LAN)	192.168.2.1	255.255.255.0	X	192.168.2.1
Client (poste LAN)	DHCP	DHCP	DHCP	DHCP

Schéma réseau :



| Etude de l'impact sur le SI existant |

Étant donné que ce travail s'inscrit dans un contexte de formation, il n'existe aucun système d'information (SI) préexistant, à l'exception de l'accès à Internet. L'ensemble de l'infrastructure réseau nécessaire doit donc être entièrement créé et configuré dans le cadre de ce travail pratique. La mise en place de pfSense permet de centraliser la gestion du réseau en assurant les fonctions de pare-feu, de passerelle et de serveur DHCP. L'utilisation du service DHCP de pfSense permet d'automatiser l'attribution des adresses IP, de simplifier l'administration du réseau et de réduire les risques d'erreurs de configuration lors de l'ajout de nouveaux équipements. Dans un contexte professionnel, le déploiement de pfSense au sein de l'entreprise permettrait d'améliorer la sécurité du réseau, d'optimiser la gestion des flux réseau et de faciliter l'intégration de nouveaux postes ou équipements, tout en conservant une infrastructure centralisée, fiable et évolutive.

| Phasage de l'intervention |

Dans un premier temps, je procéderai à la création et à la préparation d'une machine virtuelle hébergeant pfSense, destinée à assurer les fonctions de pare-feu, de passerelle et de serveur DHCP du réseau. Après l'installation de pfSense, je configurerai les interfaces réseau, notamment l'interface WAN pour l'accès à Internet et l'interface LAN pour le réseau interne. Dans un second temps, j'activerai et configurerai le service DHCP sur l'interface LAN de pfSense. Je définirai la plage d'adresses IP à distribuer, le masque de sous-réseau, la passerelle par défaut ainsi que les serveurs DNS. J'ajusterai également la durée du bail en fonction des besoins du réseau. Une fois ces paramètres appliqués, je vérifierai le bon fonctionnement du service DHCP. Enfin, je testerai la configuration en connectant une machine cliente au réseau afin de m'assurer qu'elle obtient automatiquement une adresse IP et les paramètres réseau fournis par pfSense, validant ainsi la bonne mise en œuvre de l'infrastructure.

| Prévision des tests et validation |

Lors de la configuration du service DHCP sur pfSense, je procéderai à plusieurs vérifications afin de m'assurer de son bon fonctionnement. Je vérifierai tout d'abord que le service DHCP est bien activé sur l'interface LAN et qu'il distribue correctement les adresses IP selon les paramètres définis dans la plage d'adresses. Après la configuration et l'activation de la plage DHCP, je contrôlerai que les options essentielles, telles que la passerelle par défaut, les serveurs DNS et la durée du bail, sont correctement appliquées et prises en compte par pfSense. Enfin, une fois la configuration terminée, je testerai l'attribution des adresses IP en connectant une machine cliente au réseau. Je m'assurerai que celle-ci reçoit automatiquement une adresse IP valide, les bons paramètres réseau, et que la communication entre le poste client et pfSense s'effectue sans erreur. Ces vérifications permettront de valider entièrement la configuration du service DHCP sur pfSense.

Mise en place

Téléchargement & Préparation

1. Se rendre sur le site officiel : https://www.pfsense.org/download/
2. Sélectionner l'architecture **AMD64 (64-bit)**.
3. Choisir le type d'installateur **DVD Image (ISO)**.
4. Télécharger et monter l'ISO sur la machine virtuelle.

