pfSense

Installation et Configuration du Pare-feu

Sécurisation Complète de l'Infrastructure Réseau

STADIUM COMPANY

Réalisé par : Laurent HUSTIN
Formation : BTS SIO Option SISR - 2ème année
Établissement : IRIS
Année : 2025-2026
Entreprise : E-Nova (Alternance)

Contexte : Mission Stadium Company

1. INTRODUCTION ET CONTEXTE

1.1 Mission et Objectifs

Dans le cadre de mon alternance chez E-Nova, j'ai été chargé de mettre en place et configurer le pare-feu pfSense pour sécuriser l'infrastructure réseau de Stadium Company. Cette mission critique vise à protéger l'ensemble du système d'information contre les menaces externes.

Stadium Company, gestionnaire d'un grand stade accueillant événements sportifs et concerts, héberge des données sensibles : informations clients, données bancaires de la billetterie, et systèmes de sécurité du stade. La protection de cette infrastructure est donc primordiale.

1.2 Architecture Réseau Stadium Company

L'infrastructure est segmentée en 3 zones distinctes pour appliquer le principe de défense en profondeur :

Zone	Réseau	Description
WAN	192.168.44.0/24	Connexion Internet
LAN	172.20.1.0/24	Serveurs internes
DMZ	172.20.4.0/24	Services publics (Web, Mail)

1.3 Configuration du Pare-feu

Paramètre	Valeur
Nom d'hôte	heimdall.stadiumcompany.local
Version pfSense	2.7.2-RELEASE
WAN IP	192.168.44.254/24
LAN IP	172.20.1.1/24
DMZ IP	172.20.4.1/24

PARTIE 1 : INSTALLATION

2. INSTALLATION DE pfSENSE

2.1 Présentation de pfSense

pfSense est une distribution firewall/routeur open source basée sur FreeBSD. C'est une solution professionnelle utilisée par de nombreuses entreprises pour sécuriser leur infrastructure réseau.

J'ai choisi pfSense pour Stadium Company car :

- Solution gratuite et open source (économie de licences)
- Interface web intuitive pour l'administration
- Support de fonctionnalités avancées (VPN, IDS/IPS, QoS)
- Communauté active et documentation complète
- Mises à jour de sécurité régulières

2.2 Installation du Système

J'ai installé pfSense 2.7.2 sur une machine virtuelle dédiée avec 3 interfaces réseau (WAN, LAN, DMZ). L'installation s'est déroulée sans problème via l'ISO officiel.

Après le premier démarrage, pfSense affiche un menu console permettant la configuration initiale.

3. ASSIGNATION DES INTERFACES

3.1 Identification des Interfaces

La première étape consiste à assigner les interfaces réseau physiques aux différentes zones (WAN, LAN, DMZ).

J'ai utilisé l'option 1 du menu :