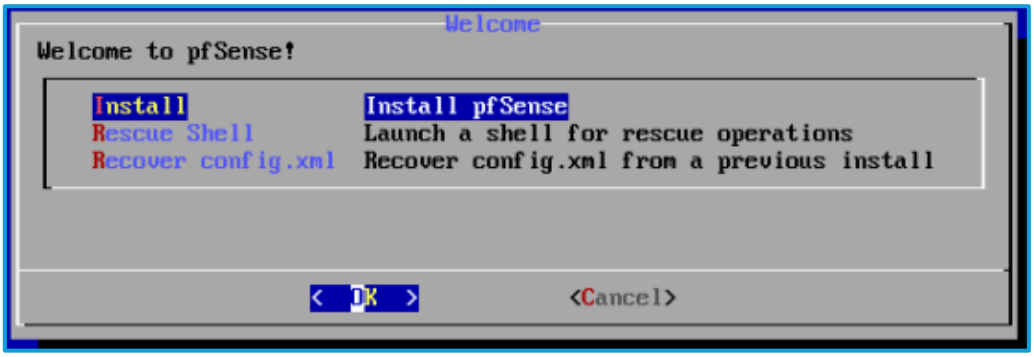
Installation du Système

Étape 1 : Démarrage

Démarrer la machine sur l'ISO. Au menu de bienvenue, appuyer sur **Entrée** pour lancer l'installation.

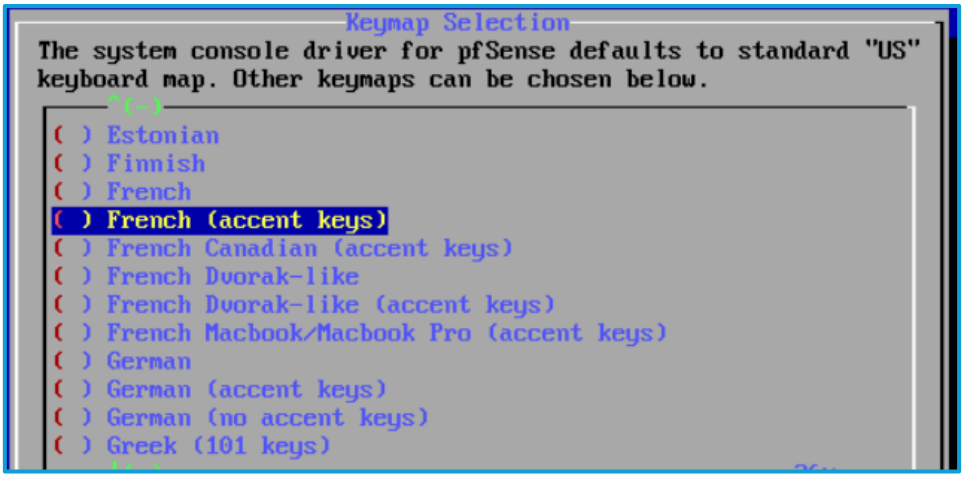
Étape 2 : Licence et Options

1. **Accept** : Valider les conditions d'utilisation.
2. **Install** : Choisir "Install pfSense" et valider.



Étape 3 : Configuration Clavier

Sélectionner la disposition du clavier correspondante (ex: "French" pour AZERTY) ou garder par défaut et valider.



Étape 4 : Partitionnement

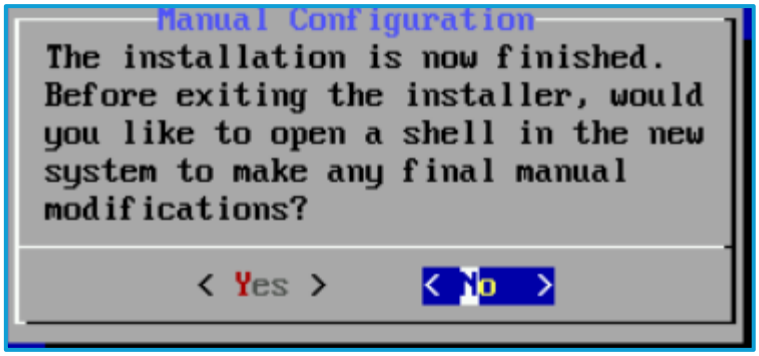
Choisir le mode **Auto (UFS) BIOS** (ou ZFS selon préférence, mais UFS est standard pour les petites VM).

1. Confirmer le formatage du disque.

INSÉRER CAPTURE D'ÉCRAN : Menu "Partitioning" avec choix "Auto (UFS)"]

Étape 5 : Finalisation

L'installation copie les fichiers. À la question "Manual Configuration", répondre **No**.
Sélectionner **Reboot** et retirer l'ISO du lecteur virtuel.

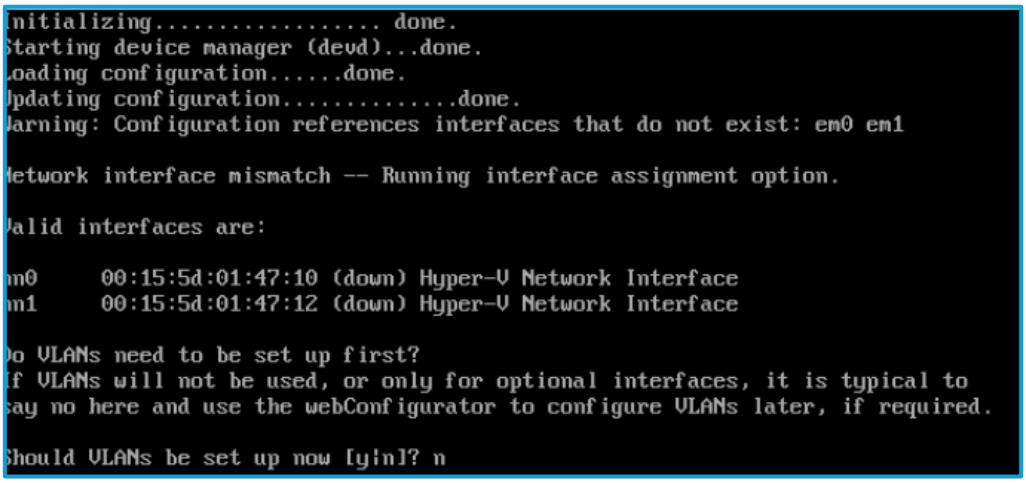


Configuration Initiale (Console)

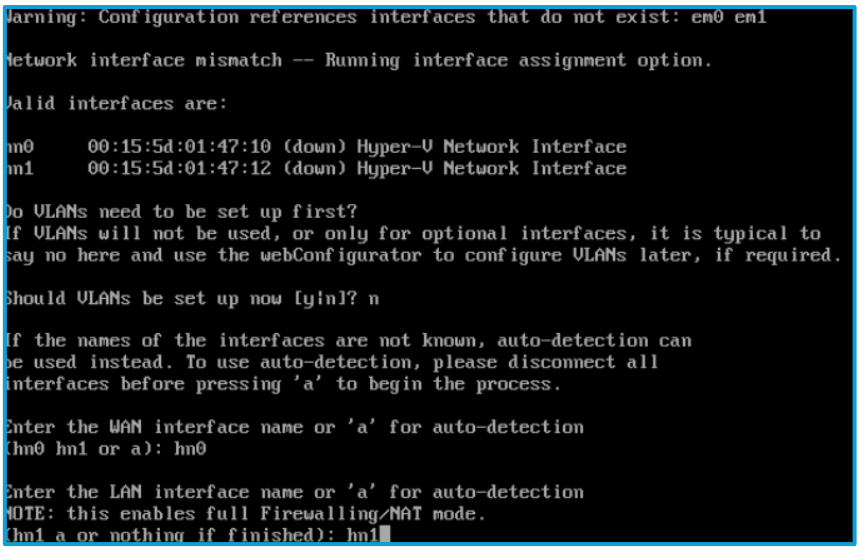
Au redémarrage, pfSense lance son assistant de configuration des interfaces en mode texte.