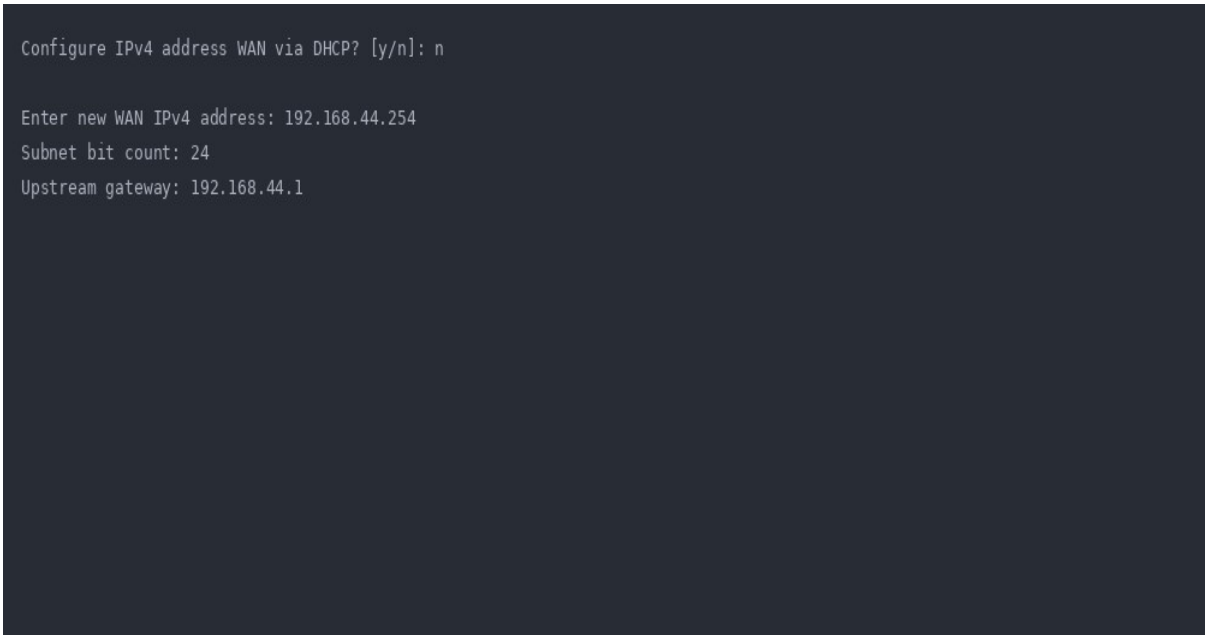
Configuration effectuée :

- **em0** → **WAN** (connexion Internet)
- **em1** → **LAN** (réseau serveurs)
- **em2** → **OPT1 (DMZ)** (services publics)

4. CONFIGURATION DES ADRESSES IP

4.1 Configuration de l'Interface WAN

L'interface WAN permet la connexion à Internet. J'ai configuré une adresse IP statique fournie par le FAI de Stadium Company.



Paramètres WAN :

- IP : 192.168.44.254/24
- Gateway : 192.168.44.1
- Type : Static IPv4

4.2 Configuration de l'Interface LAN

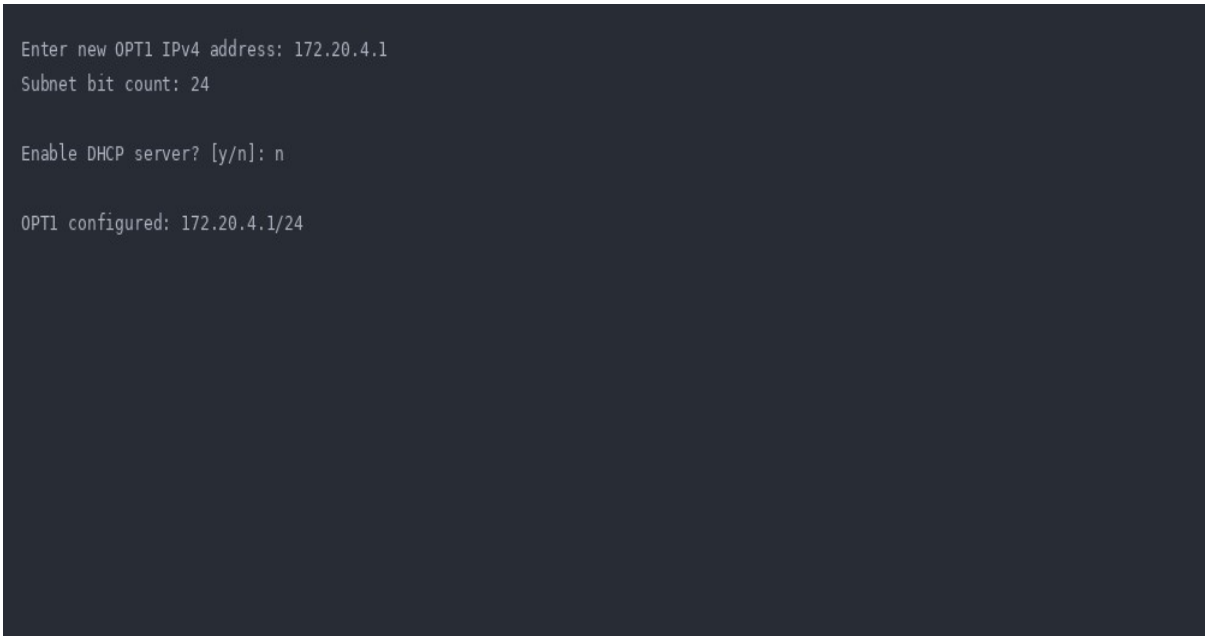
Le LAN héberge tous les serveurs de Stadium Company (AD, GLPI, etc.). J'ai également activé le serveur DHCP pour faciliter l'attribution des adresses.

Paramètres LAN :

- IP : 172.20.1.1/24
- DHCP activé : 172.20.1.20 à 172.20.1.30
- DNS : 172.20.1.2 (Hermes)

4.3 Configuration de la DMZ

La DMZ (Demilitarized Zone) héberge les services accessibles depuis Internet (serveur web, mail). Cette zone est isolée du LAN pour des raisons de sécurité.

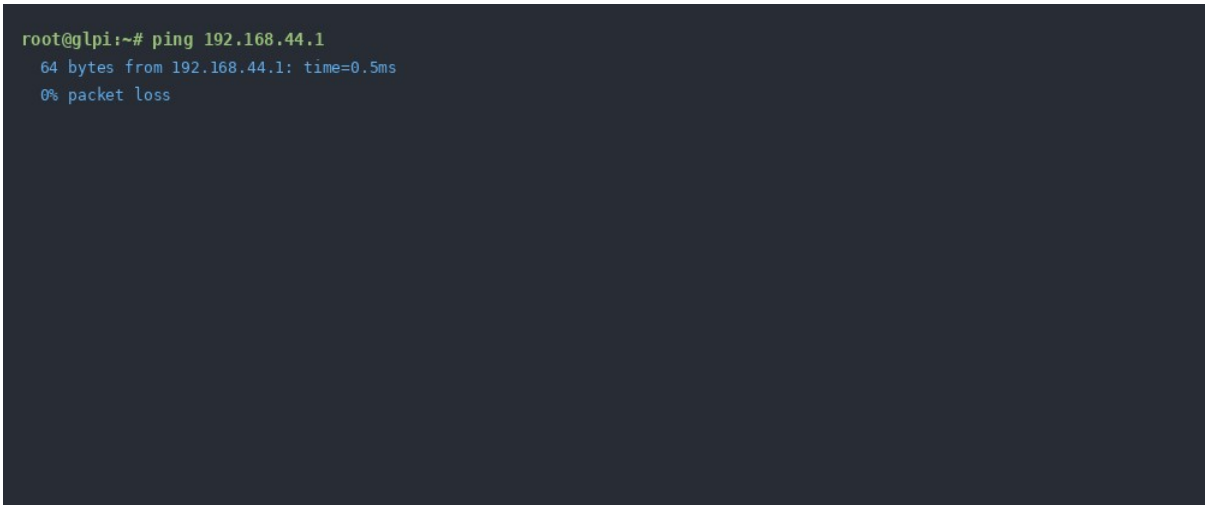


Paramètres DMZ :

- IP : 172.20.4.1/24
- DHCP désactivé (IPs statiques obligatoires)

4.4 Tests de Connectivité

Une fois toutes les interfaces configurées, j'ai effectué des tests de connectivité depuis les différents réseaux.