Assignation des Interfaces

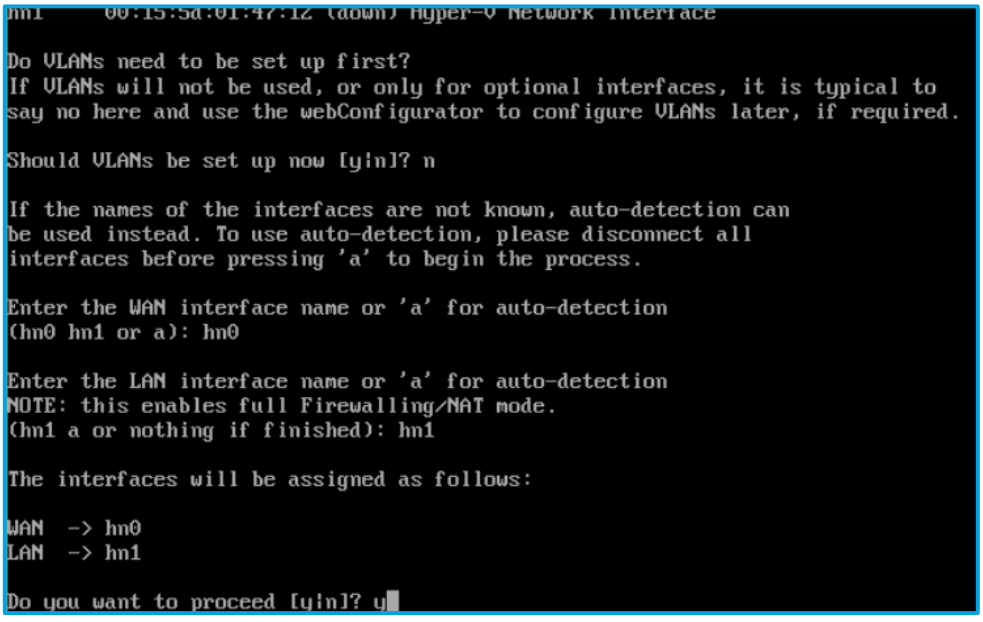
1. **VLANs** : À la question Should VLANs be set up now [y|n]?, répondre **N**.



1. **WAN** : Indiquer le nom de l'interface connectée à Internet (ex: em0).
2. **LAN** : Indiquer le nom de l'interface réseau interne (ex: em1).



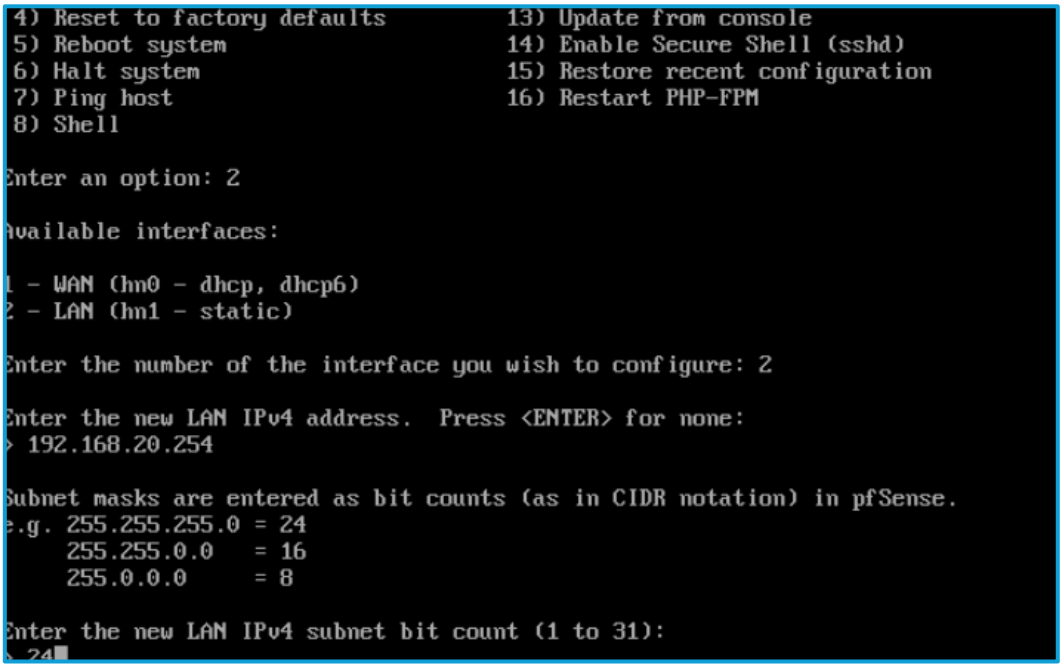
1. **OPT1 (DMZ)** : Si une 3ème carte est présente, l'indiquer ici (ex: em2), sinon appuyer sur Entrée.
2. Valider la configuration avec **Y**.