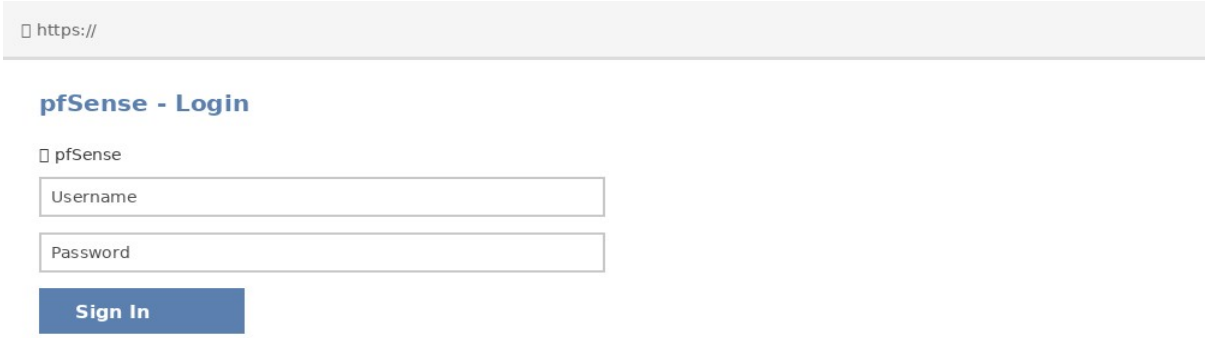
✅ Tous les tests sont positifs. Le routage fonctionne correctement entre les différentes zones.

PARTIE 2 : CONFIGURATION AVANCÉE

5. INTERFACE WEB D'ADMINISTRATION

5.1 Première Connexion

Maintenant que les interfaces sont configurées, je peux accéder à l'interface web de pfSense depuis le réseau LAN via https://172.20.1.1



Identifiants par défaut :

- Username : admin
- Password : pfsense

⚠️ J'ai immédiatement changé le mot de passe par défaut pour sécuriser l'accès.

5.2 Tableau de Bord

Le dashboard affiche un aperçu complet de l'état du pare-feu : charge système, interfaces, version, etc.

 https://

pfSense - Dashboard

System Information

- Name: heimdall.stadiumcompany.local
- Version: 2.7.2-RELEASE

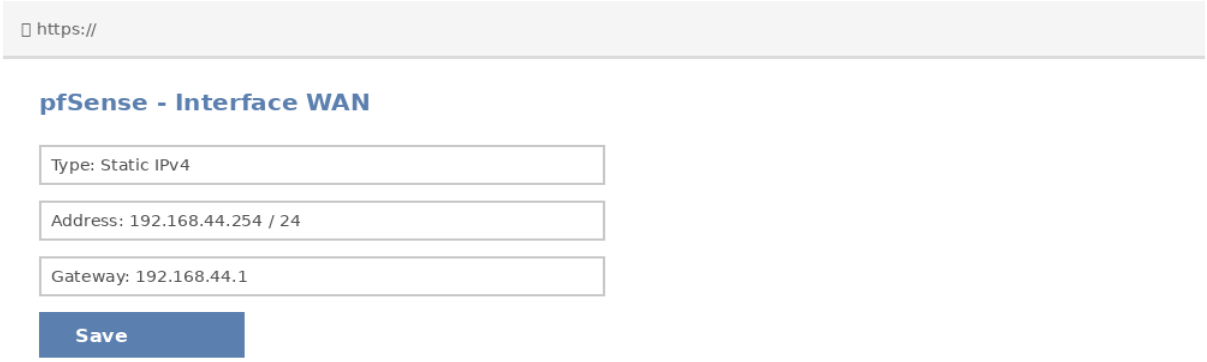
Interfaces

- WAN: 192.168.44.254/24
- LAN: 172.20.1.1/24
- DMZ: 172.20.4.1/24

6. CONFIGURATION DÉTAILLÉE DES INTERFACES

6.1 Interface WAN

Depuis l'interface web, j'ai vérifié et ajusté les paramètres de l'interface WAN pour optimiser la sécurité.