Configuration des Adresses IP (Menu Console)

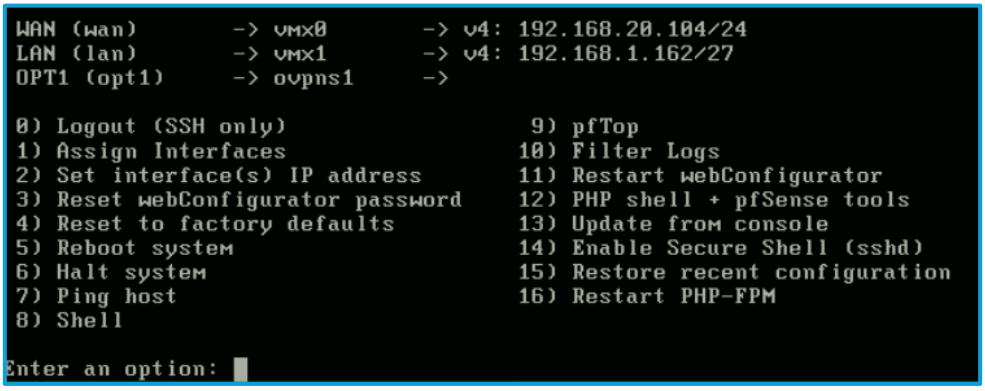
Une fois le menu principal affiché (options 1 à 16) :

1. Choisir l'option **2) Set interface(s) IP address**.
2. Sélectionner l'interface **LAN (2)**.
3. Entrer l'adresse IP souhaitée (ex: 192.168.1.1).
4. Entrer le masque de sous-réseau (ex: 24 pour 255.255.255.0).



1. **Gateway** : Appuyer sur Entrée (aucune pour le LAN).
2. **IPv6** : Appuyer sur Entrée (aucune).
3. **DHCP** : Répondre y pour activer le DHCP sur le LAN, définir la plage (ex: .10 à .100).

(Répéter l'opération pour la DMZ si nécessaire : IP 10.0.0.1/24)



Configuration Web & Règles

Accès au WebConfigurator

Depuis un poste client connecté au réseau LAN :

1. Ouvrir un navigateur web.
2. Accéder à https://192.168.1.1 (ou l'IP définie précédemment).
3. Identifiants par défaut :
    - **Utilisateur :** admin
    - **Mot de passe :** pfsense

Assistant de configuration (Wizard)

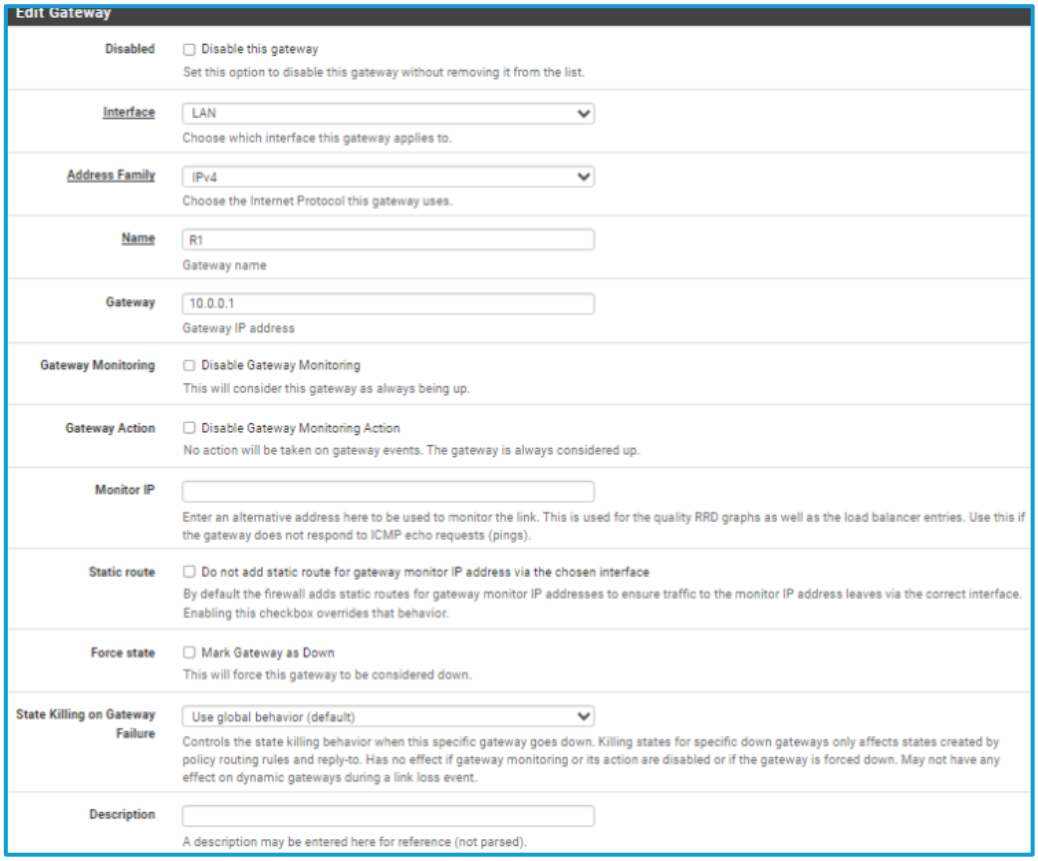
Suivre les étapes :