6.2 Serveur DHCP LAN

Configuration du serveur DHCP pour le réseau LAN avec attribution automatique des adresses aux nouveaux serveurs.

 https://

pfSense - DHCP Server LAN

Enable:

Range: 172.20.1.20 - 172.20.1.30

DNS: 172.20.1.2

Save

7. RÈGLES DE PARE-FEU

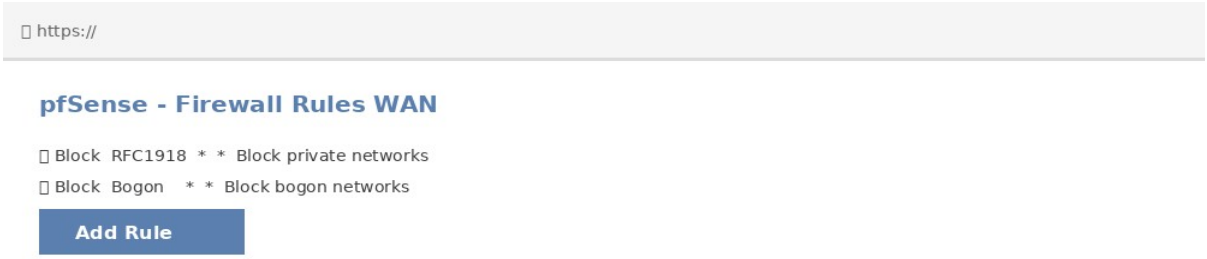
7.1 Principe de Sécurité

J'ai appliqué le principe du "deny all, allow specific" : tout est bloqué par défaut, seuls les flux nécessaires sont autorisés explicitement.

Cette approche garantit une sécurité maximale pour Stadium Company.

7.2 Règles WAN

Sur l'interface WAN, j'ai configuré des règles pour bloquer automatiquement les réseaux privés et bogons.



7.3 Règles LAN

Le LAN dispose d'une règle par défaut permettant tout le trafic sortant. Les serveurs peuvent accéder à Internet pour les mises à jour.

https://

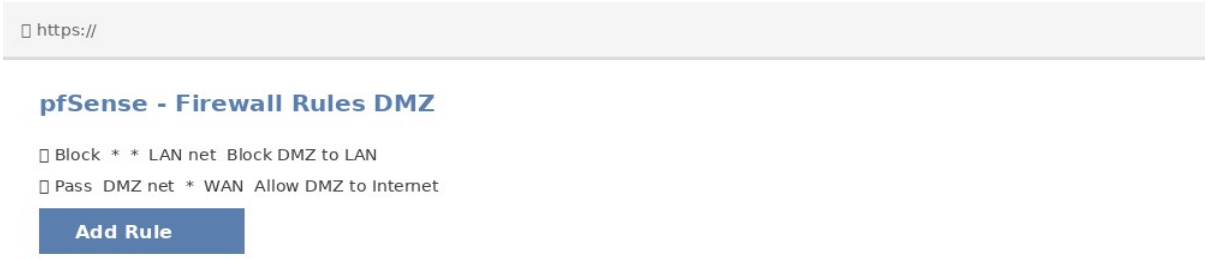
pfSense - Firewall Rules LAN

Pass LAN net * * Default allow LAN to any

Add Rule

7.4 Règles DMZ (Zone Critique)

La DMZ nécessite une configuration particulière :



Règles configurées :

- **BLOQUER :** DMZ → LAN (empêche une compromission de se propager)
- **AUTORISER :** DMZ → Internet (pour mises à jour uniquement)

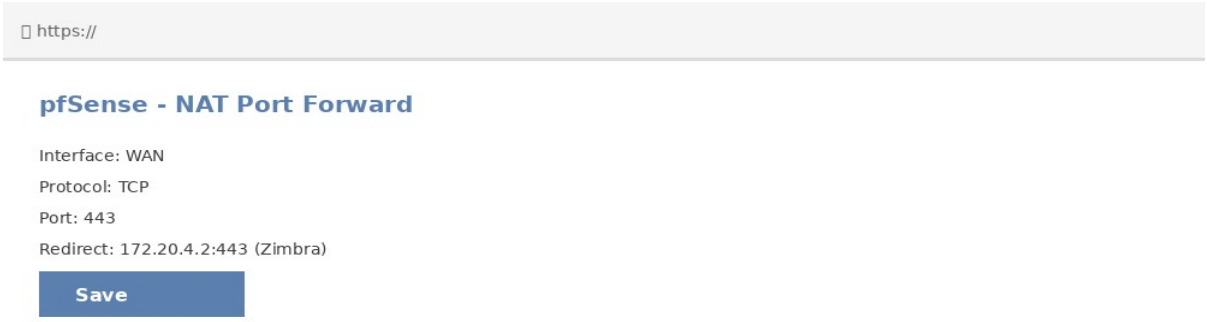
8. NAT ET REDIRECTION DE PORTS

8.1 Principe du NAT

Le NAT (Network Address Translation) permet de rediriger le trafic Internet entrant vers les serveurs en DMZ.

Pour Stadium Company, j'ai configuré une redirection pour le serveur de messagerie Zimbra.

8.2 Configuration Port Forward



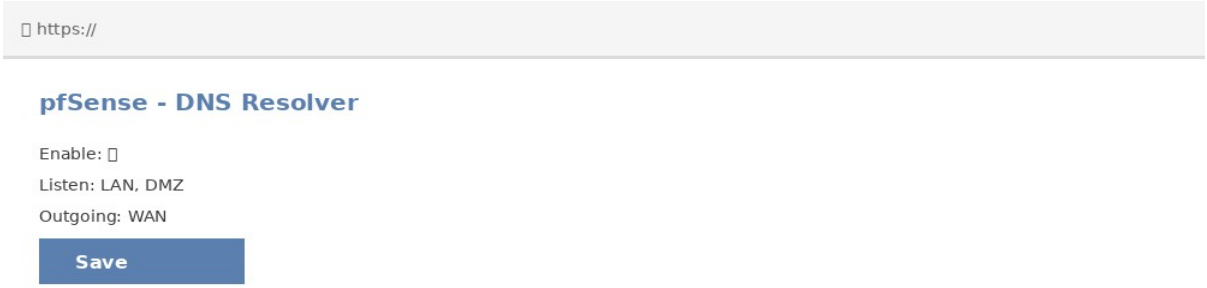
Redirection configurée :

- Port 443 (HTTPS) → 172.20.4.2 (Zimbra)
- Protocole : TCP

9. SERVICES RÉSEAU

9.1 DNS Resolver

J'ai configuré le DNS Resolver pour que pfSense serve de serveur DNS cache pour les réseaux LAN et DMZ, améliorant ainsi les performances.



10. COMPÉTENCES ET BILAN

10.1 Compétences Techniques Acquises

- Installation et configuration d'un pare-feu pfSense
- Segmentation réseau avec VLANs (WAN, LAN, DMZ)
- Configuration de règles de pare-feu avancées
- Mise en place du NAT et redirections de ports
- Configuration de services réseau (DHCP, DNS)
- Application des bonnes pratiques de sécurité réseau

10.2 Lien avec le Référentiel BTS SIO

Bloc	Compétence
B2	Administrer les systèmes et les réseaux
B3	Sécuriser les infrastructures

10.3 Conclusion

La mise en place du pare-feu pfSense pour Stadium Company a été un projet technique enrichissant qui m'a permis de mettre en pratique mes connaissances en sécurité réseau.

J'ai réussi à déployer une solution professionnelle de sécurisation réseau, avec une segmentation en 3 zones distinctes (WAN, LAN, DMZ) et des règles de pare-feu robustes respectant les bonnes pratiques de sécurité.

L'infrastructure réseau de Stadium Company est désormais protégée efficacement contre les menaces externes, tout en permettant l'accès sécurisé aux services publics hébergés en DMZ.