- Changer le Hostname (ex: parefeu-principal).
- Changer le mot de passe administrateur (**Important**).
- Reload pour appliquer les changements.

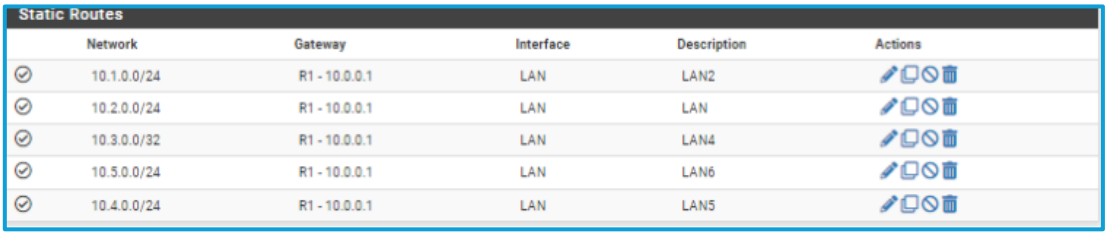
Création des Règles de Pare-Feu (DMZ)

Pour isoler la DMZ tout en permettant l'accès aux services :

1. Aller dans Firewall > Rules > DMZ.
2. Cliquer sur Add (Flèche vers le haut).
3. **Configurer la règle :**
    - Action : Pass
    - Interface : DMZ
    - Protocol : TCP
    - Source : Any
    - Destination : DMZ Address
    - Dest. Port : 80 (HTTP)
4. Sauvegarder et appliquer (Apply Changes).



Créez des routes statiques vers les réseaux qui ne sont pas voisins de votre pare-feu



Enfin vous pouvez créer vos règles dans l'onglet Firewall/Rules/LAN en spécifiant :

- Le protocole
- Le réseau de source
- Le port
- La destination
- etc...

Votre pare-feu est maintenant opérationnel.

Conclusion

La mise en place et la configuration de pfSense m'ont permis de déployer une solution de pare-feu (firewall) et de routage performant pour sécuriser le réseau. En configurant les interfaces WAN et LAN, j'ai pu établir une segmentation claire entre le réseau externe et le réseau privé.
Les tests effectués, notamment la mise en place de règles de filtrage et la vérification de la translation d'adresses (NAT), ont démontré que pfSense assure une gestion fluide et sécurisée du trafic. Grâce à cette solution open-source, l'administration du réseau est centralisée via une interface web intuitive, offrant un contrôle total sur la sécurité et la connectivité des postes clients.

Auto-évaluation

Le temps imparti de quatre heures a été respecté, grâce à une bonne préparation en amont, notamment le téléchargement anticipé des ISO et la connaissance préalable de la procédure d'installation.
Cette anticipation m'a permis d'optimiser le déroulement du TP et d'atteindre les objectifs fixés dans les délais.